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

22/10/2013

Dependable Technologies For Critical Systems

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. Conclusions and Future Work

REFARCH: Reference Architecture for High Dependability On-Board Computers

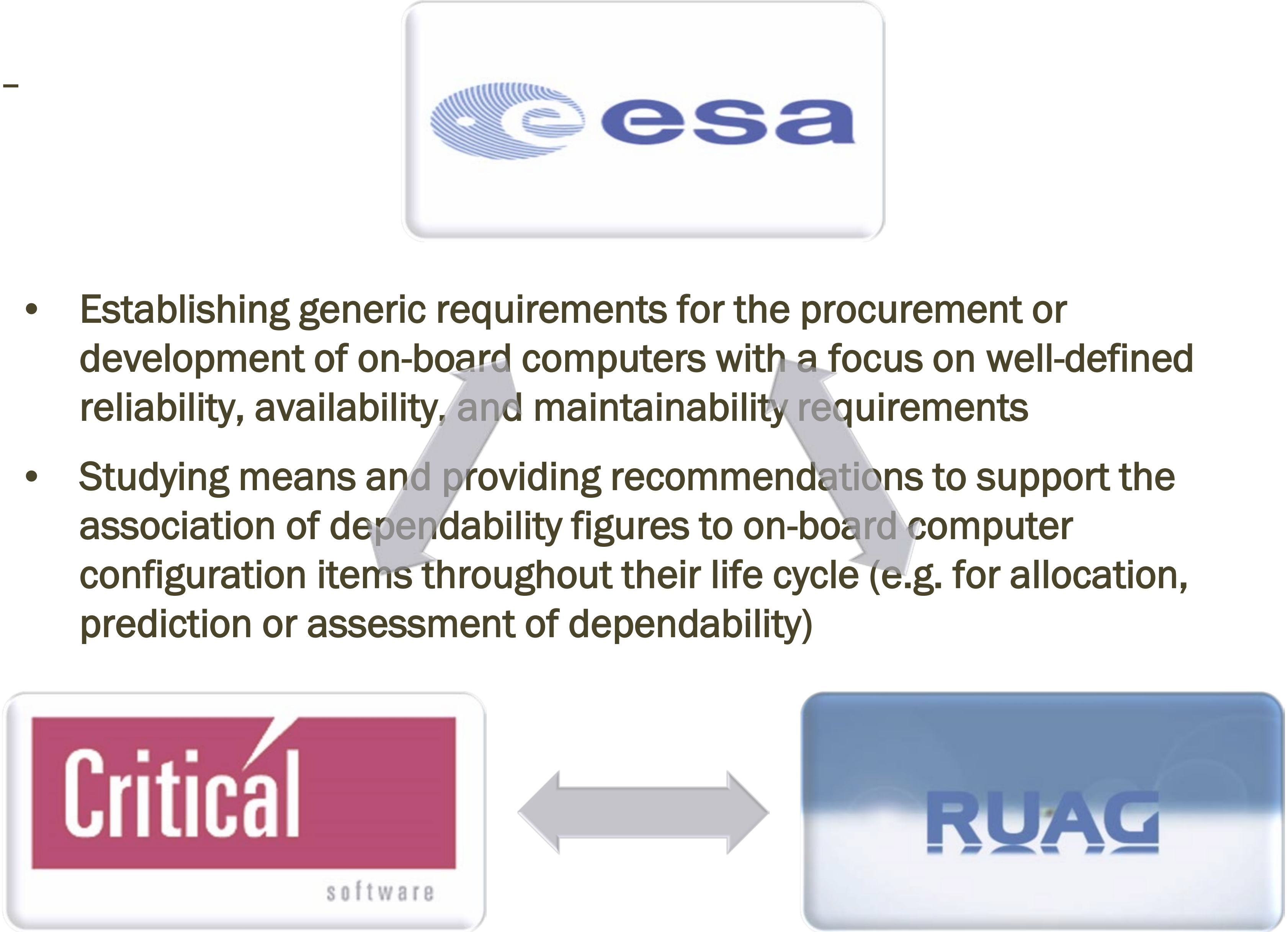
1. Introduction

