

# REFARCH: Reference Architecture for High Dependability On-Board Computers

Nuno Silva, Alexandre Esper, Ricardo Barbosa, Critical Software SA

Johan Zandin, RUAG Space AB

Claudio Monteleone, European Space Agency, ESTEC

12/12/2013

# Agenda

---

1. Introduction
2. On-Board Computers Generic Requirements
3. On-Board Computers Dependability Planning
  - Life Cycle Model for On-Board Computers
  - OBC Dependability Approach
4. On-Board Computers Dependability Measurement
  - Reliability Analysis Methodology
    - HW Reliability
    - SW Reliability
5. On-Board Computers Dependability Assurance
  - Contribution of Computer-Aided Environment to OBC Dependability Assurance
6. Feasibility Discussion
7. Application Study
8. Conclusions and Future Work

# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 1. Introduction

# 1. Introduction

---

- Harmonisation policy of ESA:
  - Deployment of enhanced and homogeneous industrial processes in the area of avionics embedded systems and on-board computers for the space industry

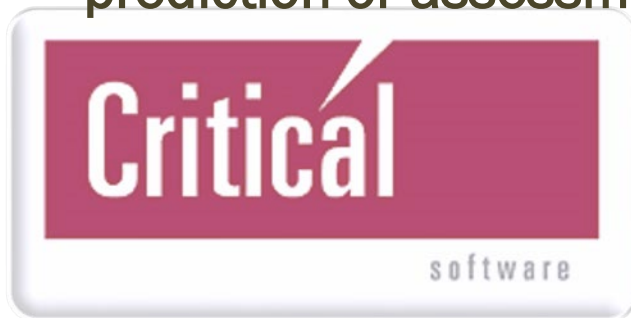


- SAVOIR:
  - Federate initiatives towards avionics standardization and innovation and to help concentrate all the efforts from industry, national agencies and ESA towards the shared objectives.

## 2. Introduction



- Establishing generic requirements for the procurement or development of on-board computers with a focus on well-defined reliability, availability, and maintainability requirements
- Studying means and providing recommendations to support the association of dependability figures to on-board computer configuration items throughout their life cycle (e.g. for allocation, prediction or assessment of dependability)



# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 2. On-Board Computers Generic Requirements

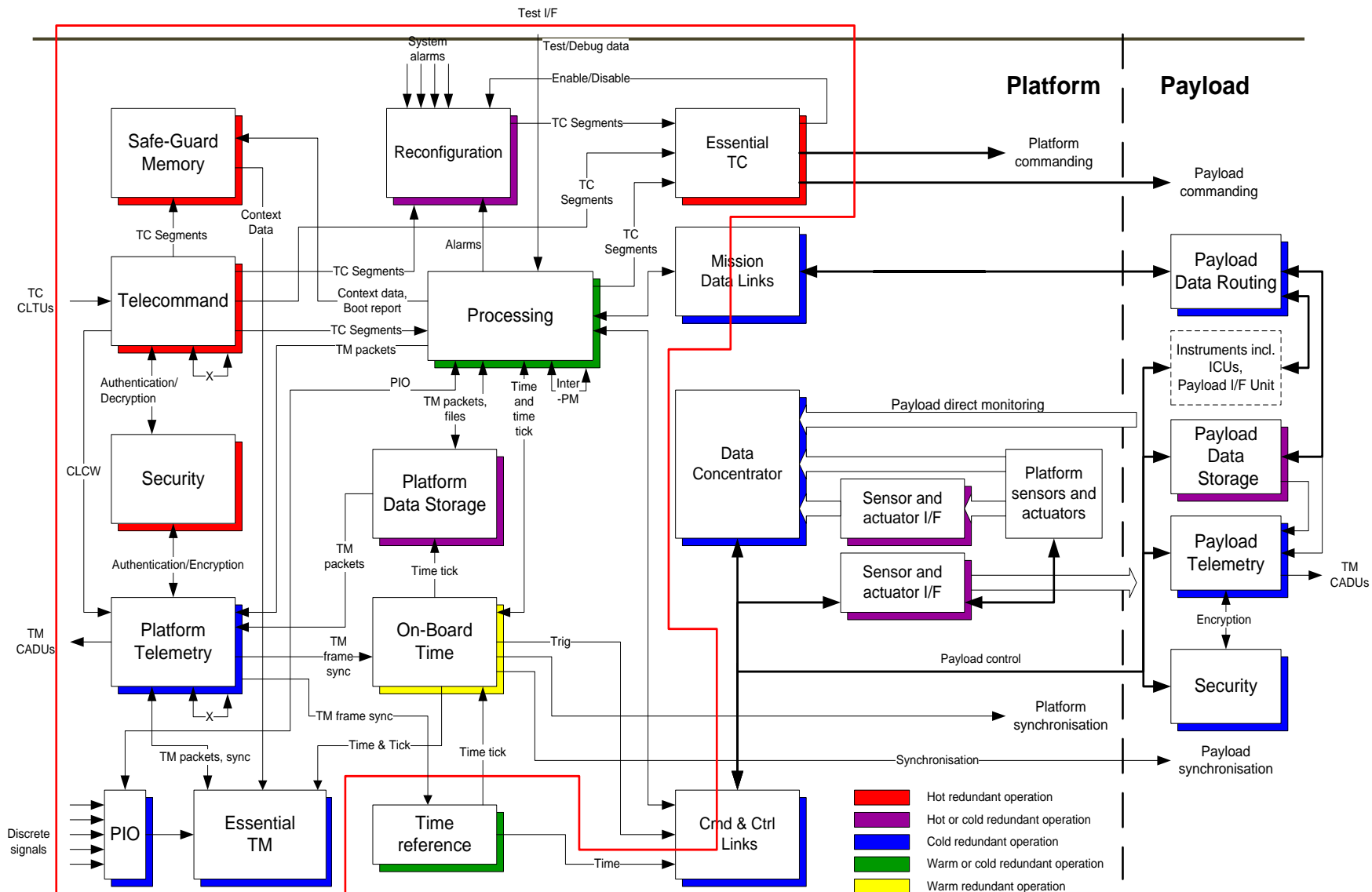
## 2. On-Board Computers Generic Requirements

---

- Generic enough to be applicable for a typical onboard computer (OBC):
  - Science and an earth observation missions
  - Telecom missions
  - Commercial earth observation missions
    - Excluded: manned missions and launchers
- Relevant for the REFARCH study, e.g. identifying a major function of the OBC or specifying details that have a particular impact on reliability and/or availability.




