Capitolato Tecnico

Acquisto ed Implementazione nuova soluzione di Sicurezza IoT/OT

Sommario

1 Introduzione e contesto

La seguente sezione ha l'obiettivo di introdurre la struttura del Gruppo Autostrade per l'Italia, la sua vision, i suoi valori ed i macro-obiettivi societari.

1.1 Vision e Mission di Gruppo

Vision: Creare valore economico e sociale per il Paese, attraverso l'investimento su infrastrutture all'avanguardia, in grado di offrire servizi di mobilità che rendano unica l'esperienza di viaggio e permettano lo sviluppo dei territori.
Mission: Rendere la mobilità sempre più sostenibile, sicura, innovativa, efficiente e rispondere alle esigenze presenti e future della società e delle sue comunità.

1.2 Il Gruppo ASPI

Autostrade per l'Italia, insieme alle altre concessionarie, gestisce attualmente circa 3.000 km di rete (pari a circa il 50% dell'intera rete nazionale a pedaggio). La rete attraversa 15 regioni e 60 province e presenta 218 Aree di Servizio, circa 4.200 tra ponti e viadotti e oltre 420 km di gallerie.
È in corso una trasformazione profonda del Gruppo che lo porterà a diventare un operatore integrato di mobilità di livello europeo.

Le società del Gruppo
Le società controllate operano in sinergia nel settore dei servizi di ingegneria, di costruzione e della realizzazione di soluzioni tecnologiche al servizio di una mobilità sicura, moderna e sostenibile.

AMPLIA INFRASTRUCTURES — Società leader di costruzione, specializzata nella realizzazione, manutenzione e ammodernamento di infrastrutture complesse tramite materiali e tecniche sostenibili

Opera nel campo dei servizi di ingegneria, della progettazione, della direzione lavori e del coordinamento della sicurezza per progetti chiave nell'evoluzione della rete autostradale

Sviluppo e integrazione di soluzioni innovative di Intelligent Transport Systems nell'ambito della smart mobility

Sviluppa servizi avanzati di mobilità offrendo soluzioni tecnologiche e sostenibili finalizzate a migliorare l'esperienza di viaggio a 360°

Nata nel 2022 per la produzione di energia pulita attraverso la progettazione, la realizzazione e la gestione degli impianti rinnovabili lungo e intorno alla rete autostradale

Altri servizi

Gestisce i servizi amministrativi, generali e immobiliari per l'intero Gruppo e tutte le attività di recupero crediti e fatturazione pedaggi

Svolge attività di pulizia e manutenzione su piazzali esterni, superfici a verde e servizi igienici delle Aree di Servizio della rete in gestione

Commercializza spazi, servizi pubblicitari ed eventi nelle Aree di Servizio

Inoltre, le società concessionarie autostradali del Gruppo Autostrade per l'Italia sono:

- Società Italiana per Azioni per il Traforo del Monte Bianco;
- Raccordo Autostradale Valle d'Aosta;
- Tangenziale di Napoli;
- Società Autostrada Tirrenica.

1.3 Obiettivo del documento

Obiettivo del presente è descrivere e disciplinare le prestazioni rientranti nel perimetro dell'appalto per l'acquisizione ed implementazione di una nuova soluzione di Industrial Control System Asset Management (da qui in avanti "ICS-AM") per la gestione dei dispositivi degli Industrial Automation and Control Systems (IACS) aziendali, le modalità d'erogazione dei servizi richiesti, le figure professionali necessarie a costituire il Team di Progetto, i livelli di servizio attesi e le relative penali in caso di mancato rispetto dei livelli stessi.

Con il termine "Autostrade" o "ASPI" o "Committente" va intesa la società Autostrade per l'Italia S.p.A. mentre con il termine "Gruppo" vanno intese tutte le società del Gruppo Autostrade che utilizzano i sistemi in ambito, con il termine "Fornitore" o "Appaltatore" va intesa l'impresa aggiudicataria dell'appalto.

Quando non diversamente specificato, con "Capitolato" si intende il presente documento, con "Contratto" si intende il contratto che verrà sottoscritto a seguito dell'aggiudicazione dell'appalto, con "Fornitura" si intende il complesso delle attività e dei prodotti che l'Appaltatore è chiamato ad eseguire/fornire nell'ambito della durata contrattuale.

1.4 Acronimi e definizioni

Tutti i termini definiti, contenuti nel presente documento, avranno lo stesso significato ad essi attribuito nell'ambito del Contratto e nei documenti ad esso allegati.
Nella seguente tabella, si riportano le definizioni e gli acronimi impiegati nel testo.

Acronimo/ Definizioni	Significato
AdS	Amministratore di Sistema
ASPI	Autostrade per l'Italia / Committente
SLA	Service Level Agreements
OT	Operational Tecnology
IoT	Internet of Things
I-IoT	Industrial Internet of Things

2 Premessa

Le Unità Organizzative (U.O.) Chief Technology Officer e Chief Information Security Officer (di seguito rispettivamente DIDT/CTO e DIDT/CISO) della Direzione IT e Digital Transformation rappresentano le strutture di Autostrade per l'Italia S.p.A. incaricate dell'erogazione dei Servizi IT e di Sicurezza Informatica aziendali, rivolti altresì verso le società controllate e concessionarie.

Oltre al sedime autostradale, ASPI gestisce un apparato tecnologico a supporto all'erogazione di informazioni di traffico e di sicurezza in tempo reale[1], oltre ad apparati che realizzano gli impianti di automazione di Gallerie[2] ed il processo di Esazione. ASPI è un operatore di sistemi di trasporto intelligenti (ITS), settore ad alta criticità come definito dalla Direttiva (EU) 2022/2555 (NIS2), all'Annesso 1, 2, 2(d). Negli ultimi anni, ASPI sta realizzando il suo piano di trasformazione digitale[3] che ha fra gli scopi il rinnovo dei sistemi di supporto agli impianti tecnologici adiacenti al sedime stradale.

ASPI sta cercando quindi un **sistema combinato di asset management, network monitoring e vulnerability analysis** (da qui in avanti *sistema*) per i suoi dispositivi OT e applicativi di controllo a supporto (Industrial Automation and Control System, IACS) che:

i) si integri e riceva informazioni dai sistemi di asset inventory già esistenti;

ii) offra funzionalità tipiche di questo tipo di tecnologie quali:

- **Asset Discovery**, intesa come la capacità di rilevamento di device attivi attraverso sia analisi del traffico di rete diretto (generato dai device stessi) e indiretto (attraverso la correlazione di informazioni provenienti da altre piattaforme di controllo e sicurezza), sia attraverso query attive;
- **Asset Inventory,** intesa come la capacità di gestire l'inventario dei device attivi in modalità CMDB-like (e.g., aggregazione per sottoreti, tipologia, protocolli, zone di rischio omogenee secondo la IEC 62443, zona geografica);
- **Network and Events Monitoring,** intesa come la capacità di riconoscere eventi relativi alla mancanza di disponibilità, integrità, e confidenzialità degli IACS;
- **Vulnerability Monitoring, and Management** intesa come la capacità di associare e mantenere aggiornata la lista di vulnerabilità ed eventuali exploit dei dispositivi, includendo anche la gestione del loro ciclo di vita.

