



# CARES

## *Certification Assessment Requirements for ESA Software*

*Contract N° 14899/01/NL/JA*

### **Executive Summary**

|                      |  |   |
|----------------------|--|---|
| <b>Identifier</b>    | <b>ES</b>  |   |
| <b>Version</b>       | <b>1.0</b>   |   |
| <b>Date of issue</b> | <b>15/01/2004</b>  | <b>Signatures</b>   |
| <b>Prepared by</b>   | <b>name</b><br>JF Muller<br><b>company</b><br>EADS ASTRIUM<br><b>name</b><br>Jean-Paul Blanquart<br><b>company</b><br>EADS ASTRIUM |  |
| <b>Verified by</b>   | <b>name</b><br>Jean-François Muller<br><b>company</b><br>EADS ASTRIUM  |  |

### **Abstract**

*This document constitutes the Executive Summary of the CARES study (Certification Assessment Requirements for ESA software) granted by ESA/ESTEC (contract ESTEC 14899/01/NL/JA) to a consortium led by EADS ASTRIUM (France) with Adelard (United Kingdom), Critical Software (Portugal), DNV (Norway) and EADS Airbus (France).*

## ESA STUDY CONTRACT REPORT

|                                     |  |  |
|-------------------------------------|--|--|
| ESA CONTRACT No.:<br>14899/01/NL/JA | SUBJECT: Certification scheme for software within a space system | CONTRACTOR:<br><b>EADS Astrium</b>         |
| *ESA CR( )No.:                      | *STAR CODE:  | No. of volumes: 1<br>This is volume No.: 1 |
|                                     |  | CONTRACTOR'S REF.:<br>CARES_ES_02          |

### STUDY ABSTRACT:

The “Certification scheme for software within a space system” study was granted by ESA/ESTEC to a consortium led by EADS ASTRIUM with Adelard, Critical Software, DNV and EADS Airbus. The objectives of the study were the elaboration of a generic certification scheme for the software aspects of space systems, under the form of:

- Tailored ECSS E40B and Q80B with modified and added clauses supporting the activities and justifications related to certification. These proposed amendments are discussed and justified in [TN5]. Complete amended ECSS were produced, as well as a browser tool to support on-line electronic navigation through the amended ECSS and the various justifications;
- A generic certification plan provided in [TN6] with guidance on how to organize and plan the certification related activities for space software;
- A set of requirements, provided in [TN7] applicable to organizations seeking accreditation to offer services related to certification of software within space systems (certification services, Independent Software Verification and Validation services), including organizational requirements, qualification requirements for assessors, and selection of assessment and evaluation teams.

The elaboration of this generic certification scheme has been based on an in-depth survey and analysis of the state of the art and the practice, reported in intermediate outputs of the study:

- A collection of feedback on current certification schemes and organizations in various domains, synthesized in [TN1];
- A survey of dependability and safety software methods and standards applied to safety critical software in the various domains. This is reported, along with a classification of ESA software, in [TN2];
- A collection and description of the various software dependability and safety methods and techniques, with an analysis of their applicability in the context of space software and particularly for safety critical space systems as a support to certification [TN3/4].

The proposed certification scheme covers all the major issues concerned with software certification (organization, development, validation, accreditation, training, etc.). It has been based on the currently existing scheme for space software both in terms of software process and product standards and in terms of organizational requirements. It is readily usable, with minimum impact, by all actors involved in software for critical space system. It can be tailored to various levels of criticality and to various certification scenarios, from self-certification up to the production of structured evidence in front of existing external certification and regulation authorities.

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

Names of authors: JP Blanquart / JF Muller EADS Astrium

NAME OF ESA STUDY MANAGER:  
Juan Maria Carranza  
 DIV: QQS  
 DIRECTORATE: TOS

\*\* ESA BUDGET HEADING: 060(GSP)

\* Sections to be completed by ESA  
 \*\* Information to be provided by ESA Study Manager

The CARES project is an ESA project which is conducted by EADS-ASTRIUM with DNV, EADS-Airbus, ADELARD and CSW. For further information on CARES please contact:

**ESTEC, European Space Agency**  
PO Box 299, NL-2200 AG Noordwijk ZH-The Netherlands  
Juan CARRANZA, CARES ESTEC Technical Officer  
Tel: (31) 71 565 3734 Fax: (31) 71 565 4798  
[Juan.carranza@esa.int](mailto:Juan.carranza@esa.int)

