



Analisi di un sottosistema di posizionamento ferrotramviario

Corso di Laurea Magistrale in Informatica
Curriculum “*Resilient and Secure Cyberphysical Systems*”

Candidato: Alex Foglia

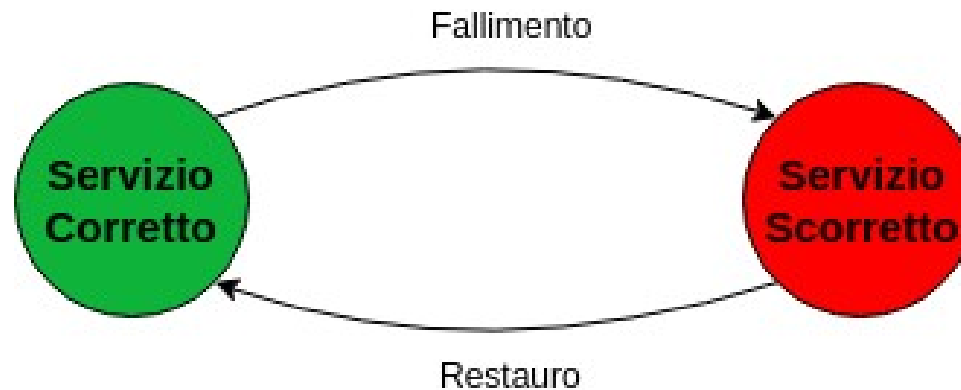
Relatore: Prof. Andrea Bondavalli

Indice

- **Dependability dei Sistemi Informatici**
- Stato dell'arte
- Descrizione del sistema analizzato
- Ambiente di analisi
- Risultati
- Conclusioni

Dependability

In letteratura, per **dependability** si intende **la capacità che ha un sistema di fornire un servizio corretto.**



Dependability – Elementi Chiave

Viene **valutata** rispetto a specifiche **misure**:

- Availability
- Reliability
- Maintainability
- Safety
- Coverage
- Altre...

È **minacciata** dai **threats**:

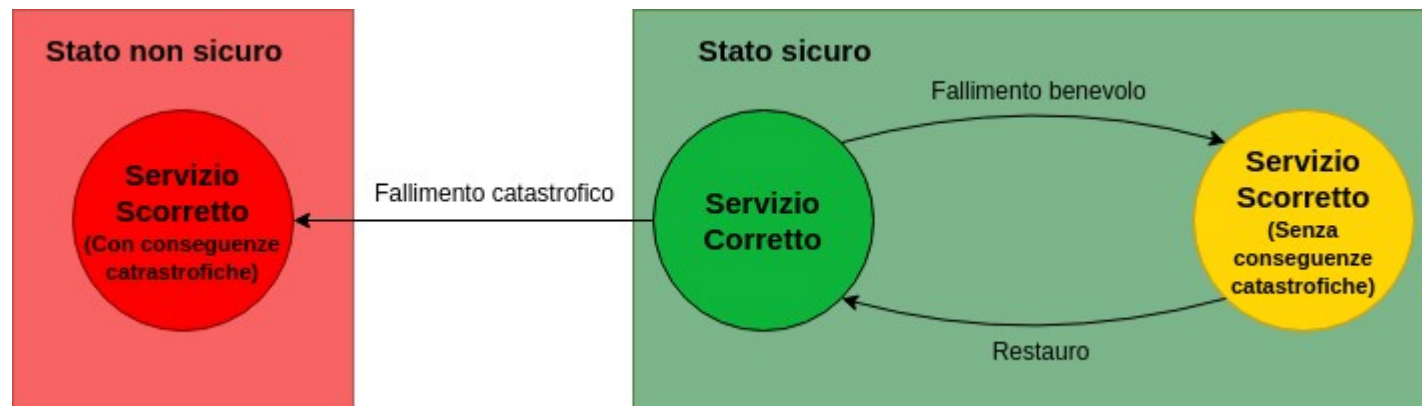
- Guasti
- Errori
- Fallimenti

È **raggiunta** attraverso l'utilizzo di opportune tecniche, i **means**:

- Fault Prevention
- Fault Removal
- Fault Tolerance
- Fault Forecasting

Sistemi Safety-Critical

La **safety** estende il concetto di **reliability**.



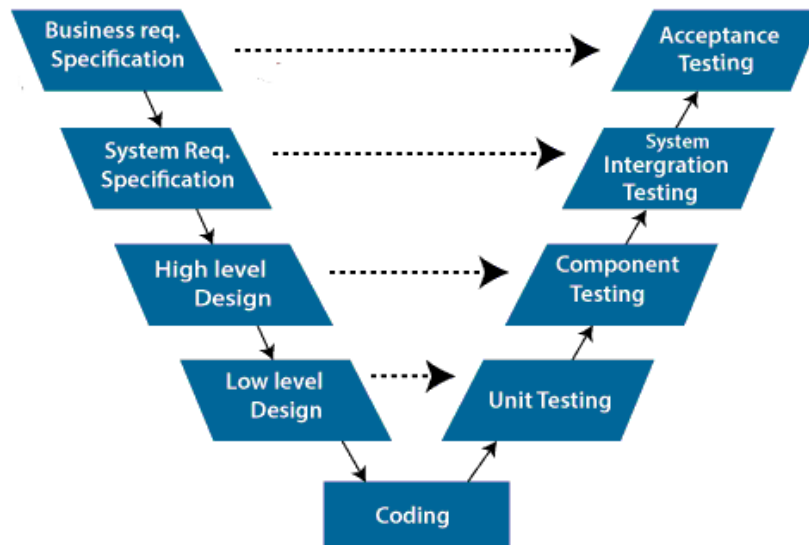
Quando esiste la possibilità di osservare un fallimento catastrofico, il sistema è detto **safety-critical**.