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

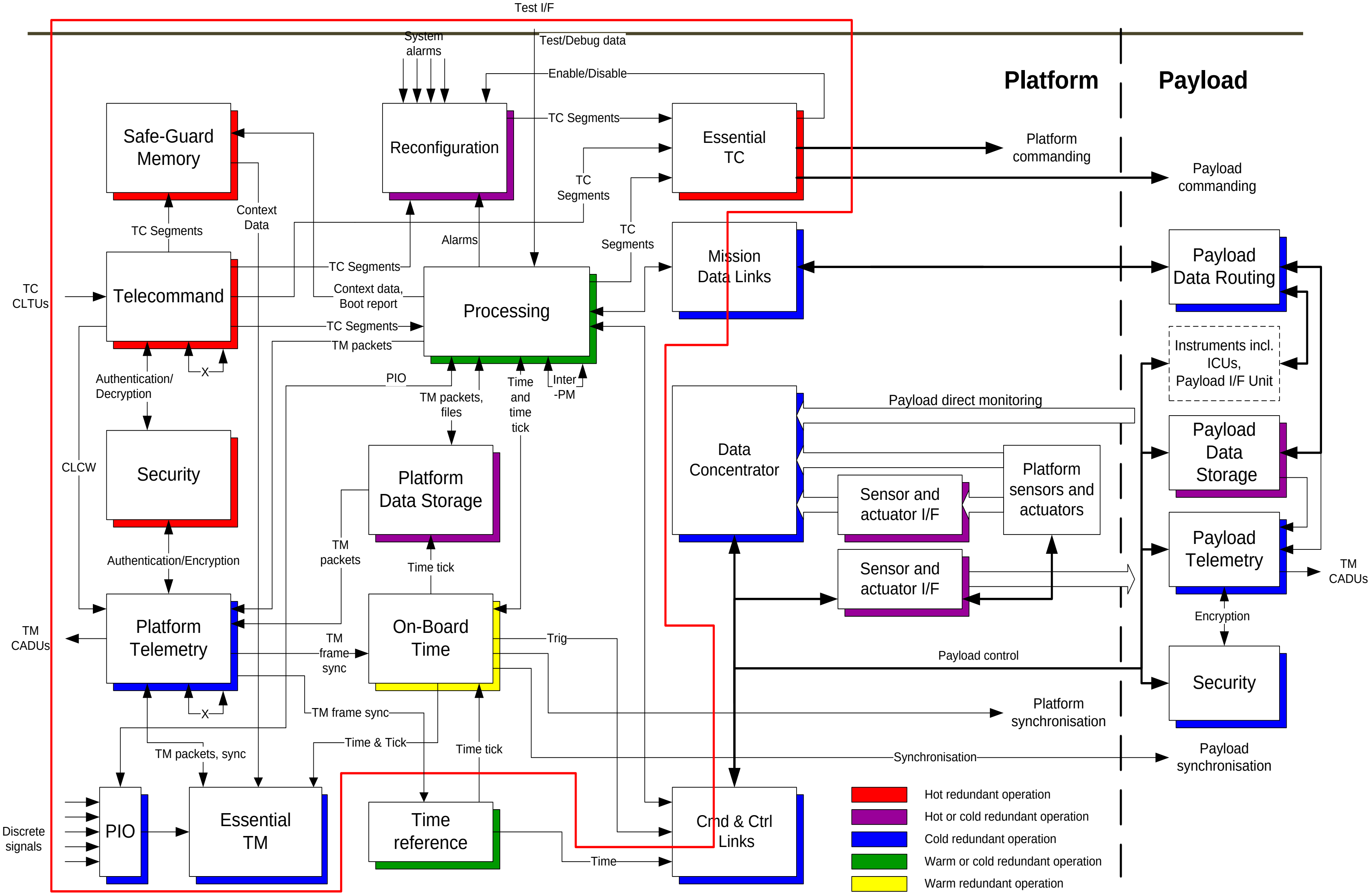
Dependable Technologies For Critical Systems

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 – tailoring of SAVOIR specification

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 Chock 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.

