



Allegato 1
(articolo 1, comma 1)

ISTRUZIONI TECNICHE DI CUI AL DECRETO N. 108 DEL 11 MAGGIO 2015

1. Caratteristiche generali

Premessa

Il nucleo informativo dell'AIA è costituito dalla Banca Dati Sinistri (BDS) dell'IVASS, che raccoglie dati sulle segnalazioni di sinistri da parte delle imprese assicurative nazionali, cui il legislatore ha stabilito di integrare una serie di banche dati esterne gestite da enti pubblici e privati, riguardanti informazioni inerenti i sinistri. Sulla base di questo archivio centralizzato è possibile implementare un sistema di supporto alle indagini in grado di fornire una serie di strumenti avanzati di analisi ed esplorazione dei dati, per il contrasto e la prevenzione della frode alle assicurazioni.

La complessità del progetto e la necessità di disporre in tempi brevi di informazioni più articolate e puntuali per l'attività antifrode, hanno portato a una scelta progettuale di tipo modulare. In sintesi, i principali obiettivi del progetto sono la realizzazione dell'impianto base, che comprende l'individuazione ed il collegamento a un primo insieme di archivi di rilevante interesse informativo, l'implementazione dei flussi di alimentazione ed, infine, il calcolo e la fruizione di indicatori di anomalia a supporto della fase liquidativa dei sinistri, nonché la realizzazione delle funzionalità di consultazione da parte delle imprese assicuratrici.

La soluzione vede l'AIA come un sistema indipendente, regolato da proprie norme, con le seguenti caratteristiche:

- **Modularità.** Moduli funzionali con un adeguato livello di disaccoppiamento che permettano uno sviluppo graduale e incrementale del progetto, oltre a garantire una grande flessibilità e manutenibilità.
- **Prestazioni.** Predisposizione di ambienti idonei al trattamento di grandi volumi di dati e all'acquisizione di significative quantità di informazioni, garantendo la loro elaborazione in tempi contenuti.
- **Sicurezza.** Data la natura e la criticità dei dati trattati, la sicurezza deve essere gestita ai massimi livelli in termini di protocolli, standard, infrastrutture, metodi operativi e procedure organizzative.
- **Riuso.** Sia per questioni di tempi, che per ragioni di costo, si dovranno riusare le infrastrutture ed i software disponibili presso l'IVASS, senza che ciò debba compromettere il raggiungimento degli obiettivi prefissati.

Tutte le funzionalità della piattaforma AIA si basano su un data warehouse costituito da un archivio di sinistri integrato, contenente le informazioni dei soggetti e dei veicoli coinvolti a vario titolo nei sinistri,



nonché tutti gli indicatori di dettaglio calcolati su di essi. Questo archivio permette una visione dettagliata dei sinistri in un modo unificato, indipendente dalla visione parziale dei sinistri che ha ogni impresa di assicurazione. L'alimentazione del data warehouse avviene con procedure automatiche di acquisizione dati e data integration, che provvedono anche a normalizzare ed unificare le informazioni di diversa provenienza.

Principali funzionalità

- Integrazione con la BDS e con le banche dati esterne. Al fine di aggiornare periodicamente il database dell'AIA, l'acquisizione dei dati è selettiva ed incrementale, secondo logiche prestabilite per evitare di riportare più volte la stessa informazione e di ripetere inutilmente le interrogazioni.
- Calcolo di indicatori (indici di anomalia). Per ogni entità di rilievo, cioè sinistri, veicoli e soggetti, vengono calcolati una serie di indicatori di anomalia che permetteranno di stimare il rischio frode. Dopo ogni aggiornamento dei database, per i dati che abbiano subito modifiche, sono ricalcolati tutti gli indicatori associati. Infine, per ogni entità viene calcolato un indice sintetico di anomalia (score).
- Flusso di ritorno per le assicurazioni. È predisposto un servizio automatico, che per ogni impresa di assicurazione, elabora e trasmette un flusso di dati con tutte le segnalazioni di anomalia sui sinistri che la coinvolgono. La segnalazione automatica all'impresa avviene ogni qualvolta c'è una variazione negli indicatori di rilevanza frode.
- Servizio di interrogazione per le assicurazioni (consultazione a richiesta). È realizzato un servizio automatico, che per ogni impresa di assicurazione, dato un flusso dati di interrogazione con gli identificativi dei sinistri che la riguardano, predispone un flusso dati di ritorno con le informazioni dei sinistri in questione.