**EADS ASTRUM**  
31, rue des Cosmonautes, ZI du Palays  
31 402 Toulouse Cedex 4 – France  
Jean-Francois MULLER, Project Manager  
Tel: (33) 5 6219 5846 Fax: (33) 5 6219 7780  
[Jean-francois.muller@astrium.eads.net](mailto:Jean-francois.muller@astrium.eads.net)

**DNV (DET NORSKE VERITAS AS)**  
Veritasveien 1  
N-1322 Hovik –Norway  
Patrick ADAMCIK, DNV Project Manager  
Tel: (47) 6757 8647 Fax: (47) 6757 9705  
[pat.adamcik@dnv.com](mailto:pat.adamcik@dnv.com)

**EADS Airbus**  
316 Route de Bayonne  
31 000 Toulouse – France  
Gerard LADIER, EADS Project Manager  
Tel: (33) 5 6193 6630 Fax: (33) 5 6193 0354  
[Gerard.ladier@airbus.com](mailto:Gerard.ladier@airbus.com)

**ADELARD**  
Drysdale Building  
Northampton Square  
London E3 2DA United Kingdom  
Dr George CLELAND, ADE Project Manager  
Tel: (44 ) 20 7940 9450 Fax: (44) 20 7940 9451  
[george.cleland@adelard.co.uk](mailto:george.cleland@adelard.co.uk)

**CSW (Critical Software Lda)**  
Rua Pedro Nunes, IPN  
3030-199 Coimbra – Portugal  
Joao CARREIRA, CSW Technical responsible  
Tel: (351) 239 700 945 Fax: (351) 239 700 905  
[Jcar@criticalsoftware.com](mailto:Jcar@criticalsoftware.com)

| <b>DOCUMENT HISTORY</b> |             |   |
|-------------------------|-------------|---|
| <b>Version</b>          | <b>Date</b> | <b>Comments</b>                         |
| 0.0                     |             | Creation of the document                |
| 0.1                     | 15/10/2003  | First version submitted to final review |
| 1.0                     | 15/01/2004  | Updates after final review              |

# Table of Contents

|  |           |
|--|-----------|
| <b>1. INTRODUCTION .....</b>                   | <b>6</b>  |
| 1.1. Purpose .....                             | 6         |
| 1.2. Acronyms and Abbreviations .....          | 6         |
| 1.3. Applicable and Reference Documents .....  | 7         |
| 1.3.1. Applicable documents .....              | 7         |
| 1.3.2. Reference documents .....               | 7         |
| <b>2. CARES STUDY DESCRIPTION.....</b>         | <b>8</b>  |
| 2.1. Objectives.....                           | 8         |
| 2.2. Logic of the study.....                   | 8         |
| 2.3. The partners.....                         | 11        |
| 2.4. List of Work Packages and WBS.....        | 12        |
| 2.4.1. List of work packages .....             | 12        |
| 2.4.2. Work Breakdown Structure .....          | 12        |
| <b>3. CARES STUDY DELIVERABLES.....</b>        | <b>15</b> |
| <b>4. CONCLUSION AND RECOMMENDATIONS .....</b> | <b>16</b> |
| 4.1. Conclusion .....                          | 16        |
| 4.2. Recommendations .....                     | 17        |
| 4.2.1. Experimentation .....                   | 17        |
| 4.2.2. Special cases and evolutions .....      | 17        |
| 4.2.3. Organization of safety evidence .....   | 17        |

# 1. Introduction

## 1.1. Purpose

That document is the executive summary of the CARES study. It presents a synthesis of the context of the study, its objectives and the main results.

## 1.2. Acronyms and Abbreviations

|                     |   |
|---------------------|---|
| AD.....             | Applicable Document   |
| ADE .....           | Adelard   |
| CARES.....          | Certification Assesment Requirements for ESA Software                       |
| CSW.....            | Critical SoftWare   |
| DNV.....            | Det Norske Veritas  |
| DRD .....           | Document Review Discrepancy   |
| EADS .....          | European Aeronautic Defence and Space                                       |
| ECSS .....          | European Co-operation for Space Standardisation                             |
| EGSE .....          | Electrical Ground Segment Equipment   |
| ESA.....            | European Space Agency   |
| ESTEC .....         | European Space Technology Centre  |
| GNSS .....          | Global Navigation Satellite System  |
| GNSS2/Galileo ..... | Normally meaning the European-led Galileo Space and Ground Control segments |
| NA.....             | Not Applicable  |
| PM.....             | Progress Meeting  |
| RD.....             | Reference Document  |
| SOW.....            | Statement of Work   |
| TBC.....            | To Be Confirmed   |
| TBD.....            | To Be Defined   |
| TM.....             | Technical Meeting   |
| TN .....            | Technical Note  |
| WBS.....            | Work Breakdown Structure  |
| WP.....             | Work Package  |
| WPD.....            | Work Package Description  |
| Wrt .....           | with respect to   |

