Embedded System Development for Distributed Networked Computing Platforms
Content

1. The SPEEDS Project

2. Distributed Networked Computing Platform

3. Using SPEEDS for IMA Development
The SPEEDS Project

SPEEDS is funded by the European Commission under Contract IST-033471

SPEculative and Exploratory Design in System’s Engineering
SPEEDS technological contribution

- “Fool-proof” representations of Systems [HRC: Heterogeneous Rich Components].

- Formal technical analyses to verify compatibility, consistency, of Systems [ADT; Analysis Design Techniques].

- Process Control/Monitoring Techniques to evaluate the progress, maturity, of Systems Projects. [SDS; Speculative Design and Seamless Access; Process Adviser].

- Integrated development with transparent access to information and transfer of data between tools [Speeds Bus].
„Heterogeneous Rich Components“ – Objectives

- To provide a characterization of components of electronic components
  - supporting all phases, levels, and viewpoints of electronic system design
  - Allowing complete re-use (across multiple platforms, across multiple organizations, and/or as part of design libraries)
  - Allowing characterization of allowed/assumed environments of component (for all viewpoints)
  - Basis for (de-facto) standardization, compatible with Autosar Component Model

- As basis for tool-independent meta-model for capturing and validating function networks
  - Supporting semantic based integration of industry standard System & SW design tools (UML, Matlab-Simulink/Stateflow, ASCET, …)
  - Supporting view-point specific and cross viewpoint requirement capturing, modeling, analysis and design
Follows Design by Contract Paradigm:

- **Assumptions**
  - Reflect current degree of knowledge of anticipated design context
  - Determine boundary conditions on actual design context for each viewpoint under which component is promising its services
  - Are decorated with confidence levels
  - Horizontal and vertical

- **Promises**
  - Are **guaranteed** if component is used in assumed design context
  - Horizontal and vertical

Is organized per viewpoint:

- Behavior, Coordination, Safety, Real-Time, ….
- But allow specification of cross viewpoint dependencies
SPEEDS Design Entities

User’s View: COTS modeling tools

Speeds Metamodel

Speeds Semantic Foundation

for all viewpoints \( v \):
\[
\bigcap L(A(OutI.v.prj)) \subseteq \bigcap L(A(InI.v.assm_i))
\]
HRC Meta-model

- Based on SysML
- Added Features
  - Contracts (Assumptions, Promises)
  - Various Viewpoints
  - Linking layers (Functional Network, LRU/ECU, Physical Architecture, ...)
- Available as Standalone Meta-model or SysML Profile
- Heterogeneous Modelling
  - Integration of Design Tools
  - Multiple Viewpoints (Functional, Real-Time, Safety, ...)
- Analysis
  - Functional and non-functional characteristics
  - Interaction between viewpoints
- Design Space Exploration
Distributed Networked Computing Platform
Distributed Networked Computing Platform

IMA-Core

Global Functions:
Consolidation,
BITE, Diagnostic

IMA-core-bricks

AFDX

Field-Bus:
TT-Bus, A429, CAN, ...

Function A

IMA-Core

Function B

Common:
- HW Components
- Development Process
- Tools

Function C
Different IMA Topologies

Fully integrated and centralized CPIOMs

CPM centralized – IOM/ RDC distributed

... and the right Function to Resource Allocation?

CPM centralized – IOMs/ RDCs per section
A380 IMA – Development Process Aspects

- Classification of Configuration Parameter (Module, Global, Local).
- Hardware/OS specific configuration parameter.
- Manual assignment of resources supported by databases.
- Automated tool-chain to produce the load.

Information & Data Flow for one Module Type
Specification architecture & validation

ATA 42-10 IMA

“Equipment” Level

TLAR, TLSRD

“Aircraft” Level

“System” Level

SRD

preliminary sizing

specific requirements

common requirements

Module PTS

“Equipment” Level

Bare module

Bare mod. supplier

development

V&V

ATA 42-10 IMA

ATA XX

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SDD, SID

PTS

SES

XX application

MACT

ALCS

V&V

development

common requirements

ATA XX

ATA 42-10 IMA

TLAR, TLSRD

SDD, SID

CCD

SRD

SRD
Using SPEEDS for IMA development
Needed Improvements of Development Process

- Ubiquitous seamless model-based design access
  - hiding heterogeneity and semantic diversity of representations and methods, and
  - providing a design-centric access to all design activities.
- During all design phases, process steps must be guided by an estimation how far overall requirements (e.g. safety, costs) are fulfilled. This “speculative” design can be based on HRC analysis methods.
- High flexibility and robustness with respect to late changes and overlapping design activities.
- More guidance and tool support is required for systematic and structured:
  - system requirements analysis
  - system concept evaluation
  - system design & system equipment specification
Assumption:
Status available every $t$ ms