# 2. On-Board Computers Generic Requirements





## 2. On-Board Computers Generic Requirements

---

- REFARCH requirements cover several functionalities
    - TC decoding and distribution
    - TC and TM security
    - TM collection, formatting and coding
    - Essential TC
    - Mass Memory for storage of data, e.g. TM
    - On-Board Time counting and distribution
    - Application software execution platform (=processing)
    - Communication links to platform and payload equipment
    - Discrete interface communication to platform and payload equipment
    - FDIR function
    - Safeguard memory
    - Essential TM
    - Reconfiguration function
    - Power supply
- 

## 2. On-Board Computers Generic Requirements

- REFARCH functional aspects – tailoring of SAVOIR spec

Aspects Covered	Description
Functional requirements	Provided capabilities, Commandability, Observability, Criteria for failure.
Interface requirements	External interfaces, Physical dimensions, Physical mass, Input voltage, Power consumption.
Operational requirements	Thermal environment, Radiation environment, Vibration and Shock resistance, Operational modes, Limitations.
Performance requirements	Response time, Throughput, Start-up time.
Dependability requirements	Lifetime, Reliability, Availability, Maintainability.
Design Requirements	Redundancy, Resource utilisation, Internal interfaces, Development process.

## 2. On-Board Computers Generic Requirements

- REFARCH functionalities and redundancy type

Functions	Redundancy Type
Processing	Warm or cold redundant
On-Board Time Management	Warm redundant
Platform Data Storage	Hot or Cold redundant
Command & Control Link	Cold redundant
Mission Data Links	Cold redundant
Safe Guard Memory	Hot redundant
Essential TM	Cold redundant
Essential TC	Hot redundant
Parallel IO	Cold redundant
Reconfiguration Module	Hot or Cold redundant
Power Supply	Hot redundant

## 2. On-Board Computers Generic Requirements

- REFARCH requirements - Packet Telecommand Handling

Requirement ID	Description
TC.10	<p><b>Number of TC Decoders</b></p> <p>The OBC shall provide two TC decoders operating in hot redundancy.</p> <p><i>Requirement Rationale:</i> It shall be possible to send data to any TC decoder chain from ground without knowing the spacecraft configuration. At least two are needed to avoid single point of failure. Additional ones operating in cold redundancy are allowed.</p>
TC.60	<p><b>TC Segment Distribution</b></p> <p>The decoded TC segments shall be distributed to Essential TC (CPDU) or Currently Active PM.</p>
TC.70	<p><b>TC Decoder Telemetry Output</b></p> <p>Each TC decoder shall provide its status for inclusion in the TM downlink.</p>
TC.100	<p><b>TC Decoder Input Configuration</b></p> <p>Each TC Decoder shall receive telecommand data on &lt;TC_INPUTS&gt; inputs, of which one is dedicated to the EGSE.</p> <p><i>Requirement Rationale:</i> Typical values: 3 if option TC X-strap = No, 5 if option TC X-strap = Yes.</p>

## 2. On-Board Computers Generic Requirements

- REFARCH requirements - Platform TM Encoder

Requirement ID	Description
TM.10	<p><b>Number of Platform TM Encoders</b></p> <p>The OBC shall provide two Platform TM Encoders operating in cold redundancy.</p> <p><i>Requirement Rationale:</i> At least two are needed to avoid single point of failure. Additional ones operating in cold redundancy are allowed. The TM protocol is not suitable for running in warm or hot redundancy.</p>
TM.30	<p><b>Platform TM Encoder In-flight Programming</b></p> <p>It shall be possible to change parameters of the active Platform TM Encoder.</p> <p><i>Requirement Rationale:</i> Different mission phases may require different telemetry settings</p>
TM.40	<p><b>Selecting Active Platform TM Encoder</b></p> <p>It shall be possible to select the Active Platform TM Encoder in at least one of the following ways:</p> <ul style="list-style-type: none"><li>• via CPDU Command</li><li>• via ASW</li></ul> <p><i>Requirement Rationale:</i> Both concepts are used by current hardware.</p>
TM.70	<p><b>Number of Virtual Channels</b></p> <p>The Active Platform TM Encoder shall provide up to 8 Virtual Channels.</p>