2. Contenuti Informativi

A regime, AIA riceve un flusso di segnalazioni proveniente dalla BDS, che poi dovranno essere integrate, completate e validate con le informazioni acquisite da database esterni all'IVASS, come previsto dall'allegato A del decreto n. 108 del 11 maggio 2015.

I dati presenti nella BDS sono verificati o integrati con quelli delle basi dati esterne per costituire un quadro più integrale e coerente del sinistro. Tutte le informazioni provenienti dalle diverse fonti di approvvigionamento sono tracciate e documentate in modo da sapere in ogni momento l'origine di un qualsiasi dato, indicatore o elaborazione prodotta dall'AIA. In questo modo è possibile garantire che i fatti e le indicazioni che emergeranno dall'AIA possono essere verificati dalla fonte originale.

Il risultato sarà un unico archivio unificato, ovvero un data warehouse, contenente un patrimonio informativo con un valore addizionale fornito dalla messa a sistema di informazioni provenienti da fonti diverse e precedentemente scollegate. L'archivio informatico integrato è un database composto principalmente da tre tipi di informazione:

- Evento sinistro, identificato dal codice unico, che a sua volta è costituito da una serie di partite di danno segnalate dalle imprese e descritte da un insieme di danni, lesioni e pagamenti eseguiti.
- Dati anagrafici costituiti da veicoli e soggetti (persone fisiche e giuridiche) coinvolti/interessati a vario titolo in uno o più sinistri.

- Indicatori di dettaglio a livello di singolo sinistro, veicolo e soggetto riguardanti statistiche varie e indicatori di rischio frode di diverso tipo derivati dai dati dei sinistri e informazioni anagrafiche.

Nella figura 1 si riporta uno schema concettuale illustrativo dell'archivio integrato sinistri.