Dependability – Valutazione

Valutare la **dependability** di un sistema è parte integrante del processo di **validazione**: si vuole determinare se un sistema è conforme alle sue specifiche funzionali.

Quando si misura?

In generale, durante **tutte le fasi** del ciclo di vita del sistema.



Come si misura?

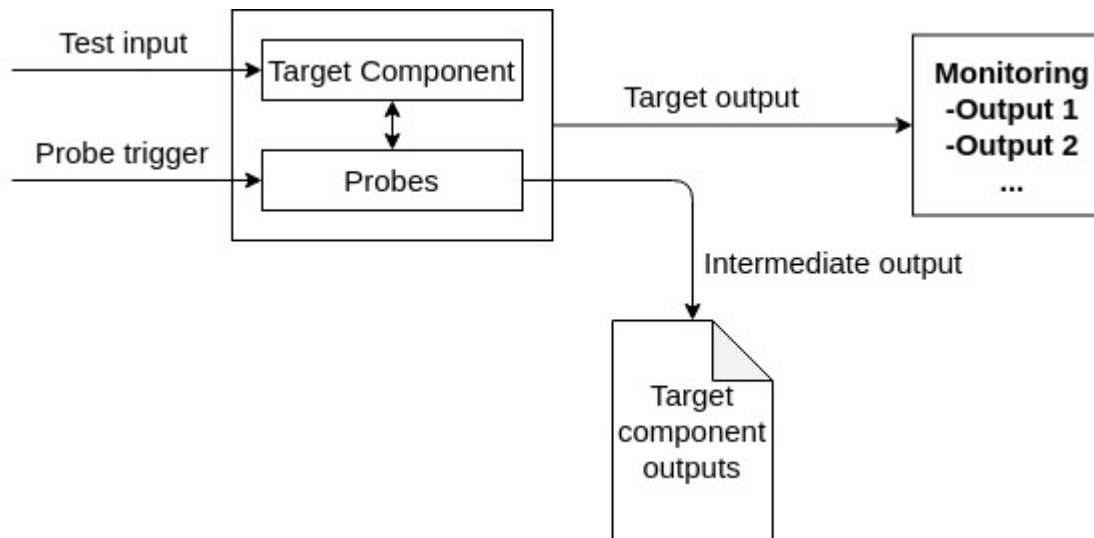
Modelli **combinatori**;

Modelli basati su **processi casuali**;

Osservazione del sistema.

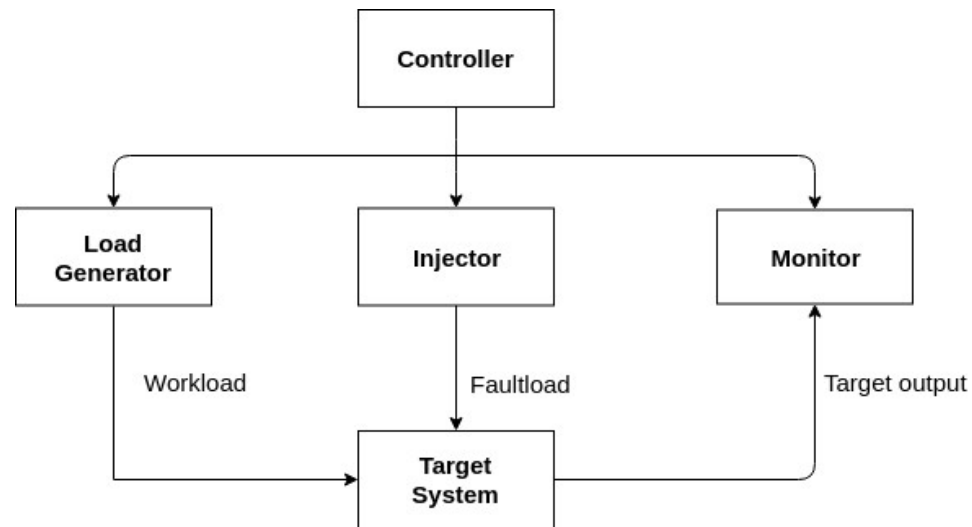
Monitoring

Il **monitoring** di un sistema consiste nell'osservazione del comportamento dello stesso nel suo ambiente operativo, allo scopo di effettuare **misure sperimentali**.



Fault Injection

Fault Injection è un caso particolare di **monitoring**: si vuole osservare il comportamento del sistema **in presenza di guasti**, volontariamente inseriti dall'osservatore.



Per effettuare una campagna Fault Injection affidabile, devono essere rispettati alcuni principi fondamentali, come **rappresentatività**, **fattibilità**, **ripetibilità** e **non intrusività**.

Indice

- Dependability dei Sistemi Informatici
- **Stato dell'arte**
- Descrizione del sistema analizzato
- Ambiente di analisi
- Risultati
- Conclusioni

Stato dell'arte – Posizionamento

I sistemi ferrotramviari nascono come derivazione dai classici sistemi ferroviari, e con questi ne condividono il problema del **posizionamento**.

Il posizionamento ferroviario, o ferrotramviario, consiste nella determinazione della posizione di un treno lungo una traccia, espressa come **progressiva chilometrica** rispetto a un punto di riferimento noto. Un sistema di posizionamento è un sistema **safety-critical**.