Inoltre, saranno richiesti servizi a valore aggiunto di presidio delle tecnologie descritte nel dettaglio nei paragrafi successivi. In questo documento i termini DEVE, DOVREBBE, sono definiti secondo RFC 2119.

3 Situazione Attuale – Il contesto di Autostrade

La gran parte degli apparati tecnologici di ASPI sono connessi tramite una rete di trasporto mista, basata prevalentemente su tecnologie in Fibra Ottica e in minor parte da connessioni 4/5G. Le tipologie di apparati sono sia sistemi commerciali (e.g., PLC, SCADA, o Fixed C-ITS Stations), sia sistemi legacy sviluppati internamente, ma basati comunque su sistemi operativi commerciali (quali Linux, Windows, o VxWorks). La rete geografica di comunicazione, composta all'incirca da 8000 switch e più di 700 router, abilita la connessione di circa 30.000 dispositivi, fra attuatori e sensori.

[1] Si veda, per informazioni sulla tipologia di informazioni gestite dall'arredo tecnologico, https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/safety-related-traffic-information-srti-real-time-traffic-information-rtti_en (ultimo accesso 16 Maggio 2023)

[2] Si veda, per informazioni sulla tipologia di apparati presenti in galleria, il report di Agence nationale de la sécurité des systèmes d'information, ANSSI, disponibile all'indirizzo https://www.ssi.gouv.fr/en/guide/ics-cybersecurity-a-road-tunnel-case-study/ (ultimo accesso 16 maggio 2023)

[3] Si veda Next to Digital, https://www.autostrade.it/en/chi-siamo/next-to-digital

3.1 Architettura, utenti e sistemi target

L'infrastruttura centrale di ASPI è formata da due data center proprietari, situati a Firenze, che contengono le applicazioni di controllo dei sistemi remoti.

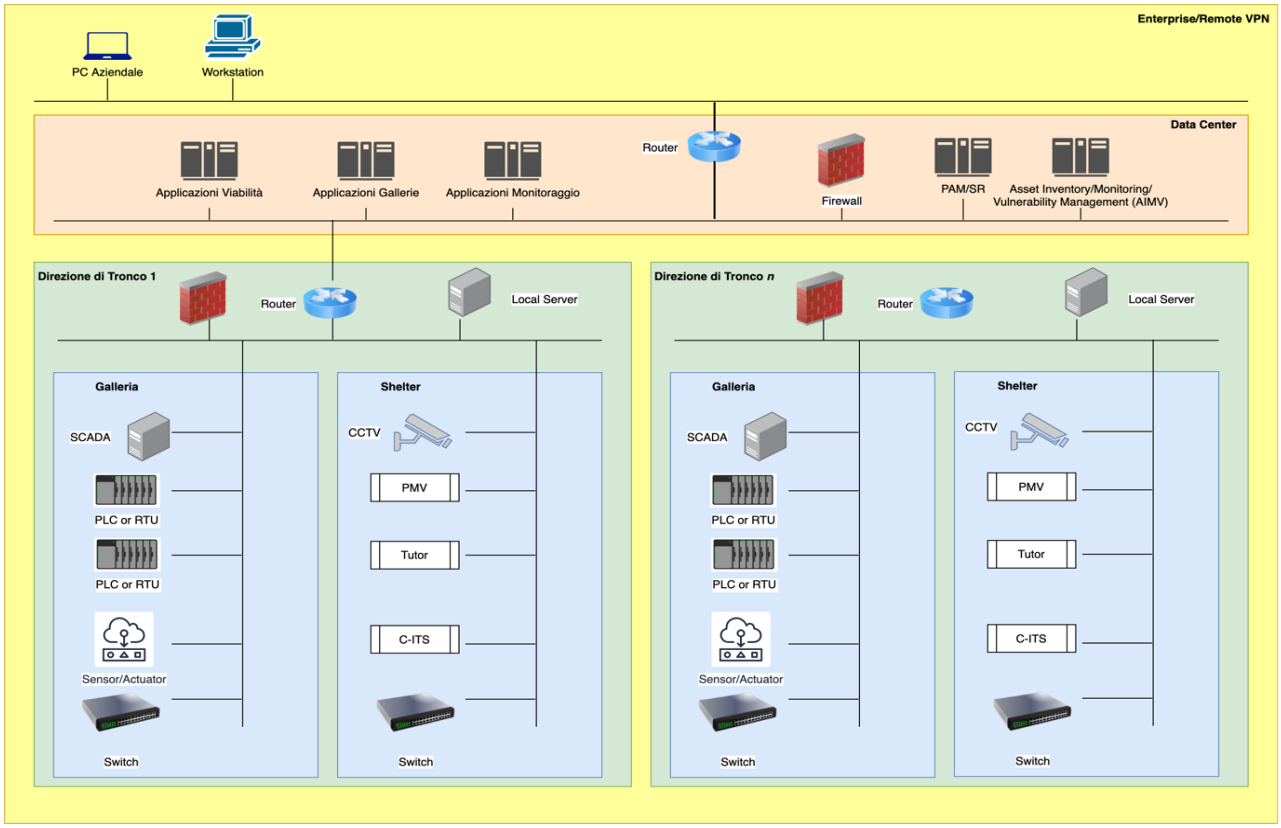


Figura 1 Descrizione delle Zone di ASPI di alto livello

In Figura, viene mostrata l'organizzazione di alto livello della rete seguendo il paradigma di *Zone & Conduit* tipico della famiglia ISA/IEC 62443. In particolare, ASPI segue le esigenze del sistema di gestione previsto dalle ISA/IEC 62443-2-1 e l'approvvigionamento di prodotti tramite un'autovalutazione effettuata dal fornitore definita dalle ISA/IEC 62443-4-2.

Per quanto riguarda l'architettura della rete e dei sistemi di controllo come Gallerie, Pannelli a Messaggio Variabile (PMV), viene seguita la norma ISA/IEC 62443-3-3 dove viene considerato un *Security Level Target (SL-T)* di almeno 2[4]. L'utilizzo della famiglia ISA/IEC 62443, assieme al *Framework Nazionale di Cybersecurity*[5], fornisce gli strumenti tecnici e tecnologici per l'organizzazione dei sistemi di controllo e di automazione.

Tipicamente, un utente accede ai dispositivi di produzione e alla rete del *data center (DC)* mediante la zona Enterprise (tipicamente denominata *rete corporate*), sia dall'interno della medesima rete di accesso, sia tramite una tecnologia di accesso remoto Zero-Trust like, attraverso un *PC Aziendale,* o una *Workstation* esterna all'organizzazione (e.g., Workstation del vendor/system integrator) mediante account forniti da ASPI stessa.

