New Reliability Prediction Methodology Aimed at Space Applications

Briefing Meeting with Industry

Luigi Bianchi
Head of Dependability and Safety Assurance Section
ESA/ESTEC Product Assurance and Safety Department

22/04/2016
Table of Contents

1. Introduction
2. ESA Reliability Initiative
3. New Reliability Prediction Methodology (General Study Program)
4. Conclusions
5. Q&A Session
Introduction – Why this briefing?

The “New Reliability Prediction Methodology Aimed at Space Applications” proposal (ESA/IPC(2015)1,add.54) was approved, as in IPC 295th MoM (24 March 2016)

i. we would like to interest all potential bidders;

ii. we would like to present objectives of the activity;

iii. we would like to present the future outcome of the activity
2. ESA Reliability Initiative
2. ESA Reliability Initiative

To identify shortcomings in the current reliability assessment methodologies and practices, and possible solutions for improvement.

- **In line with TEC-QQD Roadmap objectives**
  - Enhance safety and mission assurance capabilities (RAMS) to support ESA missions according to strategic needs, improving modeling and practices, and addressing development of new standards, handbooks, methodologies and tools.

- **How can ESA Reliability Initiative help? (despite limited R&D budget...)**
  - Enhance dialogue and cooperation with European space agencies and industry on best reliability practices and techniques
  - Encourage experts in industry as well as from academia to investigate innovative solutions to reliability technical issues
  - Share lessons learned and experiences with other domains, particularly for COTS utilization and complex critical systems
  - Identify R&D needs, coordinate efforts and harmonize initiatives in the reliability domain
  - Advance reliability disciplines innovation and promote their application in the European space (and non space) community
  - Reinforce reliability support to PA in evolving reliability engineering technologies for trade-off and prediction analyses
  - Strengthen monitoring field reliability vs. objectives and solicit user / customer feedback to ensure added value to product reliability within cost and schedule constraints
  - Evaluate the Supplier capability to implement effective practices for product reliability
2. Reliability Initiative (1/3) - Achieved

- Internal ESA WGs - 2011
  - Gaps Analysis (GA) – preliminary results (#20 issues identified)

- Dedicated technical meetings with Primes (AD&S, OHB, TAS) - 2012
  - Receive Industry feedbacks, consolidation of GA results and proposed solutions

- 1st Reliability Assessment W/S with Primes - 2013
  - Common challenges and shared concerns → harmonized Roadmap + Workplan (solutions to be pursued and priorities)

- 1st AWARE W/S (Advanced Workshop on Assessment of RELiability) - 2014
  - Larger cooperation, harmonization and coordinate efforts
  - Extend participation to non-space actors

⇒ **Product Assurance & Safety Dpt Head (TEC-Q) issued a memo reinforcing the request of adequate R&D funding to concerned ESA Directorates (Ref: Memo – “System reliability assessment: shortcomings and R&D needs” - Apr15)**
2. Reliability Initiative (2/3)  
- Achieved / Planned

- **White Paper → “Effective Reliability Prediction for Space Applications”** (Draft, currently under internal review)
  - The goal is to improve the reliability prediction process and to increase the cost effectiveness of ESA space systems development programs
    - Describes current situation in the RP (end-to-end process), highlights inadequacies and limitations, and proposes advancements with a clear implementation strategy

- **GSP 2016 → #1 R&D study proposal approved at IPC/Nov15**
  - “New Reliability Prediction Methodology aimed at Space Applications” (KO 2Q16, d:24m)
    - Develop a new reliability prediction methodology to overcome the inherent limitations of the current prediction practices

- **TECNET 2016-2017/TRP → #2 R&D study proposals approved at IPC/Nov15**
  - “Reliability Model Enabling Satellite Life Extension and Safe Disposal” (d:24m)
    - Develop a spacecraft reliability degradation model, identify its required inputs to enable quantitative risk based decision-making on satellite life extension and safe disposal

- **Cooperation with Agencies**
  - Coordinate efforts with CNES and NASA in new R&D initiatives, focus on common goals, share results, organize events of mutual interests (e.g. Workshops, Trilaterals). Interaction with DLR initiated.
2. Reliability Initiative (3/3)  
- Recently Completed / On going R&D Study Contracts