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

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

Dependable Technologies For Critical Systems

3. On-Board Computers Dependability Planning

Definition of a lifecycle model for OBC – HW and SW

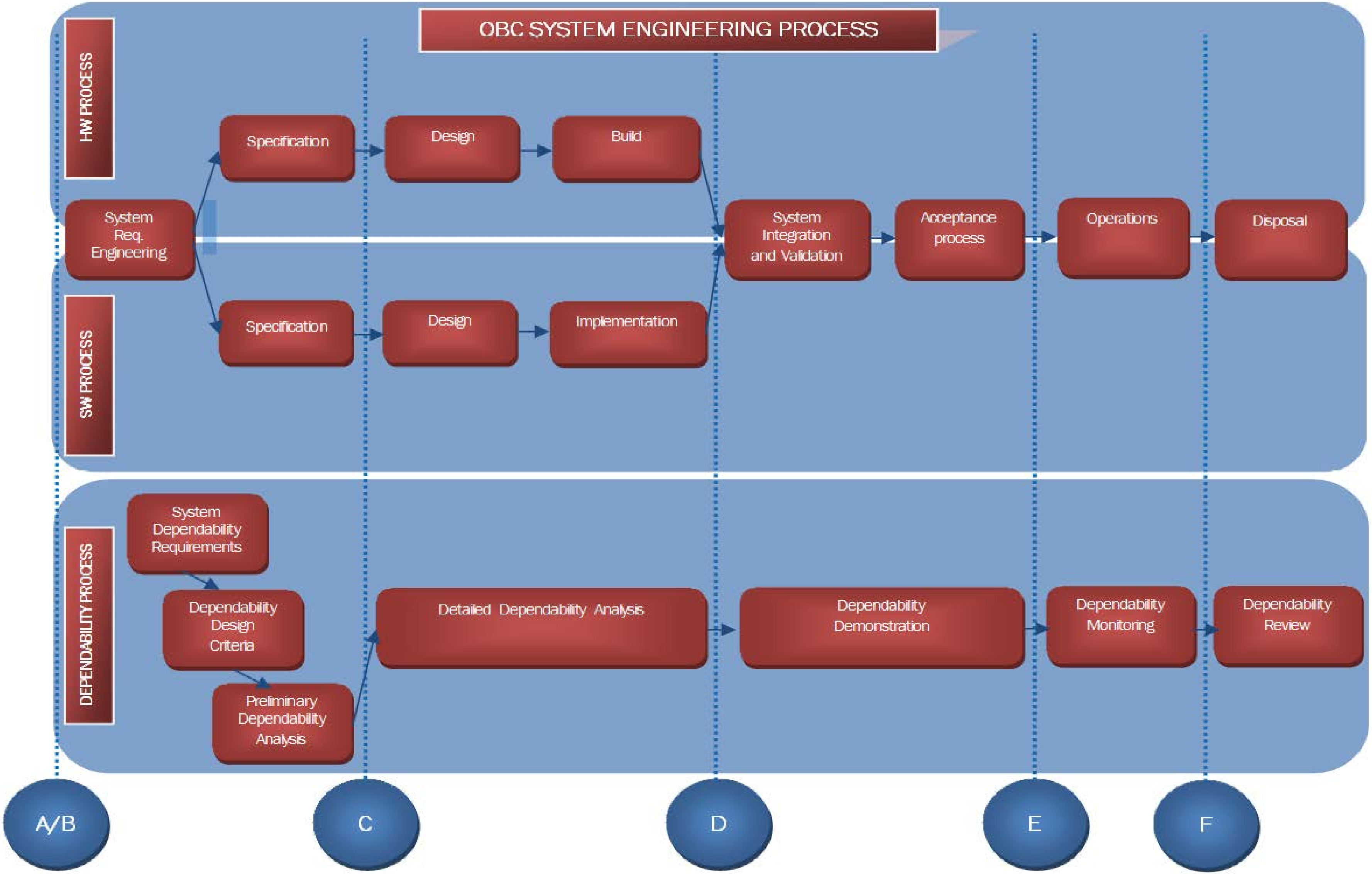
Process descriptions:

- 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


OBC SYSTEM ENGINEERING PROCESS
HW PROCESS
SW PROCESS
DEPENDABILITY PROCESS
System Req. Engineering
Specification
Design
Build
Specification
Design
Implementation
System Integration and Validation
Acceptance process
Operations
Disposal
System Dependability Requirements
Dependability Design Criteria
Preliminary Dependability Analysis
Detailed Dependability Analysis
Dependability Demonstration
Dependability Monitoring
Dependability Review
A/B
C
D
E
F