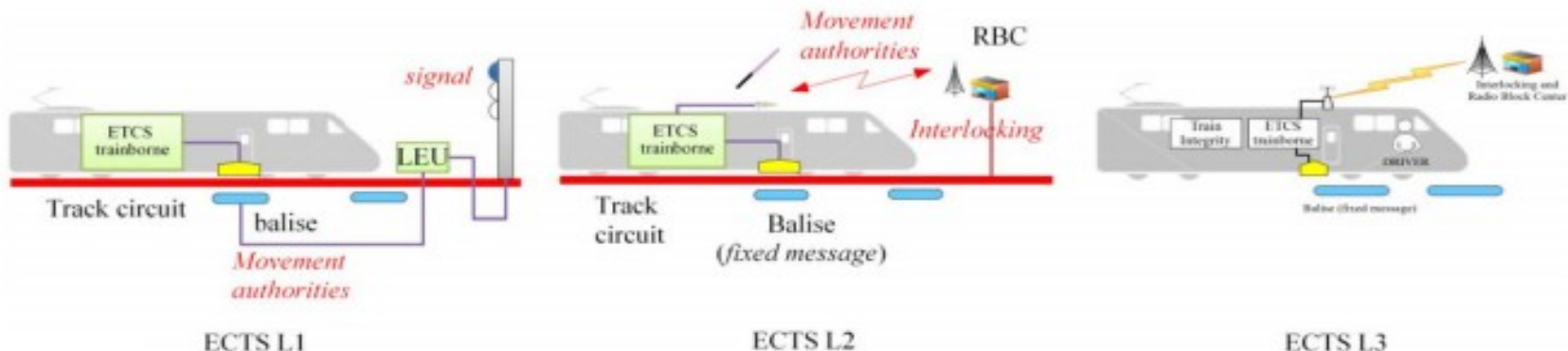
Nel dominio ferroviario, lo standard di riferimento per la realizzazione di sistemi di posizionamento è **ERTMS/ETCS** (European Rail Traffic Management System / European Train Control System).

Tradizionali tecniche di posizionamento – ETCS

Una traccia ferroviaria viene suddivisa in **blocchi**. Le tecniche di posizionamento si basano principalmente sull'utilizzo di strumenti installati a terra, chiamati **beacon** (o balises).

Un beacon, posizionato all'entrata di ciascun blocco, ha lo scopo di rilevare il passaggio di un treno. Un sistema di odometria installato a bordo posiziona il treno rispetto all'**ultimo beacon incontrato**.

Esistono specifici livelli di *compliance* che un sistema di posizionamento possiede rispetto a ETCS.



Verso ETCS-3

L'utilizzo di apparati di terra è **costoso** e ha un **impatto ambientale** non trascurabile: è necessario pianificare una migrazione verso sistemi di posizionamento autonomi (ETCS-3).

Nel dominio ferroviario, la quasi totalità dei sistemi di posizionamento è ETCS-1 o ETCS-2. Nel ferrotramviario vige la regola della **marcia a vista**, tuttavia esiste una tendenza di fatto a rispettare le linee guida ERTMS/ETCS.

Il sistema analizzato è conforme alla filosofia ETCS-3:

- Non prevede l'utilizzo di segnali provenienti dalla linea
- Opera interamente a bordo treno
- Basa il suo funzionamento su un algoritmo noto come **Sensor Fusion Algorithm** (SFA)

Indice

- Dependability dei Sistemi Informatici
- Stato dell'arte
- **Descrizione del sistema analizzato**
- Ambiente di analisi
- Risultati
- Conclusioni

Il Sistema analizzato – Descrizione Generale

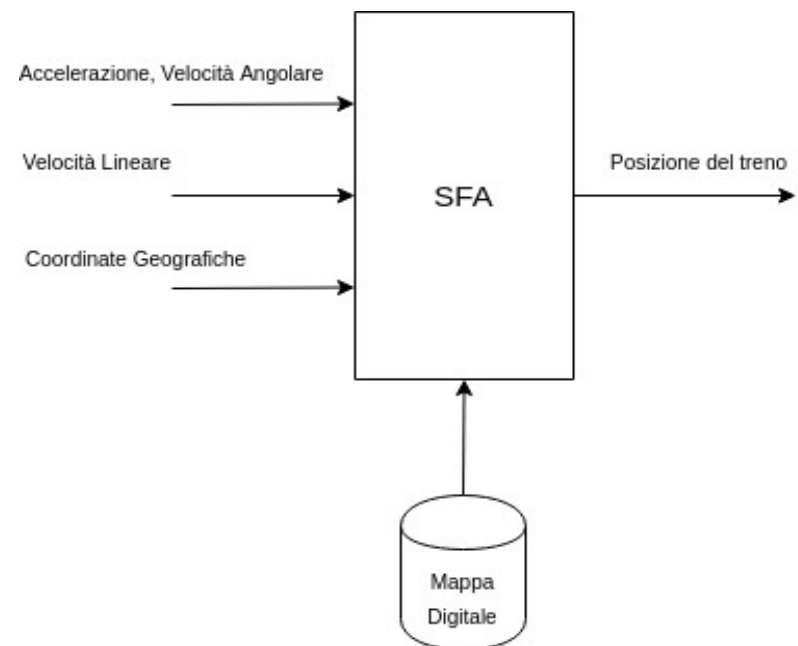
Da un punto di vista architetturale, il sistema analizzato è un **Cyber-Physical System**.

Scopo del sistema: fornire un servizio di posizionamento basato su SFA.

SFA permette di produrre una **stima statistica affidabile** della posizione del treno attraverso l'integrazione di più sorgenti di misura. In questa applicazione le misure processate sono:

- Accelerazione e velocità angolare;
- Velocità lineare;
- Coordinate geografiche.

Le misure vengono processate assieme a un'apposita **mapa digitale** della traccia su cui si muove il treno. L'uscita è prodotta in termini di progressiva chilometrica e coordinate ECEF.