## REFARCH: Reference Architecture for High Dependability On-Board Computers

### 3. On-Board Computers Dependability Planning

- Life Cycle Model for On-Board Computers
- OBC Dependability Approach

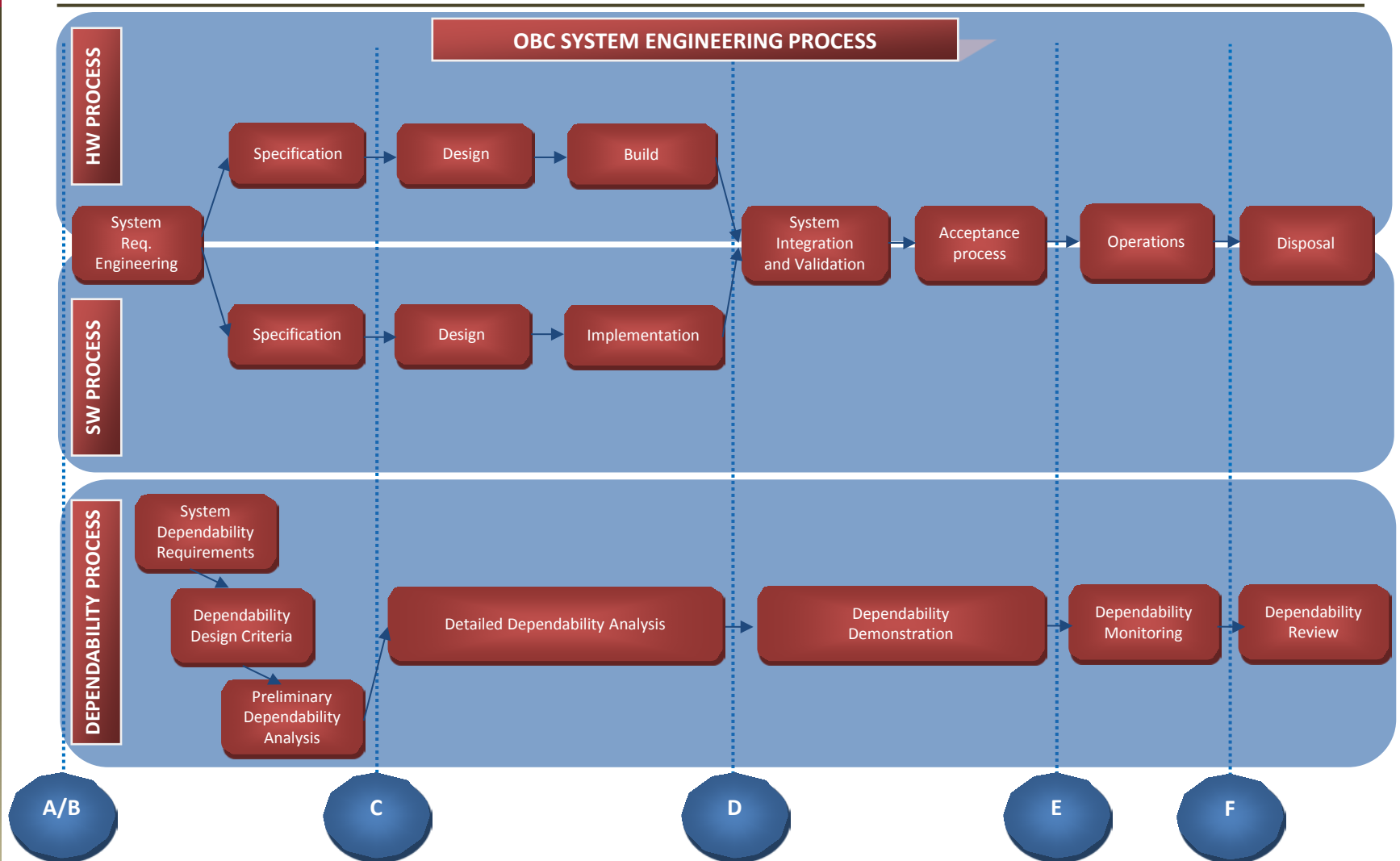
# 3. On-Board Computers Dependability Planning

---

## REFARCH Dependability Plan High Level Structure

- Definition of a lifecycle model of OBC which covers both HW and SW
- Process descriptions:
  - Description of the OBC (lifecycle) process - purpose and set of outcomes
  - Detailed description of the dependability tasks applicable to each phase of the OBC lifecycle
  - Rough order of magnitude estimation of the needed resources for each task per phase of the OBC lifecycle (e.g. facilities, models, amount of work, applicable techniques)
- Description of the dependability organization and management.
- Description of the configuration item levels to which the dependability tasks are applicable.

# 3. On-Board Computers Dependability Planning





# 3. On-Board Computers Dependability Planning

- HW process activities description

Activity	Description
Definition Phase	<ul style="list-style-type: none"><li>- Establishment of the hardware items requirements</li><li>- Ensure the consistency of the requirements with the design implementation, the system and software requirements</li></ul>
Architectural Design	<ul style="list-style-type: none"><li>- Produces a high-level architecture design<ul style="list-style-type: none"><li>- e.g. functional block diagrams, architectural descriptions, assembly outlines, and chassis sketches</li></ul></li><li>- Allows the assessment of the design feasibility, i.e. its potential to meet the requirements</li></ul>
Detailed Design	<ul style="list-style-type: none"><li>- Produces detailed design data using the hardware item requirements and conceptual design data as the basis for the detailed design</li></ul>
Layout	<ul style="list-style-type: none"><li>- Generate the complete hardware layout of electrical and mechanical items in preparation for the prototype production</li></ul>
Prototype implementation	<ul style="list-style-type: none"><li>- Production and delivery of the committed number of prototypes prior to the Flight Module (FM), so that the design validation can be performed</li></ul>
Design validation and release	<ul style="list-style-type: none"><li>- Confirm the achievement of all OBC functional, performance, interface and compatibility requirements</li></ul>

# 3. On-Board Computers Dependability Planning

- SW process activities description

Activity	Description
SW System requirements specification	- Establishment of the software functional and performance requirements baseline (including interface requirement specification) (RB) of the software development
Requirements & architecture engineering	- Elaboration of the technical specification, including the preliminary definition of the software ICD (TS), and the architectural design document
Design and implementation engineering	- Detailed design of the software items identified in the software product tree
Validation	- Software product testing against both technical specification and the requirements baseline
Verification	- Confirm that adequate specifications and inputs exist for every activity - Confirm that the outputs of the activities are correct and consistent with the specifications and inputs
Delivery and acceptance	- Prepare the software product for delivery and testing in its operational environment (as specified in the RB).