3. On-Board Computers Dependability Planning

- OBC Dependability Approach

Task	Description
1	Establishment of dependability requirements
2	Establishment of dependability design criteria: • Severity Classification • Failure Tolerance • Design approach (functional and physical)
3	Preliminary dependability analysis: • Identification of undesired events • Preliminary classification of critical items

Task	Description
4	Detailed dependability analyses • Dependability method selection (data sources, technique, tools) • Reliability Analyses (modeling, allocation, prediction) • Maintainability Analyses • Availability Analysis • Dependability critical items list • Dependability recommendations • Implementation of recommendations
5	Dependability demonstration
6	Dependability monitoring & review

REFARCH: Reference Architecture for High Dependability On-Board Computers

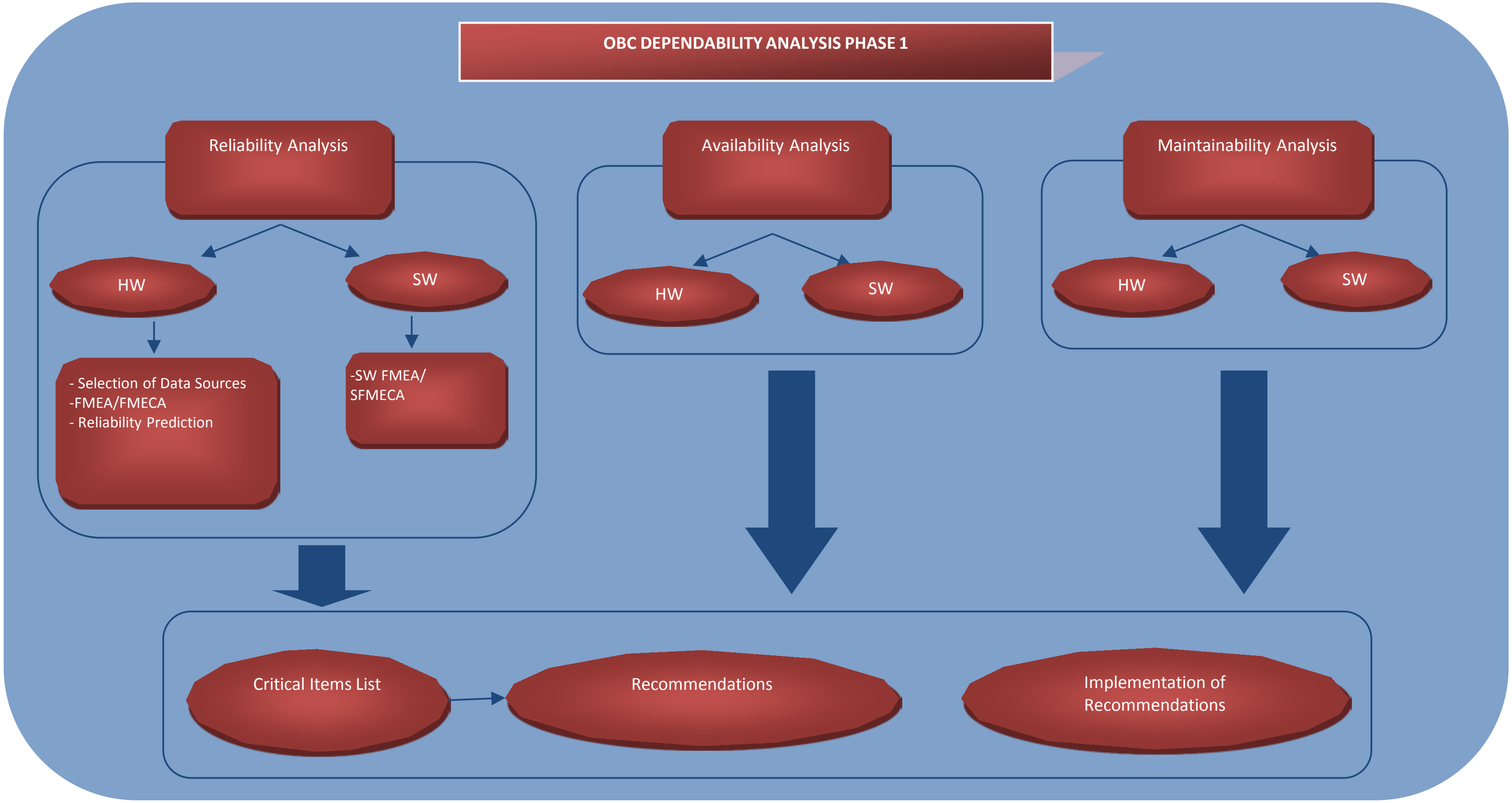
4. On-Board Computers Dependability Measurement

