

Accepted Manuscript

A Methodology for Secure Recovery of Spacecrafts based on a Trusted Hardware Platform

Marcio Juliato, Catherine Gebotys

PII: S0273-1177(16)30640-8
DOI: <http://dx.doi.org/10.1016/j.asr.2016.11.014>
Reference: JASR 12971

To appear in: *Advances in Space Research*

Received Date: 3 March 2016
Accepted Date: 9 November 2016



Please cite this article as: Juliato, M., Gebotys, C., A Methodology for Secure Recovery of Spacecrafts based on a Trusted Hardware Platform, *Advances in Space Research* (2016), doi: <http://dx.doi.org/10.1016/j.asr.2016.11.014>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

A Methodology for Secure Recovery of Spacecrafts based on a Trusted Hardware Platform

Marcio Juliato*

*Dept. of Electrical and Computer Engineering, University of Waterloo
200 University Avenue West, Waterloo, ON, Canada, N2N3G1*

Catherine Gebotys

*Dept. of Electrical and Computer Engineering, University of Waterloo
200 University Avenue West, Waterloo, ON, Canada, N2N3G1*

Abstract

This paper proposes a methodology for the secure recovery of spacecrafts and the recovery of its cryptographic capabilities in emergency scenarios recurring from major unintentional failures and malicious attacks. The proposed approach employs trusted modules to achieve higher reliability and security levels in space missions due to the presence of integrity check capabilities as well as secure recovery mechanisms. Additionally, several recovery protocols are thoroughly discussed and analyzed against a wide variety of attacks. Exhaustive search attacks are shown in a wide variety of contexts and are shown to be infeasible and totally independent of the computational power of attackers. Experimental results have shown that the proposed methodology allows for the fast and secure recovery of spacecrafts, demanding minimum implementation area, power consumption and bandwidth.

Keywords: Fault Tolerance; FPGA Implementation; Space Systems Security; Platform Recovery; Trusted Platform.

*Corresponding author

Email addresses: mrjuliato@uwaterloo.ca (Marcio Juliato),
cgebotys@uwaterloo.ca (Catherine Gebotys)

Download English Version:

<https://daneshyari.com/en/article/5486289>

Download Persian Version:

<https://daneshyari.com/article/5486289>

[Daneshyari.com](https://daneshyari.com)