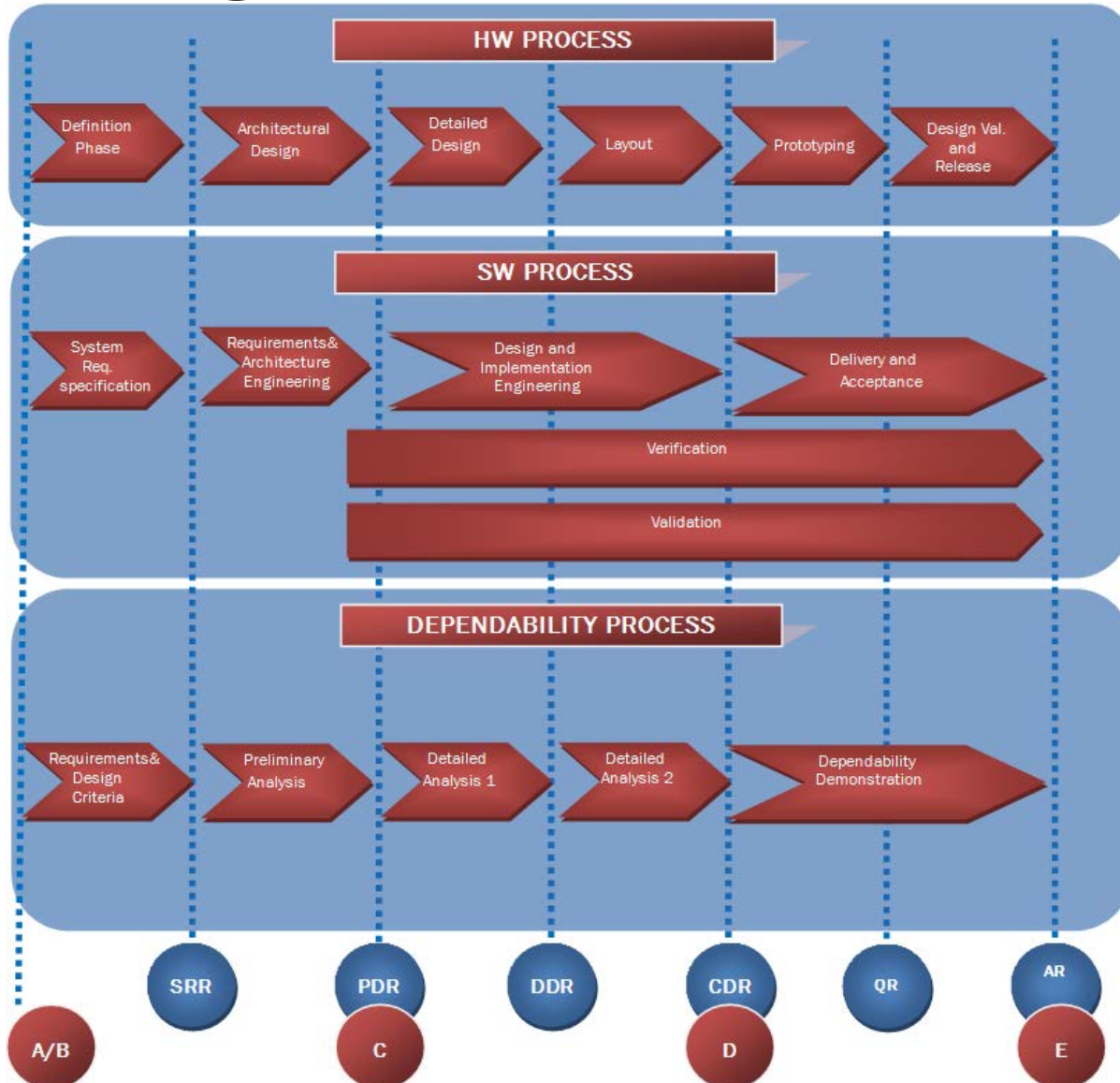
# 3. On-Board Computers Dependability Planning

## ■ OBC Dependability Approach

Task	Description
1	Establishment of dependability requirements
2	Establishment of dependability design criteria: <ul style="list-style-type: none"><li>• Severity Classification</li><li>• Failure Tolerance</li><li>• Design approach (functional and physical)</li></ul>
3	Preliminary dependability analysis: <ul style="list-style-type: none"><li>• Identification of undesired events</li><li>• Preliminary classification of critical items</li></ul>

Task	Description
4	Detailed dependability analyses <ul style="list-style-type: none"><li>• Dependability method selection (data sources, technique, tools)</li><li>• Reliability Analyses (modeling, allocation, prediction)</li><li>• Maintainability Analyses</li><li>• Availability Analysis</li><li>• Dependability critical items list</li><li>• Dependability recommendations</li><li>• Implementation of recommendations</li></ul>
5	Dependability demonstration
6	Dependability monitoring & review

# 3. On-Board Computers Dependability Planning



# 3. On-Board Computers Dependability Planning

## ■ OBC Dependability Activities

Activity	Description
Establishment of dependability requirements	<ul style="list-style-type: none"> <li>-Included into the technical specifications</li> <li>- Then applied during the preparation and review of the design and test specifications</li> </ul>
Establishment of dependability design criteria	Criteria based on: <ul style="list-style-type: none"> <li>• Severity classification</li> <li>• Failure tolerance</li> <li>• Design approach</li> </ul>
Preliminary Analysis	Performed very early in the lifecycle to support the definition of the conceptual design and the system and software requirements: <ul style="list-style-type: none"> <li>• Identification of undesired events</li> <li>• Preliminary classification of critical items</li> </ul>
Detailed Dependability Analyses Phase 1	<ul style="list-style-type: none"> <li>- Main output : updated Dependability Analysis Report (DDR)</li> <li>- Main topics covered (subsections):               <ul style="list-style-type: none"> <li>• Reliability Analysis                   <ul style="list-style-type: none"> <li>○ Selection of Reliability Data Sources and Methods</li> <li>○ FMEA/FMECA</li> <li>○ Reliability Prediction</li> </ul> </li> <li>• Maintainability Analyses</li> <li>• Availability Analysis</li> <li>• Dependability Critical Items List (CIL)</li> <li>• Dependability Recommendations</li> <li>• Implementation of Recommendations</li> </ul> </li> </ul>

# 3. On-Board Computers Dependability Planning

## ■ OBC Dependability Activities

Activity	Description
Detailed Dependability Analyses Phase 2	Main activity : <ul style="list-style-type: none"> <li>• verify that the proposed recommendations and new derived requirements from Phase 1 have been incorporated into the design and are properly covered by validation tests.</li> </ul>
Dependability demonstration	Validation and/or production of dependability evidence material and data collection: <ul style="list-style-type: none"> <li>• <b>Reliability demonstration</b> <ul style="list-style-type: none"> <li>○ Validate the capability of the hardware to operate with software in accordance with the specifications;</li> <li>○ Validate failure modes and effects;</li> <li>○ Check failure tolerance, failure detection and recovery;</li> <li>○ Validate the justification for the selected data bases used for theoretical demonstrations.</li> <li>○ Demonstrate the reliability of critical items;</li> <li>○ Obtain statistical failure data to support predictions and risk assessment;</li> <li>○ Consolidate reliability assessments;</li> </ul> </li> <li>• <b>Availability demonstration</b> <ul style="list-style-type: none"> <li>○ Validate results of availability analysis or simulations;</li> <li>○ Validate the list of potential outages and their cause;</li> <li>○ Validate RM performance test results for outage detection and recovery;</li> </ul> </li> <li>• <b>Maintainability demonstration</b> <ul style="list-style-type: none"> <li>○ Detect, diagnose and isolate faulty OBC units;</li> <li>○ Check that the OBC is fully functional after the completion of maintenance actions;</li> <li>○ Demonstrate that the maintenance operations can be performed within the applicable constraints, including the operations necessary to prepare the OBC during the launch campaign.</li> </ul> </li> </ul>

# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 4. On-Board Computers Dependability Measurement

- Reliability Analysis Methodology

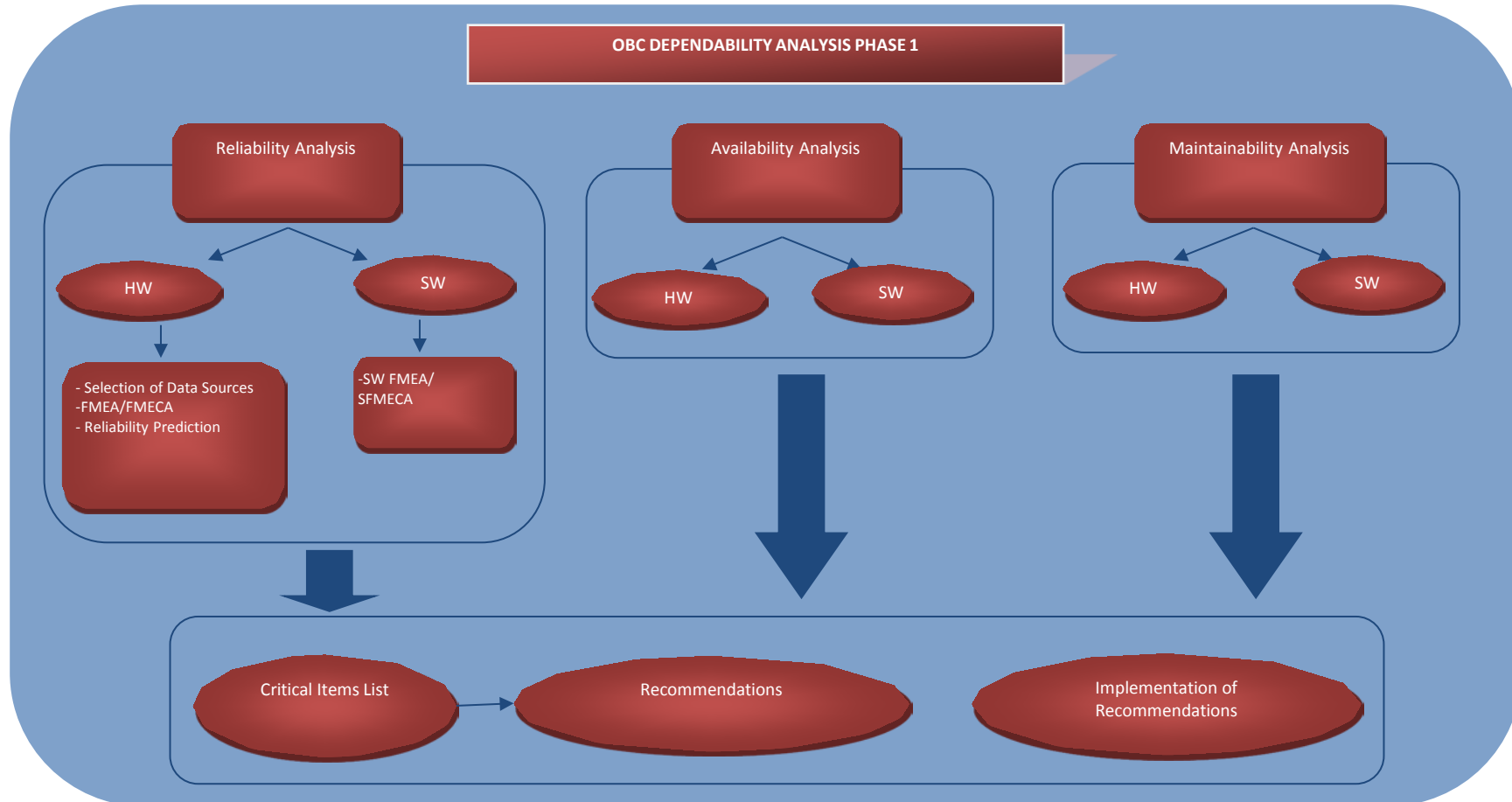
# 4. On-Board Computers Dependability Measurement

---

- Objective:
  - Provide a set of guidelines about associating dependability figures to computer configuration items throughout their life cycle
- HW and SW reliability analysis are ideally performed in parallel flows
- The HW analysis is mainly quantitative, with the support of some qualitative analysis to ensure the feasibility of the analysis and the consistency of the results
- For SW only a qualitative reliability analysis is recommended (and realistic)

