

Vantaggi

- Metodologia di valutazione del rischio nel GNSS che include rischi di bassa probabilità ma forte impatto
- Rilevazione, identificazione, localizzazione e analisi dell'impatto di interferenze RF avanzate od emergenti, di attacchi fisici e informatici
- Soluzioni di protezione e mitigazione che comprendano raccomandazioni per la riconfigurazione contro le interferenze RF e gli attacchi sia fisici che informatici
- Sicurezza avanzata nella trasmissione di informazioni e dati
- Aumento dell'intelligenza dell'architettura GNSS per limitare la necessità di introdurre future ridondanze nel sistema.

Partners



Contatto

Nicolas Ribière-Tharaud

Atomic Energy and Alternative Energies Commission
(Commissariat à l'Energie Atomique et aux Energies Alternatives)

Tel: +33 5 65 10 54 32

nicolas.ribiere-tharaud@cea.fr

Stephen Crabbe

Crabbe Consulting Ltd

Tel: +49 361 644 8842

stephen.crabbe@crabbe-consulting.com

www.progress-satellite.eu



La ricerca che ha condotto a questi risultati ha ricevuto un finanziamento dal Settimo Programma Quadro dell'Unione Europea (FP7/2007-2013), sotto l'accordo di sovvenzione n. 607679.

Il progetto è cominciato il 1° Maggio 2014 e ha l'obbligo di concludersi entro il 31 ottobre 2017.

v3.0 (2017)

PROGRESS

Protezione & Resistenza delle Infrastrutture di Terra dei Sistemi Spaziali Europei

www.progress-satellite.eu



Motivazione

Le tecnologie di Posizionamento, Navigazione e Sincronizzazione (PNT) basate sui Sistemi Satellitari di Navigazione Globale (GNSS) sono utilizzate in tutte le infrastrutture e settori più importanti, e questa tendenza è destinata a continuare.

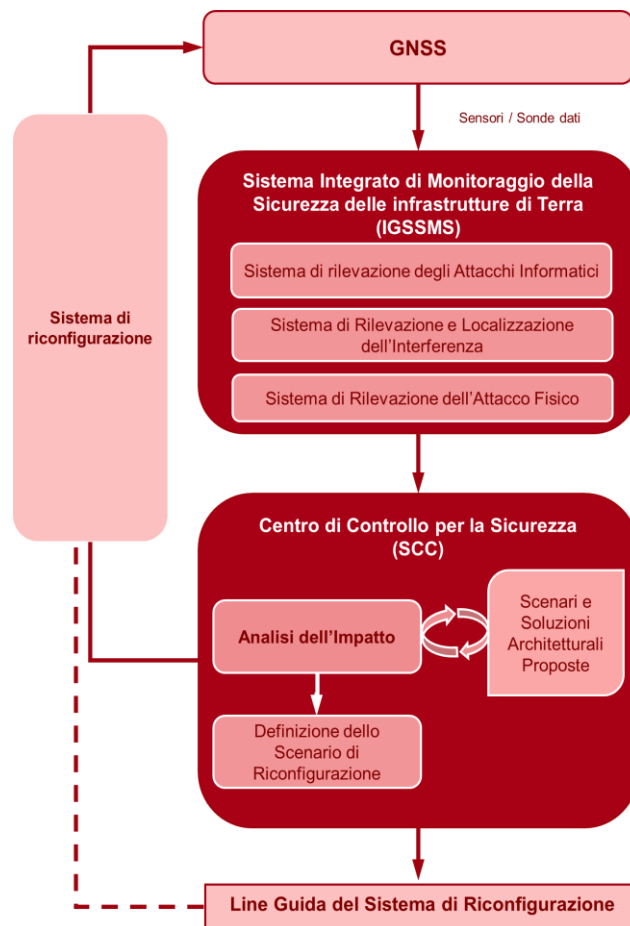
Le performance di queste tecnologie sono caratterizzate da parametri di precisione, disponibilità, continuità e integrità oltre che dalla riservatezza dei dati, sia in movimento che da fermi.

PROGRESS si focalizza sul rilevamento e mitigazione delle intrusioni nel GNSS effettuate da attaccanti esperti, il cui numero potrebbe crescere nel prossimo futuro. L'obiettivo ultimo è di incrementare l'intelligenza nelle architetture GNSS in modo tale da garantire l'ininterrotta prestazione dei servizi. Il potenziale impatto degli attacchi sarà ridotto attraverso soluzioni di protezione. Gli attacchi saranno localizzati analizzandone l'impatto e dove necessario saranno riconfigurati gli elementi del GNSS coinvolti.

Obiettivi di sviluppo

- Uno strumento di valutazione del rischio olistico
- Un Sistema Integrato di Monitoraggio della Sicurezza delle infrastrutture di Terra (IGSSMS) per le interferenze a Radio Frequenza (RF) e per gli attacchi fisici e informatici
- Soluzioni per la protezione dalle minacce e mitigazione delle stesse
- Un Centro di Controllo per la Sicurezza (SCC) per l'analisi dell'impatto delle minacce e per il suggerimento di procedure di mitigazione, comprese le procedure di riconfigurazione
- Integrazione del IGSSMS e del prototipo SCC nella Soluzione di Gestione della Sicurezza (SMS)
- Canali di Telemetria, Puntamento e Controllo (TT&C) più sicuri
- Test e valutazione del prototipo
- Aumento della conoscenza riguardo l'impatto sociale del GNSS

Prototipo sulla Gestione della Sicurezza in **PROGRESS**



Strumenti chiave

▪ Metodologia di valutazione del rischio

Una metodologia olistica che consente di valutare gli scenari di minaccia nel GNSS, includendo il potenziale impatto sulla società.

▪ Soluzione di Gestione della Sicurezza (SMS)

Soluzione centralizzata capace di rilevare automaticamente gli attacchi, di analizzare il loro impatto e di proporre azioni di mitigazione, includendo la riconfigurazione al fine di garantire la qualità globale dei servizi GNSS. Il SMS consisterà in:

➤ Un Sistema Integrato di Monitoraggio della Sicurezza delle infrastrutture di Terra (IGSSMS)

con rilevatori integrati di attacchi informatici (es. attacchi del tipo "Negazione del Servizio" (DoS)); interferenza RF (es. jamming e spoofing); e attacchi fisici (es. esplosivi e microonde ad alta potenza).

➤ Un Centro di Controllo per la Sicurezza (SCC) che

analizzi l'impatto degli eventi riportati dall' IGSSMS e che attivi le procedure di protezione e/o mitigazione, includendo raccomandazioni per la riconfigurazione del sistema.

La nostra missione:

"Migliorare la sicurezza per i cittadini ed intensificare la competitività nell'industria spaziale europea"