Avancées

- Méthodologie d'analyse de risque sur les infrastructures GNSS incluant les risques de faible probabilité dont l'impact est élevé
- Détection, identification, localisation et analyse d'impact pour des modalités d'attaques émergentes: interférences RF, attaques physiques et cyberattaques.
- Solution de protection et de réduction d'impact y compris par des recommandations de reconfiguration; pour les attaques RF, les attaques physiques et les cyberattaques.
- Techniques évoluées pour la sécurité de l'information et de la transmission des données
- Aller vers des infrastructures GNSS plus intelligentes et réduire le besoin de recourir à de nouvelles redondances

Partenaires

Contact

Nicolas Ribière-Tharaud

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

Les recherches menant aux présents résultats ont bénéficié d'un soutien financier du septième programme-cadre de l'Union européenne (7e PC/2007-2013) en vertu de la convention de subvention n° 607679.

Les travaux du projet PROGRESS ont débuté le 1er mai 2014 et seront menés jusqu'au 31 octobre 2017.

v3.0 (2017)

PROGRESS

Protection et durcissement des infrastructures au sol opérant les systèmes satellitaires européens

www.progress-satellite.eu

Contexte

Les produits Positionnement, Navigation et Temps (PNT) issus des systèmes de positionnement par satellites (GNSS), sont utilisés dans un grand nombre de secteurs d'activités et cette tendance est amenée à évoluer.

Les produits sont caractérisés par leurs performances en termes de précision, de disponibilité, de continuité, d'intégrité et de confidentialité des données et des services proposés.

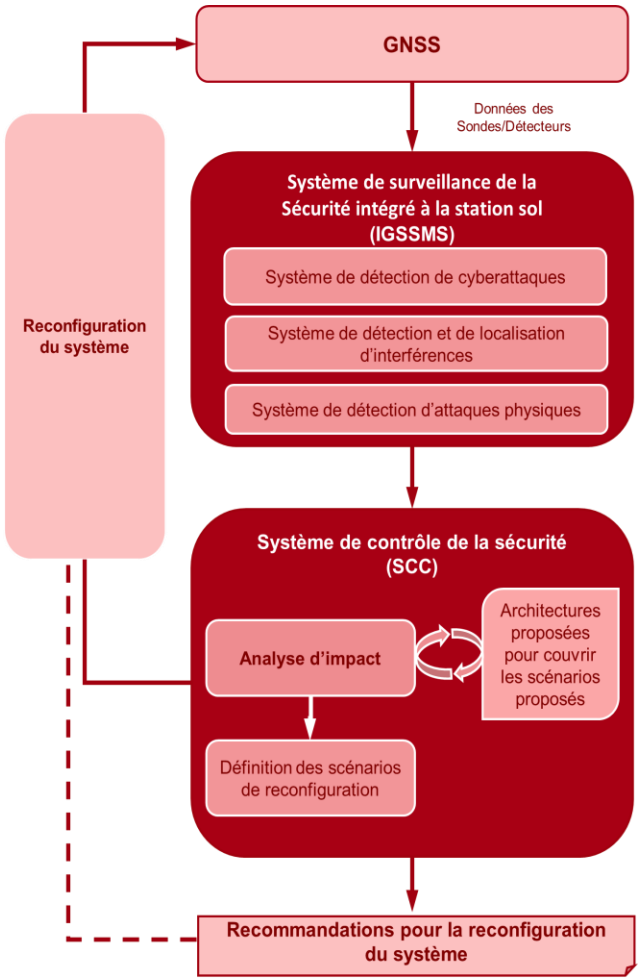
Le projet PROGRESS cible la détection et la limitation d'intrusions sur un système GNSS par des personnes malveillantes, très organisées et efficaces, dont le nombre est susceptible de croître dans le futur. L'objectif final est de produire une architecture de système GNSS intelligente permettant d'assurer la continuité des services tout en maintenant leur niveau de qualité. Les effets produits par une éventuelle attaque seront limités à l'aide de solutions de protection. Les agressions seront détectées, les impacts potentiels analysés et quand cela sera nécessaire, les éléments affectés du système à protéger seront reconfigurés.

Objectifs de développements

- Un outil d'analyse exhaustive des risques
- Un système de surveillance de la Sécurité intégré à la station sol (IGSSMS) pour des attaques de type radiofréquence (RF), physiques, et sur les réseaux informatiques
- Des solutions de protection et de durcissement face aux menaces identifiées
- Un Centre de Contrôle de la Sécurité (SCC) analysant l'impact d'une attaque et proposant des mesures de recouvrement, y compris une reconfiguration du système si nécessaire
- Une Solution de gestion de la sécurité (SMS) intégrant les modules SCC et IGSSMS
- Une protection accrue de la télémétrie et des télécommande et poursuite (liaison montante, TT&C)
- Des tests et des évaluations des performances des outils développés
- Une connaissance accrue de l'impact socio-économique des systèmes de positionnement par satellites

PROGRESS

Prototype pour la gestion de la sécurité



Outils clés

- **Méthodologie pour l'analyse de risque**

Une méthodologie exhaustive permettant l'analyse des menaces sur les systèmes GNSS en fonction des scénarios et prenant en compte l'impact socio-économique.

- **Une solution de gestion de la sécurité (SMS)**

Une solution centralisée et automatisée capable de détecter la menace, d'analyser son impact et de proposer des actions contre-mesures, allant jusqu'à une reconfiguration permettant de conserver la qualité de service du système GNSS. L'outil SMS comprendra:

- **Un système de surveillance de la sécurité intégré à la station sol (IGSSMS),** incluant des détecteurs dédiés aux cyberattaques (par exemple, aux attaques de type déni de service), aux attaques par interférences RF (brouillage et leurrage) et aux attaques physiques (explosifs, micro-ondes de fortes puissances).
- **Un centre de contrôle de la sécurité (SCC)** chargé d'analyser les impacts associés aux évènements détectés par le module IGSSMS et en mesure de déclencher des procédures de protection, de réduction d'impact, ainsi que de proposer des recommandations pour une reconfiguration de l'infrastructure.

Notre mission:

"Accroitre la sécurité des citoyens et améliorer la compétitivité de l'industrie spatiale européenne"