- **RIDE2 - RAMS In-orbit Data Exploitation [completed, Jul15]**
  - Consolidation of RIDE-1 concept, by assessing reusability of existing ESA infrastructure and tools, defining the process and interfaces with existing tools, validating the approach with a prototype

- **IFA - Integrated Failure Analysis [completed, Nov15]**
  - Failure analysis including organizational, complexity and human dependability issues

- **Use of quantitative reliability requirements for space applications [completed, Feb16]**
  - Where and why quantitative reliability requirements should be used for systems and elements

- **Reliability prediction (RP) data sources and methodologies for space applications [FP Jun16]**
  - Reliability data sources suitability as an alternative to the obsolete MIL-HDBK-217 RP handbook

- **Reliability of mechanical systems and parts [FP Jul16]**
  - Most suitable methods to assess the reliability of non-electronic systems and parts and for reliability verification by testing

- **CFDA - Catalogue of Failure Data [FP Sep16]**
  - Provides a catalogue of failure event input data and supports all phases of the program with data sets for functional, physical failures, software errors, human operator errors, operational failures etc. (not quantitative data)
2. Reliability Workshops – Important Contributions, Common Experience and Shared Concerns (1/2)

- Assessments do not adequately reflect the real applications in orbit. Large variations exist between performance prediction and field (in-orbit) reliability. High percentage of systematic failures / non component causes (i.e. from manufacturing defects, design deficiencies, software etc) rather than parts failure

**Key area for improvements:** A more holistic approach to reliability prediction accounting for **non-parts related system failures causes**

- Uncertainties with quantitative estimations (e.g. failure rate, MTBF, service life, MTTR etc) are high. Outputs of current methods are inadequate as a basis for tradeoffs. **Data sources** do not reflect the continuous improvements in components quality. Increased complexity affects **tools adequacy** (i.e. more ICs and more complex – model limitations)

**Key area for improvements:** Adequacy of reliability prediction / assessment / demonstration **methods and input data** currently available for **quantitative calculations**

- Reliability Prediction (RP) not only as an absolute figure estimate of field reliability, but also to support design trade-off decisions/design optimization. RP as a process, not a one-time activity

**Key area for improvement:** Substantiation and allocation of contractual **quantitative reliability targets** and associated **verification requirements**
2. Reliability Workshops – Important Contributions, Common Experience and Shared Concerns (2/2)

- **Different methods** have increased the skepticism over the usefulness and the exact techniques used for the calculation of reliability data (e.g. combine prediction & observation, corrective factors)

  Key area for improvement: **Harmonized approach to credible reliability predictions using in-orbit performance feedback**

- **New challenges** from space system design and rapid technology evolution requesting more efficient RP methodologies (to enable the insertion of new technologies e.g. DSM)

  Key area for improvement: **Adequate knowledge of materials and process conditions driving failure mechanisms, and uniformity of modeling practices**

IC Reliability (Example) - Microprocessors

- **90nm Microprocessors**
  - 150-200 FIT over 5 years (0.11% AFR)

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Node</th>
<th>Field FBR Failure Rate (FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H7T1653P35440-10B84</td>
<td>Hynix 354 SDRAM</td>
<td>150x</td>
<td>689</td>
</tr>
<tr>
<td>H47065S2D400-06333</td>
<td>Samsung 512x8 DDRAM</td>
<td>130x</td>
<td>41.5</td>
</tr>
<tr>
<td>HYA0321X0048F6-02</td>
<td>Hynix 1G DDRAM</td>
<td>130x</td>
<td>82.1</td>
</tr>
<tr>
<td>H264HC1G08F12F7</td>
<td>PoweMax Microcontroller</td>
<td>90x</td>
<td>221</td>
</tr>
<tr>
<td>RH05316M3C32LS7BN</td>
<td>Intel 1.6GHz Pentium</td>
<td>90x</td>
<td>144</td>
</tr>
</tbody>
</table>

- **65nm Microprocessors**
  - 422 FIT over 5 years (0.37% AFR)

