FORUM
CYBER 4.0

Applicazioni automotive per la localizzazione (SHINE-ON)

Alessandro NERI

7 giugno 2023

RadioLabs

drivesec

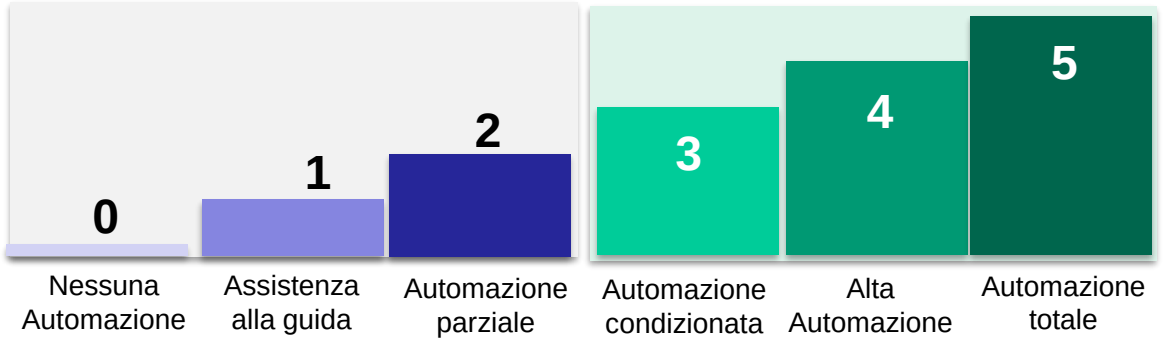
Introduzione

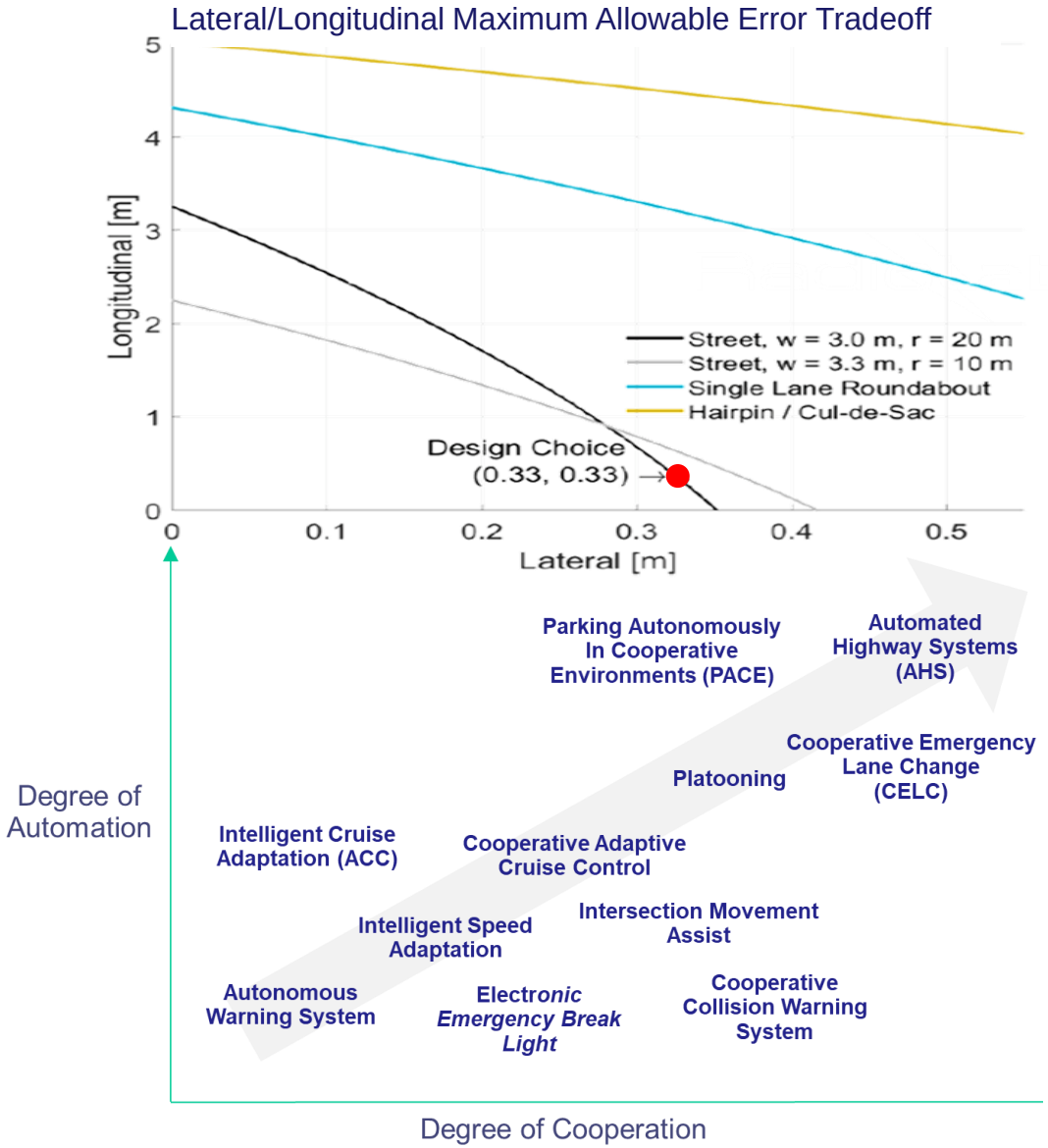
- Il posizionamento GNSS è una tecnologia fondamentale per l'automazione dei sistemi di trasporto
- Il fattore chiave di differenziazione rispetto ad altre applicazioni è l'attributo di **SAFETY**

Requisiti di base

Guidatore Umano

Sistema di guida automatico



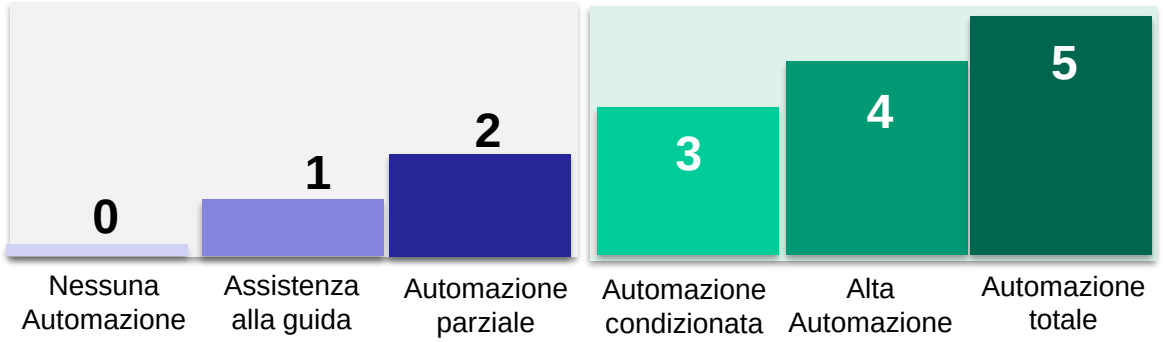


Kay Massow and Ilja Radusch, “A Rapid Prototyping Environment for Cooperative Advanced Driver Assistance Systems,” Journal of Advanced Transportation, vol. 2018, Article ID 2586520, 2018.