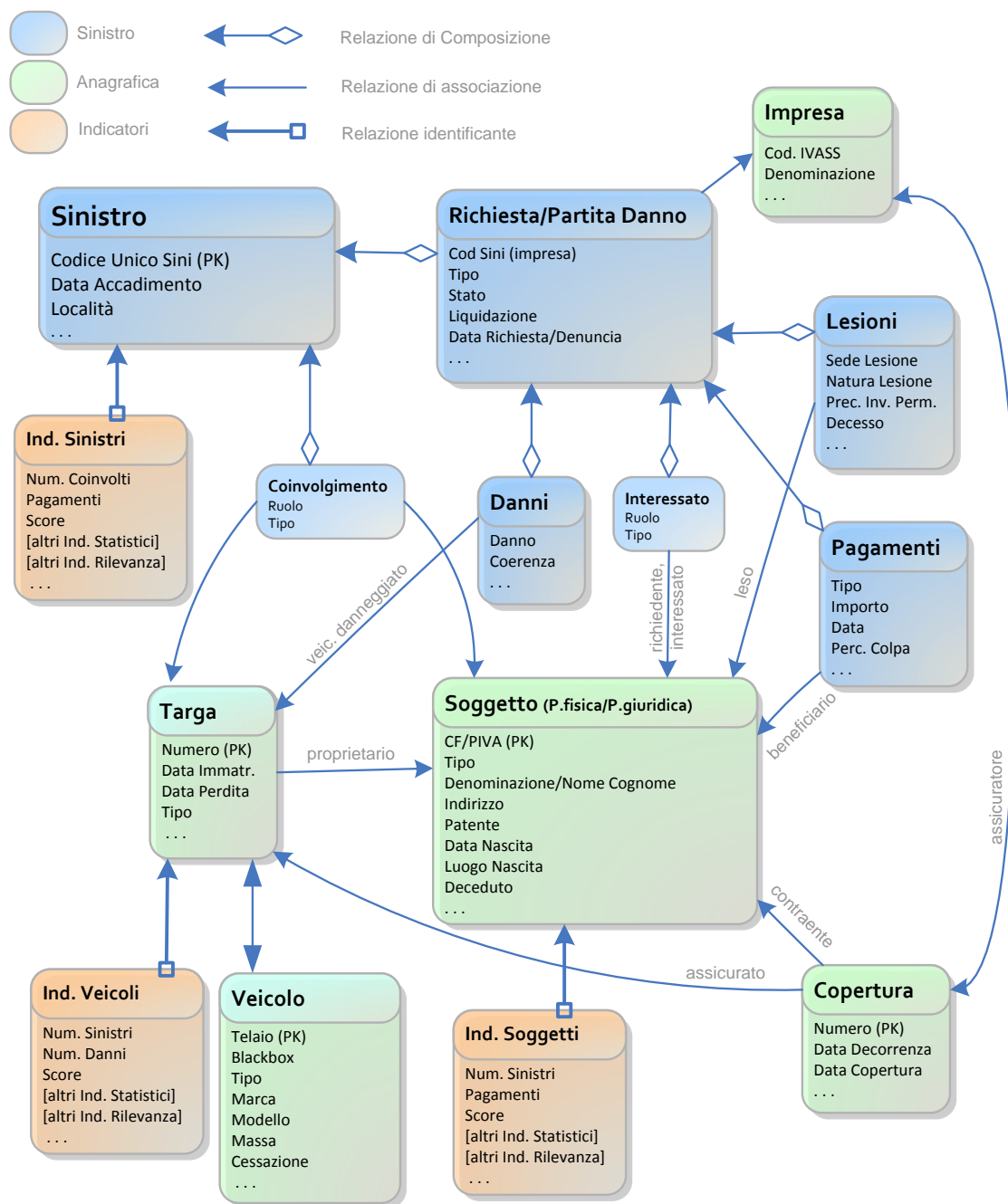


Fig. 1 Modello concettuale dell'archivio integrato sinistri (BDS e informazioni provenienti dai DB esterni).

3. Descrizione dei Flussi

Nella figura 2 viene dettagliato il flusso informativo generale dell'AIA, partendo dalle informazioni che arrivano dalla BDS e dalle banche dati esterne (Data Acquisition). Questi dati vengono processati nelle fasi intermedie di elaborazione (Data Integration). Infine, nella fruizione i dati elaborati confluiscono nei sistemi esterni tramite interoperabilità applicativa.