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



OBC DEPENDABILITY ANALYSIS PHASE 1

Reliability Analysis

HW

SW

- Selection of Data Sources
-FMEA/FMECA
- Reliability Prediction

-SW FMEA/
SFMECA

Availability Analysis

HW

SW

Maintainability Analysis

HW

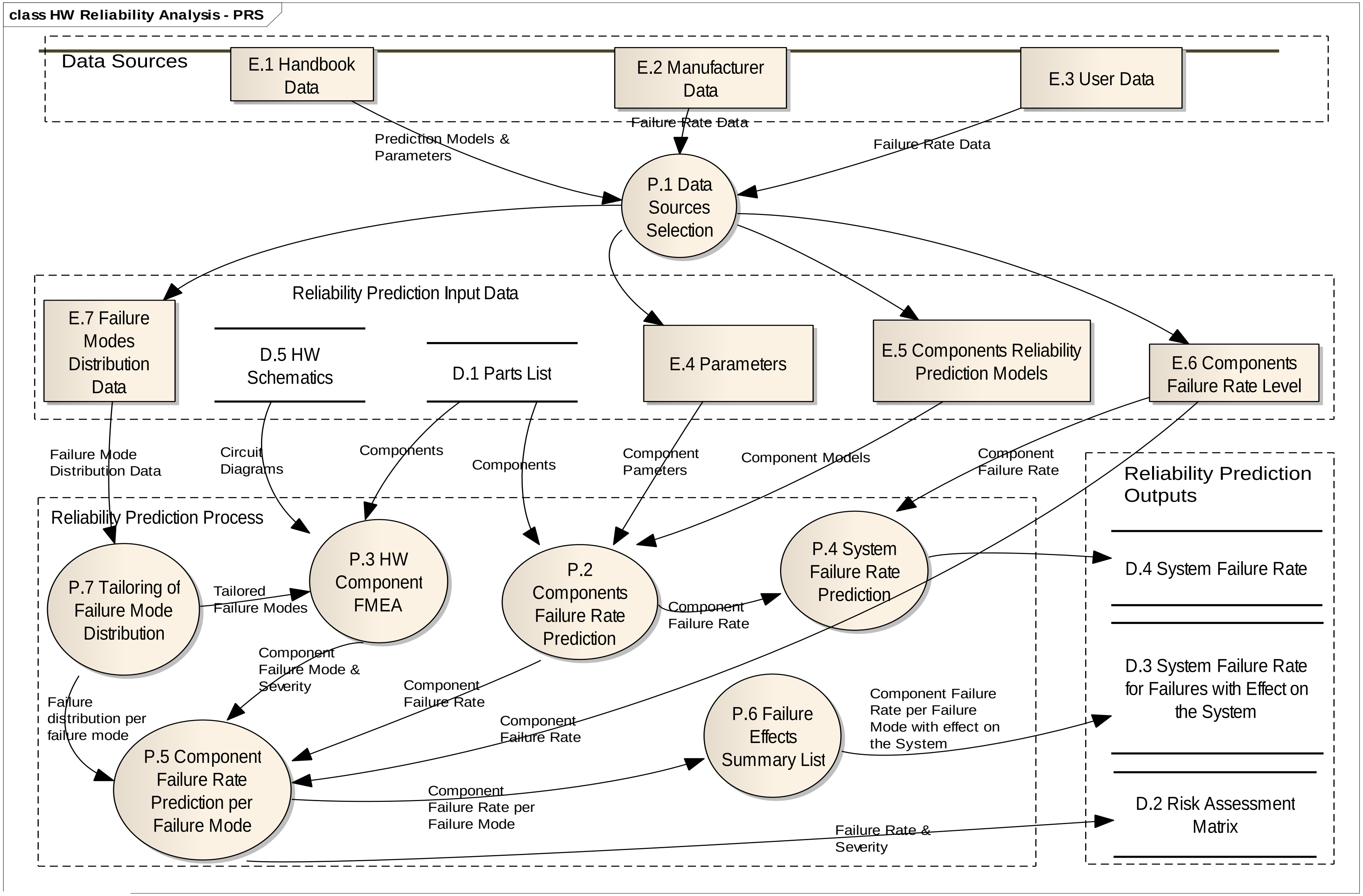
SW

Critical Items List

Recommendations

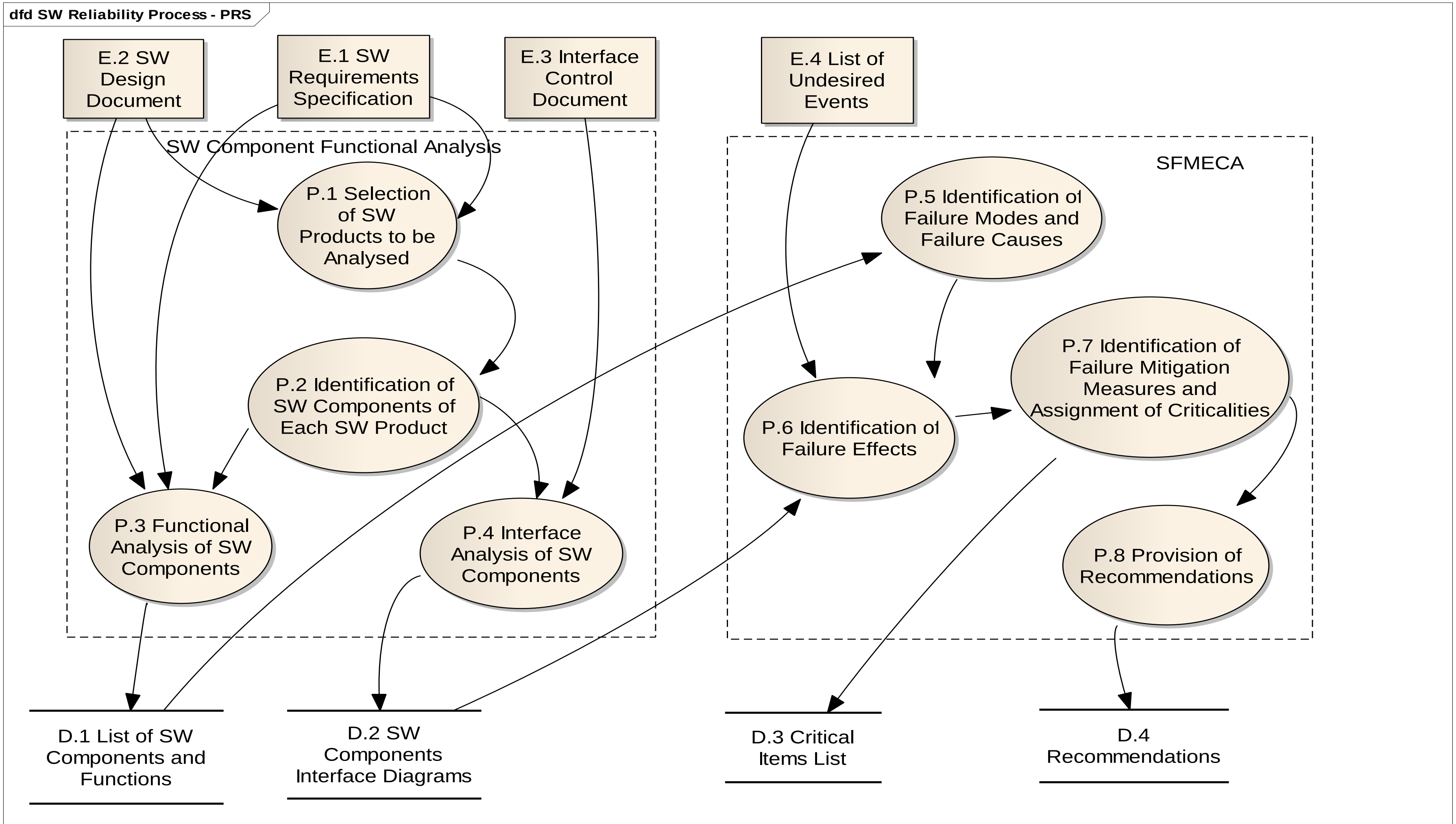
Implementation of Recommendations

4. On-Board Computers Dependability Measurement


class HW Reliability Analysis - PRS
Data Sources
E.1 Handbook Data
E.2 Manufacturer Data
E.3 User Data
Failure Rate Data
Prediction Models & Parameters
Failure Rate Data
P.1 Data Sources Selection
Reliability Prediction Input Data
E.7 Failure Modes Distribution Data
D.5 HW Schematics
D.1 Parts List
E.4 Parameters
E.5 Components Reliability Prediction Models
E.6 Components Failure Rate Level
Failure Mode Distribution Data
Circuit Diagrams
Components
Components
Component Pameters
Component Models
Component Failure Rate
Reliability Prediction Outputs
Reliability Prediction Process
P.7 Tailoring of Failure Mode Distribution
Tailored Failure Modes
P.3 HW Component FMEA
P.2 Components Failure Rate Prediction
Component Failure Rate
P.4 System Failure Rate Prediction
D.4 System Failure Rate
Component Failure Mode & Severity
Component Failure Rate
Failure distribution per failure mode
Component Failure Rate
P.6 Failure Effects Summary List
Component Failure Rate per Failure Mode with effect on the System
D.3 System Failure Rate for Failures with Effect on the System
P.5 Component Failure Rate Prediction per Failure Mode
Component Failure Rate per Failure Mode
Failure Rate & Severity
D.2 Risk Assessment Matrix

4. On-Board Computers Dependability Measurement

- SW Reliability Analysis Methodology


dfd SW Reliability Process - PRS
E.2 SW Design Document
E.1 SW Requirements Specification
E.3 Interface Control Document
E.4 List of Undesired Events
SW Component Functional Analysis
P.1 Selection of SW Products to be Analysed
P.2 Identification of SW Components of Each SW Product
P.3 Functional Analysis of SW Components
P.4 Interface Analysis of SW Components
SFMECA
P.5 Identification of Failure Modes and Failure Causes
P.6 Identification of Failure Effects
P.7 Identification of Failure Mitigation Measures and Assignment of Criticalities
P.8 Provision of Recommendations
D.1 List of SW Components and Functions
D.2 SW Components Interface Diagrams
D.3 Critical Items List
D.4 Recommendations

