Cybersecurity engineering in space SW products

Author: Patricia Rodriguez Dapena – NTT Data Spain SLU.

Space-based services are more and more needed in essential services such as military, utilities, aviation and emergency communications and therefore makes them particularly attractive, especially at times of geopolitical problems, for cyberattacks, with unpredictable impacts. As one example, in February 2022, just when the Russian invasion of Ukraine started, a large number of satellite modems in Ukraine and elsewhere in Europe were subject to a cyberattack and disabled, requiring global operator Viasat to do a hard-reset following which it could continue to deliver vital communication, including to Ukrainian refugees in Slovakia [1].

Satellite engineers have long been skilled in hardware and network security and are experienced in serving sectors with strict security requirements such as governments, military, oil & gas, etc.; as well as increasingly use cybersecurity tools and products to provide enhanced security to key customers and missions. Nevertheless, there are not much guidance about how the cyber vulnerabilities are to be systematically analysed and how the satellite systems and specially its software products, while being developed and operated, are to be protected.

Understanding that the cybersecurity subject needs to tackle different matters in order to ensure all vulnerable matters to put cybersecure space systems into operations (e.g. Secure system, Secure technology, Secure infrastructure and environment, Secure operations, Secure personnel and organizations…), the focus of this presentation will only be on one part of the problem: provision of guidance for the engineering of cybersecurity while space systems and in particular SW are developed. An initial guidance is currently under development for ESA. This cybersecurity engineering approach shall aim to identify, assess, and manage risks related to the confidentiality, integrity, and availability of the targeted system/component. Various methods for cybersecurity engineering have been proposed in the literature, that focus on different phases of the system lifecycle. General approaches assess and manage the overall security risk of a system, whilst methods also exist that facilitate the analysis in a particular phase of the lifecycle such as the requirements engineering, the threat analysis, the vulnerability analysis, or the risk analysis phases. In the guidance under development an analysis of these different approaches will be performed, identifying the steps to be performed while the software product is under development, in line with current ECSS standards (including considerations of CCSDS standards, etc). The selected TARA method will be presented step-by-step.

An important aspect to include in this guidance is the harmonization between safety and security. Safety and security issues are increasingly converging on the same critical systems, leading to new situations in which these closely interdependent notions should now be considered together. The related requirements, technical and organizational measures can have various interactions and side-effects ranging from mutual reinforcements to complete antagonisms. These interdependencies are analysed to ensure a controlled level of risk for the systems concerned by such a convergence. For example, three types of such dependencies have been identified [2]:

1. Conditional dependencies: Safe operations may be conditioned by cybersecurity, for example, malicious modifications of sensor data or control programs may prevent safety systems from protecting an installation in accidental conditions. Conversely, safety may be a condition for cybersecurity, for example, when unmanaged catastrophic conditions weaken the security posture of a system or an organization, and lead to opportunistic malicious acts.

2. Reinforcement: Safety and cybersecurity measures can be complementary, for example, event and activity logging may be used both for attack detection and accident anticipation, as well as post-event analysis.

3. Conflict: If safety and cybersecurity are considered separately for the same system, it is possible that conflicting requirements or measures may be identified, for example, a safety requirement for an automatic door shutting system, would be to leave the door open, whereas a security requirement would be lo leave the door locked in case of failure.

This paper will present how to engineer cybersecurity while space software is being developed.

[1] Russia hacked Ukrainian satellite communications, officials believe. BBC. 25 March 2022. bbc.com
[2] Future Internet | Free Full-Text | Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey (mdpi.com)