Il Sistema analizzato – Sistemi Costituenti

I sistemi costituenti che compongono il sistema di posizionamento sono:

- Sensor Set, composto da:
 - Un *Inertial Measurement Unit (IMU)*, che campiona **accelerazione** e **velocità angolare**;
 - Un odometro, che campiona la **velocità lineare**;
 - Un ricevitore GPS, che campiona le **coordinate geografiche** del treno.
- Piattaforma di elaborazione dati (Nvidia TX-Jetson). Esegue la libreria SFA;
- On Board Control Unit (OBCU). Riceve la posizione e interagisce con il sistema di *interlocking*.

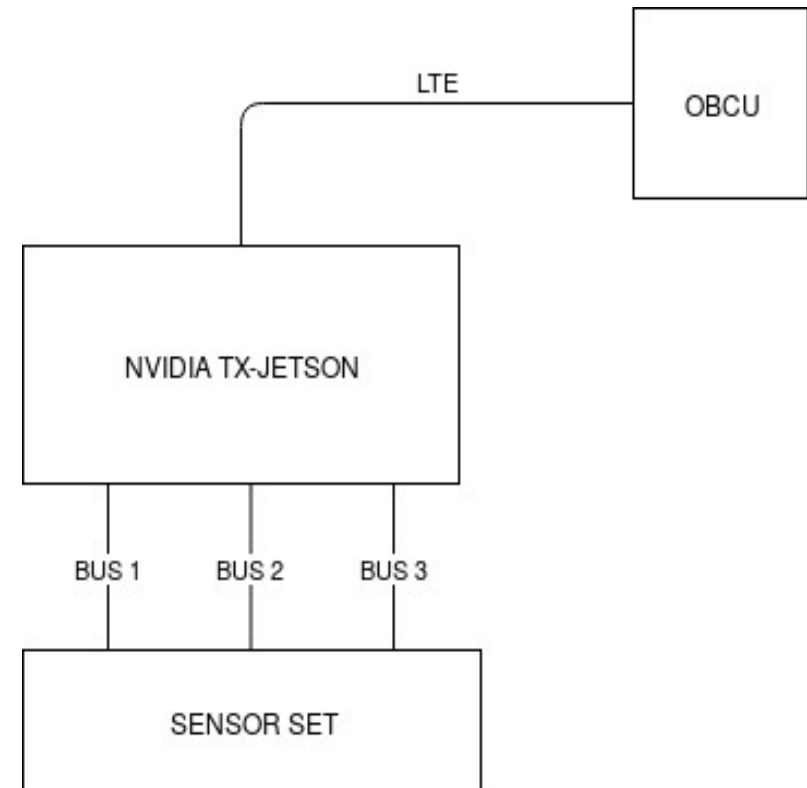
Il Sistema analizzato – Interfacce e interazioni

L'esecuzione del sistema è una continua iterazione di due distinte fasi logiche:

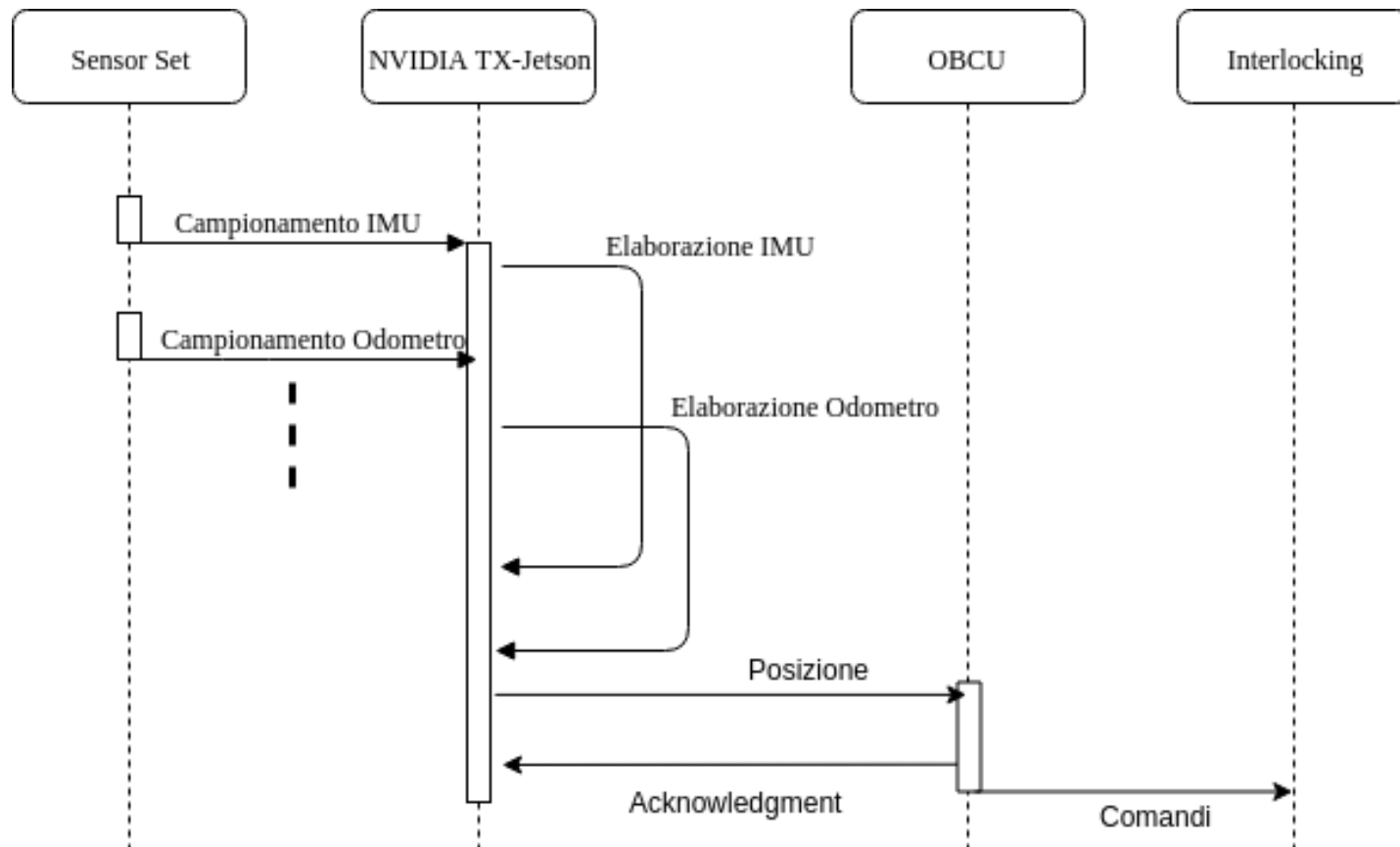
- Acquisizione delle misure;
- Stima e acquisizione della posizione del treno.