## 1.3. Applicable and Reference Documents

### 1.3.1. Applicable documents

- AD 1 Certification Scheme for Software within a Space System, Statement of Work, TOS-QQ/9902-54/JC, issue 1.3
- AD 2 CARES Proposal, PTI.PC.ON.1 871.00

### 1.3.2. Reference documents

- RD 1 [DO178B] RTCA/EUROCAE, *DO-178B/ED-12B – Software Considerations in Airborne Systems and Equipment Certification*, December 1992.
- RD 2 [EN 45004] EN 45004:1995, General criteria for the operation of various types of bodies performing inspection.
- RD 3 [EN 45011] EN 45011:1998, General requirements for bodies operating product certification systems.
- RD 4 [GNSS2 TN4Part1] Tailoring of ECSS Software Standards for GNSS/2 Galileo system, Study of GNSS2/Galileo System Software Certification, *TN 4 Part 1 – Tailoring of ECSS Software Standards for GNSS-2/Galileo System, Issue 1*, 19-3-2001.
- RD 5 [IEC 61508] International Electrotechnical Commission, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, IEC 61508, Parts 1 to 7.
- RD 6 [SPEC TN3] “*Software Product Evaluation and Certification - Space Domain Specific Software Product Quality Models, Requirements and Related Evaluation Methods*”, ESA Contract n°12650/97/NL/NB(SC), Technical Note 3 issue 3.4, February 20, 2002
- RD 7 [TN1] “*Software Certification Feedback Collection and Catalogue of Organisations*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 1, issue 2.0, January 25, 2002.
- RD 8 [TN2] “*Current use of methods and standards for development and certification of safety-critical software*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 2, issue 1.0, November 8, 2002.
- RD 9 [TN3/4] “*Description of methods and techniques for software development, verification and validation*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 3/4, issue 1.0, February 17, 2003.
- RD 10 [TN5] “*Requirements for development of software in space systems to be certified*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 5, issue 1.0, January 13, 2004.
- RD 11 [TN6] “*Generic certification plan for space systems*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 6, issue 1.0, December 17, 2003.
- RD 12 [TN7] “*Organisational and personnel requirements for accreditation of certification*”, CARES Project, ESA Contract n°14899/01/NL/JA, Technical Note 7, issue 1.0, February 02, 2004.

## **2. CARES Study Description**

### **2.1. Objectives**

The part of software in ESA space systems is drastically growing while space system criticality increases. Space systems are part of other safety related and safety critical systems. Even if space actors are deeply involved in quality control, there are actually no certification schemes related to space software systems.

In this context, ESA has already sponsored a number of studies related to dependability and safety, process improvement and certification, the most recent being the GNSS-2 study related to the software aspects of certification of the GNSS-2 system. These studies are more dealing with specific aspects of Reliability Availability, Maintainability and Safety (RAMS) techniques or tied to a specific application as the GNSS-2 system. The objectives of the study are to define generic requirements on software development and verification and validation, a global certification scheme and a generic certification plan.

CARES uses a complementary approach more quality oriented taking into account the results of the ESA SPEC study and considering that the certification process injects constraints on the quality process which is in charge of verifying the certifiability of the software system under development.

CARES covers all kinds of ESA space systems and not only positioning systems as GNSS and considers other domains such as civil aviation, nuclear, railway, automotive and medical domains.

A complete set of standards is addressed and particularly those concerning civil aviation domain which is already tied to certification and whose problematic seems closer to the space system.

The generic certification scheme is defined to be adaptable to different scenarios in terms of type of certification, organisations, etc.

### **2.2. Logic of the study**

The CARES study consists of 2 phases :

- A review of current practices in different domains
- A definition of the space software certification scheme

The major output of the study is a set of technical notes allowing for the tailoring of ECSS standards concerning certification aspects.



2.2.1.1. Study logic

The following figures show the organisation of the study, the relationships between the different tasks and the major outputs from the study. They are based on IDEF like diagrams. The first level (figure 1) shows inputs and outputs from and to other studies and projects. The other two diagrams (figure 2 and 3) represent more details on each of the 2 phases of the project.

