



**Common Criteria & ECSS: Best integration of a Common Criteria evaluation in a space product development process compliant with the ECSS (European Cooperation for Space Standardization) system**

**11th ICCC, Antalya, 21-23 September 2010**

- ▶ Introduction
- ▶ Presentation of the ECSS system
- ▶ Comparison between the ECSS system and the CC system
- ▶ Integration of a CC evaluation within an ECSS development process
- ▶ A dream of convergence
- ▶ Questions



- ▶ **Thales-CEACI ITSEF:**
  - ⇒ HW & embedded SW ITSEF
  - ⇒ Under ANSSI agreement

- ▶ **Speaker: Thomas BEN ([thomas.ben@thalesgroup.com](mailto:thomas.ben@thalesgroup.com))**
  - ▶ Evaluator for 10 years
  - ▶ 4 years experience in space industry

- ▶ Introduction
- ▶ Presentation of the ECSS system
  - ▶ Definitions / Objectives of using the ECSS system
  - ▶ Structure and Architecture of the ECSS system
  - ▶ Customer-supplier model / Tailoring Process
  - ▶ Structure of an ECSS Standard
- ▶ Comparison between the ECSS system and the CC system
- ▶ Integration of a CC evaluation within an ECSS development process
- ▶ A dream of convergence
- ▶ Questions



## ▶ Definitions

- ▶ ECSS : European Cooperation for Space Standardization
- ▶ Cooperative effort of ESA (European Space Agency), National space agencies (CNES in France), and European industry associations to develop and maintain common standards

## ▶ Objectives of using the ECSS system

- ▶ Achieve cost effective space programs in Europe
- ▶ Improve competitiveness of European space industry
- ▶ Improve quality & safety of space projects and products
- ▶ Facilitate clear & unambiguous communication between parties
- ▶ Reduce risks & guarantee interoperability



## ▶ Structure and Architecture of the ECSS System

### ▶ 3 types of documents :

- **Standards** ⇒ state verifiable **Requirements**
- Handbooks ⇒ provide information on a specific point
- Technical Memoranda ⇒ provide general information on a subject

### ▶ 3 branches

- Management (M-branch) ⇒ Project management aspects
- Engineering (E-branch) ⇒ Technical aspects
- Product Assurance (Q-branch) ⇒ Assurance for mission accomplishment aspects



- ▶ Customer-supplier model
  - ▶ Space projects imply many actors
  - ▶ All actors are either **Customer** (top level), **Supplier** (lower level), or both (intermediary levels)
  - ▶ ECSS standards are applicable at any customer-supplier interface level.
  - ▶ Customers cascade ECSS requirements to their suppliers
  
- ▶ Tailoring Process
  - ▶ Process of adapting the requirements to a project specificities
  - ▶ **Applicable requirements** are expressed by the customer to its suppliers in an Applicability Requirements Matrix (EARM) .
  - ▶ **Compliance** to the above EARM is expressed by the supplier in an Compliance Matrix (ECM)



## ▶ Structure of an ECSS Standard

⇒ 4 main sections

- ▶ Preliminary : Introduction, Scope, Terms and definition
- ▶ **Principles** : Principles supported by the standard
- ▶ **Requirements** : Requirements to which customer/supplier must conform in order to ensure that the standard Principles are respected
- ▶ Annexes : DRDs (Document Requirements Definition) that contains requirements for the content of **Evidences** produced by the supplier.

- ▶ Introduction
- ▶ Presentation of the ECSS system
- ▶ Comparison between the ECSS system and the CC system
  - ▶ Details on the ECSS approach
  - ▶ CC vs ECSS approach
- ▶ Integration of a CC evaluation within an ECSS development process
- ▶ A dream of convergence
- ▶ Questions



## ▶ Details on the ECSS approach (1/3)

▶ ECSS requirements are expressed into Standards within 3 branches

▶ Management branch (M-Branch)

⇒ Standards with requirements for Project Management activities  
(applicable at each level of the customer-supplier chain)

- Project Management Plan
- Project Life Cycle
- Configuration Management Plan



## ▶ Details on the ECSS approach (2/3)

### ▶ Engineering branch (E-Branch)

⇒ Standards with requirements for architecture definition & design activities (applicable at each level of the customer-supplier chain)

- Customer functional requirements analysis & Supplier functional requirements formulation
- Functional Spec, Architectural & Detailed Design, Implementation (incl. mechanical, thermal, electrical... disciplines)
- Internal Validation & Customer Acceptance
- User Manuals
- Tools & Techniques
- Maintenance
- Exception : SW development Life Cycle is addressed in the SW engineering standard of the E-Branch