Promise:
Status == enabled
implies
Out == $V$ within $t'$ ms

Contract Specification:
Textual: Pattern Language
Graphical: Extended State Machines
RCM-based Process for a Single Function

Formalized Communication btw. OEM and Supplier:

✓ Concept and Definition Phases (new System policy)
✓ Functional System Definition
✓ Non-functional aspects
✓ Use of design assumptions

Specification Documents:
- FRD / TLSRD (Top Level System Req.)
- SRD ATA XX (System Req. Document)
- SDD / SID ATA XX (System Description / Interfaces)
- PTS (Equipment TBD)

Formal Specifications by HRCs:
- A/C System Black-box Model
- A/C System White-box Model

Contracts (A, P)

Behavioral and Functional System Definition

Non-functional aspects

Use of design assumptions

Complexity
Alignment of IMA and System Specifications

- Integrated Performance & Resources Model based on Contracts.
- Evaluation and optimization of different IMA architectures.

Abstract Fkt. A
Abstract Fkt. B
Abstract Fkt. C

...
RCM for IMA development – Overview

IMA

System X

Requirements

Performance & Resources Model

Design Space Exploration

Decomposition of Contracts

Contracts (A, P)

Contracts (Ai, Pi)

System Specification

System Design

Contracts for Comp

Contracts for P3

Contracts for P2

Contracts for P1
RCM for IMA development – Requirements Model

System Red
- F1
- F2
- F3

System Green
- F1
- F2
- F3

System Blue
- F1
- F2
- F3

Vertical Assumptions

High-level IMA constrains
- CPM
- IOM_A
- IOM_B
- AFDX
- Switch
- CAN
- RDC

Requirements Model

Performance & Resources Model

Design Space

Exploration

Decomposition

Contracts

Guaranteed by
OEM (resp. other suppliers)

To be Guaranteed by Supplier
RCM for IMA development – Architecture Analysis

- Requirements
- Performance
- Resources
- Design Space
- Exploration
- Decomposition
- Contracts
  - Guaranteed by OEM (resp. other suppliers)
  - To be Guaranteed by Supplier

Analysis and Evaluation of possible architectures and mappings
RCM for IMA develop. – Architecture Optimization

Requirements

Performance & Resources Model

System Design

Architectural Layer

Logical Architecture

Function net

Topological Architecture

Cable & harness & modules

Technical Architecture

Modules & busses

Engineering Bus

Objective Function

Process Advisor

HRC
FMEA
FTA

HRC
SSA
RBD

HRC
Weight model

DOC
COO
LCC

Production model

Health monitoring

HRC
signal interfaces

SOA Services

Web Service

Data/File Services

© AIRBUS DEUTSCHLAND GMBH. All rights reserved. Confidential and proprietary document.

Page 23
RCM for IMA develop. – Contract Decomposition

Requirements

Performance & Resources Model

Design Space

Exploration

Architectural Layer

Contracts

Assm: ...
Promise:
„Local End-to-End Deadlines“

Decomposition with local contracts based on architectural decisions

F1

F2

F3

F1

F2

F3

To be Guaranteed by Supplier

Guaranteed by OEM (resp. other suppliers)
RCM for IMA development – Overview

- Requirements
- Performance & Resources Model
- Design Space Exploration
- Decomposition of Contracts
- IMA
- Contracts \((A, P)\)
- System X
- System Specification
- System Design
- Contracts \((A_i, P_i)\)
SPEEDS Methodology supports:

- Formal system specifications including non-functional aspects.
- Early identification of errors in the specification due to formal analysis.
- Multi-System Integration in early phases based on contracts.
- Increased transparency of system functionality during implementation at the supplier.