Requisiti di base

Guidatore Umano

Sistema di guida automatico



ORIZONTE ELETTRONICO

Veicoli e utenti della strada

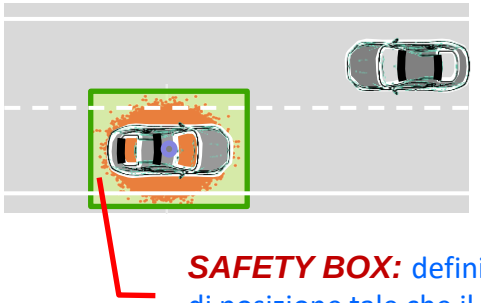
- **Posizione, velocità, accelerazione**
- Intenzioni di guida
- Traiettoria pianificata

Infrastruttura

- **Mappe digitali ad alta accuratezza**
  - Ostacoli statici
  - Lavori in corso
- **Corsie preferenziali dinamiche**
- **Segnaletica elettronica**

Da altre sorgenti

- traffico
- meteo



Il **LIVELLO DI INTEGRITÀ** specifica la PROBABILITÀ che la posizione reale non cada nella safety box e non venga dato alcun avviso tempestivo in merito.

SAFETY BOX: definisce il massimo errore di posizione tale che il veicolo possa ancora essere utilizzato in sicurezza

Alta Accuratezza Alta Integrità: come ottenerle

Per soddisfare i requisiti di accuratezza e integrità devono essere mitigati due tipi di pericoli non intenzionali:

Pericoli globali

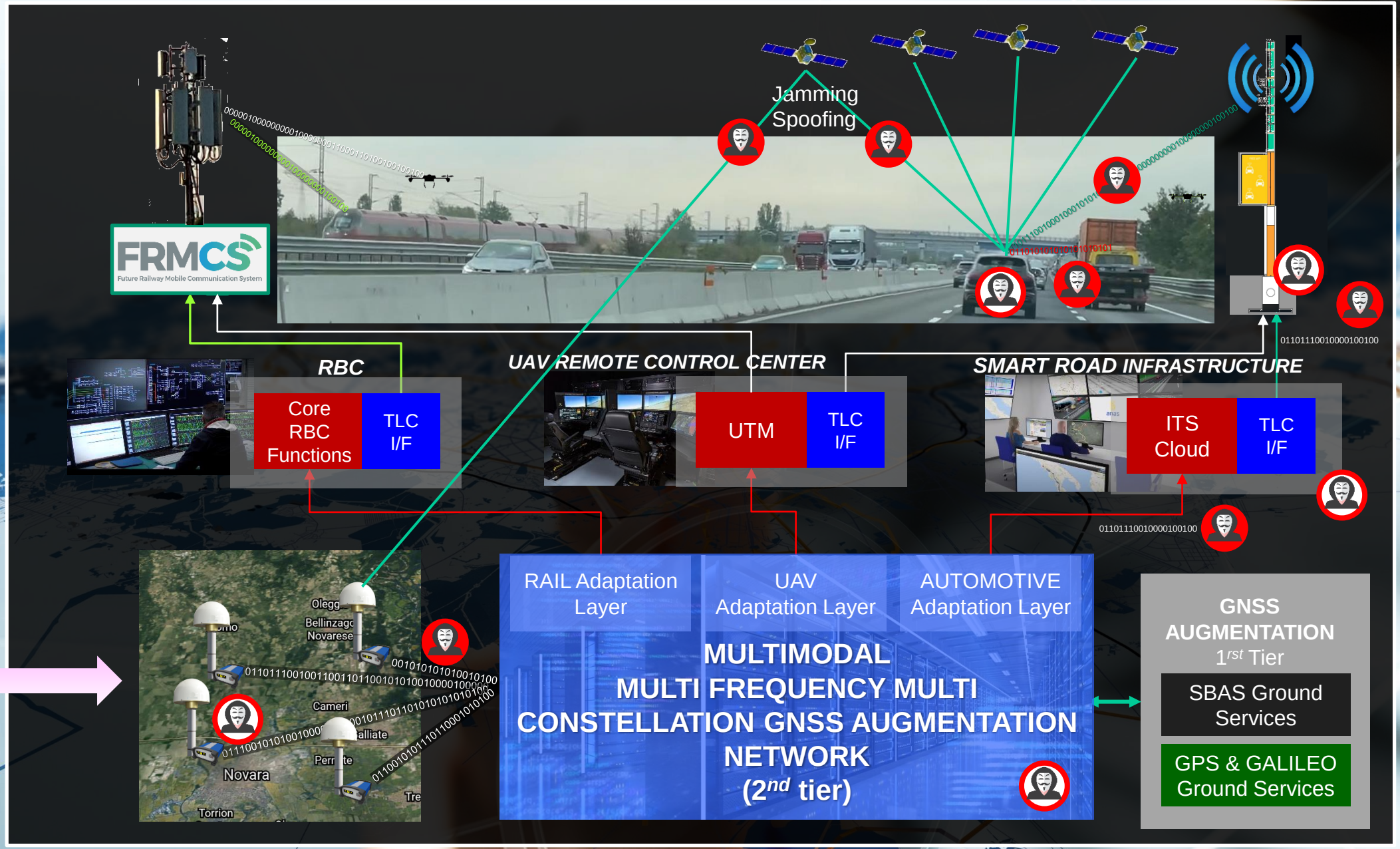
- Posizioni dei satelliti errate
- Errori degli orologi dei satelliti
- Ritardi incrementali introdotti dalla troposfera e dalla ionosfera

Pericoli locali

- Cammini multipli

Inoltre, devono essere affrontati gli **attacchi** alla **sicurezza** mirati ai segnali trasmessi dai satelliti (Signal in Space - SiS)

Mitigazione dei pericoli globali



Impiego di una rete di stazioni in posizioni note per monitorare lo stato di salute dei satelliti e stimare le correzioni