Le principali interfacce del sistema sono:

- I bus dati che collegano il Sensor Set alla piattaforma di elaborazione;
- Il collegamento LTE che collega la piattaforma di elaborazione a OBCU.



Il Sistema analizzato – Interfacce e interazioni



Indice

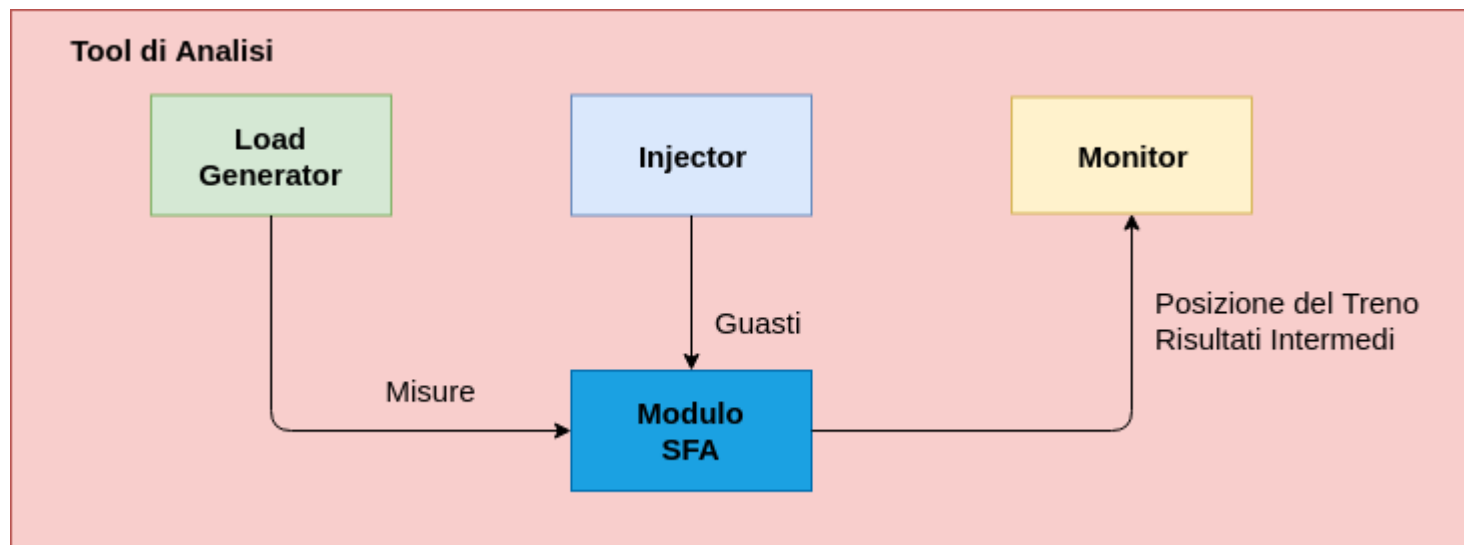
- Dependability dei Sistemi Informatici
- Stato dell'arte
- Descrizione del sistema analizzato
- **Ambiente di analisi**
- Risultati
- Conclusioni

Ambiente di Analisi

L'analisi condotta è di tipo **fault-injection**.

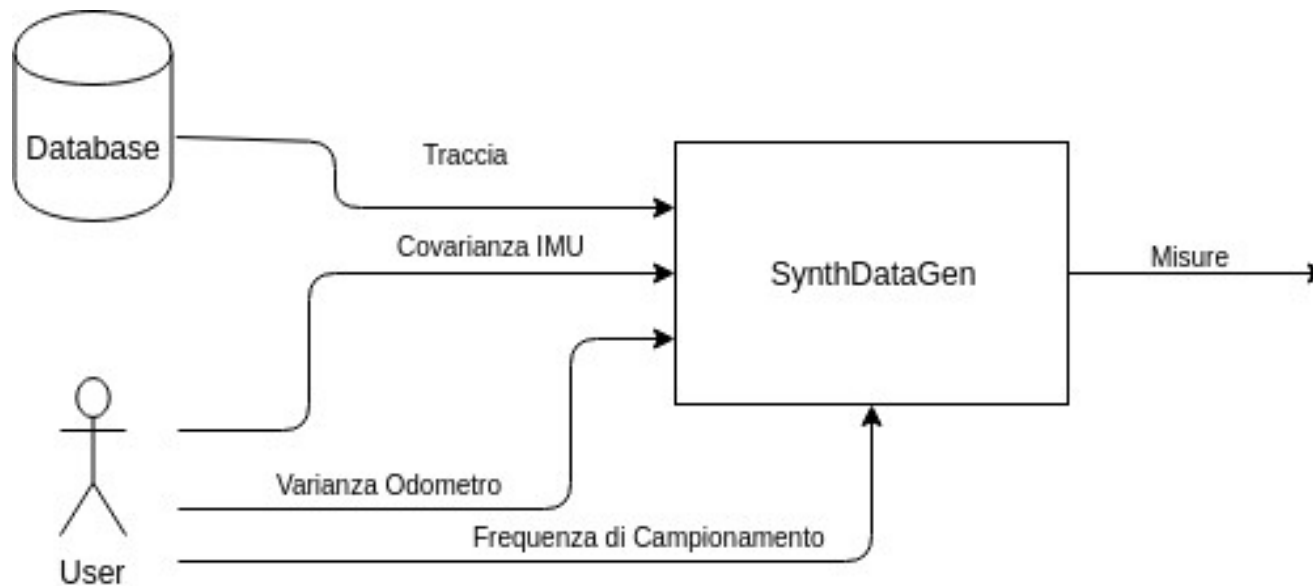
Il **target component** dell'analisi è la libreria che esegue SFA (*SensorFusionLib*).

