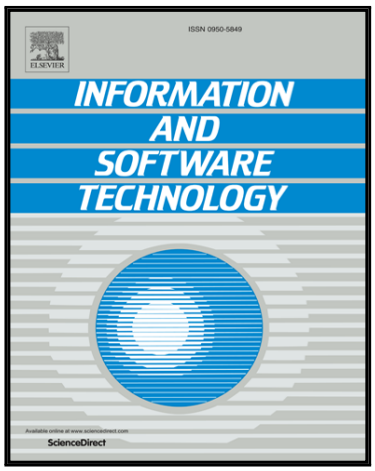

An Architecture, System Engineering, and Acquisition Approach for Space System Software Resiliency

Dewanne M. Phillips , Thomas A. Mazzuchi , Shahram Sarkani

PII: S0950-5849(17)30057-5
DOI: 10.1016/j.infsof.2017.10.006
Reference: INFSOF 5893

To appear in: *Information and Software Technology*

Received date: 17 January 2017
Revised date: 4 October 2017
Accepted date: 8 October 2017

Please cite this article as: Dewanne M. Phillips , Thomas A. Mazzuchi , Shahram Sarkani , An Architecture, System Engineering, and Acquisition Approach for Space System Software Resiliency, *Information and Software Technology* (2017), doi: 10.1016/j.infsof.2017.10.006

An Architecture, System Engineering, and Acquisition Approach for Space System Software Resiliency

Dewanne M. Phillips (PhD Candidate), Dr. Thomas A. Mazzuchi, and Dr. Shahram Sarkani

School of Engineering & Applied Science (Engineering Management and Systems Engineering), George Washington University, Washington, DC 20052

ABSTRACT

Context: Software-intensive space systems can harbor defects and vulnerabilities that may enable external adversaries or malicious insiders to disrupt or disable system functions, risking mission compromise or loss. Mitigating this risk demands a sustained focus on the security and resiliency of the system architecture including software, hardware, and other components.

Objective: In this paper we offer methodical approaches for improving space system resiliency through software architecture design, system engineering, and increased software security, thereby reducing the risk of latent software defects and vulnerabilities.

Method: We conducted a systematic review of existing architectural practices, standards, security and coding practices, various threats, defects, and vulnerabilities that impact space systems from hundreds of relevant publications and interviews of subject matter experts. We expanded on the system-level body of knowledge for resiliency and identified a new software architecture framework and acquisition methodology to improve the resiliency of space systems from a software perspective with an emphasis on the early phases of the systems engineering life cycle. This methodology involves seven steps: 1) Define technical resiliency requirements, 1a) Identify standards/policy for software resiliency, 2) Develop a request for proposal (RFP)/statement of work (SOW) for resilient space systems software, 3) Define software resiliency goals for space systems, 4) Establish software resiliency quality attributes, 5) Perform architectural tradeoffs and identify risks, 6) Conduct architecture assessments as part of the procurement process, and 7) Ascertain space system software architecture resiliency metrics.

Results: Data illustrates that software vulnerabilities can lead to opportunities for malicious cyber activities, which could degrade the space mission capability for its user community. Reducing the number of vulnerabilities by improving architecture and software system engineering practices can contribute to making space systems more resilient.

Conclusion: Since cyber-attacks [1] are enabled by shortfalls in software, robust software engineering practices and an architectural design are foundational to resiliency, which is a quality that allows the system to "take a hit to a critical component and recover in a known, bounded, and generally acceptable period of time" [2]. To achieve software resiliency for space systems, acquirers and suppliers must identify relevant factors and systems engineering practices to apply across the life cycle, in software requirements analysis, architecture development, design, implementation, verification and validation, and maintenance phases.

Keywords: Software, Architecture, Resiliency, Systems Engineering, Life Cycle, Vulnerabilities, Threats, Cybersecurity