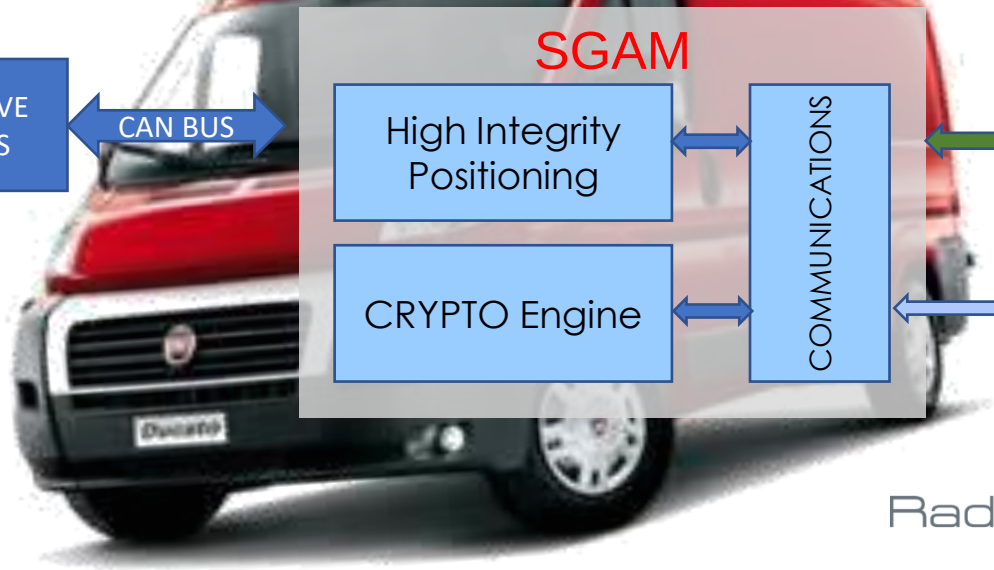
CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SHINE-ON: Secured **HI**gh accuracy localizatio**N E**quipment for automotive applicati**ON**s

ECU innovativa ad alta accuratezza e alta Integrità del posizionamento del veicolo con elevati livelli di security conformemente al nuovo standard **ISO/SAE DIS 21434**

GNSS DFMC Receiver+IMU

NVIDIA JETSON AGX ORIN 32 GB

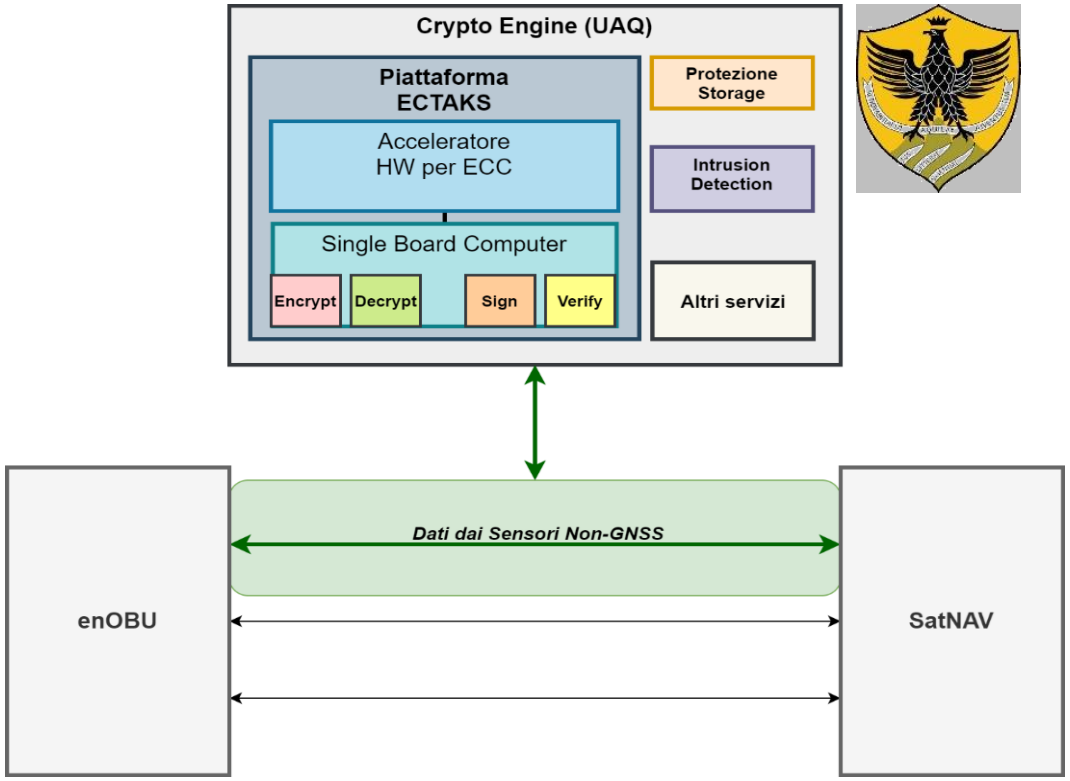


RadioLabs drivesec

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CRYPTO ENGINE

- **ECC-based Topology Authenticated Key Scheme (ECTAKS**) per i servizi di crittografia/firma digitale (schema ECDHE-like basato su curve ellittiche conformi alle direttive NIST)
- Livello di sicurezza conforme ai protocolli di sicurezza automotive (IEEE 1609.x)
- Robustezza contro gli attacchi all'integrità topologica della rete
- Generazione di segreti condivisi sulle sessioni di comunicazione con topologia arbitraria
- Scalabilità effettiva delle sessioni multicast e convergenti

