Software Elements for Security - Partition Communication Controller

Future missions like Earth Observation, Telecommunication or any other kind are likely to be exposed to various threats aiming at exploiting vulnerabilities of the involved systems and communications. Moreover, the growing complexity of systems coupled with more ambitious types of operational scenarios imply increased security vulnerabilities in the future.

Current missions that require security are protected through their TM/TC gateways and on-board architecture is specifically designed and evaluated for security, e.g. resources are duplicated such that on-board data is physically separated into individual classification domains. As a consequence security introduces an overhead in terms of mass, volume and power for spacecraft design. A higher level of integrated software applications can reduce these penalties while incorporating the advantages of software to security functions typically implemented in hardware (ASIC or FPGA based crypto units).

The present ESA study 'Software Elements for Security – Partition Communication Controller' concentrates on higher levels of integrated software applications executing on the same computing node. Time and Space Partitioning (TSP) allows fault isolation of independent flight software applications. This increases the robustness of the system while at the same time reduces the effort of the software integration, verification and validation process. A separation Kernel is responsible for enforcing the temporal and spatial isolation of the partitions.

The Software Elements for Security - Partition Communication Controller (SPCC) has been implemented on flight representative hardware which consists of two major elements: the I/O board and the SPCC board. The SPCC board provides the interfaces with ground while the I/O node interfaces with all spacecraft equipment. Both boards are physically interconnected by a high speed spacewire (SpW) link.