**Concurrent design practices for enhanced security of space systems**

D. Wiemer*1\*; M. Merialdo2; S. Gerené3.*

*1RHEA Group, Wavre, Belgium, \*Primary author contact details:* [*d.wiemer@rheagroup.com*](mailto:d.wiemer@rheagroup.com)

*2 RHEA Group, Wavre, Belgium, \*Co-author contact details:* [*m.merialdo@rheagroup.com*](mailto:m.merialdo@rheagroup.com)

*3 RHEA Group, Wavre, Belgium, \*Co-author contact details:* [*s.gerene@rheagroup.com*](mailto:s.gerene@rheagroup.com)

1. **Introduction**

Hardly a day goes by when there isn’t a new article published about the growing concern of cyber-attacks on critical systems. Recent publications such as the “Space Security Index 2017” [1] and “Global Counterspace Capabilities: An Open Source Assessment”[2], both highlight the growing cyber-threat to space assets. Meanwhile, the reality of economic pressures for “pooling and sharing” space based capabilities and communication capacity across the European Union, creates higher levels of demand for security of commercial space operations.

In view of the growing threat, the RHEA Group, in collaboration with the European Space Agency (ESA) and the Belgium Science Policy Organization (BelSPO) have taken steps toward improving the security and resiliency of space systems. To further advance the state-of-the-art of security and resilience of space assets, the RHEA Group has entered an agreement with ESA to establish the Cyber Security Centre of Excellence (CSCE), based at the European space Security and Education Centre (ESEC) in Redu, Belgium. Sponsored by BelSPO the mission of the CSCE is to become the international enabler for security analysis of space systems and related critical infrastructures. Meanwhile, the European Space Operations Centre (ESOC) has initiated a project to enhance security requirements analysis and risk assessment of software in space systems. As part of these mandates, RHEA has initiated development of tools to support “security-by-design” for space systems which are intended to enable system security engineering as a discipline in a concurrent design process.

This paper will summarize the concepts and benefits of the Security Engineering Support Tool (SEST) and Security Aware Concurrent Design Platform (SA-CDP) projects as a domain specific tools supporting a concurrent design process applied to development of space systems and solutions. SEST is an ESOC project, developed by RHEA, to enable security requirements analysis and risk assessment in complex space systems software. Meanwhile SA-CDP expands the SEST concept to provide risk assessment support across an entire space assets system and software life-cycle..

1. **Figures**

None.

1. **Tables**

None.

1. **Equations**

None.

1. **File format and page dimensions**

Compliant.

1. **References**

[1] West, J. (Editor): Space Security Index 2017, 14th Edition, Spacesecurityindex.org, September 2017.

[2] Weeden, B. and Samson, V. (Editors): Global Counterspace Capabilities: An Open Source Assessment, Secure World Foundation, April 2018.