<table>
<thead>
<tr>
<th>Time in Use</th>
<th>Operating Reliability Goals</th>
<th>Cumulative Failure Rate (%)</th>
<th>Average Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 1 Year</td>
<td>0FIT (6760 hrs)</td>
<td>0.24%</td>
<td>274 FIT</td>
</tr>
<tr>
<td>0 - 3 Years</td>
<td>323 FIT (26280 hrs)</td>
<td>0.85%</td>
<td>242 FIT</td>
</tr>
<tr>
<td>0 - 5 Years</td>
<td>422 FIT (43800 hrs)</td>
<td>1.85%</td>
<td></td>
</tr>
</tbody>
</table>

3X increase in AFR with decrease in node size

[Source: Reliability of State-of-the Art Digital Electronics, 4th NEPP W/S – DfR]

Wearout (Integrated Circuits)

Key area for improvement: Harmonized approach to credible reliability predictions using in-orbit performance feedback

Need to develop a **new reliability prediction methodology** to remove the current shortcomings and contribute to the **sustainability and affordability of future space systems** within highly competitive markets.
3. New Reliability Prediction Methodology (GSP)
3. New Reliability Prediction Methodology - GSP R&D Study (1/2)

Background

- Traditional handbook-based RP methods (e.g. Mil-Hdbk-217, still the most widely used) have limitations with regards to obsolescence of its part type failure rate models, technology evolution and data base incompleteness. A significant amount of in-orbit anomalies due to non random failures are not covered (e.g. design and/or manufacturing related failures).

- Actual in-orbit performances have often shown that RP with current tools/methods/data sources are largely conservative, hence suggesting potential over-design, and reduced performance and cost effectiveness.

Objective

- Develop a new reliability prediction methodology for space systems to overcome the inherent limitations of the prediction practices currently based on outdated or limited handbooks.
3. New Reliability Prediction Methodology  
- GSP R&D Study (2/2)

**Technical description**

- Assess RP applications, identify reference missions and in-orbit reliability data
- Benchmark current RP with field reliability estimates, identify needs and define improvement strategy covering e.g. development process, technology evolution etc.
- Update existing / develop new RP models, incl. non-electronic part models, combining test and/or in-orbit experience and consider non-part related failure causes
- Validate for an actual project to demonstrate feasibility and practicality
- Develop a new Reliability Prediction Methodology Handbook as input to ECSS development process.
3. New Reliability Prediction Methodology
   - Topics to Be Addressed Include

   • Industry “best practices” e.g. potential adaptation of ICs reliability modelling
   • Mixing most widely used RP models and extrapolation based on experiences / “engineering judgment”
   • RP of COTS and comparison of RP results
   • Actual root causes for predicted vs achieved reliability differences
   • Systematic / Non part failures modeling including uncertainties (i.e. manufacturing, design, software etc)
   • Complex ICs modelling and emerging new technology challenges (e.g. DSM)
   • Appropriate Physics of Failure methods (PoF) (e.g. from PCB/package to component level)
   • Suitable Life Testing methods for predictions (e.g. at appropriate level)
3. Suggested Expedients to Achieve Study Objectives

- **Consensus based approach** to RP methodology improvements from all interested parties, including LSIs, SME, Suppliers, Customers

- **Cooperative efforts** on common goals and adequate coordination to provide the technical / academic knowledge (Industry, Universities etc) and to harmonize new reliability practices

- **Shared experiences and lessons learned** on successful reliability methodologies within space industry, as well as non-space

- **Address confidentiality issues / proprietary info** for utilization of test data, field / in-orbit feedback and info on failure mechanisms.
3. Expectations and Benefits

- Allow evaluation of the conservativeness of design margins with respect to cost savings opportunities and enable design-to-cost despite the increase of complexity.

- Enhance modeling capability to accomplish continued improvement in reliability performances.

- Ensure credibility, consistency and repeatability for reliability prediction estimations to support the analysis of alternative design solutions and verification approaches.