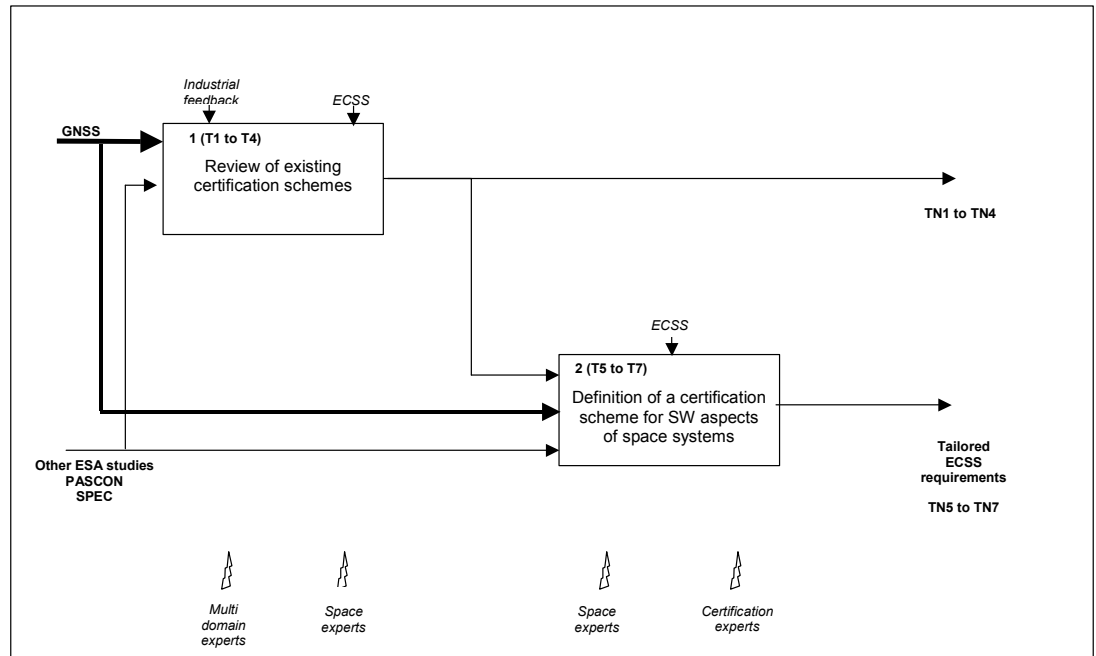


Figure 1. Logic of the Study (overall)