[4] Come definito in ISA IEC 62443-1-1:2009, Sezione 5.11, *"Security levels provide a qualitative approach to addressing security for a zone. […] Security level corresponds to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit".* In particolare, ASPI considera livelli superiori al SL-T 2, come definite in ISA IEC 62443-3-3:2013, Sezione A.3.2.4, *"SL2: Protection against intentional violation using simple means with low resources, generic skills and low motivation".*

[5] Si veda: https://www.cybersecurityframework.it

ASPI ha una topologia di rete a stella, in cui nei due DC sono implementate le infrastrutture IT per le applicazioni di monitoraggio degli impianti, i quali sono collocati logicamente nelle zone all'interno delle nove *direzioni di tronco (DDTT)* dell'azienda. Ogni direzione di tronco è responsabile della manutenzione dei dispositivi connessi alla propria sottorete. In ogni DDTT si possono trovare le seguenti tipologie di impianti, a titolo esemplificativo:

1) Impianti di Galleria: sono composti da reti ad anello o *spine-and-leaf* in cui sono comprese due o più cabine elettriche (CE); locali tecnici adatti a gestire apparati di elaborazione come server 1 RU. Esistono anche poche istanze di gallerie composte da rete punto-punto, dove è prevista una sola cabina elettrica e non vi è ridondanza. All'interno delle CE vi sono i router che si occupano di inoltrare il traffico attraverso la rete geografica; inoltre, ci sono diversi switch che collegano le varie VLAN. Tipicamente si può assumere come configurazione tipo per ogni galleria, due SCADA con due PLC master (in failover) che controllano i dispositivi PLC slave (attuatori). Gli attuatori gestiscono, a loro volta, i dispositivi dello IACS, quali ad esempio: ventilatori, sensori di fumo o cavi fibrolaser. I sistemi di monitoraggio di tutti gli SCADA sono gestiti dalle control room (ne esiste una per ogni DDTT) il cui traffico viene dirottato verso i DC. Gli impianti di galleria sono da considerarsi *safety-critical*, e gli algoritmi di attuazione sono sviluppati ad Hoc per ogni galleria. All'interno di tutti i sistemi di galleria si trovano circa 600 PLC fra ABB e Siemens[6].

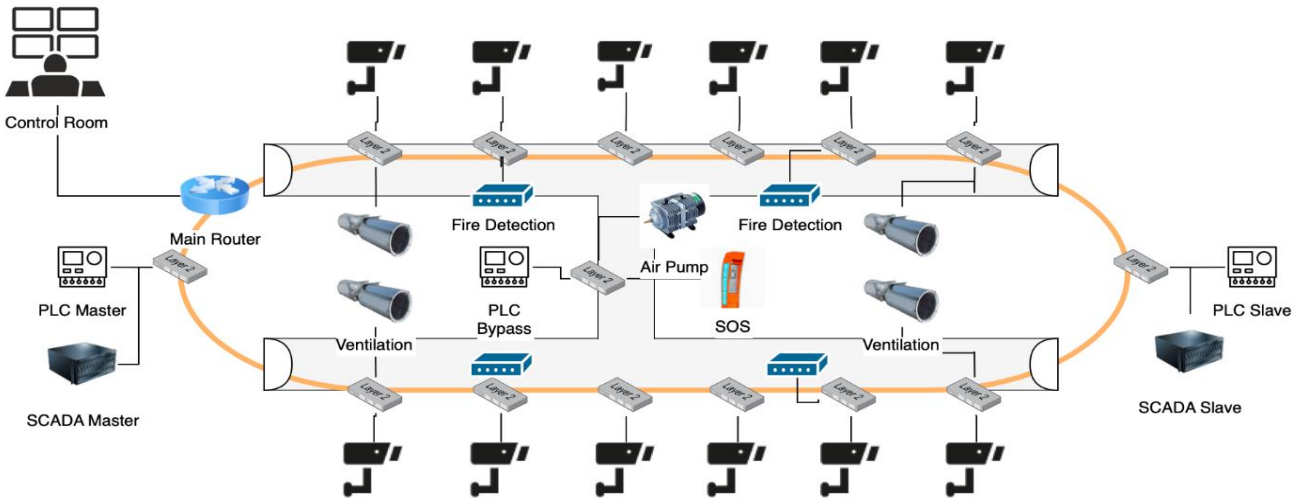


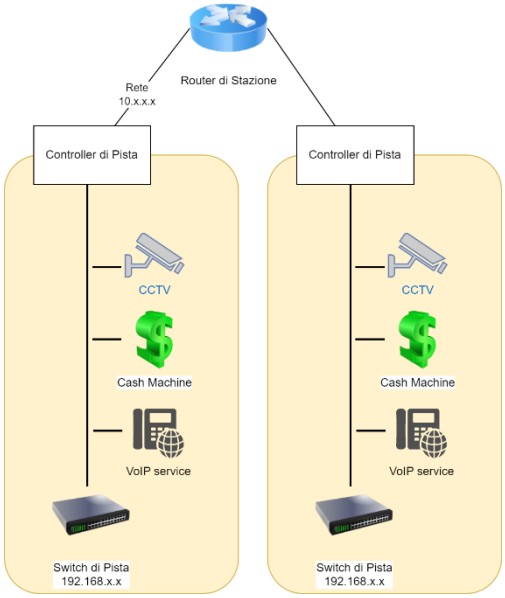
Figura 2 Schema logico di un sistema di galleria[7]

2) Impianti di Esazione. Hanno come scopo calcolare e ottenere il pedaggio autostradale. Sono installate 240 stazioni di esazione; ogni stazione è a sua volta composta da un certo numero di piste, variabile (da 2-3 piste a 30). Ogni pista di esazione, come da figura, è collegata ad un router di stazione (si contano all'incirca 2200 piste di esazione). Ogni controller di pista (PC industriale con una distribuzione Linux e VxWorks in condivisione) espone due interfacce: una verso la rete geografica ASPI, e una interfaccia privata per la rete di pista; ogni controller di pista è dotato di un firewall.

[6] Le tipologie di PLC sono, fra le altre, ABB PM554, PM573, PM591 e Siemens S7

[7] Immagine da *Massimiliano Masi, Giovanni Paolo Sellitto, Helder Aranha, Tanja Pavleska: Securing critical infrastructures with a cybersecurity digital twin. Softw. Syst. Model. 22(2): 689-707 (2023)*

Figura 3 Schema Logico di un impianto di Esazione



3) Shelter in itinere: sono locali tecnici posti sul sedime autostradale composti da router e switch a cui si collegano dispositivi quali telecamere (IP ONVIF e analogiche), video encoder basati su Linux, pannelli a messaggio variabile (tecnologia NTCIP – http, ftp). Sono stimati circa 500 shelter ognuno dei quali è equipaggiato con un router;

Una parte rilevante del traffico di rete sia quello proveniente dai dispositivi periferici, sia quello amministrativo verso i dispositivi periferici, passa attraverso il conduit dei DC. Per ogni comunicazione da un dispositivo verso il DC (o, eventualmente, un sistema Cloud), **esistono sempre due rotte attraverso le stazioni di esazione o le DDTT**.
L'accesso remoto ai dispositivi è gestito tramite una tecnologia di Privileged Access Management (PAM) / Secure Remote Access (SRA).
Questa funzionalità deve essere implementata sia in maniera attiva (facendo query sicure direttamente ai dispositivi) sia passiva (facendo, appunto, DPI).
ASPI ha un sistema di Network Access Control (NAC) basato su tecnologia Fortinet, che sta estendendo alla rete di produzione, in grado di ottenere informazioni sui MAC address dei dispositivi collegati agli switch e di implementare regole dinamiche di blocco e di isolamento di rete, allo scatenarsi di determinati eventi di sicurezza.