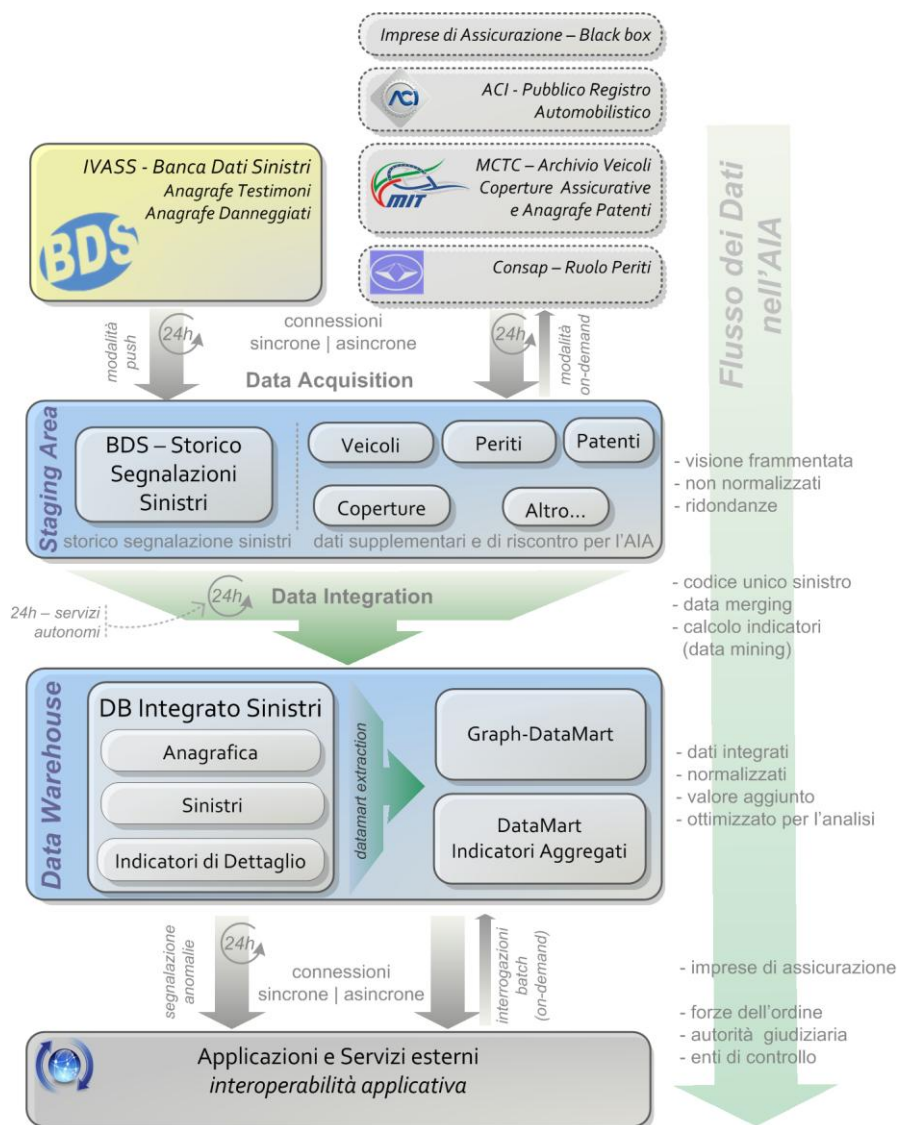


Fig2 Flusso informativo generale dell'AIA.

Data Acquisition

L'AIA acquisisce le informazioni principalmente in due modalità:

- modalità push – usata unicamente per il canale interno di alimentazione della BDS. Giornalmente arrivano dei flussi consolidati dalla BDS che vanno ad aggiornare, in modalità insert/update, l'archivio storico delle segnalazioni sinistri della Staging Area dell'AIA.



- modalità on-demand – usata per l’interrogazione alle altre banche dati esterne dalle quali si ottengono informazioni aggiuntive e di riscontro. Anche queste informazioni vengono aggiornate in modalità insert/update. Una funzione autonoma di acquisizione, che con certe logiche (principalmente sui nuovi dati della BDS), attiva le interrogazioni nelle banche dati esterne. Le comunicazioni avvengono in modalità sincrone e asincrone tramite accesso a Web Services o scambio di archivi tramite protocolli prestabiliti e concordati con gli enti titolari del servizio, secondo le modalità individuate nelle convenzioni di cui all’art. 5, comma 4 del decreto n. 108 del 11 maggio 2015.

I dati acquisiti su questi canali sono memorizzati nella Staging Area dell’AIA e costituiscono la base informativa su cui si effettuano le elaborazioni per alimentare il data warehouse.

Data Integration

In questa fase la procedura di data integration esegue tutte le elaborazioni di trasformazione e normalizzazione dei dati. In questo processo si calcola anche codice univoco evento. Una volta ricostruiti dati anagrafici e sinistri, vengono calcolati gli indicatori tramite le procedure di data mining e vengono derivati dei data mart per l’analisi di rete e per le statistiche aggregate. Questa procedura si attiva quando ci sono nuovi dati da processare nella Staging Area.

Fruizione

Le informazioni dell’AIA possono essere accedute con due modalità:

- Flusso di ritorno–La procedura comunica , in funzione del profilo della utenza applicativa e degli esiti delle consultazioni, le informazioni relative ai nuovi sinistri e a quelli che hanno subito cambiamenti rilevanti nei loro indicatori.
- Servizio di interrogazione–Il servizio riceve una richiesta di interrogazione su sinistri, soggetti e veicoli, ed in base al profilo dell’utenza applicativa, viene elaborata una risposta.

Servizi di Interoperabilità Applicativa

I servizi di interoperabilità applicativa sono ideati per utenze applicative che accedono tramite le infrastrutture messe a disposizione per la comunicazione dati fra applicazioni, ovvero, tramite scambio file asincrono autenticato e con cifratura della comunicazione (canali di scambio archivi).