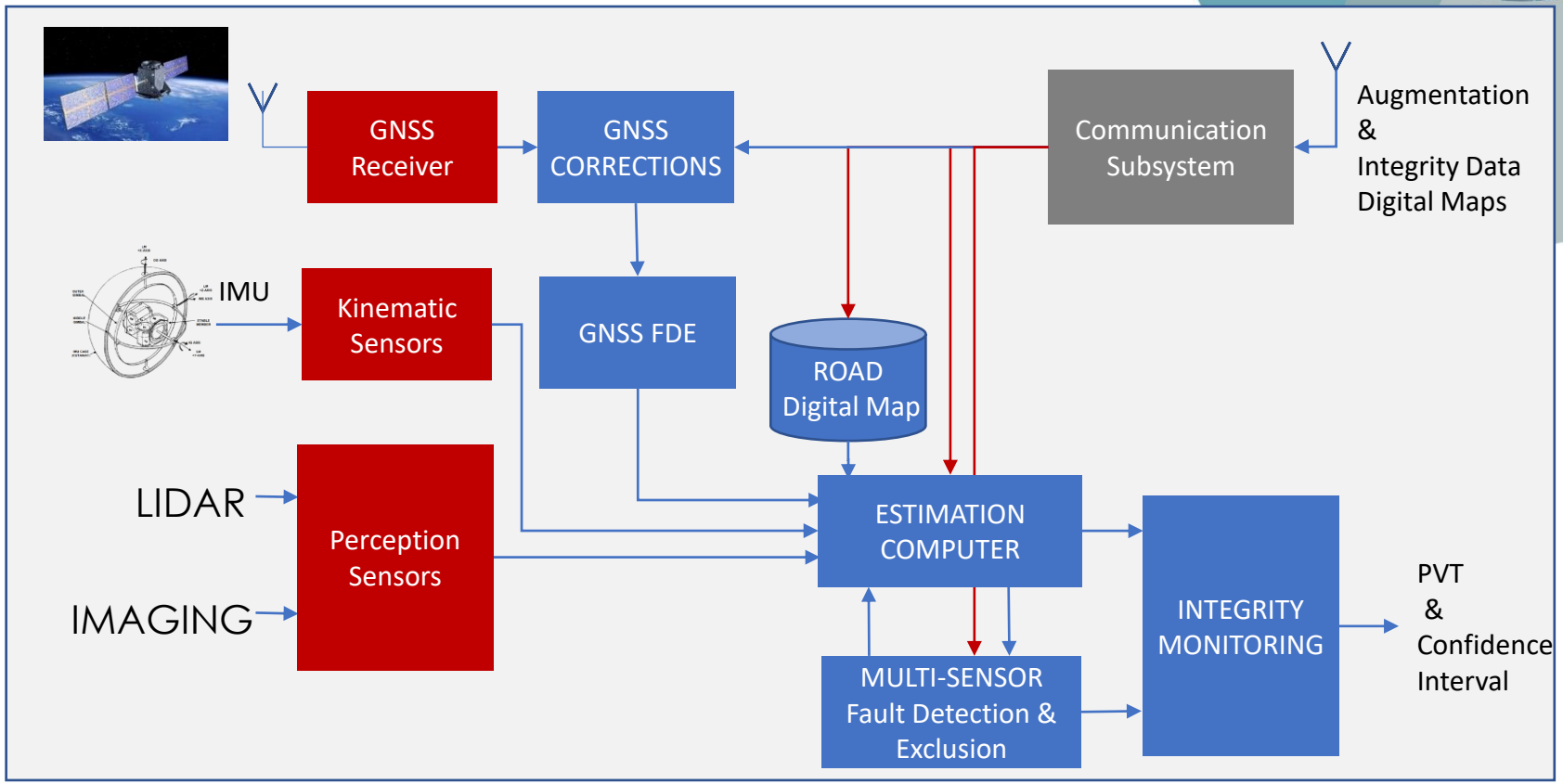


RadioLabs driveSec

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Posizionamento ad alta integrità

- Ricorso all'elaborazione congiunta dei dati forniti da più sensori (GNSS + IMU+ Odometro meccanico+ Video + Lidar + ...)
- procedura di monitoraggio dell'integrità che stima i livelli di protezione e garantisce l'integrità del sistema
- **Monitoraggio** degli attacchi ai **Segnali** ricevuti dai **Satelliti** basato sulla **coerenza** tra i dati forniti da tutti i sensori



RadioLabs drivesec

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CARATTERISTICHE

Test della centralina contro attacchi esterni tramite piattaforma di validazione IoTcy di Drivesec al fine di dimostrare l'efficacia delle misure di sicurezza implementate.

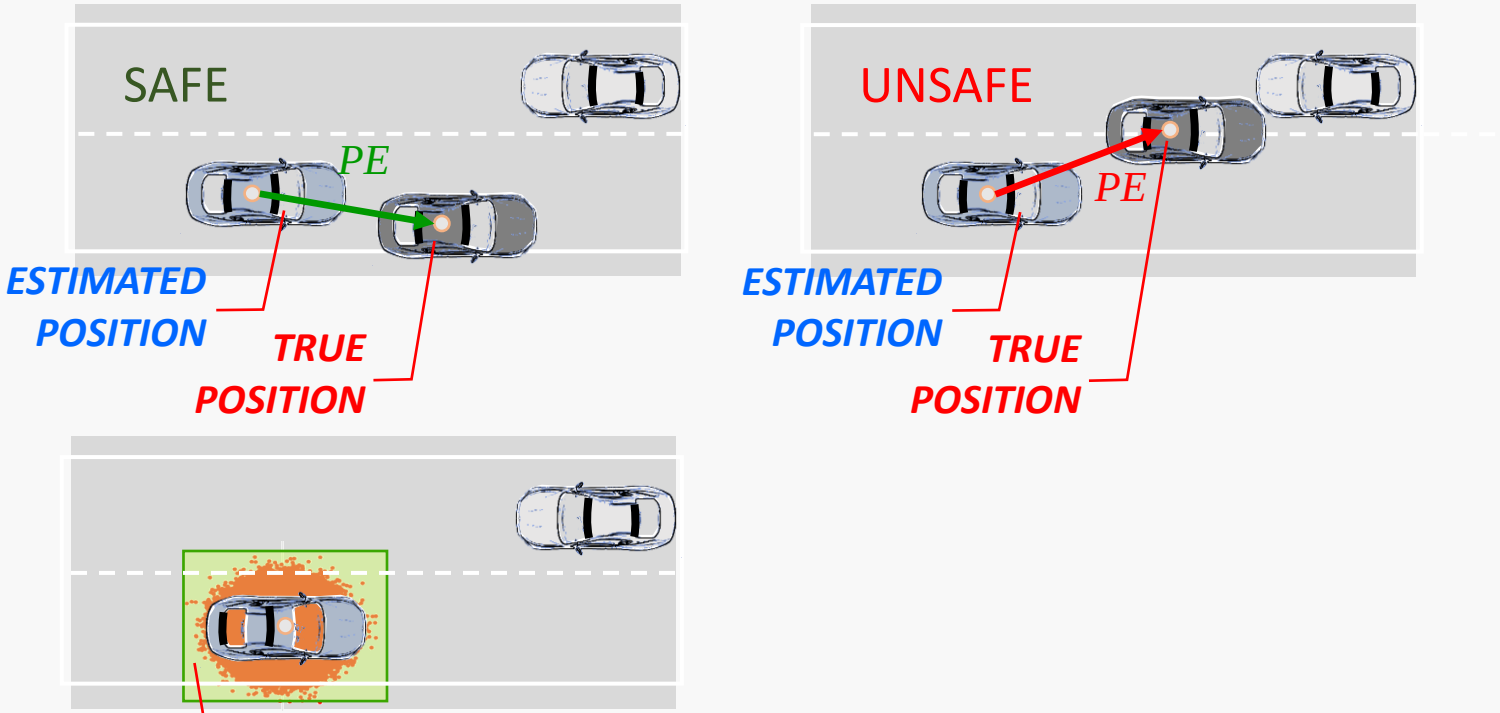
Verifica dei requisiti cyber attraverso un approccio innovativo di **Penetration Test basato su accesso remoto ai sistemi da testare** con possibilità di eseguire test in ambiente realistico, azzerando i tempi di logistica e set up.
Piattaforma IoTcy progettata per supportare i processi di certificazione.