4 Oggetto dell'appalto

4.1 Casi d'uso

La soluzione proposta deve essere in grado di supportare i seguenti casi d'uso, alcuni comuni agli impianti industriali, altri specializzati per il contesto autostradale. I casi d'uso sono relativi ad integrazioni e processi aziendali.

Caso 1: Integrazione con piattaforma di asset inventory esistente

I cespiti di ogni dispositivo industriale sono gestiti tramite un sistema di asset inventory statico alimentato manualmente ed aggiornato di pari passo ai cicli passivi per l'approvvigionamento dei device. Ogni dispositivo è univocamente identificato tramite un UUID.

Il sistema dovrà importare gli UUID dalla piattaforma di asset inventory ed essere in grado di correlare in maniera automatica (i.e., tramite SDK o API) o manuale un dispositivo riconosciuto con un UUID. Deve inoltre essere possibile avere diversi utenti con diversi profili autorizzativi.

Caso 2: Sonda Centrale

Essendo la gran parte del traffico indirizzato tramite il DC, al fine di effettuare: un monitoraggio efficiente, la DPI sui protocolli industriali più comuni (e.g., MODBUS, Profinet, RTP, ONVIF), la rilevazione di eventuali comportamenti anomali che possono presagire ad un attacco in corso, il sistema deve prevedere la presenza di una o più sonde centrali, gerarchiche, collegate ai router di backbone della rete geografica, in grado di espletare le funzionalità in ambito della fornitura, anche da sistemi non raggiungibili tramite sonde periferiche.

Caso 3: Rugged Box

Dove non sia possibile effettuare query dal data center verso dispositivi periferici non direttamente raggiungibili(e.g., reti air gapped o in presenza di un firewall), i tecnici specializzati di ASPI avranno a disposizione una "rugged box" (una per ogni DDTT e due per le direzioni centrali), ovvero un pc industriale con a bordo un sistema che faccia query attive (o che sia passivo) in grado di fare asset discovery collegandosi direttamente allo switch (non necessariamente sulla sua span port). Queste informazioni ottenute dovranno poi essere correlate e inoltrate verso il sistema di asset inventory centrale.

Caso 4: Zone IEC 62443-2-1

ASPI ha suddiviso i suoi IACS in Zone e Conduit, seguendo le linee guida della IEC 62443-2-1. Il sistema oggetto della fornitura deve essere in grado di aggiungere ed etichettare in maniera automatica e manuale un tag relativo alla zona di sicurezza ed opzionalmente fare valutazioni fra le capabilities di sicurezza (SL-C secondo IEC 62443-4-2) e il target della zona (SL-T, secondo IEC 62443-2-1).

Caso 5: Gestione di feed di threat intelligence ed esportazioni

Il sistema dovrebbe essere in grado di gestire feed di threat intelligence in formato standard, oltre a quelli definiti dal produttore.

4.2 Scopo dell'appalto

Come descritto nelle sezioni precedenti, lo scopo della fornitura è da considerarsi nei seguenti ambiti:

- **Asset Discovery (CODICE OT-AD);**
- **Asset Inventory (CODICE OT-AI);**
- **Network and Events Monitoring (CODICE OT-NE);**
- **Vulnerability Monitoring and Management (CODICE OT-VM);**
- **Servizio di SOC OT** (da considerarsi come 1 FTE on premises business day + nighttime remote). Questa FTE è da considerarsi il target aziendale che si occuperà di fare tuning dei sistemi e di iniziare a ricevere gli allarmi e classificare i falsi positivi. Inoltre, si occuperà di prendere accordi con il Service Desk di ASPI e i vari Centri di Monitoraggio per le operazioni tipiche di SOC;
- **Servizio (opzionale) di Threat Intelligence OT,** ovvero l'offerta di un servizio di feed di CTI dedicati alle tecnologie ICS.

Nota Bene: Le funzionalità indicate potranno essere espletate anche da più prodotti, comunque integrabili tramite connettori standard, o custom tramite SDK o API.

Architettura centrale

La soluzione proposta deve essere erogata totalmente on-premise, con l'asset inventory nei DC di ASPI. In particolare, la soluzione deve essere predisposta, a livello centrale, in alta affidabilità, così che se il sistema primario di OT-AV dovesse subire un guasto hardware, il sistema potrà essere ripristinato sul sitema ridondato.
Per ottenere le funzionalità desiderate, ASPI vuole adottare un approccio in due fasi i cui obiettivi potranno essere raggiunti in varie modalità a seconda della tecnologia. Di seguito i requisiti:

1. Fasi di Progetto:
   - Nella prima fase verranno implementate le funzionalità di OT-AD, OT-VM, e OT-AI; si prevede una integrazione con il NAC, l'adozione di un sistema che permetta di fare Active Queries sia centralmente che tramite un dispositivo creato ad Hoc (i.e., la Rugged Box), e l'uso di una sonda centrale passiva che sia in grado di analizzare il traffico entrante dalle direzioni di tronco verso il DC. Questa fase dovrà essere completata entro 12 mesi dalla DIL.
   - Nella seconda fase, verrà implementato il sistema di monitoraggio (OT-NE). Questa funzionalità potrà essere implementata sia con l'utilizzo di sonde passive dislocate per ogni sito remoto (due sonde per sito in alta affidabilità), sia tramite tecnologia in grado di effettuare Query Attive dal centro. Questa fase dovrà essere completata entro 6 mesi dalla data di fine della Fase 1.

2. Modalità di deploy delle sonde passive periferiche:
   - Possibilità di utilizzo di sonde gerarchiche collegate come Daisy Chains, con una concentrazione maggiore dove gli apparati utilizzino protocolli di discovery implementati a Layer 2 (e.g., PLC ABB). In questo caso l'ordine di grandezza è di 180 sonde in galleria (90x2 sonde in alta affidabilità), più eventuali sonde intermedie (e.g., nelle direzioni di tronco) e appliance centrali nel DC.

4.3 Perimetro dell'appalto

Si riporta, di seguito, l'elenco dei prodotti e dei servizi oggetto del presente appalto:

a) Le componenti software necessarie alla realizzazione delle funzionalità richieste (ed eventualmente hardware) in licenza d'uso con validità triennale (anche in forma di sottoscrizioni).
b) I servizi propedeutici all'avvio in produzione delle soluzioni (tra cui, pianificazione del progetto, formazione, revisione dei processi in essere, etc.).
c) L'implementazione di quanto previsto nel capitolo *4.1 Casi d'Uso e 4.2 Scopo della fornitura*.
d) I servizi di supporto operativo ed evolutivo delle piattaforme oggetto di fornitura, unitamente ai servizi necessari al rispetto degli SLA.
e) I servizi professionali di assistenza specialistica sulle nuove soluzioni, da utilizzare anche per l'integrazione e configurazione delle nuove soluzioni con le tecnologie esistenti (e.g., il NAC).
f) Il servizio di passaggio delle conoscenze necessario al trasferimento del know-how sui servizi e sui sistemi oggetto del presente Capitolato al personale della Committente e/o a terzi da questa designati, con l'obiettivo di rendere la Committente totalmente autonoma nella gestione delle successive evoluzioni delle piattaforme OT-AD, OT-AI, OT-VM, e OT-NE.
g) Corsi di formazione con voucher per esame finale volti all'ottenimento di certificazione sulle piattaforme selezionate dal Fornitore per un numero minimo di 5 dipendenti della Committente.

