

EARTH OBSERVATION SYMPOSIUM (B1)
Earth Observation Data Management Systems (4)

Author: Mr. Michael Koller
European Space Agency (ESA), Germany

Mr. Max Pignède
European Space Agency (ESA), Germany

Dr. Daniel Fischer
European Space Agency (ESA), Germany

Mr. Pier Bargellini
European Space Agency (ESA), Germany

PREPARING FUTURE MISSION DATA SYSTEMS FOR SECURE SPACE COMMUNICATIONS

Abstract

Over the last years, the number of threats to a space mission's infrastructure has increased dramatically. This is mostly due to the use of open standards and the ease of access to communication hardware. As stakeholders rely on the availability of the mission products, the mission assets need to be protected from unauthorised access. To address the increased threat factor, most of today's missions specify security requirements for the communications link. ESA is implementing the space component for the Global Monitoring for Environment and Security GMES of the European Commission. The main objective of GMES is to support Europe's goals regarding sustainable development and global governance of the environment. The ESA Sentinels spacecraft constitute the first series of operational satellites responding to the Earth Observation needs of the GMES programme. In the case of the Sentinel spacecraft, the need for telecommand authentication and integrity has been a main design driver. All spacecraft are equipped with on-board authentication units which ensure that no commands from any un-authorised source are accepted by the spacecraft. The introduction of security features into the communications link has clear impacts on all elements involved in the communication with the spacecraft. The basic design approach of ESA for new missions is to apply standards as far as possible - all ESA missions are based on the Packet Utilisation Standard. It is obvious that certain considerations need to be taken in order to allow for secure communications while still in line with the underlying standard. Over the last years, ESA has followed a strict re-use concept on the side of the ground data systems, namely the Mission Control System and the Operational Simulator. The re-used generic components do not yet support secure communications and therefore need to be upgraded in this respect. In order to avoid problems with backward compatibility of software, special care has to be taken to ensure that the existing functionality implemented by the kernel remains unchanged as much as possible. This paper presents all aspects of secure telecommanding introduced by the Sentinel spacecraft. The impact on the usage of the standard is addressed first, followed by the key aspects of the secure commanding. The operational concept of the Sentinel spacecraft is presented. Finally, the paper presents the challenges faced on the side of the mission data systems and how they will be upgraded to support the secure operations.