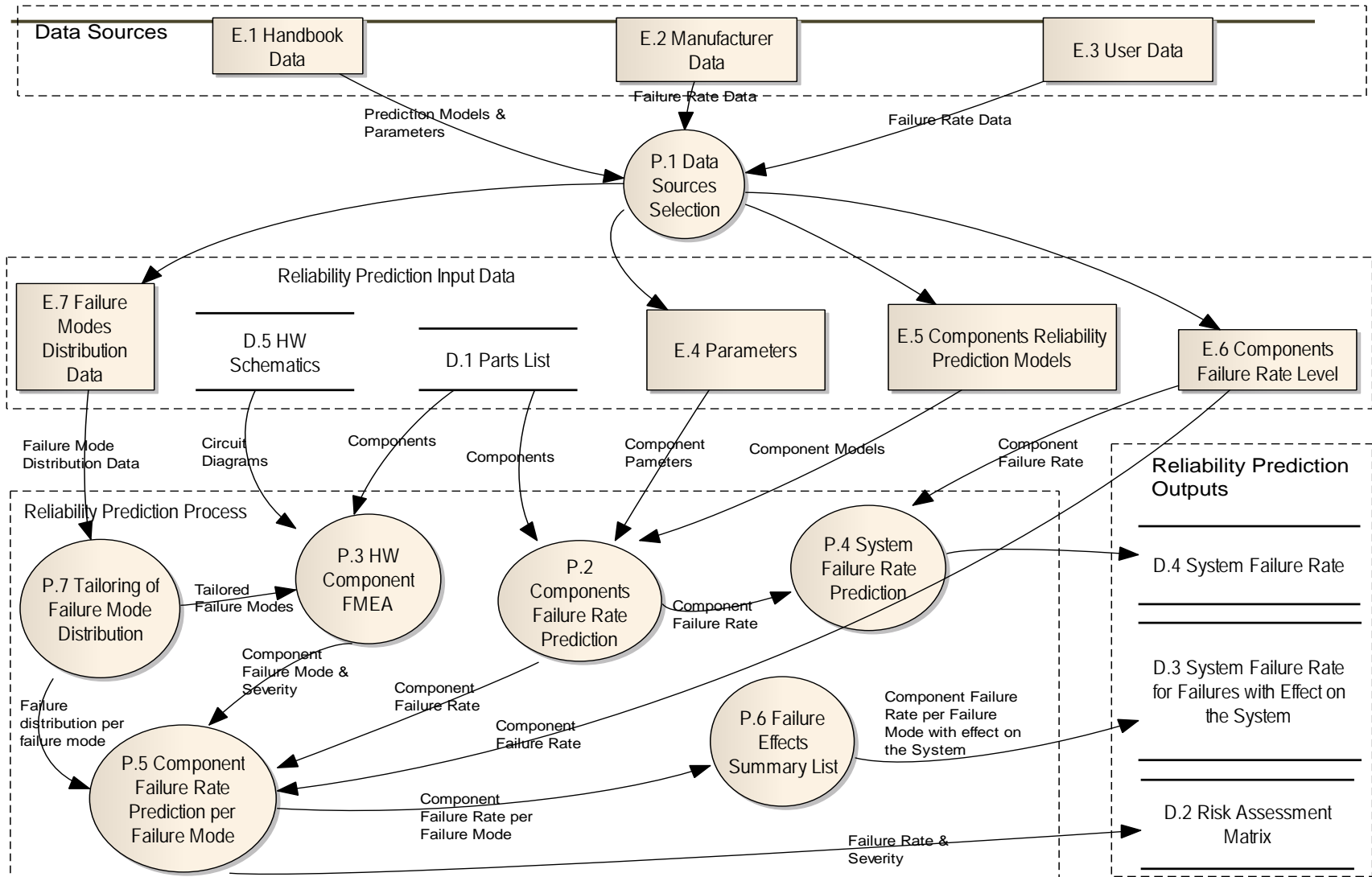


# 4. On-Board Computers Dependability Measurement



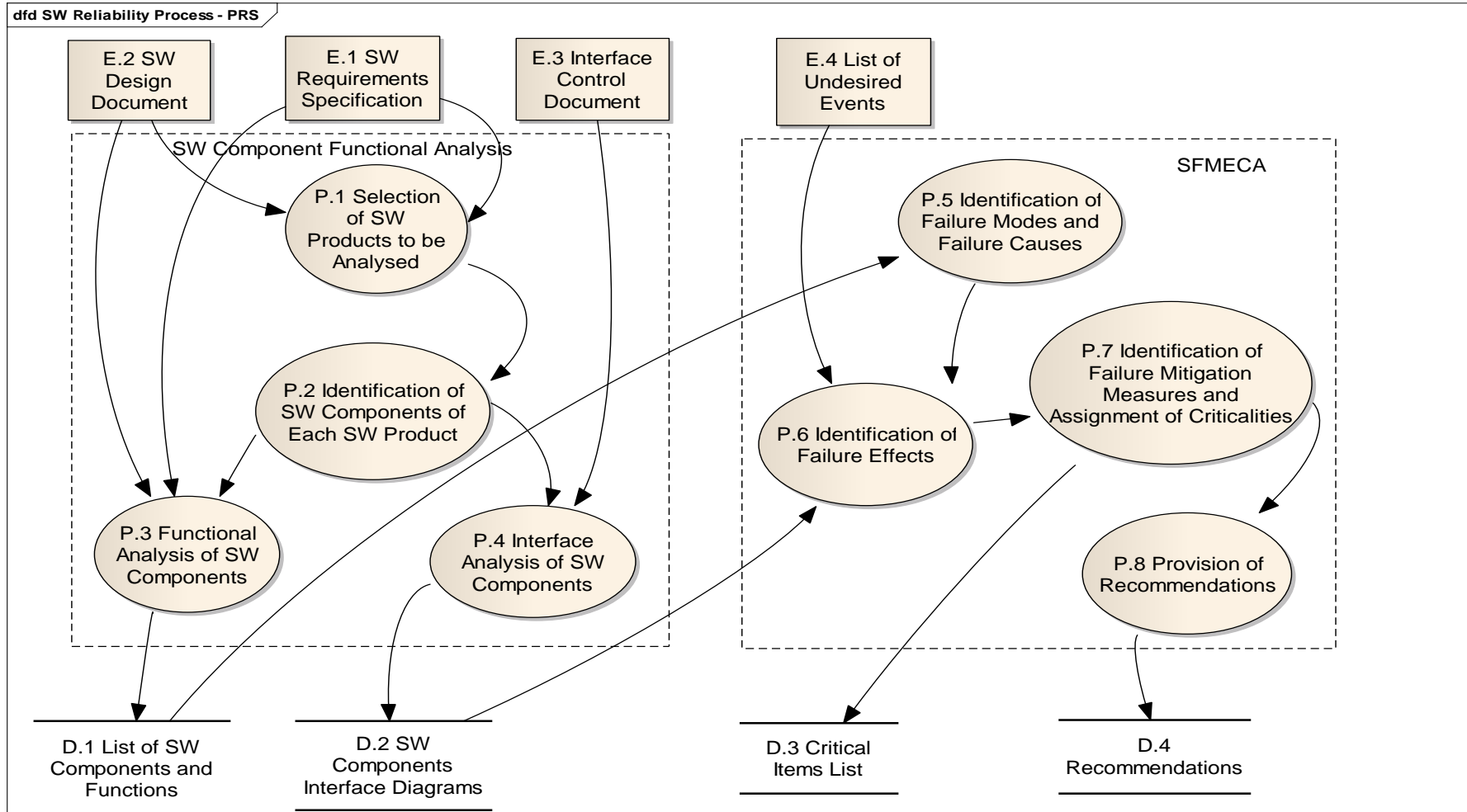
# 4. On-Board Computers Dependability Measurement

class HW Reliability Analysis - PRS



# 4. On-Board Computers Dependability Measurement

- SW Reliability Analysis Methodology



# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 5. On-Board Computers Dependability Assurance

- Activities
- Contribution of Computer-Aided Environment to OBC Dependability Assurance