L'Appaltatore dovrà predisporre il disegno tecnico della soluzione secondo i requisiti ed i limiti espressi nel presente Capitolato ed un documento specifico nel quale riporterà tutti gli elementi utili alla comprensione della soluzione stessa. Relativamente alle prestazioni di cui alla lett. a), l'Appaltatore è tenuto a garantire che:
- tutte le componenti oggetto della fornitura siano le più recenti tra quelle ufficialmente rilasciate dal produttore e disponibili sul mercato, fermo restando il rispetto dei requisiti minimi indicati nel presente Capitolato;
- tutte le componenti oggetto della fornitura siano pienamente supportate dal produttore alla data di sottoscrizione del contratto e per tutta la durata triennale dello stesso.

In nessun caso potranno rientrare nella fornitura prodotti che non siano ancora disponibili sul mercato o non più supportati dal produttore alla data di presentazione dell'offerta. Non potranno inoltre rientrare nella fornitura apparati di cui sia stata annunciata la data di end of sales o di end of support software.

L'Appaltatore è inoltre tenuto a garantire che le licenze software dei prodotti oggetto di fornitura e i prodotti hardware (esempio: appliance, sonde di traffico...) siano intestati ad ASPI in modalità perpetua+maintenance o in modalità subscription (in entrambi i casi con copertura triennale).
L'Appaltatore dovrà anche fornire, senza oneri aggiuntivi per ASPI, licenze o sottoscrizioni da utilizzare durante lo svolgimento delle fasi del progetto.
Nel caso in cui il supporto di una funzionalità richieda specifiche licenze (eventualmente anche sotto forma di sottoscrizione) esse dovranno essere incluse nella fornitura con validità tale da garantire la copertura dell'intero periodo di vigenza contrattuale.

L'attivazione delle licenze software dovrà avvenire a conclusione della Fase di set-up del sistema centrale, a valle dell'implementazione della nuova soluzione, e comunque entro 3 mesi dalla data di sottoscrizione del contratto. Laddove l'attivazione delle licenze avvenga oltre il suddetto termine, l'Appaltatore è tenuto a garantire un'estensione della validità delle licenze oltre alla scadenza di tre anni per un periodo pari alla durata di setup e comunque non inferiore a 3 mesi.

4.4 Durata dell'appalto

La durata del contratto è di 36 mesi solari consecutivi decorrenti dalla data di sottoscrizione del contratto stesso.
È richiesta l'attivazione delle licenze a partire dal completamento dell'installazione e della messa a punto della **Fase 1** (vedi par. 4.2) con l'implementazione delle nuove piattaforme, previo accordo con la Committente.

4.5 Team di Progetto

4.5.1 Obblighi dell'Appaltatore

L'Appaltatore deve prevedere, per tutta la durata contrattuale, coerentemente con la pianificazione delle attività concordata con la Committente, la disponibilità delle risorse componenti il Team di progetto i cui CV sono stati presentati in fase di gara. Eventuali richieste di sostituzioni dovranno esser debitamente motivate e potranno comunque esser effettuate solo previo benestare della Committente, salvo ragioni di congiunturale urgenza. Le sostituzioni dovranno avvenire con risorse di analoga professionalità ed esperienze, documentata e certificata e le risorse proposte in sostituzione dovranno essere sottoposte a successiva ed insindacabile accettazione da parte della Committente.
L'Appaltatore è tenuto comunque a rispettare il numero massimo di risorse sostituite definito negli SLA al cap. *6 Service Level Agreement e Penali* (escluse le sostituzioni dovute a cause di forza maggiore).
Rispetto all'insieme di figure professionali presenti nel Team di progetto si specifica comunque che l'Appaltatore, in accordo con la Committente, dovrà procedere ad una pianificazione dettagliata delle attività per ciascuna Fase del progetto, specificando l'impegno e l'allocazione delle figure professionali necessarie al buon esito del progetto. La composizione del Team di progetto dovrà in ogni caso prevedere sia personale dal profilo tecnico che personale dal profilo gestionale e di Project Management.

4.5.2 Idoneità delle risorse impiegate

Al fine di garantire la massima qualità del servizio, la Committente si riserva di valutare, anche in corso di esecuzione, l'idoneità delle figure professionali effettivamente impiegate per l'esecuzione dell'appalto.
Ove la Committente ritenga che la/e figura/e professionale proposta/e o utilizzata/e non sia idonea allo svolgimento delle attività previste, ne darà comunicazione all'Appaltatore che si impegna a reperire una nuova risorsa idonea entro il termine di 15 giorni lavorativi dalla predetta comunicazione e, se richiesto, a sospendere l'impiego - anche con effetto immediato - della risorsa ritenuta non adeguata.
L'eventuale sostituzione delle risorse nel Team di Progetto non deve incidere sullo svolgimento delle attività previste dal Piano di progetto.

Il Team di progetto dovrà prevedere obbligatoriamente almeno i seguenti profili:

- **Responsabile di Commessa**: risorsa di comprovata esperienza manageriale di almeno 10 anni che rappresenta il responsabile unico delle attività contrattuali cui ASPI farà riferimento. Il Responsabile di commessa assume il ruolo di principale interlocutore per tutti gli aspetti, sia contrattuali che gestionali, relativi ai contenuti e all'andamento della fornitura; ha la responsabilità di assicurare il corretto svolgimento del progetto nel rispetto dei tempi e dei costi pianificati, evidenziare le problematiche rilevate, proporre le opportune soluzioni ed intraprendere, in accordo con Autostrade per l'Italia, le necessarie azioni correttive. Il Responsabile di commessa ha inoltre la responsabilità di garantire il massimo grado di stabilità del gruppo di lavoro previsto per le attività di progetto.

- **OT Asset Management Project Manager**: risorsa di comprovata capacità tecnica con almeno 8 anni di esperienza in progetti di disegno ed implementazione di soluzioni complesse di OT Asset Management. Ha la responsabilità dell'intero ciclo di vita progettuale garantendo la corretta progettazione ed esecuzione del progetto, dalla fase di analisi della situazione attuale fino al rilascio in produzione delle nuove piattaforme e all'implementazione delle funzionalità oggetto del presente capitolato. Tale figura provvederà quindi a gestire il servizio, monitorandone lo stato di avanzamento delle attività, intervenendo con eventuali azioni correttive e coordinando le attività pianificate per ciascuna Fase di progetto, nel rispetto della qualità dei deliverable e delle scadenze concordati. La figura di Project Manager rappresenta il single point of contact per la totalità dei servizi erogati nell'ambito del progetto. Dovrà essere prontamente reperibile durante tutte le attività operative e progettuali ed assicurare la disponibilità degli specialisti di prodotto per la risoluzione dei problemi e l'efficienza del team e dei servizi erogati rispetto ai SLA indicati nel presente Capitolato. Il PM deve inoltre monitorare il raggiungimento degli obiettivi di progetto e relazionare periodicamente alla Committente sull'avanzamento dei lavori per analizzare le esigenze e le funzionalità attese.