Evoluzione SHINE-ON: Sistema in grado di produrre e rilasciare report automatici per dimostrare la compatibilità del processo di sviluppo della ECU SGAM con i requisiti dello standard ISO 21434.

RadioLabs drivesec


GRAZIE PER L’ATTENZIONE

Requisiti Safety Critical



SAFETY BOX: definisce il massimo errore di posizione tale che il veicolo possa ancora essere utilizzato in sicurezza

Il **LIVELLO DI INTEGRITÀ** specifica la PROBABILITÀ che la posizione reale non cada nella safety box e non venga dato alcun avviso tempestivo in merito.

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Secured **HI**gh accuracy localizatio**N** **E**quipment for automotive applicati**ON**s

OBIETTIVI

- Sviluppo di una **ECU** innovativa che consenta di aumentare l'accuratezza del posizionamento del veicolo garantendo elevati standard di sicurezza secondo le indicazioni del nuovo standard di ISO/SAE DIS 21434.

- Integrazione della **ECU** in un contesto Automotive reale e complesso sul nuovo veicolo Ducato Stellantis in sinergia con progetto EMERGE-Navigazione coordinato da Radiolabs.

- Test in campo della centralina contro attacchi esterni tramite piattaforma di validazione remota IoTcy di Drivesec al fine di dimostrare l'efficacia delle misure di sicurezza implementate e la possibilità di generalizzare l'architettura realizzata su larga scala

RadioLabs drivesec

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

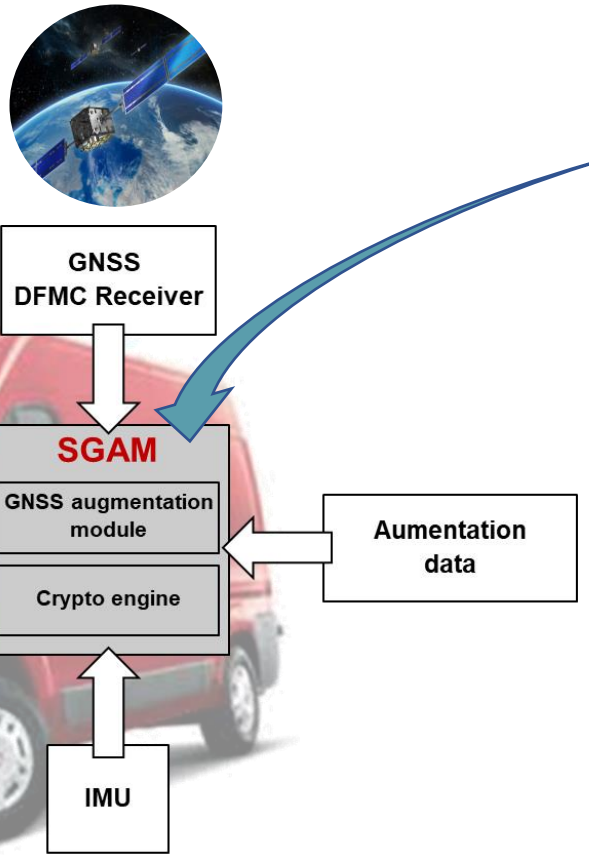
STATO DELLE ATTIVITA'

Attività Concluse:

WP1 - Processo di Cybersecurity Engineering e metodologia di validazione

In Corso:

- WP2 - Progettazione e Realizzazione della ECU SGAM



NVIDIA JETSON
AGX ORIN 32 GB

Local Aumentation Network

RadioLabs

drivesec

University of Rome Tor Vergata, University of Roma Tre, University of L'Aquila, Hitachi Rail STS S.p.A., WESTPOLE S.p.A.

Il Crypto Engine in SHINE-ON

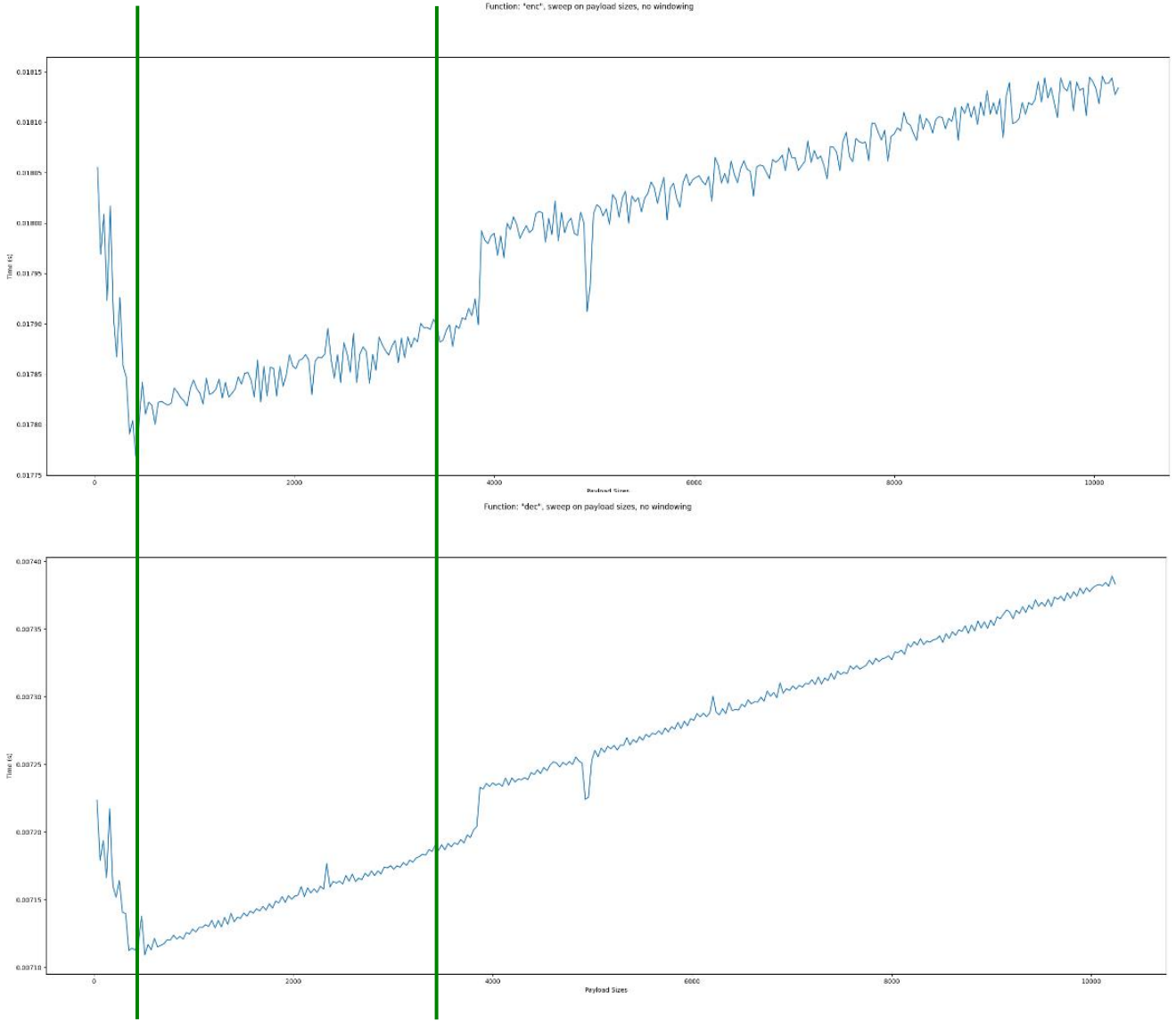
- La maturità di sviluppo del Crypto Engine è posto a **TRL5** in quanto la tecnologia è stata convalidata in un progetto automotive (progetto EMERGE) .
  - il modulo è stato sviluppato su scheda Single Board Computer (SBC) propedeutica ad una successiva fase implementativa HW ottimizzata per le esigenze di prestazione del progetto.
  - al fine di far fronte alle necessità di performance e bassa latenza, il Crypto Engine è dotato di un acceleratore HW su cui sono presenti le implementazioni HW delle operazioni di base ECC. Questo consente di incrementare sostanzialmente le performance delle operazioni crittografiche ad un minimo costo energetico.
  - Sono state effettuate delle campagne di misura dell'upper bound di prestazione in cui:
    - si sono registrate discontinuità legate ai fenomeni presenti nell'esecuzione concorrenziale di software su di un sistema operativo.
    - da un'analisi in frequenza, non si sono evidenziate evidenti correlazioni con disturbi periodici né la presenza esplicita di essi per ogni primitiva e per ogni dimensione di payload presa in considerazione.