Il servizio riceve e restituisce flussi di dati strutturati (provenienti dal data warehouse) secondo formati prestabiliti in base alle funzionalità accedute. Le funzionalità di primo livello sono basate su Web Services e vengono implementate a livello di servizio, le funzionalità esposte mediante “canali di scambio archivi”, sono di secondo livello, ovvero sviluppate come wrappers su quelle di primo livello.

Ogni accesso ai canali di comunicazioni prevede il riconoscimento certo e sicuro dell’utenza applicativa che accede, in modo da poter garantire la profilazione e un adeguato livello di sicurezza stabilito nelle procedure di scambio.

I servizi di interoperabilità applicativa esposti sono:

- Segnalazione Sinistri – per comunicare automaticamente l’esito del primo calcolo degli indicatori nonché delle loro successive eventuali modificazioni.



- Interrogazione Sinistri – per permettere l’interrogazione “a richiesta” dei sinistri per ottenere informazioni sugli indicatori e storica.

L’accesso ai servizi (utenza, connessione, funzionalità, durata, descrizione informazioni scambiate) verrà monitorato e registrato tramite l’apposito sistema di logging.

Servizio Segnalazione Sinistri

Questo è un servizio autonomo che monitora continuamente, dopo ogni aggiornamento, i cambiamenti sugli indici sintetici di rilevanza frode relativi a sinistri, soggetti e veicoli. Dopodiché predispone un flusso per ogni utenza registrata, segnalando ogni entità che ha subito un cambiamento significativo e che riguarda direttamente l’utenza in questione.

Il servizio memorizza per ogni utenza le ultime segnalazioni trasmesse, in modo da poter determinare in un secondo momento se ci sono variazioni significative.

Le principali funzionalità che garantisce il servizio sono:

- **impostazione** tramite configurazione delle “soglie di allarme” per sinistri, soggetti e veicoli in modo da poter regolare la sensibilità del sistema nel fare scattare le segnalazioni
- **impostazione** tramite configurazione “intervallo di variazione significativa” per sinistri, soggetti e veicoli in modo da poter regolare la sensibilità del sistema nel far scattare segnalazioni successive dovute a variazioni significative degli score
- **Messa a disposizione**, oltre all’identificativo e in base al valore dello score di sintesi, per ogni entità segnalata, degli indici analitici che hanno contribuito allo score e della sua descrizione analitica. Inoltre per ogni score viene reso disponibile un indicatore di affidabilità.

Servizio Interrogazione Sinistri

Il servizio di interrogazione sinistri permette di ottenere le informazioni relative alle entità provenienti dal data warehouse. Il servizio si attiva trasmettendo nella richiesta un insieme di identificativi di sinistri. Il risultato è un flusso con tutta l’informazione descrittiva e analitica delle entità interrogate provenienti dal data warehouse. I risultati saranno in corrispondenza con il profilo dell’utenza, per cui le imprese di assicurazione potranno interrogare solo sinistri, soggetti o veicoli coinvolti o interessati dai sinistri che risultino di loro competenza.

L’interrogazione avviene in modalità asincrona in base al codice sinistro, per ottenere gli indicatori di rilevanza frode e score dei sinistri di propria competenza. Ciò ha luogo per mezzo di un canale di comunicazione nel quale l’utenza invia un flusso di interrogazione in modalità asincrona e riceve la risposta dopo l’elaborazione.

4. Infrastrutture e connettività

Presso l’infrastruttura IT dell’IVASS è costituito un sistema informatico altamente scalabile e pienamente ridonato, destinato a erogare i servizi dell’Archivio Integrato Antifrode interfacciando una molteplicità di banche dati istituzionali e private.



Il colloquio con i diversi interlocutori e sistemi cooperanti avviene mediante meccanismi atti ad assicurare la riservatezza, l'integrità e l'autenticità delle comunicazioni.

In particolare per gli scambi dati con le imprese di assicurazione e con alcuni enti privati vengono usate delle infrastrutture di approvvigionamento su "canali di scambio archivi". Queste infrastrutture si basano su canali cifrati di scambio dati che permettono il trasferimento controllato e sicuro di archivi con grosse quantità di dati.