- **Specialista di prodotto**: risorsa con elevate competenze sulle soluzioni che saranno implementate e buona conoscenza dei processi definiti dalle quattro macro-funzionalità. Risorsa con almeno 2 anni di esperienza in progetti implementativi delle soluzioni scelte di cui almeno uno sulla tecnologia selezionata. La risorsa deve essere in possesso di certificazione delle nuove piattaforme che saranno implementate.
  Lo specialista di prodotto deve essere ricoperto da almeno una risorsa dedicata presente in maniera continuativa per l'intera durata del contratto.

5 Requisiti

5.1 Requisiti Tecnici Obbligatori

Si riportano, nella tabella seguente, i requisiti tecnici minimi che il sistema deve soddisfare. Tali requisiti sono da considerarsi come requisiti obbligatori **a pena di risoluzione del contratto**.

Description	Affected Macro Features			
	Vulnerability Mgmt (OT-VM)	Asset Discovery (OT-AD)	Asset Inventory (OT-AI)	Network Environment (OT-NE)
Il sistema deve gestire l'intero ciclo di vita di un asset: discovery, inventory, produzione, dismissione, ecc…	X	X	X	
Il sistema deve essere in grado di effettuare DPI (deep packet Inspection) tramite sonda centrale e periferica (confrontare Caso d'uso 2 del Capitolato).				X

Il sistema deve permettere l'interrogazione attiva dei dispositivi connessi alla rete con vari protocolli nativi dei dispositivi OT più comuni. In particolare, sono richiesti: MODBUS, PROFINET, SNMP, SSH, RDP.	X	X		X
Il sistema deve fornire segnalazione e log di comportamenti anomali dell'asset.				X
Il sistema deve utilizzare anche i feed privati dei fornitori e costruttori di dispositivi (OEM) su vulnerabilità che vengono rese pubbliche. Feed proprietari sono ammessi.	X		X	
Il sistema deve rendere disponibile una esecuzione di tipo "rugged box" in caso di reti air gapped o sistemi di test (cfr caso d'uso 3). Nota: per rugged box si intende una valigetta con un PC industriale che possa essere collegata ad una span port, o una porta normale che abbia le stesse funzionalità del sistema connesso.	X	X	X	X
Il sistema deve avere la funzionalità di Asset/Device Onboarding, ovvero di inserire automaticamente un asset dopo la fase di discovery e dare la possibilità di aggiornare ed editare il record per importare anche identificativi esterni.		X	X	
Il sistema deve avere un Data Collection (asset, vulnerabilità, topologia di rete,…) quotidiano; inoltre, deve essere possibile fare Data Collection on-demand basata su query attive.	X	X		X
Il sistema deve avere funzionalità avanzate di logging delle attività di tutti gli utenti che vi accedano, in modo da poterle ricostruire, con una profondità temporale da definire con il committente (per gli AdS almeno 6 mesi), fruibile attraverso una console ed in grado di registrare eventi (quali login, logout, richiamo ad attività specifiche).	X	X	X	X
La console deve integrarsi con ADFS o tramite federazione SAML / OpenID	X	X	X	X
Il Sistema deve avere una console di gestione centralizzata per l'aggregazione degli eventi provenienti da tutte le sonde periferiche.	X	X	X	X
Il sistema deve inviare notifiche Mail al raggiungimento di soglie di allarme preimpostate da specifici KRI.	X		X	X
Il sistema deve fornire un popolamento automatico e manuale dell'asset inventory .		X	X	
Il sistema deve fornire supporto evolutivo per aggiungere nuovi protocolli OT, in particolare relativamente all'asset discovery (e.g.: nuovi device introdotti sul mercato, protocolli proprietari sviluppati internamente ad ASPI).	X	X		X
Il sistema deve avere un supporto di formati più comuni (Excel, csv) per l'import/export di informazioni asset .	X	X	X	X
Il sistema deve fornire API REST per accedere alle funzionalità .	X		X	X
Il sistema deve correlare dati ricevuti da più sorgenti e farli confluire nel profilo dell'asset. In particolare, la soluzione dovrà essere interoperabile con la tecnologia NAC, ovvero dovrà arricchire le informazioni dei MAC address sotto la gestione del NAC con informazioni dettagliate tramite integrazioni mutue con API o SDK.	X		X	X
Il sistema deve essere accessibile via browser usando un'interfaccia sicura (HTTPS con SSO ed MFA).	X	X	X	X

Il sistema deve essere disponibile secondo i dettagli definiti in Sezione "Architettura Centrale" (all'interno del paragrafo 4.2 "Scopo della Fornitura") del Capitolato. In particolare, il sistema deve essere disponibile in modalità degradata di tipo "island mode" e "fail close", secondo la definizione IEC ISA 62443-3-3 SR 5.2 RE 2.	X	X	X	X
Il sistema deve poter essere utilizzato anche offline (e.g., senza connessione ad Internet) eventualmente ricevendo soltanto informazioni dai sistemi gestiti e generando alert in caso di anomalie riscontrate, senza perdere le configurazioni implementate, i rilevamenti, in modo da garantire un adeguato presidio fino al momento in cui viene ripristinata la connessione verso Internet. Durante la fase Offline è ammessa la momentanea mancanza dello storico oltre i 5gg.	X	X	X	X
Il sistema deve avere una opzione che garantisca il suo Disaster Recovery; i requisiti dovranno essere di RPO <= 1 ora ed RTO <= 1 ora; tuttavia, è desiderabile che siano entrambi tendenti a 0.	X	X	X	X
Il sistema deve integrarsi con i sistemi SIEM (QRadar) ma anche con ulteriori prodotti leader di mercato (Splunk, Microsoft, Securonix, Exabeam, etc.) della Committente, per l'invio di eventi di sicurezza quali ad esempio l'accesso alle interfacce delle soluzioni. La soluzione tramite protocollo SYSLOG è preferita	X	X	X	X
La soluzione proposta deve garantire la creazione/ personalizzazione di report ad hoc per indirizzare specifiche esigenze di sicurezza, business, compliance e audit.	X	X	X	X
La soluzione proposta deve garantire la possibilità di scaricare e salvare la reportistica in formati diversi (almeno PDF, CSV e/o Excel).	X	X	X	X
La soluzione proposta deve garantire la creazione di report custom da interfaccia web, senza ricorrere a tool e linguaggi (es. SQL o LDAP) terzi.	X	X	X	X

5.2 Data di inizio dei lavori

Entro 10 giorni solari dalla sottoscrizione del contratto, ASPI organizzerà il primo incontro (kick-off meeting) con l'Appaltatore per:

- presentare il team che si occuperà del progetto;
- definire i passi preliminari per l'inizio delle attività;
- validare il Piano di Progetto.