Il Crypto Engine in SHINE-ON

- Sono definite delle regioni di comportamento ottimale in termini di ritardo di inserzione minimo per ogni primitiva attraverso l'analisi dell'andamento delle medie di ritardo di inserzione con payload "dummy" variabile da 32 a 10240 bytes senza finestramento calcolato su n. 8192 campioni di misura.
- **Primitive ENCRYPT e DECRYPT**. Per evitare problemi di cache miss, TLB miss o Page Fault, è opportuno adottare payload di dimensione **compresa tra 300 bytes e 3000 bytes**. In questa fascia, si stima che le primitive abbiano un tempo di esecuzione:
  - **Encrypt**: <0,0179 secondi (17,9ms)
  - **Decrypt**: < 0,0072 secondi (7,2 ms)
- **Primitive SIGN e VERIFY**. Queste primitive sono immuni ai fenomeni di TLB miss/Page Fault. Per questo motivo si consiglia solo di utilizzare payload con dimensione **superiore a 300 bytes**. Si può stimare un tempo di esecuzione di:
  - **Sign**: < 0,00776 secondi (7,76 ms)
  - **Verify**: <0, 01552 secondi (15,52 ms).

- **L'obiettivo della successiva implementazione HW è l'abbattimento di queste stime di almeno un ordine di grandezza con annullamento virtuale degli effetti di interferenza per concorrenza con un**