Lo scambio con le imprese assicurative avviene su internet con protocollo prestabilito. Questo protocollo usa certificati conformi allo standard X.509 per l'autenticazione ed il riconoscimento dell'utenza applicativa e per l'attivazione dei meccanismi di cifratura del canale di comunicazione.

Per l'accesso ai servizi delle banche dati esterne presso altri enti, devono essere implementate le modalità di accesso previste da tali enti, con il conseguente adeguamento delle infrastrutture AIA per una interrogazione ottimale e nel rispetto delle norme di sicurezza già in atto per il servizio in questione.

In base alle specificità degli enti coinvolti ed in base alle convenzioni da stipulare, le modalità di connessione sono:

- per la Motorizzazione Civile, mediante connessione VPN su internet e accesso con modalità Web Services, con l'uso dello standard WS-Security per le fasi di autenticazione ed autorizzazione. Successivamente i servizi di interscambio verranno migrati sul Sistema Pubblico di Connettività (SPC) ed integrati attraverso la porta di dominio;
- per il PRA, mediante connessione VPN su internet e accesso con modalità Web Services, con l'uso dello standard WS-Security per le fasi di autenticazione ed autorizzazione. In caso di successivo passaggio di comunicazione su infrastruttura SPC sarà adottato il solo meccanismo di gestione della sicurezza dei WS (standard WS-Security);
- per la fruibilità periodica dei dati del Ruolo Periti della CONSAP si fa uso di un canale SFTP su internet

5. Gestione della Sicurezza

Autenticazione e autorizzazione

Nell'AIA è previsto un servizio di autenticazione che garantisce il riconoscimento sicuro delle utenze applicative e fornisce standard di sicurezza adeguati alle attuali norme per la protezione dei dati. Inoltre il servizio gestisce anche i profili di autorizzazione degli utenti, fornendo informazioni applicative sulla profilazione delle utenze per assicurare un adeguato accesso a dati e funzionalità in accordo con i livelli di servizio, riservatezza e sicurezza che sono stati adottati. Il meccanismo di profilazione è flessibile ed interamente configurabile in modo da potersi adattare ad ogni esigenza attuale e futura.

In particolare il servizio consente:

- Autenticazione e riconoscimento delle utenze applicative.
- Gestione delle credenziali.
- Raggruppamento delle utenze in organizzazioni in modo da poter stabilire schemi di condivisione applicativa.
- Profilazione con grants e ruoli a più livelli gerarchici.



- Mappatura dei grants a livello di moduli funzionali.
- Mappatura dei grants a livello di dati (con granularità sinistro).

Logging e monitoraggio

Per garantire e controllare la sicurezza, la protezione dei dati e l'operatività del sistema, l'AIA è dotato di un sistema di logging e monitoraggio che permette la registrazione, la visualizzare e l'analisi di tutte le attività. La registrazione avviene a livello di utente operatore del sistema e di utenza applicativa esterna, con dettaglio di data e ora, operazione eseguita, dati e parametri coinvolti ed esito dell'operazione. Inoltre, il sistema di logging permette la registrazione di tutti i log di sistema contenenti le segnalazioni e messaggi a livello di traccia, avvisi o problemi critici che possano essere causa di perdite di informazione e/o malfunzionamenti. La registrazione di tali segnalazioni/messaggi riporta le informazioni relative a: data e ora, tipo di segnalazione, operazione, eventuali dati, parametri e utenze coinvolte.

Parallelamente viene attivato un sistema di monitoraggio in tempo reale che tiene sotto controllo i principali indicatori funzionali del sistema e notifica automaticamente agli amministratori e al personale di servizio le anomalie nell'operatività del sistema rilevate.

Auditing

Sulla base dei dati di logging relativi al funzionamento del sistema, l'IVASS eseguirà delle attività di auditing periodiche in relazione all'operatività, la sicurezza, le prestazioni e la qualità del servizio. L' IVASS eseguirà con i propri mezzi delle analisi sui dati rappresentate tramite report, statistiche e grafiche riassuntive, in modo da avere una visione globale dell'andamento dei sistema per prevenire e poter scoprire in tempo eventuali problematiche che possano sorgere.