ASPI si riserva la possibilità di posticipare, sulla base delle proprie esigenze, il kick-off meeting oltre ai 10 giorni sopra indicati. La data del kick-off meeting sarà assunta come Data di inizio dei lavori (DIL).

5.3 Luogo e orario di lavoro

Le attività oggetto dell'appalto saranno svolte da personale incaricato dall'Appaltatore durante i giorni lavorativi, all'interno della fascia oraria 08:00-18:30. ASPI si riserva la facoltà di richiedere all'Appaltatore l'erogazione del servizio anche al di fuori dell'orario sopra indicato (ovverosia nella fascia oraria 18:30-08:00) e nei giorni non lavorativi (sabato, domenica e festivi), senza oneri aggiuntivi per ASPI, fino a una quota massima del 3% del totale dell'impegno (c.d. *effort*) previsto per l'intero periodo di progetto.

La Committente metterà a disposizione i locali, gli strumenti di lavoro e le abilitazioni informatiche per consentire al personale di poter prestare i servizi richiesti.

Il luogo di lavoro sarà principalmente Firenze. Eventuali trasferte on-site (e.g., in galleria, o in stazioni di esazione) sono possibili per installazioni, manutenzioni, o messe a punto. La fornitura sarà erogata in maniera ibrida (on site e da remoto).

5.4 Piano complessivo delle attività

A partire dalle Fasi progettuali sotto individuate e descritte, l'Appaltatore dovrà predisporre un Piano Complessivo di progetto dettagliando le attività, le milestones e i deliverables relativi a ciascuna fase qui sottoindicata. Il Piano di progetto dovrà essere allegato all'Offerta tecnica.

Le fasi progettuali sono così definite:

- Fase 1: Implementazione piattaforma OT-AD, OT-AI, OT-VM
- Fase 2: Attivazione piattaforma OT-NE

A partire dalla data di completamento della Fase 1 di cui sopra, l'Appaltatore deve garantire un **Servizio di manutenzione e supporto evolutivo** sulla piattaforma stessa per le soluzioni di OT-AD, OT-AI, e OT-VM.

A partire dalla data di completamento della Fase 2 di cui sopra, l'Appaltatore deve garantire un **Servizio di manutenzione e supporto evolutivo** sulla piattaforma stessa per le soluzioni di OT-NE.

Deliverables minimi fase 1:

- Documentazione architetturale, documentazione relativa alle configurazioni di dettaglio di tutti i sistemi coinvolti (inclusi gli schemi logici a livello di rete), etc.;
- Documentazione sugli step e i dettagli di integrazione avvenuta con il NAC in uso in ASPI.
- Manuali tecnici di Amministrazione delle piattaforme OT-AD, OT-AI, OT-VM;
- Formazione, manuale, tutorial per utente operativo.
- Piattaforma funzionante con lista di apparati e piano di integrazione con le piattaforme di asset inventory esterne per l'importazione degli UUID

Deliverables minimi Fase 2:

- Documentazione architetturale, documentazione relativa alle configurazioni di dettaglio di tutti i sistemi coinvolti (inclusi gli schemi logici a livello di rete), etc.;
- Documentazione sugli step e i dettagli di integrazione con la piattaforma OT-AI.
- Manuali tecnici di Amministrazione della piattaforma OT-NE;
- Formazione, manuale, tutorial per utente operativo.

5.5 Modalità di esecuzione delle prestazioni

Qualsiasi attività riguardante la progettazione, l'esecuzione o la modifica di servizi o infrastrutture compresi nel contratto dovrà esser preventivamente concordata ed autorizzata dalla Committente.

L'Appaltatore dovrà redigere, prima di ogni fase del progetto, un documento di sintesi nel quale riporterà i requisiti attesi. Il documento dovrà esser preventivamente condiviso con la Committente per l'approvazione. Solo ad approvazione ricevuta, l'Appaltatore potrà dare avvio alle implementazioni. L'Appaltatore dovrà eseguire le attività seguendo le fasi, i processi e le procedure approvate dalla Committente attenendosi al Piano definitivo di progetto.

L'Appaltatore dovrà altresì predisporre e condividere con la Committente la documentazione tecnica e funzionale relativa ad ogni implementazione prevista dal Piano di Progetto nelle varie Fasi e mantenere sempre aggiornata tale documentazione.

5.6 Attività di supporto operativo ed evolutivo

Le attività di supporto operativo ed evolutivo si avvieranno allo scopo di manutenere ed evolvere le nuove piattaforme a partire dalla data di passaggio in produzione (prevista al termine della Fase 1), a supporto delle strutture interne di riferimento.

In ogni caso, visti i potenziali impatti elevati sulla rete autostradale in caso di disservizio, le attività sugli ambienti di produzione dovranno essere effettuate secondo quanto descritto nella procedura aziendale di Change Management che verrà condivisa fin dalla prima riunione di kick-off, e comunque solo a seguito di specifica approvazione scritta da parte del personale interno di Autostrade per l'Italia.

Il Fornitore sarà tenuto ad una rendicontazione su base settimanale degli interventi eseguiti e anomalie risolte utilizzando strumenti da concordare con gli uffici DIDT/CTO/SCR e DIDT/CISO/SAE. A conclusione degli interventi più rilevanti il Fornitore dovrà consegnare ai referenti ASPI un *rapporto di chiusura attività* con indicazione dell'esito e del tempo impiegato.

Gestione delle emergenze

Al fine di gestire con la massima efficacia situazioni di emergenza (malfunzionamenti di ogni genere, errori, instabilità, cadute dei sistemi, perdita di funzionalità, oppure Incidenti di Sicurezza etc.) che interessino gli ambienti di produzione della piattaforma oggetto di assistenza e che causino l'indisponibilità del servizio, il Fornitore sarà chiamato ad intervenire con la massima tempestività al fine di ripristinare i servizi nel minor tempo possibile, con risorse specialistiche su tutti gli ambiti previsti nel perimetro del contratto.
Per lo svolgimento di tali attività il Fornitore dovrà fornire un servizio di reperibilità da remoto e un punto di contatto unitario (composto da numero di telefono e indirizzo mail) che sia disponibile e raggiungibile fuori dall'orario di lavoro standard, cioè nei giorni feriali dalle ore 18.30 alle ore 08.00 e nei giorni festivi per l'intera giornata, tramite il quale attivare le risorse specialistiche necessarie a seconda dell'ambito impattato.
Tale Servizio di Gestione delle Emergenze, attivabile per sua stessa natura H24 365 gg/anno, verrà consuntivato in modalità "a ticket" o "a chiamata", in base agli specifici eventi.

Servizio di SOC OT

Il servizio è da considerarsi come costituito almeno da 1 FTE business day + nighttime (remote) a partire dal termine della Fase 1 di progetto. Questa FTE è da considerarsi il target aziendale che si occuperà di fare tuning dei sistemi, e di iniziare a ricevere gli allarmi e classificare i falsi positivi. Inoltre, si occuperà di prendere accordi con il Service Desk di ASPI e i vari Centri di Monitoraggio per le operazioni di remediation tipiche di SOC.
Al servizio di SOC OT può aggiungersi il **servizio (opzionale) di Threat Intelligence OT,** ovvero un servizio di feed di CTI dedicati alle tecnologie ICS.