## ▶ Details on the ECSS approach (3/3)

### ▶ Product Assurance branch (Q-Branch)

⇒ Standards with requirements for assessment of product compliance to the customer request (incl. documentation). Ensure that :

- The management process and quality process are respected
- The produced evidences are compliant to the ECSS DRDs
- The product is tested according to the ECSS requirements and behaves like specified
- The suppliers are compliant with ECSS requirements (incl. audits)

### ▶ Exception : ASIC & FPGA program management, engineering, and quality assurance are addressed in one unique standard of the Q-Branch



## ▶ CC vs ECSS approach (1/2)

- ▶ Both systems can be qualified as development methodology based on functional and development assurance requirements
- ▶ Both systems rely on the same assurance principles through their own specific organization
  - ECSS M-Branch ⇒ CC ALC assurance class (LCD, FLR, CMC/CMS partially)
  - ECSS E-Branch ⇒ CC ADV (FSP, TDS, AGD, ATE) and ALC (TAT, CMC/CMS partially) assurance classes
  - ECSS Q-Branch ⇒ can be compared to CC CEM
- ▶ ECSS does not cover CC requirements specific to security (ASE, AVA, ADV\_ARC, ALC\_DVS, ALC\_DEL)



## ▶ CC vs ECSS approach (2/2)

### ▶ ECSS philosophy

- Ensures the targeted quality level of the final system (related to space constraints) through requirements
- No security oriented functional requirements (contrary to thermal, mechanical, electrical...disciplines)
- Compliance to the requirements is assessed by the developer

### ▶ CC philosophy

- Ensures the targeted security level of the TOE through requirements
- Provides a standardized metric to assess the assurance and resistance level of the TOE
- Compliance to the requirements is assessed by 3rd party (ITSEF)

- ▶ Introduction
- ▶ Presentation of the ECSS system
- ▶ Comparison between the ECSS system and the CC system
- ▶ Integration of a CC evaluation within an ECSS development process
  - ▶ From the developer point of view
  - ▶ From the evaluator point of view
- ▶ A dream of convergence
- ▶ Questions



- ▶ From the developer point of view
  - ▶ **Reduced** additional **effort** implied by CC evaluation :
    - Only elements of evidence specifically related to the Security Evaluation need to be added (Security Target, SFRs Traceability in design documents, Security Architecture description, Security of Development,...)
  - ▶ **Additional insurance** provided by CC evaluation. Customer & Supplier can rely on evaluation results (for requirements that are common to CC/ECSS systems) to assess :
    - The conformity of supplier documentation evidences
    - The conformity of supplier practices (through audit results)
    - The efficiency of supplier Product Assurance process



## ▶ From the evaluator point of view (1/2)

⇒ In a context of heavy evaluation processes due to the complexity of the TOEs and there operational environment, the huge documentation databases, and the program constraints

- ▶ **Minimized** evaluator **efforts** due to the documentation architecture imposed by the ECSS DRDs :
  - Homogeneous set of documentation from one project to an other and from one developer to an other
  - Reduced learning phase when confronted to complex TOEs with huge documentation database (after a first experience)



- ▶ From the evaluator point of view (2/2)
  - ▶ **Optimized** evaluator **analysis** for several assurance tasks :
    - On many CC assurance components, the ECSS requirements produce documentation evidences that are compliant with the CC requirements (~EAL4).
    - Supplier ECM (ECSS compliance matrix) can be used as an entry point to determine which ECSS requirements where taken into account
  - ▶ **Enhanced** documentation **quality** due to :
    - ECSS Product Assurance requirements that guaranty a good quality level of the evidences
    - Formal Review process implying an independent review committee with customer and sponsor

- ▶ Introduction
- ▶ Presentation of the ECSS system
- ▶ Comparison between the ECSS system and the CC system
- ▶ Integration of a CC evaluation within an ECSS development process
- ▶ A dream of convergence
  - ▶ Lightened evaluation process
  - ▶ CC integration into ECSS system
- ▶ Questions



- ▶ Lightened evaluation process
  - ▶ **Automatic PASS** verdict (assurance level to be defined) for CC assurance components that are completely covered by the ECSS requirements
    - Faster evaluation process
    - Evaluation evidences reduced to the needs of the evaluator for its security analysis
- ⇒ For this, a detailed study is mandatory to produce an exhaustive **correspondence matrix** between CC assurance components and ECSS requirements.



- ▶ CC integration into ECSS system
  - ▶ Requirements for compliance to a CC EAL can already be specified by the customer in the Technical Specification
  - ▶ Additional **requirements** could be added to the ECSS system which is an open and living system
    - To manage the **functional security** needs inside a new security discipline within the engineering branch (E-Branch)
    - To establish a **documentation database** covering completely the CC assurance components (assurance level to be defined).

► Questions ?