- Pragmatic approach, given limited R&D budget, practical applicability rather than only academic achievement.
C2: Activities in open competition, where a significant participation of non-LSIs is requested

- The C2 measure requires having a significant participation of non-Large System Integrators ("LSI") economic operators. This measure aims at an enhanced cooperation between LSI and equipment suppliers, SME and R&D institutions (including universities);
- The C2 measure was selected to ensure the fair allocation of activities among the economic operators;
- The C2 measure is proposed when the technology activity is such that Large System Integrators can bring key competences (system view);
- The C2 measure allows all potential bidders, LSIs and non-LSI to submit tenders. However, LSIs that submit tenders are requested to include in those tenders a relevant participation of non-LSIs, in quality and quantity;
3. Procurement approach – Open Competition with C-2 Industrial Policy requirements (2/2)

- The C2 measure constitutes one of the Key Acceptance Factor (KAF). Bidder shall explicitly confirm in the cover letter that the participation of non LSI economic operator(s) is significant and indicate the reference of the section(s) of the tender where the corresponding justifications can be found;
- Failure to meet the C2 measure results in the non admissibility of the Tender for evaluation;
- Currently the following economic operators are considered as being LSI:
  - Airbus Defence and Space SAS
  - Airbus DS GmbH
  - Airbus Defence and Space Limited
  - Thales Alenia Space France SAS
  - Thales Alenia Space Italia Spa
  - OHB systems AG.”
3. Procurement Policy: Competitive Tender - C2
Justification

The new methodology entails innovative physical and mathematical approaches, which requires **advanced scientific knowledge**.

- Participation of Companies with the required capability to develop out-of-the-box thinking, such as research institutes or universities, with the ability to investigate new methodologies and to explore innovative solutions for achieving the R&D objectives.

Reliability predictions are normally performed by industry through the various levels of the contractual chain, i.e. at system level by main system integrators while at equipment level by lower tier contractors. It is considered fundamental for the new methodology to be **based on the industrial experience and knowledge**.

- Participation of large- and medium-system integrators, as well as the involvement of lower-tier companies, is considered instrumental for the acquisition of the required technical and industrial expertise to respond to the specific R&D needs.

- In order to facilitate its smooth implementation by future space projects a **wide participation of all tiers** involved in space projects would be beneficial.
4. Conclusions
4. Conclusions

- ESA projects rely on consolidated reliability assurance processes, proven methodologies and standards. ESA Reliability Initiative aims to enhance Reliability assurance capabilities and to continue advancing Reliability methods according to technology evolution.

- Key areas for improvements are identified and some progress already anticipated through the recently completed or on going R&D study contracts. However, more efforts are needed e.g. improving the reliability requirements specification process and reinforcing the evaluation of Supplier’s capability to implement effective practices for product reliability.

- In particular, a major advancement is expected with the current “New Reliability Prediction Methodology” GSP study to contribute to the sustainability and affordability of future space systems within highly competitive markets.

- Cooperation between ESA, Industry and Agencies on a continual basis is a key element to promote with full consensus their efficient application in supporting Projects.
Contact Points

Technical Officer (TO):
Luigi.Bianchi@esa.int

Contract Officer (CO):
Patryk.Strzelecki@esa.int
5. Q&A Session

Thank you!
Back up slides

Luigi Bianchi

22/04/2016
Quantitative RAMS Requirements for Space Applications

**Objective**
- To develop a process of establishing systematically, consistently and traceable the quantitative reliability, availability and maintainability requirements to be applied to ESA programs.

**Main Steps**
- Identification of relevant, realistic and achievable quantitative RAMS requirements that could be applied to future ESA space programs.
- Elaboration of a methodology allowing to define quantitative RAMS requirements for mission success and safety and flow down of these requirements from system to the subsystems and unit level, depending on defined characteristics of ESA space programs.

**Outcome**
- Five classes of ESA space programmes have been defined, each being subdivided in three categories.
- Identified quantitative RAMS requirements have been mapped to the space programme classes and categories.

⇒ The developed approach needs to be mapped into project usable guidelines for application.
Concept Definition and Demonstration of RAMS In-Orbit Data Utilisation (RIDE2)

**Objective**

- To create a proof of concept demonstrator of a tool for RAMS exploitation of in-orbit data, whose concept was developed in a proceeding RIDE 1 study.

