FUNCTIONAL SAFETY AND RELIABILITY OF TUMnanoSAT SATELLITE ON-BOARD COMPUTER SOFTWARE

Alexei MARTINIUC, Nicolae SECRIERU

National Space Technologies Center, *Technical University of Moldova, 9/7 Studentilor str.,*
Chișinău, Republic of Moldova

*Corresponding author: *alexei.martiniuc@cnts.utm.md*

The TUM National Space Technologies Center team was selected by the Japan Aerospace Agency (JAXA) and the United Nations Office for Outer Space Affairs (UNOOSA) for the fourth round of the KiboCUBE Program for the launch of the TUMnanoSAT nanosatellite from the International Space Station (ISS) in 2020, with the help of the japanese experimental KiboCUBE module. The National Space Technologies Center of TUM projected the family of TUMnanoSAT's nanosatellites, according to the international CubeSat standard. In the 2019 year, NCST participated in the fourth round of the KiboCUBE Program with the nanosatellite project from the "TUMnanoSAT" family. The harsh space environment with high levels of radiation and large temperature variations (even on low earth orbits) imposes the implementation of measures and techniques to achieve high level of satellite systems reliability over its full lifetime. The on-board computer and its software play a key role in this regard.

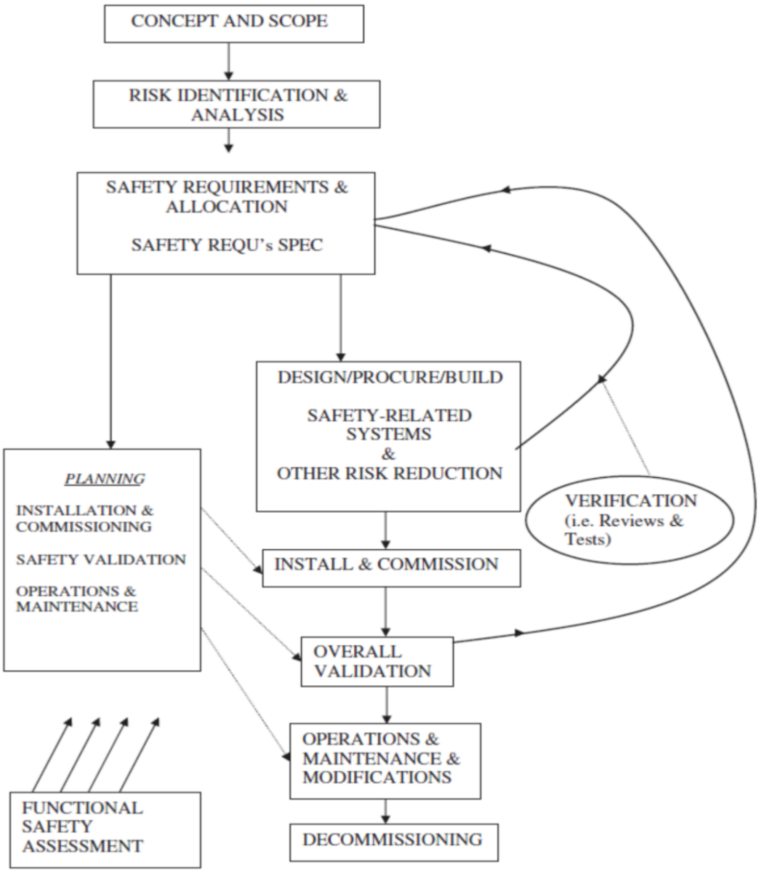
CONCEPT AND SCOPE
RISK IDENTIFICATION & ANALYSIS
SAFETY REQUIREMENTS & ALLOCATION
SAFETY REQU's SPEC
DESIGN/PROCURE/BUILD
SAFETY-RELATED SYSTEMS & OTHER RISK REDUCTION
PLANNING
INSTALLATION & COMMISSIONING
SAFETY VALIDATION
OPERATIONS & MAINTENANCE
VERIFICATION (i.e. Reviews & Tests)
INSTALL & COMMISSION
OVERALL VALIDATION
OPERATIONS & MAINTENANCE & MODIFICATIONS
FUNCTIONAL SAFETY ASSESSMENT
DECOMMISSIONING

Figure 1: Schema of safety and reliability of nanosatellite software computer.

This article describes approaches and methods used for failure risk evaluation for TUMnanoSAT nanosatellite on-board computer software. These methodologies are mainly based on IEC 31508-3 and DO-178C standards and MISRA coding rules, and aim to ensure a high level of software reliability. To achieve this goal, the measures and techniques developed are applied on all stages of software design, development and testing, starting from identification and evaluation of possible risks and vulnerabilities in whole system and ending with performance and reliability evaluation during testing. Noteworthy is the fact that the functional safety measures taken in software development process are not intended to prevent human injuries or material losses. Their goal is to ensure functional reliability of the satellite systems, including on-board computer, as in case of unrecoverable fault only the satellite will be affected.

Due to the fact that IEC 61508 is a generic functional safety standard, it is agnostic to implementation field, but imposes some requirements on particular system components such as software, described in part 3 of this standard. The DO-178C standard and MISRA coding rules are more specific and focuses on safety related software development: the first focuses on aerospace applications software development safety requirements and the second focuses on mandatory coding styles in safety-critical development of software that requires high reliability. Another important feature discussed in this article is implementation of enhanced reliability and safety techniques and approaches in software development in context of multitasking system with embedded RTOS (Real-Time Operating System)

Keywords: *nanosatellite, software, RTOS task, functional safety, nanosatellite, reliability, cosmic radiation, digital electronic memory.*

References

1. Dr David J Smith, Kenneth GL Simpson, “*The Safety Critical Systems Handbook. A Straightforward Guide To Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2016 Edition) & Related Guidance*” 4th edition, Butterworth-Heinemann, 2016;
2. Leanna Rierson, “Developing safety-critical software. A practical guide for aviation software and DO-178C”, CRC Press, 2013.
3. J. Bouwmeester, J. Guo, Survey of worldwide pico- and nanosatellite missions, distributions and subsystem technology. - Acta Astronautica 67 (2010) 854–862 pp.
4. Bostan, Ion; Secrieru, Nicolae; Ilco, Valentin; Levineţ, Nicolae; Bostan, Viorel; Candraman, Sergiu; Gîrşcan, Adrian; Margarint, Andrei. *”Educational space missions of TUMnanoSat family”* - . In: *Telecommunications, Electronics and Informatics*. *24-27 mai 2018*, Chişinău. Tehnica UTM, 2018, pp. 295-302. ISBN 978-9975-45-540-4.
5. The United Nations/Japan Cooperation Programme on CubeSat Deployment from the International Space Station (ISS) Japanese Experiment Module (Kibo) "KiboCUBE"
   – In: http://www.unoosa.org/oosa/en/ourwork/psa/hsti/kibocube_2017.html
6. CubeSat Design Specification (CDS) Rev. 13. The CubeSat Program, Cal Poly SLO, 2013. – In: http://cubesat.org