Questa viene compilata ed inclusa all'interno di un tool appositamente sviluppato per valutare le performance di SFA, denominato *RailTrackTool* (RTT).



Ambiente di Analisi – Load Generator

RTT incorpora un **load generator** (*SynthDataGen*) in grado di **generare** le misure di IMU e odometro che verosimilmente verrebbero campionate sulla traccia reale.



Non è supportata la generazione di campionamenti GPS.

Ambiente di Analisi – Injector

Come estensione del tool originario, è stato sviluppato un Injector interno a RTT in grado di iniettare guasti all'interno del sistema.

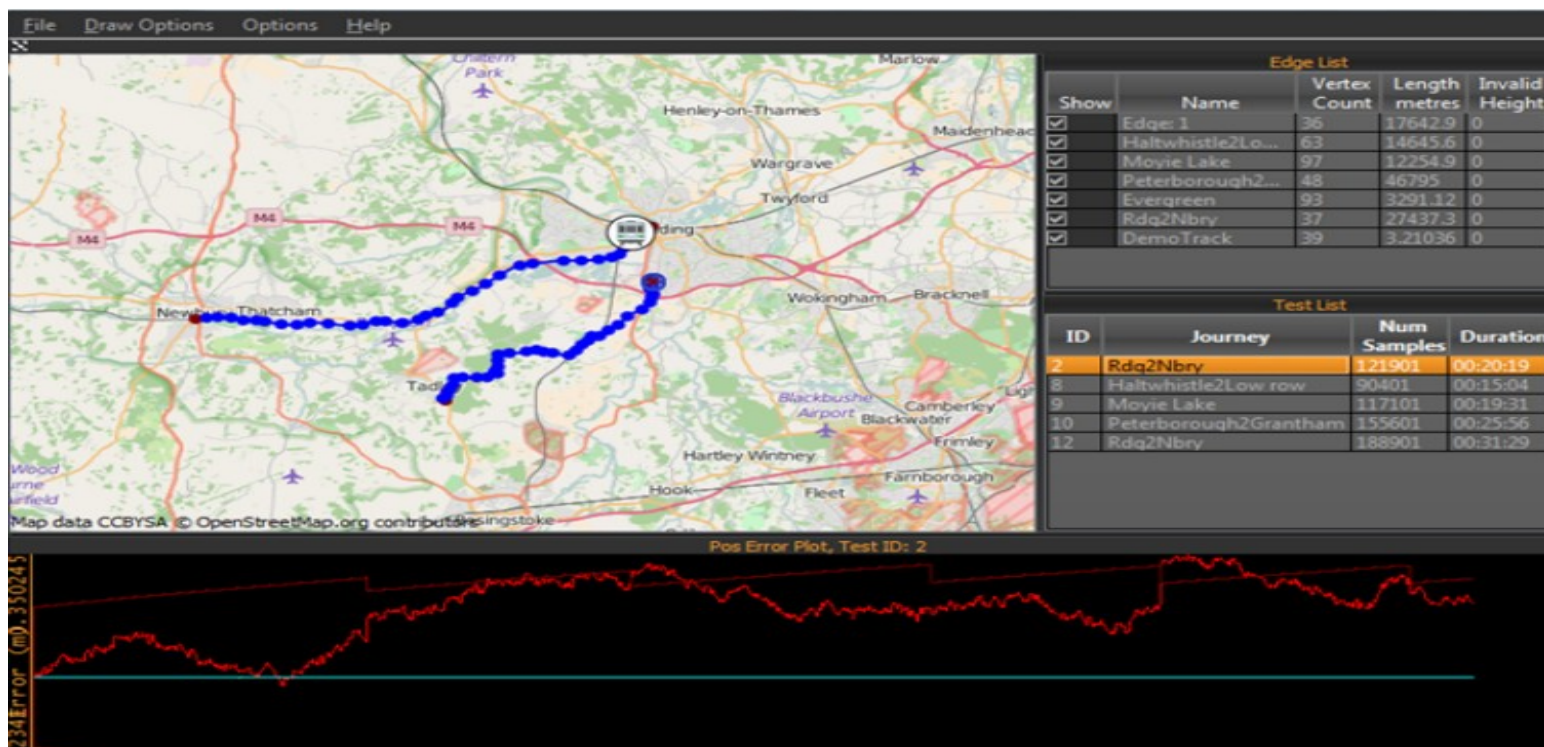
Sulla base dei requisiti del software e delle tecnologie utilizzate è stato individuato un opportuno **fault model** che l'utente è in grado di iniettare attraverso l'interfaccia di RTT.

| Tipo | Descrizione | Guasto Iniettabile | Motivazione |
|------------|--|--|---|
| Requisito | SFA deve scartare un campionamento che ha alta probabilità di non essere affidabile | Alterazione del contenuto dei messaggi provenienti dai sensori | Si vuole verificare che SFA sia in grado di riconoscere informazioni errate |
| Requisito | Un campionamento IMU scartato deve essere rimpiazzato attraverso regressione lineare, fino a un massimo di 500 campionamenti consecutivi. | Soppressione dei canali di comunicazione verso i sensori | Si vuole verificare come SFA sia in grado di tollerare una perdita di comunicazione verso i sensori |
| Tecnologia | UDP | Alterazione di contenuto e ordine dei messaggi provenienti dai sensori | UDP non garantisce integrità e ordinamento dei messaggi trasmessi |

Ambiente di Analisi – Monitor

L'interfaccia utente di RTT fornisce una mappa su cui verrà marcata la posizione del treno durante gli esperimenti.