REFARCH: Reference Architecture for High Dependability On-Board Computers

5. On-Board Computers Dependability Assurance

Contribution of Computer-Aided Environment to OBC Dependability Assurance

Dependable Technologies For Critical Systems

5. On-Board Computers Dependability Assurance

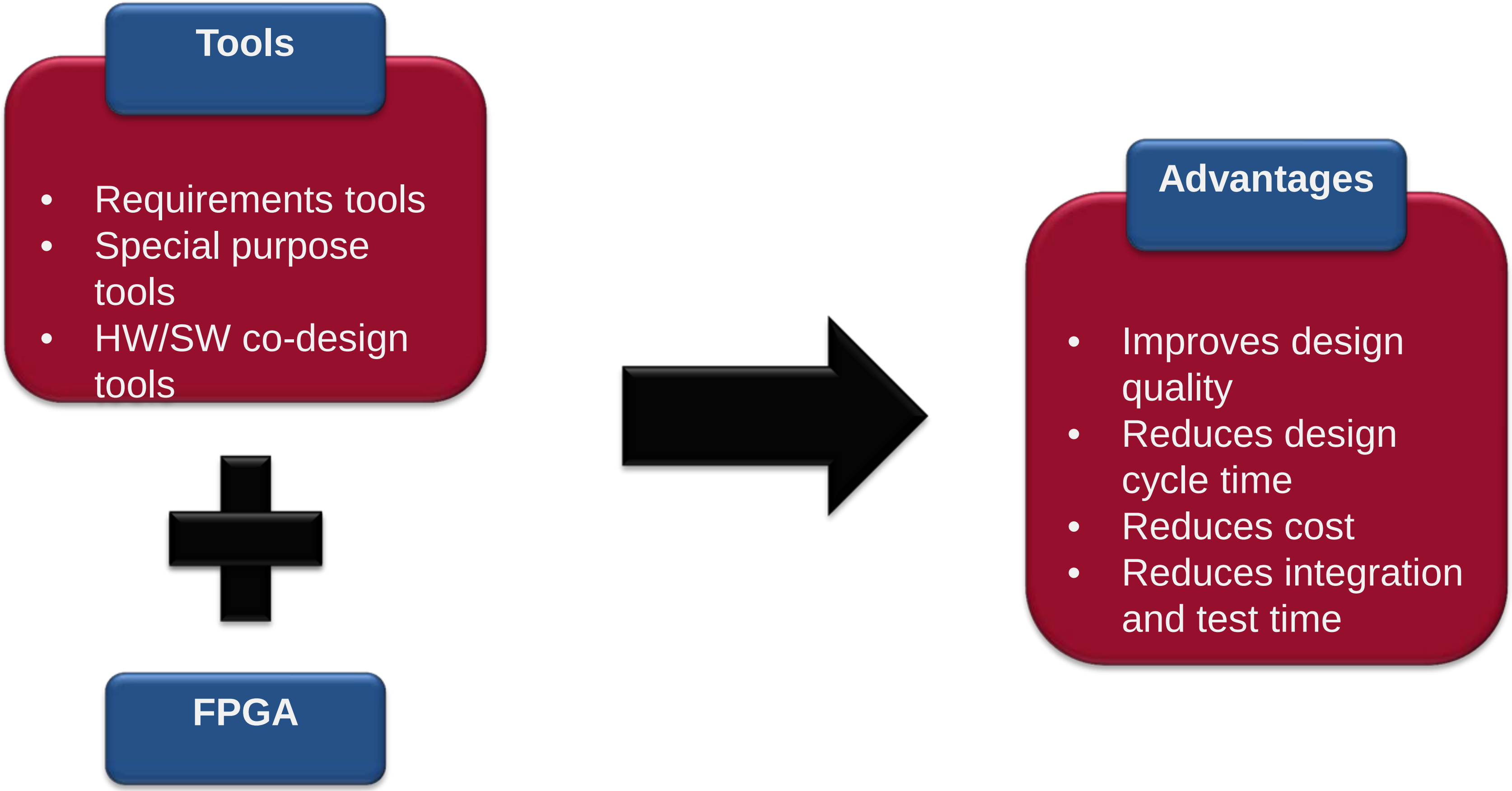
Activity	Description
Requirements Dependability Assurance	- compliance with reference requirements - requirements correctness considering system requirements
Design criteria dependability assurance	- failure severity classification according to the specified values - HW design rules and methods are used
Preliminary dependability analysis assurance	- verification of undesired events - preliminary FMEA performed at the right level of functionality decomposition
Detailed dependability analysis assurance	- data source is selected according to the defined process (in the case of HW) - documentation is complete and has already reached a satisfactory level of maturity (in the case of SW)

5. On-Board Computers Dependability Assurance

Activity	Description
Maintainability analysis assurance	-maintainability requirements (corrective and preventive maintenance tasks) are correct and complete - detailed analysis of the FDIR strategy is performed
Availability analysis assurance	-list of potential outages is complete and that their causes, probabilities of occurrence and duration are correct - all recommendations for the optimization of the system concept are traceable to the associated system architectural and design items
Critical items list assurance	- tailored criterion for identifying the OBC dependability critical items is defined and validated by all the project stakeholders, including management - control measures proposed are feasible, effective and verifiable
Recommendation list assurance	-recommendations were generated for each of the RAM analyses performed -all recommendations issued were reviewed by the HW and SW design teams for approval or rejection

5. On-Board Computers Dependability Assurance

- Contribution of Computer-Aided Environment to OBC Dependability Assurance



Tools

- Requirements tools
- Special purpose tools
- HW/SW co-design tools

FPGA

Advantages

- Improves design quality
- Reduces design cycle time
- Reduces cost
- Reduces integration and test time

REFARCH: Reference Architecture for High Dependability On-Board Computers

6. Feasibility Discussion

Dependable Technologies For Critical Systems

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

6. 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

- Study is still on-going by the time of this presentation
- Future work:
  - Apply the proposed methodology to one on-board computer developed or under development, which will be documented in an application report

Contacts

- Nuno Silva, nsilva@criticalsoftware.com
- Alexandre Esper, aresper@criticalsoftware.com
- Ricardo Barbosa, rbarbosa@criticalsoftware.com
- Johan Zandin, Johan.Zandin@ruag.com
- Claudio Monteleone, claudio.monteleone@esa.int