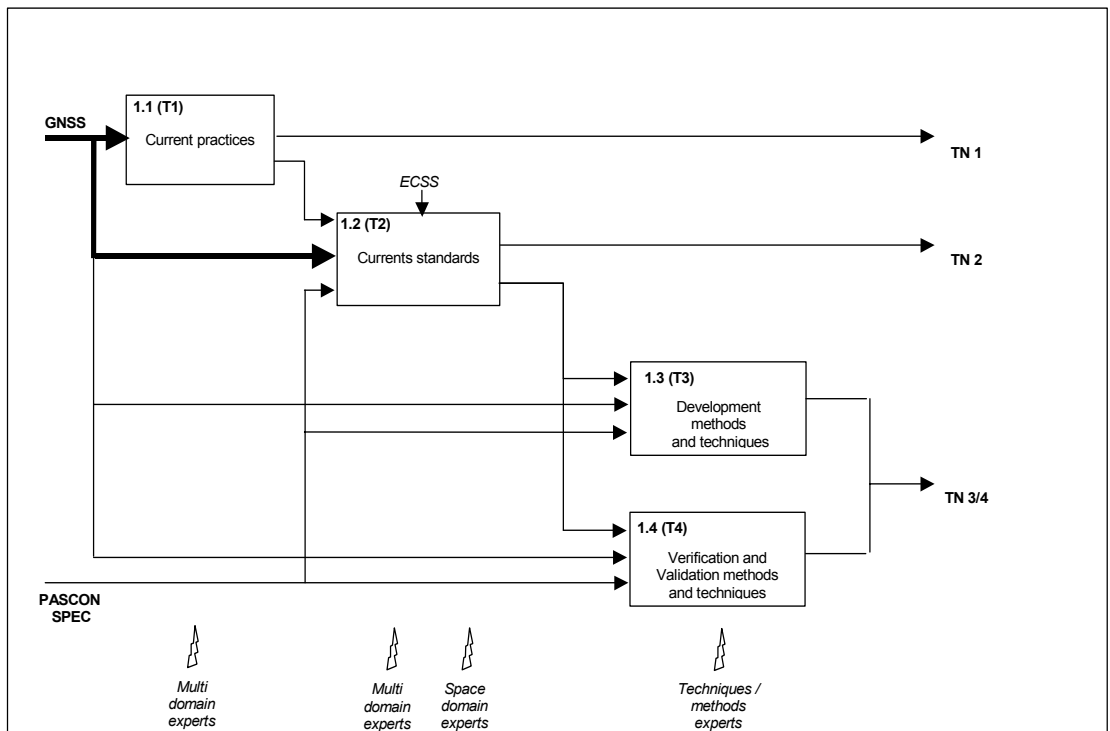
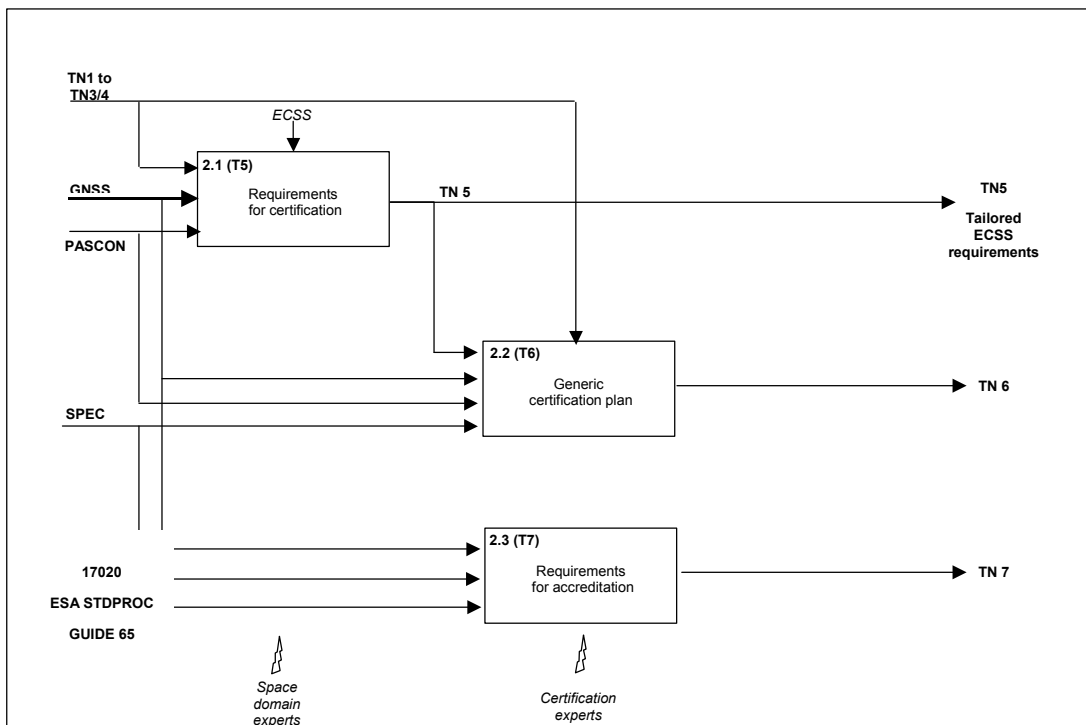


Figure 2. Logic of the Study (Review of existing certification schemes, phase 1)



**Figure 3. Logic of the Study (Definition of a certification scheme, phase 2)**

Four different roles were involved in the project:

- Space industry experts responsible for the identification of the space industry current practices and for the synthesis of results of investigations in other domains
- Multi domain experts responsible for the identification of current practices in other domain than the space industry
- Techniques and methods experts responsible for the detailed description and evaluation of practices identified in the different domains
- Certification experts responsible for the certification and assessments aspects.

Roles are identified in the bottom part of the diagrams.

## 2.3. The partners

The consortium was composed of the following partners:

- ❑ EADS ASTRIUM (Prime Contractor),
- ❑ Det Norske Veritas (Subcontractor),
- ❑ EADS Airbus (Subcontractor),
- ❑ Adelard (Subcontractor),
- ❑ Critical Software (Subcontractor).

EADS ASTRIUM has acquired a very **strong competency in the industrial development of a space system software** (for both on-board and ground software). In particular, EADS ASTRIUM has a wide experience in the design of data management system for space systems including complex system software, advanced on-board avionics and mission support.