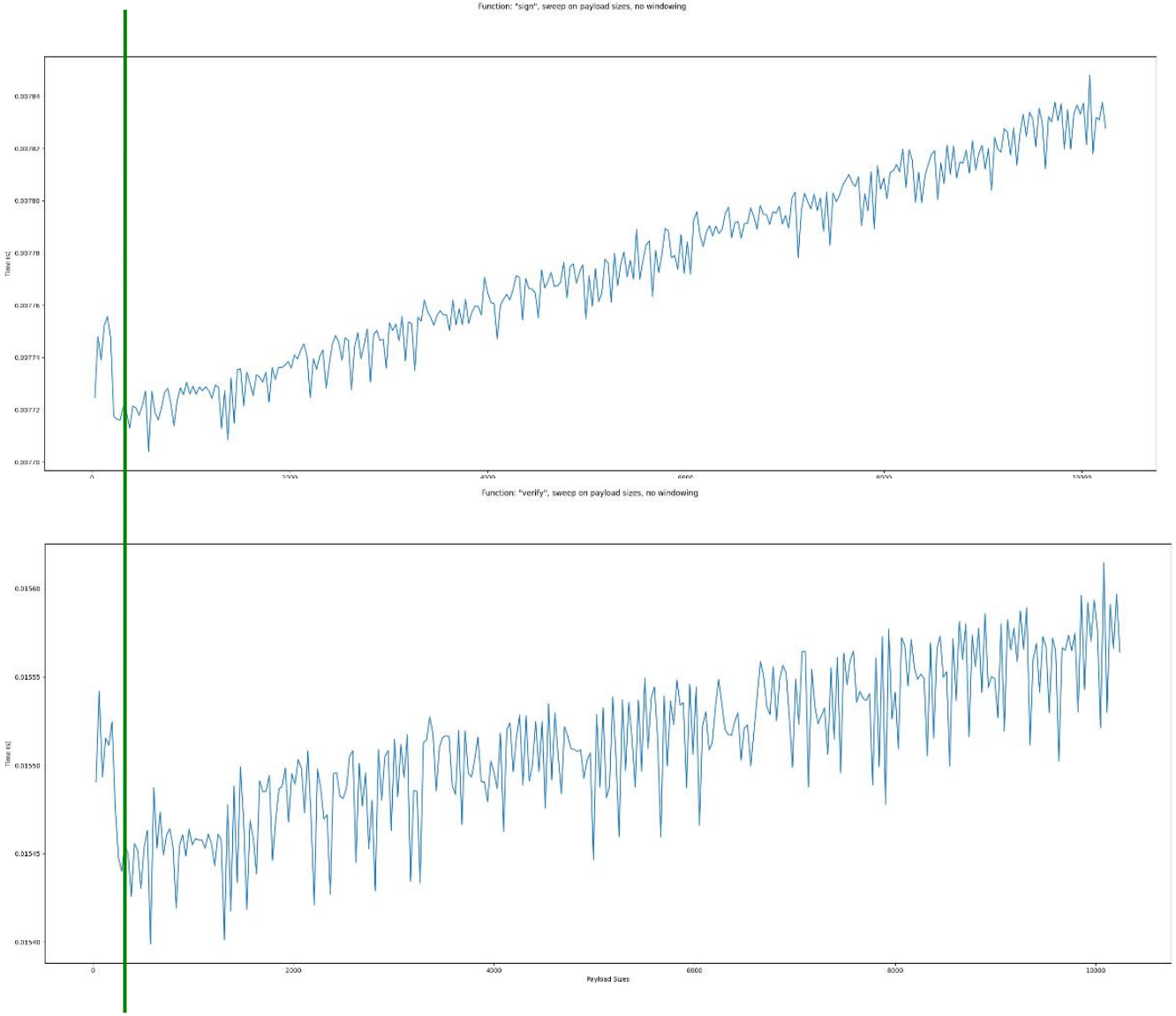
Il Crypto Engine nella ECU SGAM



ENCRYPT

DECRYPT

Il Crypto Engine nella ECU SGAM



SIGN

VERIFY

La componente ECTAKS nel Crypto Engine

- Il modulo ECTAKS (*ECC-based Topology Authenticated Key Scheme*) all'interno del modulo "Crypto Engine" offre i propri servizi di cifratura / digital signature attraverso uno schema ECDHE-compliant che utilizza curve ellittiche NIST-compliant e un apparato algebrico basato su spazi vettoriali definiti su GF(). Si avvale di componenti di chiavi private ("*Local Private Key Component*" e "*Transmitted Private Key Component*") e di chiave pubblica ("*Topology Public Key*") predistribuite sui nodi della rete secondo una topologia di sessioni di comunicazione di riferimento (autentica) impostata dal Session Manager.
- Il livello di sicurezza di ECTAKS è dimostrato essere equivalente al livello definito dal NIST a cui fanno riferimento i protocolli di sicurezza *automotive* della famiglia IEEE 1609.x: i servizi di cifratura (simmetrica) avvengono tramite algoritmo AES in modalità CCM con chiavi (ricavate tramite ECTAKS) attraverso lo schema ECIES. Per i servizi di firma a chiave pubblica viene utilizzato ECDSA con HMAC-SHA256 per la funzione di MAC e SHA256 per l'hashing del messaggio da firmare.
- I principali benefici di ECTAKS si possono riassumere in:
  - robustezza rispetto ad attacchi all'integrità topologica della rete;
  - generazione di *shared secret* su sessioni di comunicazione a topologia arbitraria;
  - scalabilità delle sessioni multicast e convergecast;
  - arbitrarietà nella scelta della *Topology Public Key* il che abilita ECTAKS anche in schemi del tipo "*Identity-based cryptography*" (IBC) dove la chiave pubblica può essere opportunamente associata ad informazioni di pubblico dominio (p.es. il numero seriale di un dispositivo o la targa di un veicolo).

Pubblicazioni selezionate

- Marchesani S., Pomante L., Pugliese M., Santucci F., *Definition and Development of a Topology-based Cryptographic Scheme for Wireless Sensor Networks*, 4th International Conference on Sensor Systems and Software (S-CUBE2013), Lucca, Jun. 2013
- Pomante L., Pugliese M., Bozzi, L. Tiberti W., Grimani D., Santucci F., *SEAMLESS Project: Development of a Permorming Secure Platform for IEEE 802.15.4 WSN Applications*, EUROMICRO Conference on Digital System Design (DSD2020), Portorož, Aug. 2020
- Tiberti W., Caruso F., Pomante L., Pugliese M., Santic M., Santucci F., *Development of an extended Topology-based Lightweight Cryptographic Scheme for IEEE 802.15.4 Wireless Sensor Networks*, International Journal of Distributed Sensor Networks, SaGe Publishing, Oct. 2020
- Civino R., Longo R., *Formal Security Proof for a Scheme on a Topological Network*, Advances in Mathematics of Communications, AIMS, vol. 15, Jan. 2021
- Aragona R., Civino R., Gavioli N., Pugliese M., *An Authenticated Key Scheme over Elliptic Curves for Topological Networks*, Journal of Discrete Mathematical Sciences and Cryptography, Taylor & Francis, May 2021.

Security Framework

drivesec

Weseth Box

- *Authenticated boot*
- *Egress/ingress local firewall based on whitelist*
- *No public IP address*
- *No exposed services*
- *User workspace separation*
- *Privilege separation*
- *Security logging and monitoring*
- *Keys security management*

Server and Web App in Cloud

- *AWS native security mechanisms*
- *Filtered Box connections relying on proxy*
- *Session monitoring and tracing*
- *Administrator interface accessed via RSA certificate*

Box to Server Comm

- *M2M Cellular connectivity though dedicated APN*
- *Reverse SSH tunneling*
- *TLS channels*
- *Event-triggered communication setup*

Sw Update Mgmt. (Box)

- *Over-The-Air update with TLS*
- *Code signing and verification*
- *Atomic updates*
- *Anti-rollback protection*

Authentication and Access Control

- *Role-based access control on resources*
- *Box and client authentication with short-lived SSH certificates*
- *Weseth users managed by AWS with 2FA*

Client to Server

- *Client authentication with short-lived SSH certificates and AWS 2FA*
- *Communication over TLS*
- *Secure file transfer via SCP*

Data and Storage

- *Role-based access to data storage*
- *Customer-defined access policies*
- *Confidentiality and Integrity of information managed by AWS native mechanisms*

Piattaforma WeSeth

- La piattaforma WeSeth è stata già installata su veicoli di diverse marche e su sistemi di simulazione

- Può essere utilizzata per numerose applicazioni, tra cui:

1. Remote Cybersecurity verification
2. Remote Design and Remote Engineering
3. Remote Monitoring in Operation

➢ Penetration Testing

L'esecuzione del PT remoto renderà il processo di test di sicurezza più efficiente e flessibile. Prima di tutto, non è necessario spedire i componenti e ricostruire i banchi di prova. Inoltre, i clienti possono controllare il processo di PT e assegnare l'attività a un esperto noto identificato dalle sue credenziali. In terzo luogo, possedere una Box in sede, riduce tempi e costi di installazione attivazione

➢ Security Requirements Validation

La remotizzazione della convalida dei requisiti di sicurezza può essere effettuata non appena il livello di maturità del sw (nelle diverse componenti) ha raggiunto un livello significativo. Quindi le funzionalità di sicurezza possono essere testate insieme a quelle non di sicurezza (test funzionali), senza attendere i PT finali. Ciò anticiperà i problemi che possono essere rilevati dal PT e ridurrà il rischio e i costi di riprogettazione (e ritardo del prodotto sul mercato)

Remote Design and Engineering

drivesec

➢ Accesso Remoto

WeSeth opera come un canale sicuro per tutte le attività di remotizzazione. Questo può rendere il lavoro di ingegneria più flessibile, e può supportare strategie di outsourcing per le attività di ingegneria. L'accesso remoto può anche ridurre il numero di banchi necessari per la progettazione del prodotto.