# 5. On-Board Computers Dependability Assurance

Activity	Description of Items Verified
Requirements Dependability Assurance	<ul style="list-style-type: none"> <li>- Compliance with <u>reference requirements</u></li> <li>- <u>Requirements correctness</u> considering system requirements</li> </ul>
Design criteria dependability assurance	<ul style="list-style-type: none"> <li>- <u>Failure severity classification</u> is according to the specified values</li> <li>- Proven <u>HW design rules and methods</u> are used</li> </ul>
Preliminary dependability analysis assurance	<ul style="list-style-type: none"> <li>- <u>Undesired events</u> are identified and classified (HW/SW)</li> <li>- Preliminary FMEA performed at the right <u>level of functionality decomposition</u></li> </ul>
Detailed dependability analysis assurance	<ul style="list-style-type: none"> <li>- <u>Data source</u> is selected according to the defined process (in the case of HW)</li> <li>- <u>Documentation</u> is complete and has already reached a satisfactory level of maturity (in the case of SW)</li> </ul>

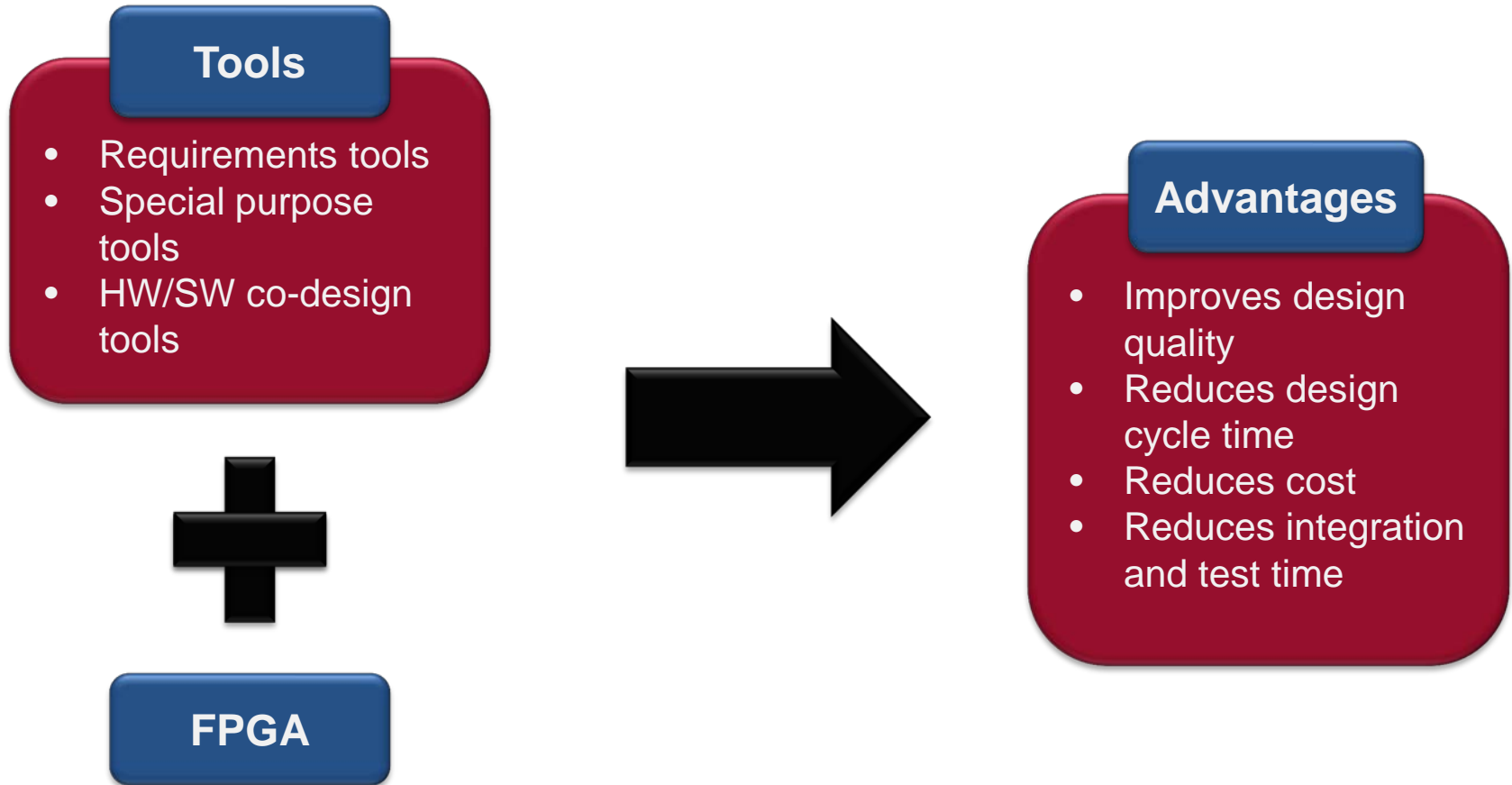
# 5. On-Board Computers Dependability Assurance

---

Activity	Description of Items Verified
Maintainability analysis assurance	<ul style="list-style-type: none"><li>- Correctness and completeness of <u>maintainability requirements</u></li><li>- Detailed analysis of the <u>FDIR strategy</u></li></ul>
Availability analysis assurance	<ul style="list-style-type: none"><li>- Completeness of the <u>list of potential outages</u></li><li>- Traceability of the <u>recommendations for the optimization of the system concept</u> to the associated system architectural and design items</li></ul>
Critical items list assurance	<ul style="list-style-type: none"><li>- Tailored criterion for identifying the OBC <u>dependability critical items</u> is defined and validated by all the project stakeholders</li><li>- Feasibility, effectiveness and verifiability of proposed <u>control measures</u></li></ul>
Recommendation list assurance	<ul style="list-style-type: none"><li>- <u>Recommendations</u> generated for each of the RAM analyses performed</li><li>- <u>Review of recommendations</u> by the HW and SW design teams for approval or rejection</li></ul>