EADS ASTRIUM has also a **very strong experience on critical real-time fault tolerant embedded systems**, gained through R&D activities, which are of particular interest to the present study.

Det Norske Veritas (DNV) has acquired a **very strong competence in all aspects of certification, quality assessment** (including qualification of personnel, assessment of process as well as product properties), independent software validation and certification and is also involved in software process improvement services, including CMM (Capability Maturity Model) evaluation.

EADS Airbus has a **unique experience as a manufacturer of software-intensive systems (AIRBUS aircraft) and safety-critical avionics which are submitted to certification** for world-wide usage. EADS has become a recognised expert involved in the definition and evolution process of certification standards and norms.

Moreover, EADS ASTRIUM, DNV and EADS Airbus were **partners in the GNSS-2/Galileo System Software Certification study** that allows to significantly strengthen synergies with CARES study.

In order to improve the generic point of view to the study (not linked to a particular project), the study was driven by the Software Quality department in ASTRIUM and the core partners of the GNSS-2 certification study was enriched by other partners providing complementary contributions:

Adelard (ADE) has an extensive experience of safety management, safety analysis, applied research on safety cases and software reliability, certification consultancy and safety related software development for **major organisations and companies including mainly civil aviation authority, railway, medical and nuclear**. Moreover, ADE has a long experience on the evolutions of various standards and norms.

The ability to leverage the Critical Software's (CSW) core competencies and R&D capabilities in terms of **software reliability, fault-tolerance verification, validation**, and engineering in the aerospace business is the main driver for its participation in the consortium.

The consortium members covered the following technical areas of the CARES study:

- EADS ASTRIUM was responsible for the identification of the space industry current practices and for the synthesis of results of investigations in other domains,
- EADS Airbus and ADE were responsible for the identification of certification current practices in other domains than the space industry (mainly civil aviation, nuclear, railway and medical),
- EADS ASTRIUM and CSW were responsible for the detailed description and evaluation of practices identified in the different domains,
- DNV was responsible for the certification aspects.

Moreover, ADE performed the first tasks of the study aiming at collecting information from various domains being certified.

## 2.4. List of Work Packages and WBS

### 2.4.1. List of work packages

The WP list (with their responsible) is given hereafter:

- WP 0000: Project Management (EADS Astrium)
- WP 1000: Software certification feedback collection (ADE)
- WP 2000: Current methods and standards for software (EADS Astrium)
  - WP 2100: Current methods and standards for software (EADS Astrium)
  - WP 2200: Civil aviation domain methods and standards (EADS Airbus)
  - WP 2300: Other domains methods and standards (ADE)
- WP 3000: Development methods and techniques (EADS Astrium)
- WP 4000: Verification and validation methods and techniques (EADS Astrium)
- WP 5000: Software requirements for certification (EADS Astrium)
  - WP 5100: Software development requirements (EADS Astrium)
  - WP 5200: Certification requirements (DNV)
- WP 6000: Generic certification plan for space systems (DNV)
  - WP 6100: Generic certification plan (DNV)
  - WP 6200: Generic certification plan validation (EADS Astrium)
- WP 7000: Organisation and personnel requirements (DNV)
- WP 8000: Software techniques description (EADS Astrium)
  - WP 8100: Space software techniques description (EADS Astrium)
  - WP 8200: Civil aviation software techniques description (EADS Airbus)
  - WP 8300: Other domains software techniques description (ADE)
  - WP 8400: Safety related mechanisms (CSW)
- WP 10100: Prototype document browser (EADS Astrium)
- WP 10200: Prototype document browser validation (DNV)

For work packages 2000, 5000, 6000, 8000 which include different subtasks, a work package technical leader was responsible of the overall consistency of the work and the effort was only given on the subtasks.

### 2.4.2. Work Breakdown Structure

The top level work breakdown structure is given in the following diagram.