**Main Steps**

- Consolidation of user needs, RAMS characteristics and related input data
- Detailed of interfacing data sources and systems
- Development and test of the demonstrator

**Outcome**

- The feasibility to implement a RAMS exploitation system for in-orbit data interfacing with and maximizing the use of existing data repositories and tools already available was demonstrated.
- A suitable concept of an operational RIDE tool was developed.
Reliability Model Supporting Satellite Life Extension or Disposal Initiation Decisions

**Objectives**

- The primary objective of this study is to develop a *spacecraft reliability degradation model* and identify its required inputs to enable quantitative risk based decision-making on satellite life extension or safe disposal.
- The reliability degradation model is to be used mainly during the operational phase of the mission but may also support decision-making after long term storage.
- In addition, a *suitable criteria* with appropriate justification shall be identified to support de-orbit decisions at the end of the nominal mission duration (end-of-life) or during the nominal mission following failures which lead to loss of redundancy of critical functions.

**Status**

ITT to be released in Q2/2016

**Expected benefits**

Minimise risk of space debris generation
Maximise return of investment by enabling safe mission extensions
System Level Integrated Failure Analysis (IFA)

Background and justification: Dependability and Safety are major drivers for system design, operations and project organization. D&S analyses involve deterministic and probabilistic modelling of associated hazard and failure scenarios, which reflect the expected system behavior with undesirable system consequences. The current D&S analysis methods as used on ESA projects do not allow to model interactive failures in increasingly complex technical systems (hardware, software, human) and organizational failures (errors or flaws in the organization and associated processes).

Objective: An advanced approach to system safety & dependability and technical risk assessment, based on innovative dependability methods to perform an integrated analysis of failures or errors of human operators, systems and organization during space operations. The approach integrates techniques from dependable computing and user-centered design in order to improve the reliability of interactive systems.

Achievements:
- Extension of advanced dependability methods (i.e. HEECA)
- Proposition of unified templates to guide the method application
- Application of the proposal to simplified case studies
- Use of existing models and tools to prototype the concept

Benefits:
- Enables assessing the recovery costs from system failures as well as from HE in terms of corrective actions
- Identifies opportunities for re-designing system and operations
- Supports the traceability of needs / requirements for operators’ training purposes
- Supports sharing information about risk analysis across several domains

Next step: Follow up with application and capitalization of the results on a more integrated case study to reach TRL 3-4. Design of an evaluation platform available for ESA stakeholders. In particular: -) Wide scope covered, although need to consolidate/extend the analysis for the human & organization case -) Tools mandatory for full exploitation, need to review existing software to identify solutions / gaps for more effective deployment of the method -) Validation of concepts on a larger case study, with more integrated inputs.
**Objective**

Elaborate a catalogue of failure data to support safety and dependability analyses of space systems

**Current status and benefits**

1\textsuperscript{st} version completed in 2011 and used by industry (such as Airbus). A new extended version is under development and to be completed in 2016

Free download of catalogue at:  
www.cfda.info
Reliability of Mechanical Systems & Parts

Objective

• Define the most suitable methods to analyse and assess reliability of mechanical systems and parts and provide methods and procedures for reliability verification by testing

Main Steps

• Analysis and assessment of existing reliability approaches.
• Development of new reliability assessment approaches of mechanical parts and system
• Application to a study cases (still on-going)

Outcome

• Structural reliability theory for reliability modelling based on the relevant failure mechanisms is the most suited alternative reliability assessment approach
• Development of a simplified part-level reliability assessment approach for extensive use
• Development of reliability estimates update methods through Bayesian approach when test or field data become available
Reliability Prediction Data Sources and Methodologies for Space Applications

**Objective**
- Propose alternatives for EEE and mechanical parts among the available data sources (FIDES, UTE 80810, 217plus, NPRD, etc.) evaluating their suitability for space application
- Propose methodologies to assess reliability at system, subsystem, and unit levels to perform more accurate forecasts of the actual field reliability
- Inputs for the update of the ECSS-Q-HB-30-08

**Main Steps**
- Review of current practices in the reliability prediction for space missions and programmes and in non-space domains.
- Analysis of the selected data sources in details (models and parameters of each kind of EEE and mechanical parts)
- Identification and assessment of reliability prediction methodologies for systems
- Application to study cases (still on-going)

**Outcome**
- Most suited data sources for reliability prediction in space domain: MIL-217, FIDES and 217Plus for EEE parts and NSWC 2011 and NPRD 2011 for mechanical parts
- FIDES is a good substitute for almost all EEE part failure rate models in terms of representativity (technology and reliability influencing factors) and accuracy (ratio between predicted and observed reliability <= 2, while 5 with MIL-217)