I risultati intermedi prodotti da SFA sono mostrati su un grafico e riportati in un file di log.



Indice

- Dependability dei Sistemi Informatici
- Stato dell'arte
- Descrizione del sistema analizzato
- Ambiente di analisi
- **Risultati**
- Conclusioni

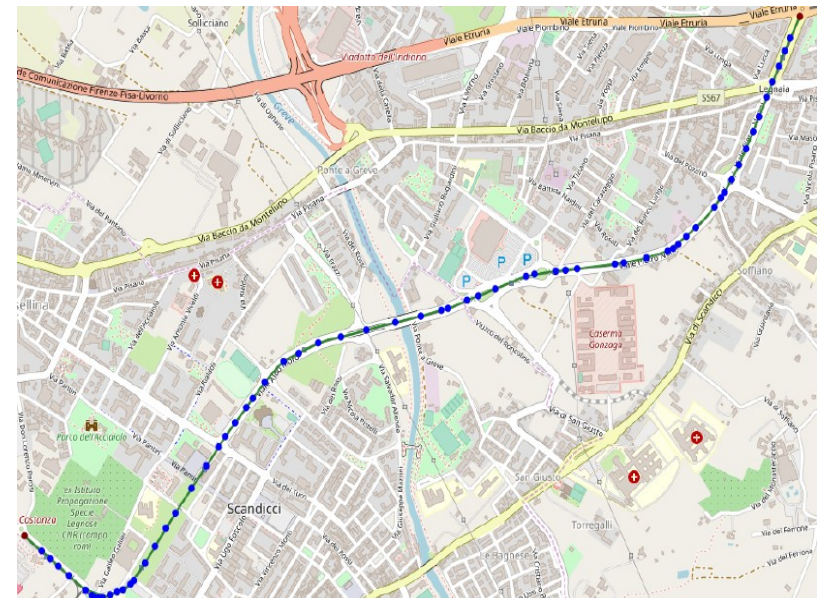
Descrizione degli esperimenti

Il codice di SFA è stato instrumentato con delle software probe atte a trasmettere verso RTT anche i risultati intermedi, oltre all'effettiva uscita dell'algoritmo.

Sono state definite le seguenti **misure di interesse**:

- Errore commesso sulla stima della velocità del treno;
- Errore commesso sulla stima della posizione del treno.

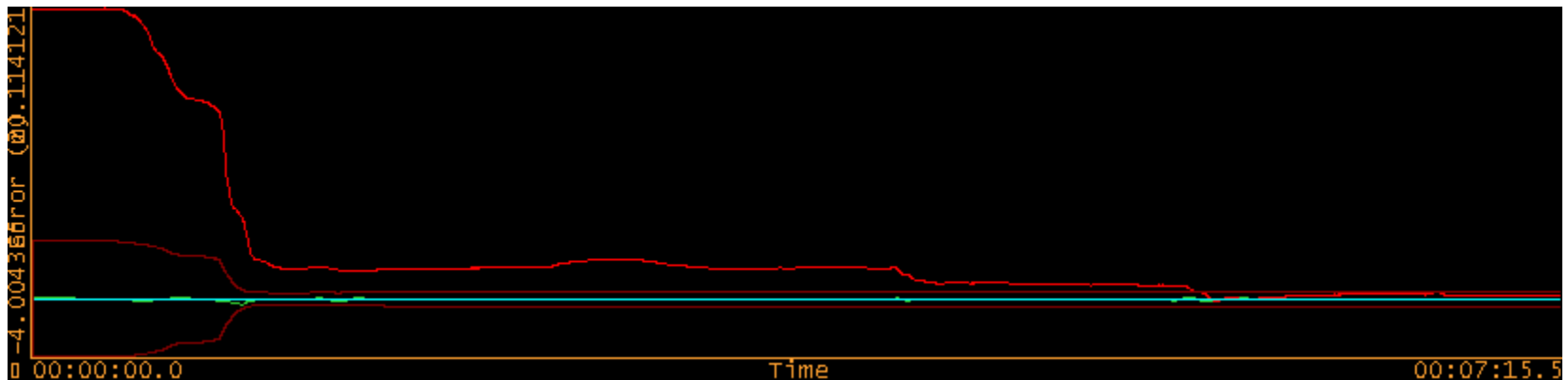
La traccia ferrotramviaria scelta per l'analisi è un sottoinsieme della linea T1 della tramvia di Firenze.