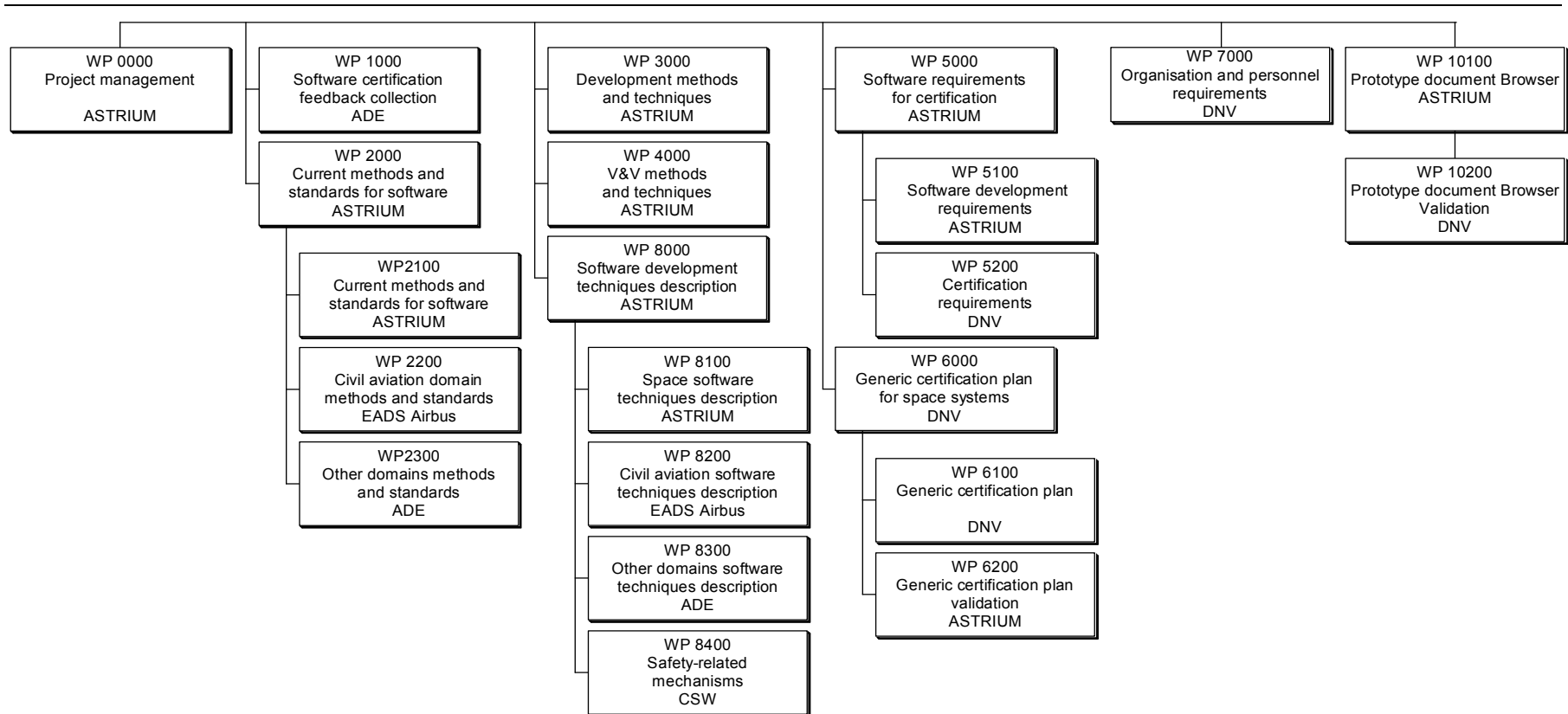


Figure 4. Work Breakdown Structure



### 3. CARES Study Deliverables

The following table gives a synthesis of the project technical deliverables.

| Identifier   | Version | Title  |
|--------------|---------|--|
| <b>ABS</b>   | 1.0     | Abstract in HTML format  |
| <b>FR</b>    | 1.0     | Final Report   |
| <b>ES</b>    | 1.0     | Executive Summary  |
| <b>EM1</b>   | 1.0     | Educational Material for top management  |
| <b>EM2</b>   | 1.0     | Educational Material for technical staff   |
| <b>TN11</b>  | 2.0     | SW certification feedback, collection and catalogue of organisations (Part1)   |
| <b>TN12</b>  | 1.0     | SW certification feedback, collection and catalogue of organisations (Part2)   |
| <b>TN2</b>   | 1.0     | Current use of methods and standards for development and certification of safety-critical software   |
| <b>TN3/4</b> | 1.0     | Description of methods and techniques for software development, verification and validation  |
| <b>TN5</b>   | 1.0     | Requirements for development of software that is part of a space system to be certified and Requirements for software aspects of the certification of space system |
| <b>TN6</b>   | 1.0     | Generic certification plan for space systems   |
| <b>TN7</b>   | 1.0     | Organisational and personnel requirements for accreditation of certification   |
| <b>DB</b>    | 1.0     | Prototype Document Browser   |