➢ Test funzionale remoto

Il test funzionale ha lo scopo principale di valutare la funzionalità del programma per identificare bug e conseguenti malfunzionamenti che possono verificarsi in determinate condizioni di utilizzo. WeSeth può consentire la remotizzazione di tutte le attività di test dei prodotti, riducendo anche il costo dei test e riducendo il numero di ambienti di test richiesti (es. veicoli di prova). WeSeth consente l'utilizzo di centri specializzati in test funzionali e crowd testing. La centralizzazione e in particolare il crowd testing permette di identificare bug che gli sviluppatori o chi già conosce il prodotto non può identificare.

➢ Aggiornamento remoto dei componenti

WeSeth può supportare il reflash remoto di sistema, componenti, controller e in generale qualsiasi sistema che può essere fornito con accesso remoto.
Le funzionalità di sicurezza WeSeth garantiscono un'esecuzione affidabile e tracciabile delle attività di riprogrammazione.

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Remote Monitoring in Operation

drivesec

➢ Analisi remote

Una questione chiave nel contesto del monitoraggio IoT remoto è la sicurezza, poiché grandi quantità di dati su processi e operazioni in corso vengono generate e trasmesse da sensori, attuatori e altri dispositivi interconnessi. WeSeth garantisce, prima di tutto, sicurezza di accesso ai dati.

➢ Diagnostica e riparazione da remoto

WeSeth può supportare l'attivazione remota di routine diagnostiche al fine di eseguire operazioni diagnostiche remote e supportare riparazioni remote. L'accesso al dispositivo, l'intervento e la disponibilità del tecnico sono immediati. Le operazioni di manutenzione non si limitano quindi alla giornata lavorativa, in quanto un tecnico o un team di tecnici, provenienti da un'altra parte del mondo e in un altro fuso orario, possono risolvere il problema.

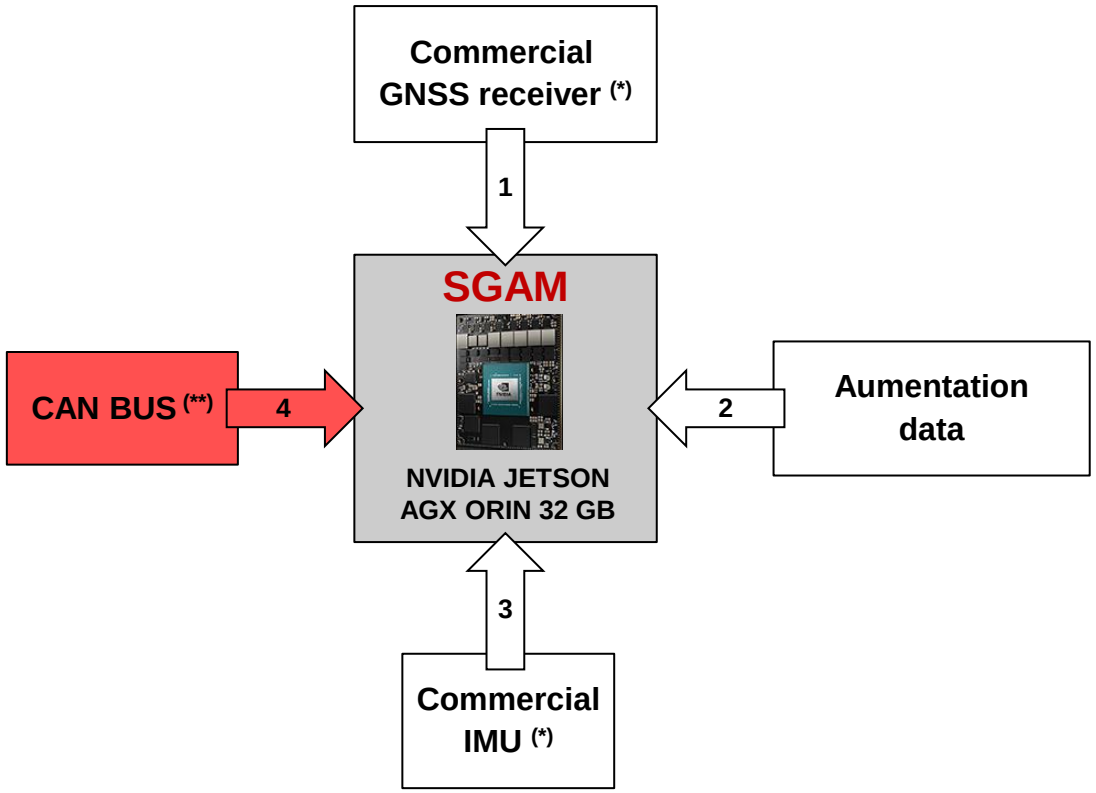
➢ Assessment continuo

Il monitoraggio continuo delle risorse, sia per motivi di sicurezza che per garantire il corretto funzionamento, può essere realizzato con WeSeth, che può supportare ingegneri e analisti anche durante le fasi operative.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

SGAM
Secured GNSS Augmentation Module

drivesec



Connection	AGX ORIN
1	USB 3.2
2	Ethernet (1-10GbE)
3	USB 3.2
4	CAN
Alimentazione (da veicolo)	15 W - 40 W

(*) Possibilità di utilizzare unico ricevitore commerciale GNSS + IMU

(**) Possibilità di testare SGAM con simulatore CAN BUS (Laboratorio P-CAR)

https://www.nvidia.com/it-it/autonomous-machines/embedded-systems/jetson-orin/

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER-SECURITY -ThReat

Level	Exposures	TYPE OF ACCESS		IMPACT POTENTIAL		
		Physical access	Wireless access	Safety	Data Privacy	Car-jacking
HIGH	OBD II port	✓		✓		
	Wi-Fi		✓	✓		
	Cellular connection (3G/4G)		✓	✓		
	Over-the-air update		✓	✓		
	Infotainment System		✓	✓		
	Smart-phone	✓		✓		
MEDIUM	Bluetooth		✓	✓		
	Remote Link Type App		✓	✓		
	KeyFobs and Immobilizers		✓			✓
	USB	✓		✓		
	ADAS System		✓	✓		
	DSRC-based receiver (V2X)		✓	✓		
LOW	DAB Radio		✓	✓		
	TPMS		✓		✓	
	GPS		✓		✓	
	eCall		✓	✓		
	EV Charging port	✓		✓		
	CD/DVD player	✓		✓		

Karahasanovic, A. ; Kleberger, P. ; Almgren, M. (2017) "Adapting Threat Modeling Methods for the Automotive Industry". ej tryckt