Golden Run

| Frequenza IMU | Frequenza odometro | Varianza Odometro | Iterazioni |
|---------------|--------------------|-------------------|------------|
| 100 Hz | 10 Hz | 0.0004 | 10 |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|----------------|----------------|------------------|
| ECEF X | 3.5826 m | 20.1141 m | 5.60308 m |
| ECEF Y | 0.0243133 m | 0.362813 m | 0.0452763 m |
| ECEF Z | 3.56432e-06 m | 3.19201e-06 m | 8.81543e-06 m |
| Velocità X | 0.0169528 m/s | 0.124472 m/s | 0.0199173 m/s |
| Velocità Y | 0.0394826 m/s | 0.847261 m/s | 0.0828195 m/s |
| Velocità Z | 0.00382241 m/s | 0.0192343 m/s | 0.00314704 m/s |



Risultati

Faultload: soppressione del canale di comunicazione verso odometro per tutta la durata dell'esperimento

Faultload: soppressione del canale di comunicazione verso odometro durante la prima metà dell'esperimento

Faultload: soppressione del canale di comunicazione verso odometro durante la seconda metà dell'esperimento

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|--------------|----------------|------------------|
| ECEF X | 861.883 m | 2431.1 m | 678.953 m |
| ECEF Y | 348.814 m | 1518.65 m | 499.222 m |
| ECEF Z | 0.123305 m | 0.155086 m | 0.567656 m |
| Velocità X | 8.20331 m/s | 30.782 m/s | 7.32822 m/s |
| Velocità Y | 23.4213 m/s | 75.1929 m/s | 20.0333 m/s |
| Velocità Z | 87.7399 m/s | 87.1907 m/s | 245.723 m/s |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|----------------|----------------|------------------|
| ECEF X | 4.3248 m | 20.5617 m | 5.41018 m |
| ECEF Y | 0.0226056 m | 0.39742 m | 0.04816 m |
| ECEF Z | 3.81041e-06 m | 3.30294e-05 m | 9.04865e-06 m |
| Velocità X | 0.0248871 m/s | 0.150687 m/s | 0.0260141 m/s |
| Velocità Y | 0.0475246 m/s | 0.908185 m/s | 0.0899591 m/s |
| Velocità Z | 0.00406042 m/s | 0.0228906 m/s | 0.00340827 m/s |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|----------------|----------------|------------------|
| ECEF X | 3.57373 m | 20.1609 m | 5.60304 m |
| ECEF Y | 0.0234386 m | 0.366496 m | 0.0445943 m |
| ECEF Z | 3.55578e-06 m | 3.19863e-05 m | 8.7636e-06 m |
| Velocità X | 0.0184494 m/s | 0.129497 m/s | 0.0222426 m/s |
| Velocità Y | 0.0396467 m/s | 0.863711 m/s | 0.084737 m/s |
| Velocità Z | 0.00355928 m/s | 0.0189619 m/s | 0.00306268 m/s |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|----------------|----------------|------------------|
| ECEF X | +23957.5 % | +11986.5 % | +12017.5 % |
| ECEF Y | +1.43456e+06 % | +4.18477e+05 % | +1.10251e+06 % |
| ECEF Z | +3.45933e+06 % | +1.77827e+06 % | +1.75916e+06 % |
| Velocità X | +48289.1 % | +24630.1 % | +36693.2 % |
| Velocità Y | +59220.6 % | +8774.82 % | +24089.1 % |
| Velocità Z | +2.29531e+06 % | +1.27743e+06 % | +2.77046e+06 % |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|--------------|----------------|------------------|
| ECEF X | +20.7168 % | +2.22531 % | -3.44275 % |
| ECEF Y | -7.02373 % | +9.53852 % | +6.36912 % |
| ECEF Z | +6.90426 % | +3.47524 % | +2.64559 % |
| Velocità X | +46.8023 % | +21.061 % | +30.6106 % |
| Velocità Y | +20.3685 % | +7.1907 % | +8.62068 % |
| Velocità Z | +6.2267 % | +19.0093 % | +8.30082 % |

| Misura | Errore medio | Errore massimo | Dev. std. errore |
|------------|--------------|----------------|------------------|
| ECEF X | -0.247586 % | +0.232673 % | -0.000714 % |
| ECEF Y | -3.59762 % | +1.01512 % | -1.50631 % |
| ECEF Z | -0.239597 % | +0.207393 % | -0.587946 % |
| Velocità X | +8.82804 % | +4.03705 % | +11.6748 % |
| Velocità Y | +0.415626 % | +1.94155 % | +2.31528 % |
| Velocità Z | -6.88388 % | -1.41622 % | -2.68061 % |

Altri risultati

La soppressione del canale di comunicazione tra IMU e modulo SFA ha prodotto una **interruzione del servizio**, quando protratta per un periodo di tempo **maggiore o uguale a 5 secondi**.

$$100 \text{ Hz} = 100 \frac{\text{campionamenti}}{\text{s}} \longrightarrow \frac{500 \text{ campionamenti}}{100 \frac{\text{campionamenti}}{\text{s}}} = 5 \text{ s}$$

L'alterazione di **contenuto e ordine** dei messaggi non ha portato a effetti rilevabili, a condizione che il sistema abbia maturato una **adeguata esperienza** circa il corretto comportamento dei sensori.

Indice

- Dependability dei Sistemi Informatici
- Stato dell'arte
- Descrizione del sistema analizzato
- Ambiente di analisi
- Risultati
- Conclusioni

Conclusioni

Seguono le principali conclusioni che emergono dalla campagna di fault injection.

- Il sistema è in grado di tollerare perdite di misure IMU fino a un massimo di 5 secondi, superata questa soglia il sistema si interrompe. Questa modalità di fallimento è comunque **safe**;
- Il sistema è in grado di stimare un intervallo di confidenza entro il quale i valori campionati dai sensori possono essere considerati processabili da SFA;
- Un messaggio ricevuto fuori ordine viene **scartato**, e gli effetti sulle performance di SFA dipendono dalla sorgente di misura scartata;
- L'odometro è particolarmente utile quando la traiettoria della vettura è caratterizzata da netti cambi di direzione, come ad esempio una curva stretta. Migliora inoltre la stima della velocità;
- Quando la stima della posizione non diverge, l'errore massimo rimane in modulo pari a circa 20 metri.

Si conclude che i risultati osservati sembrano promettenti nell'ottica di poter impiegare il sistema sul campo.



Grazie per l'attenzione