*Figure 5. List of deliverables*

## 4. Conclusion and recommendations

### 4.1. Conclusion

The CARES study has reached its objectives consisting in the elaboration of a generic certification scheme for the software aspects of space systems, under the form of:

- Tailored ECSS E40B and Q80B with modified and added clauses supporting the activities and justifications related to certification. These proposed amendments are discussed and justified in [TN5]. Complete amended ECSS were produced, as well as a browser tool to support on-line electronic navigation through the amended ECSS and the various justifications. These justifications are traced back to their origin, particularly sources of information such as existing certification standards from recognized regulation bodies. This in particular supports the identification, for a given project, of the additional requirements necessary to ensure compliance to an existing external standard when made applicable for the project;
- A generic certification plan provided in [TN6] with guidance on how to organize and plan the certification related activities for space software;
- A set of requirements, provided in [TN7] applicable to organizations seeking accreditation to offer services related to certification of software within space systems (certification services, Independent Software Verification and Validation services), including organizational requirements, qualification and training requirements for assessors and inspectors, and selection of assessment and evaluation teams.

The elaboration of this generic certification scheme has been based on an in-depth survey and analysis of the state of the art and the practice, reported in intermediate outputs of the study:

- A collection of feedback on current certification schemes and organizations in various domains, synthesized in [TN1];
- A survey of dependability and safety software methods and standards applied to safety critical software in the various domains. This is reported, along with a classification of ESA software, in [TN2];
- A collection and description of the various software dependability and safety methods and techniques, with an analysis of their applicability in the context of space software and particularly for safety critical space systems as a support to certification. This is reported in [TN3/4], including an analysis of the impact of methods on, and relationships with, various usable product and process metrics.

The proposed certification scheme covers all the major issues concerned with software certification (organization, development, validation, accreditation, training, etc.). It has been based on the currently existing scheme for space software both in terms of software process and product standards and in terms of organizational requirements. Therefore it is considered as readily usable, with minimum impact, by all actors involved in software for critical space system. It can be tailored so as to be adaptable to various levels of criticality and to various certification scenarios, from self-certification up to the production of structured evidence in front of existing external certification and regulation authorities.



## **4.2. Recommendations**

In addition to the objectives of the study, some recommendations could be identified for further work in this area, particularly on the experimentation of the proposed approach, on how to cope with special cases, particular technologies and evolutions of software engineering and on the organization of safety evidence.

### **4.2.1. Experimentation**

The proposed amendments are based, on the one hand on the existing space standards and practices and on the other hand on additional recommendations supported by standards and practices benefiting from long experience in various industrial domains. However the practical experimentation of the proposed scheme on space projects would certainly provide useful complementary information and some possibilities of adjustment or evolution of the proposed scheme.

### **4.2.2. Special cases and evolutions**

Due to its objectives, the study focused on the elaboration of a generic certification scheme. It also addressed wherever relevant some specificities due to particular techniques or solutions used or envisaged in software space systems. Nevertheless the primary focus was on the general case, be it only because a major input of the study was the set of existing certification schemes from recognized bodies, which address mainly the general case and only very slowly incorporate evolutions. Additional specific studies are therefore needed on safety or certification issues for cases such as for example the object-oriented development and languages, the automatic generation of code, the utilization of commercial off-the-shelf components or open source software, the proper utilization of in-service history data as dependability and safety argument, etc. It is particularly recommended that such studies incorporate, or even better contribute to, the evolutions of certification and safety standards in other domains e.g., through the participation to common working groups.

### **4.2.3. Organization of safety evidence**

The proposed scheme is based on the concept of safety case, at system and software level (in terms of the identification of the software contribution to the safety case). The safety case approach addresses the logical organization of claims and supporting evidence. Due to its objectives, the study focused primarily on the various elements that could be used to support a safety claim (for what concerns software), and particularly on the elements likely to be produced with limited additional effort within the general framework constituted by the ECSS software development and validation processes.

Interesting complementary results could be provided from a more general and top-down perspective. Addressing the certification issue from the logical structure of a software safety case should allow for the elaboration of simple, efficient, flexible and sound safety justification schemes, both goal- and rationale-oriented (though without guarantee of using efficiently the available or reasonably achievable additional evidence from an existing framework).

On the short-term, a safety justification based study should facilitate the presentation of safety arguments to a certification body. On a medium-term it should also facilitate the identification or incorporation of alternative justification approaches and specific evidence (in particular for special cases).