fortiss

esa

ESA STUDY CONTRACT REPORT

ESA CONTRACT No **4000117995/16/NL/ HK/as**	SUBJECT **Executive Summary Report**		CONTRACTOR **fortiss GmbH, Guerickestraße 25, 80805 Munich, Germany**
ESA CR( )No	STAR CODE:	No of volumes This is Volume No	CONTRACTOR'S REFERENCE

ABSTRACT:

In this document, we summarize the work done to analyse state of art in safety certification for GNC space systems, asses the gap in certification practices with other domains and draft a new methodology aimed at filling the gaps assessed. The draft methodology is further strengthened by forwarding technology recommendations that can be used in implementing the draft methodology.

The work described in this report was done under ESA contract. Responsibly for the contents resides in the author or organisation that prepared it.

Names of the authors: **Chih-Hong Cheng**
Tewodros A. Beyene

ESA STUDY MANAGER: Dr. Guillermo Ortega (TEC-SAG) GNC, AOCS and Pointing Systems (TEC-SA) DIRECTORATE OF TECHNOLOGY, ENGINEERING AND QUALITY (D/TEC)	ESA BUDGET HEADING:

fortiss

fortiss GmbH
Guerickestraße 25
80805 München
Deutschland

Tel: +49 89 3603522 0
Fax: +49 89 3603522 50
www.fortiss.org

Assessment of Methodologies for the Certification of Safety-Critical GNC Space Systems

Executive Summary Report

Prepared by fortiss GmbH

Contributors Tewodros A. Beyene
Chih-Hong Cheng

Editor Tewodros A. Beyene

Reference AMC-GNC-ESR1.0
Issue 1
Revision 0
Date of Issue 18/04/2017
Status Draft
Document Type Executive Summary Report (ESR)
Distribution TEC-ECN, fortiss GmbH

Approval

Title Executive Summary Report	
Issue 1	**Revision** 0
Author fortiss GmbH	**Date** 18/04/2017
Approved by	**Date**
Harald Ruess (fortiss GmbH)	
G. Ortega (HoS/TEC-ECN)	

Change Log

Reason for change	Issue	Revision	Date
Creation of document	1	0	18/04/2017

Change Record

Issue 1	Revision 1		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
Creation of document	18/04/2017		

Foreword

This executive summary report document is one of the series of documents to be delivered as part the AMC-GNC project. The project is aimed at investigating and assessing methods for the certification of the design and development of Guidance, Navigation, and Control (GNC) systems for autonomous space missions.

The general objectives of the project are:

- To improve the certification processes (verification, validation, and assurance activities) of safety GNC critical space systems with the goal to reduce the cost, manpower and time for certification.
- To perform research on alternative approaches to reliability and certification to the current practices.

The project is also focused on the technical assessment of the current technology in space, automotive and civil airplane industries with the aim of drafting a new methodology for certifying safety-critical GNC space systems.

The AMC-GNC project is a collaboration effort between the European Space Agency (ESA) and fortiss GmbH.

Executive Summary

The project is aimed at drafting a methodology for certifying safety-critical GNC space systems. This is done by first analyzing the state of art in safety-certification for GNC (and related) systems in the civil aviation, automotive and space domains, and assessing the gap among the safety certification process in these domains. The draft methodology is aimed at complementing missing methods in the current safety certification principles and practices.

We started the project by looking into the requirements that a certification process should satisfy to be considered sufficient for the certification of safety-critical GNC space systems. Before identifying the requirements, we have defined the goals that need to be achieved by a certification process and the minimum set of activities that subsumes the certification process, i.e., verification, validation and assurance activities. We have also included important certification considerations and challenges for GNC systems. These required us to look into certain missions and projects of GNC where certification was very critical but very expensive. All the safety-certification requirements, considerations and challenges that are discussed in the first activity of the project are included in "D1. Certification Requirements" document.

The next activity of the project deals with assessing the state of art in safety-certification for GNC systems for the space domain and similar systems for the civil aviation and automotive domain. We have presented first a few cross-domain safety-certification efforts, such as CESAR, OPENCOSS, pSafeCer, etc., that tried to look into the cross-domain fertilization potential among certification practices in the various domains. We have also investigated into the process-based and product-based safety certification approaches under which almost all safety-certification efforts can be classified. Then, we have assessed certification practices and standards in the three domains - space, civil aviation and automotive - which are our topic of interest. For each one of these domains, we have discussed the safety standards, safety assessment process and methods, and the safety certification processes. For the civil aviation and automotive domains, we also presented the special attention given to the software aspects of safety certification. Our analysis of the state of art for safety certification is included in "D2. State of Art Analysis" document.

Once we analyzed the state of the art for safety certification of GNC (and similar) systems in the three application domains, we have tried to assess the gap in safety certification principles and practices between the space domain and the civil aviation and automotive domains. Our gap assessment consists of two parts. In the first part, we have assessed the extent of coverage of the certification objectives in ***DO 178***, ***ARP 4761***, ***DO 254*** and ***ISO 26262*** by the ECSS standards. While ECSS standards have well covered the certification objectives in all of the mentioned standards in the other domains, we observed that ECSS standards were too generic and do not have specific guidance for GNC systems. In the second part, we have made technical gap assessment on a set of five selected safety certification issues: ***certification regime and credit***, ***severity and assurance levels***, ***safety level allocation via dependability architecture***, ***objective vs mean prescription***, and ***integrated vs external safety systems***. The findings of the gap assessment activity can be found in "D3. Gap Assessment" document.

The state of art analysis and gap assessment activities have provided us with important inputs for drafting a methodology for safety certification of GNC space systems that complements the limitations in the current certification process. The draft methodology consists of a certification process with four activities: ***requirements validation***, ***product verification***, ***product validation*** and ***product assurance***. The certification process, together with its four core activities, is aimed at enabling efficient and effective GNC safety certification in the face of current challenges such as autonomy and agile development. We have also given methods for each activity of our draft methodology that can complement the missing component in the current validation and verification methods for GNC systems. Our draft methodology is built on three important pillars, namely ***Compositionality***, ***Reusability*** and ***Continuity***, that can also complement the missing piece in the current certification approaches. Our draft certification methodology, its activities and methods for each of these activities are included in "D4. Draft Methodology" document.

Lastly, in "D5. Technology Recommendation" we recommend to further investigate four technologies (1) statistical model checking, (2) continuous integration, (3) modelling guidelines, (4) stylized requirement, as well as recent developments in run-time symbolic reasoning and verification of artificial neural networks. As these techniques all result in improving the quality of the system under design, we expect to appropriately introduce some of them to complement existing general certification process and to tailor special needs for GNC certification (i.e., application of these techniques can be viewed as an evidence claim, regarding the quality of the system being certified).