5.7 Servizio di passaggio delle conoscenze

L'Appaltatore dovrà erogare le attività relative al passaggio delle conoscenze. Tali attività comprendono quanto necessario al trasferimento del know-how sui servizi e sui sistemi oggetto del presente Capitolato al personale della Committente e/o a terzi da questa designati, con l'obiettivo di rendere la Committente totalmente autonoma nella gestione delle successive evoluzioni delle piattaforme.

Il servizio dovrà essere erogato dall'Appaltatore nel corso degli ultimi 3 mesi prima della chiusura del contratto (sia essa scadenza naturale o risoluzione anticipata su richiesta della Committente). Durante tale periodo l'Appaltatore dovrà predisporre un Piano di Passaggio delle conoscenze che specifichi le modalità che intende seguire (sessioni di training, meeting, affiancamenti, etc.), le risorse professionali coinvolte, il piano attività da svolgere, gli aspetti che saranno oggetto di approfondimento, le informazioni che saranno fornite, i materiali e la documentazione che saranno messi a disposizione.

A seguito dell'approvazione della Committente, l'Appaltatore eseguirà le attività di passaggio di consegna entro i tempi e modi definiti nel Piano di Passaggio approvato. Completate le attività, il Fornitore dovrà produrre un report di chiusura, dando evidenza delle attività svolte e del livello di conoscenza ed autonomia raggiunto dal personale subentrante.

5.8 Servizio di formazione

Nel corso della durata contrattuale, l'Appaltatore dovrà provvedere all'erogazione di corsi di formazione con voucher per esame finale volti all'ottenimento di certificazione sulle piattaforme in uso nell'ambito del presente appalto per un numero minimo di 5 dipendenti della Committente (sia in vece di Amministratori, qualora non si tratti di personale operativo posto a presidio dall'Appaltatore, sia in vece di utente finale, Analyst).
La formazione dovrà esser erogata in modalità "train the trainer" secondo le modalità indicate nel Piano di Formazione predisposto dall'Appaltatore in fase di gara. L'organizzazione delle attività di formazione ed il personale interno ed esterno coinvolto saranno concordate con la Committente.
A valle dei singoli interventi formativi, l'Appaltatore dovrà produrre, fornire ed archiviare idonea documentazione attestante lo svolgimento degli interventi formativi svolti e la partecipazione degli utenti.
L'appaltatore dovrà altresì formalizzare dei manuali utente per supporto all'utilizzo della piattaforma.

6 Service Level Agreement (SLA) e Penali

La valutazione delle attività progettuali avverrà in base al raggiungimento degli obiettivi e delle milestone di progetto entro le tempistiche massime indicate. Le penali verranno calcolate sul mancato rispetto degli SLA come definito nel presente Capitolato. Il limite massimo di applicazione delle penali è del 10% del valore complessivo del contratto.

Per quanto riguarda le **attività progettuali** sono definiti i seguenti SLA e penali:

ID	Descrizione	SLA/KPI presa in carico	Penale
SLA_P01	Turnover del team di progetto - Numero massimo di risorse sostituite (escluse le sostituzioni dovute a cause di forza maggiore come ad esempio grave malattia)	Target max 3 risorse	1‰ (uno per mille) dell'ammontare netto contrattuale per ogni sostituzione eccedente lo SLA
SLA_P02	Tempo di sostituzione di una risorsa del Team di Progetto con una nuova idonea e che rispetti i requisiti del presente Capitolato Tecnico.	Target 40 gg lavorativi dalla data di richiesta via mail da parte del Responsabile Tecnico	100 € per ogni giorno lavorativo eccedente rispetto allo SLA stabilito
SLA_P03	Rispetto delle milestone - consegna dei Deliverable richiesti entro le date fissate (milestone) dal Piano di Progetto	Target 0 gg lavorativi tra la data effettiva consegna del deliverable e la data concordata per la consegna deliverable	100 € per ogni giorno lavorativo eccedente rispetto allo SLA stabilito fino al 30° giorno. 200 € per ogni giorno lavorativo eccedente allo SLA stabilito dal 31° giorno in poi.

Per quanto riguarda il **Servizio di SOC OT**, previsto a partire dalla fine della Fase 1 di progetto, nella tabella seguente sono elencati i tempi di presa in carico relativi alle principali attività richieste.

TABELLA SERVIZI:

ID	Descrizione (Day by day)	Tempi presa in carico
T01	Presa in carico eventi a criticità ALTA	1 h
T02	Presa in carico eventi a criticità MEDIA	2 h
T03	Presa in carico eventi a criticità BASSA	8 h
T04	Gestione incidenti a criticità ALTA	1 h

T05	Gestione incidenti a criticità MEDIA	4 h
T06	Gestione incidenti a criticità BASSA	8 h
T07	Chiusura incidenti a criticità ALTA (*)	24 h
T08	Chiusura incidenti a criticità MEDIA (*)	48 h
T09	Chiusura incidenti a criticità BASSA (*)	144 h

(*) Gli SLA di chiusura di un evento sono applicabili solo in caso di autonomia operativa totale del fornitore nella risoluzione della segnalazione. Non verranno quindi conteggiati i tempi di attesa dovuti ad attività di personale tecnico interno di ASPI necessari alla risoluzione del problema.

La rilevazione del rispetto dei suddetti tempi di presa in carico sarà effettuata con cadenza trimestrale.
In merito ai tempi di presa in carico, sono fissati i seguenti SLA e penali:

ID	Descrizione	KPI (Soglia minima di accettabilità)	Penale
SLA_S01	Rispetto dei tempi presa in carico sul n. totale di eventi/incidenti gestiti nel trimestre	95,00%	**1‰ (uno per mille)** del valore del contratto per ogni punto decimale percentuale di differenza rispetto al valore target. Ad esempio, nel caso il livello raggiunto sul KPI in oggetto sia 94,5% rispetto al 95% target, la penale da applicare sarà: 95% - 94,5% = 0,5% => 5 punti decimali di differenza Penale = 5 x [1‰ del valore complessivo del contratto] = 0,5% del valore complessivo del contratto

7 Elementi dimensionali

Componente	u.m.
Licenza SW soluzione OT-AD, OT-AI, OT-VM, OT-NE con validità triennale e pagamento anticipato per la gestione dei seguenti volumi: - 40.000 dispositivi; Sonde fisiche, se necessarie, in numero tale da soddisfare i requisiti presentati nel presente capitolato. In particolare, viene suggerito: - Nr. 2 sonde per ciascuna galleria oggetto del monitoraggio; - Nr. 1 sonda per ciascuna stazione di esazione; - Nr. 4 sonde per i Data Center centrali. Supporto operativo ed evolutivo su tutte le soluzioni	Licenze triennali
Attività progettuali - Fase 1: Implementazione piattaforma OT-AD, OT-AI, OT-VM - Fase 2: Attivazione piattaforma OT-NE	A corpo
Servizio di SOC OT a partire dal termine della Fase 1 di Progetto (1 FTE on premises business day + nighttime remote)	A corpo