# 5. On-Board Computers Dependability Assurance

- Contribution of Computer-Aided Environment to OBC Dependability Assurance



# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 6. Feasibility Discussion



# 6. Feasibility Discussion

---

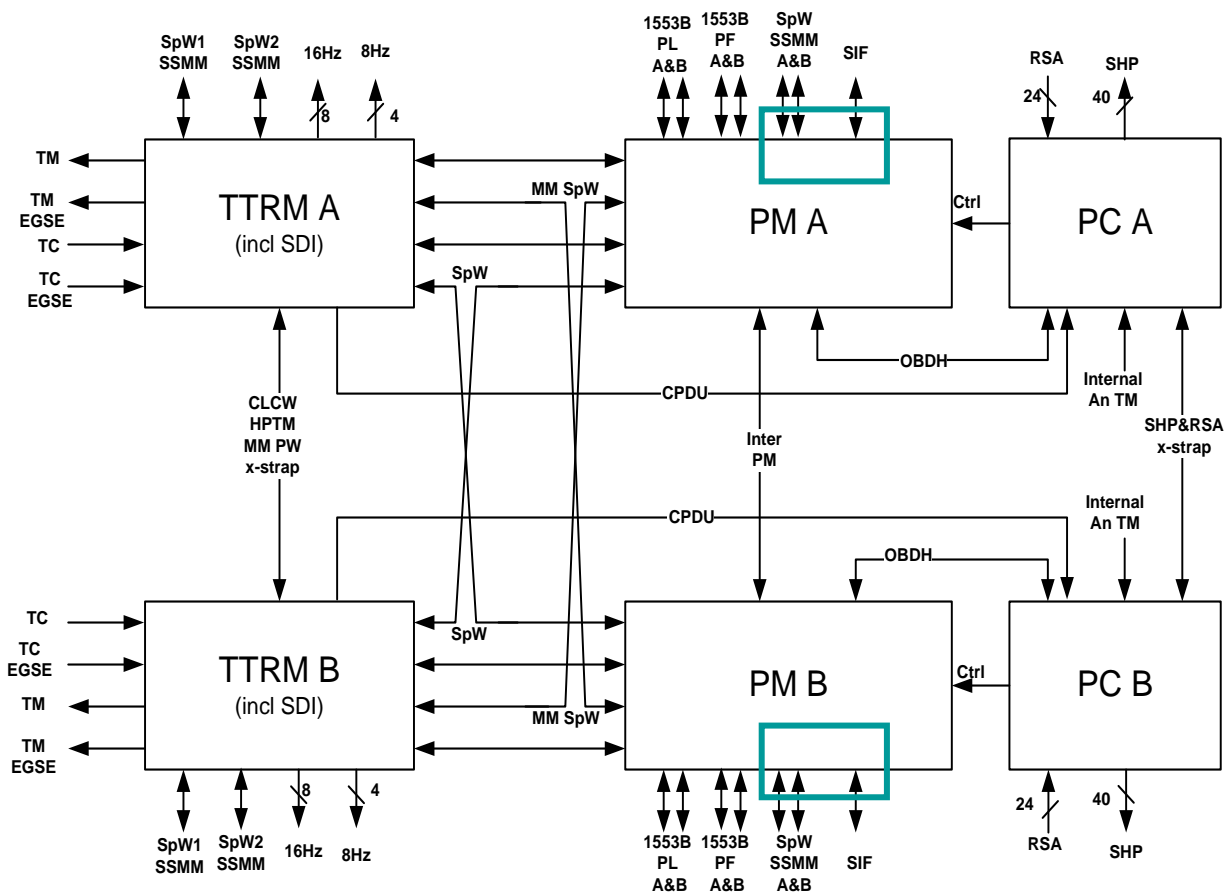
- **HW Reliability Analysis**
  - The overall logical flow of the methodology is feasible
  - Several aspects that need to be taken into consideration, such as the cost of the analyses
- **SW Reliability Analysis**
  - SW FMEA - overall methodology already demonstrated and refined along several ESA programs
  - Several aspects that need to be taken into consideration, such as the cost of the analyses
  - FMEA - can easily become a large burden on any project if the scope is not properly defined
- **Maintainability and Availability Analysis**
  - Methodology depends on the apportioned maintenance indicators (e.g. MTTR, MDT)
  - Derived and adapted to the OBC context based on known methodologies
  - No critical issue is foreseen that could compromise the feasibility of those analyses

# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 7. Application Case

# 7. Application Case

Solar Orbiter OBC: Fully redundant, 6 different boards, 2 x 3400 components.



# 7. Application Case

---

- **Component Reliability**
  - Import parts list, parts stress analysis etc. for all components
  - Calculate reliability with RIAC 217Plus
  - Compare with SOLO figures (MIL-HDBK-217F, RDF 2000 etc.)
- **Reliability and FMEA**
  - Select functional subset and corresponding components
  - Identify failure modes and effects on local/sub-system/system level
  - Calculate reliability per local and system effect
- **Defined redundancy model**
- **Calculate reliability for redundant OBC**

# 7. Application Case

---

- **Component Reliability Results**
  - Oscillators not supported → Update RIAC
  - High failure rates and low reliability (99 → 80% over lifetime)  
→ Must apply RIAC PGF (Process Grading Factors)
  - Low failure rates  
→ Consider e.g. RDF 2000 for PCB, ASIC, Memory, Connectors
  - Large variations → Select reliability model per component type
- **Reliability and FMEA**
  - ~2 failure modes per component, ~2 per pin for IC
  - Standard effect: Loss of one OBC function
  - Example: 23% of failure rate had no effect. Representative?
  - Worth the effort?

# REFARCH: Reference Architecture for High Dependability On-Board Computers

## 8. Conclusions and Future Work

# 7. Conclusions and Future Work

---

- The results of REFARCH study established:
  - Generic reference requirements for the development and procurement of onboard computers
  - Methodology for assessing the dependability of on-board computers throughout their lifecycle, including the discussion of several aspects related to the process feasibility
  - Tool and method feasible after identified improvements
- Future work:
  - Apply RIAC Process Grading Factors
  - Define appropriate reliability models per component type
  - Apply complete set of methods in a project under development



# Contacts

Critical

- Nuno Silva, [nsilva@criticalsoftware.com](mailto:nsilva@criticalsoftware.com)
- Alexandre Esper, [aresper@criticalsoftware.com](mailto:aresper@criticalsoftware.com)
- Ricardo Barbosa, [rbarbosa@criticalsoftware.com](mailto:rbarbosa@criticalsoftware.com)
- Johan Zandin, [johan.zandin@ruag.com](mailto:johan.zandin@ruag.com)
- Claudio Monteleone, [claudio.monteleone@esa.int](mailto:claudio.monteleone@esa.int)