Descrizioni Componente e Use Case

Vecchia descrizione Component D1:

- L’autenticazione non è stata specificata come caso d’uso, ma potrebbe apparire nel secondo deliverable in quanto ci sono alcuni file che vorremo passare lato client contestualmente all’autenticazione (ad esempio un file per le soglie dei parametri monitorati).

- Al lato server verrà aggiunta un’interfaccia per fornire feedback ai sensori sul loro stato di anomalia così da regolarne la frequenza di invio dei loro segnali.

Vecchia descrizione Component D2:

Come si può notare dai vari use case ed il component Diagram ci sono state molte modifiche dal primo deliverable. Le principali riguardano la gestione del dato direttamente utilizzando funzioni server, così da non fare i vari controlli sui dati in ogni singolo client, alleggerendo così il compito del client, evitanto inoltre il dover permettere la copia dei dati in ogni livello rischiando la Perdita di persistenza dei dati stessi, diminuendo quindi il quantitative di dati trasmessi e ricevuti dal server.

Nuova descrizione:

Come si può notare dai vari use case ed il component Diagram sono state apportate molte modifiche rispetto il primo deliverable. Le principali riguardano la gestione del dato direttamente utilizzando funzioni server, così da non fare i vari controlli sui dati in ogni singolo client, alleggerendo così il compito del client, evitanto inoltre il dover permettere la copia dei dati in ogni livello rischiando la Perdita di persistenza dei dati stessi, diminuendo quindi il quantitative di dati trasmessi e ricevuti dal server.

Nella versione 3 del component l’unica modifica effettuata è stata quella di rinominare il componente “FronteServer” in “Server”, questa scelta è dovuta al fatto che “FronteServer” poteva portare a confusione. Lo scopo di quel componete è quello di separare tutto quello che riguarda il lato server dall’interfaccia gestore e admin, dando così una un’idea più chiara e separata dei componenti. A sinistra del server abbiamo tutti i componenti di cattura e controllo dei segnali gestite dal server, mentre a destra le interfacce gestore e admin.

Vecchia Descrizione Use Case:

Alcune note sul diagramma:

1. Questa prima versione comprende esclusivamente requisiti ad alto livello, i requisiti di sistema e i corrispondenti scenari/casi d’uso saranno introdotti nel secondo deliverable, ciò include le funzionalità lato server, qui riportato come semplice attore. (Motivazione: Ci sono stati grandi ritardi nella prima fase)
2. La gestione in back-end sarà gestita nel prossimo deliverable, quando daremo anche un modello per i dati.
3. Abbiamo preferito separare nei 3 livelli di astrazione (edificio, distretto, città) il caso d’uso per le anomalie dei sensori dal momento che i dati (dati singoli vs dati aggregati) e i processi coinvolti (threeshold basato su sensori di backup rimanenti vs threeshold basato su rapporto sensori funzionanti / sensori totali) sono troppo eterogenei per riassumerli sotto un unico use-case.
4. Le relazioni di inclusione tra i casi d’uso 10 -> 9 , 9 -> 8 saranno probabilmente eliminate in quanto i casi d’uso 9 e 10 utilizzeranno dati che sono stati prodotti dai casi d’uso 8 e 9 ma lo faranno in modo asincrono: i trigger per questi casi d’uso sono la ricezione di nuovi dati rispetto all’area monitorata, non la disponibilità di nuovi dati relativi alle anomalie sui sensori.
5. L’aggiornamento dei dati in dashboard fa scattare il controllo sulle anomalie, mentre al termine del controllo sulle anomale , se ne sono state rilevate, verrà effettuato il controllo sui possibili pericoli; La relazione di inclusione tra casi d’uso 5 -> 2 è invece in senso stretto, dal momento che per focalizzarsi su una sotto-area, la dashboard farà richiesta al server dei dati relativi a quella sotto-area come 1-step routine.

Nuove note sull’Use Case:

Questa è la versione definitiva dell’Use case, rispetto alla prima versione dell’Use Case sono state apportate diverse modifiche, in modo particolare lato server, che inizialmente erano state trascurate. Infatti nella parte riguardante il server sono state effettuate delle importanti aggiunte, inerenti il controllo e l’aggiornamento dei dati. Per esempio i casi d’uso 22, 23 e 24 che riguardano il controllo dei dati, oppure il caso d’uso 21 che riguarda l’aggiornamento dei dati.

E’ stata presa la decisione di inserire i controlli sui dati lato server, per evitare di appesantire il lato client e quindi lasciare tutto il lato computazionale al server.

Per quanto riguarda la Dashboard, si occupa di far ricevere ai gestori i dati di interesse, con eventuali evidenziazioni di anomalie, sul sensore o sul dato e le eventuali notifiche di pericolo. Tutto questo viene gestito dai seguenti casi d’uso, l’1 richiede i dati per l’area di interesse del gestore, il 4 si occupa del livello di dettaglio al quale il gestore può accedere. Per quanto riguarda il livello di dettaglio è stato deciso di inserire questo caso d’uso in quanto non è necessario che i livelli più alti accedono a informazioni non rilevanti per loro, quindi ad ogni gestore vengono riportate le informazioni del livello di appartenenza. I casi d’uso 2,4,5,6,7 e 8 si occupano dell’evidenziare le anomalie sulla Dashboard in base alla gravità.

Per quanto riguarda la gestione Back-End del caso d’uso numero 19 non abbiamo dato una priorità alta, quindi abbiamo deciso di non sviluppare ulteriormente questo caso d’uso.