System Verification Through the Life Cycle Study Overview & next steps in Avionics domain
ADCSS 2017

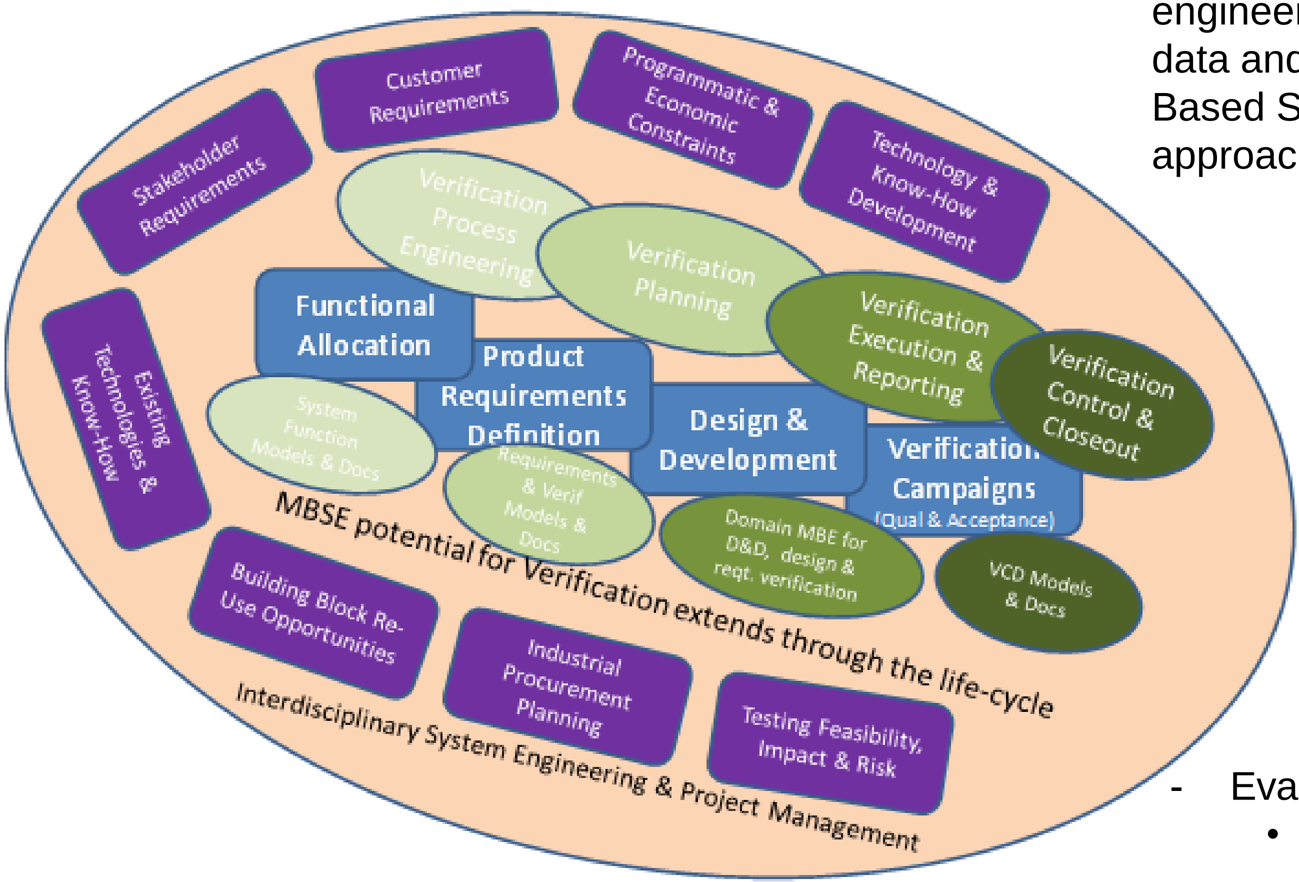
Presented by Alain Rossignol in name of Michel Janvier (Airbus Defence and Space)
18th October 2017

This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

Agenda

- SVTLC ESA Study (Airbus Defence & Space, Novabase , Scopeset)
    - Study Objectives
    - Model based potential to validate re-use approaches
    - Towards a Dynamic and Suitable Review Logic
    - Advanced Models Philosophy
    - Study outcomes : today models for Electrical & Functional domain in Airbus DS
- Next steps : Airbus Defence & Space view on MBSE approach on Avionics

SVTLC study focus : Towards Improved System Verification Practice



- Greater integration of domain engineering and system engineering data and processes through Model Based System Engineering approaches

- Improved deployment of correct, efficient and timely efforts to achieve system verification
  - Sound early planning
  - Robust implementation
  - Avoid over and under specification
  - Eliminate wasteful / low-value activities without adding risk
  - Innovate new methods and tools
- Focus on virtual models in this study

- Evaluation of Suitability of Models for Verification
  - Nomenclature linking model class with lifecycle verification objectives, aligned with ECSS TM-10-21 A
  - Concrete ideas and propositions in avionics & system domains, based on projects return of experience
  - Rigorous distinction between Qualification and Acceptance objectives

- Impact of Elements Re-Use
- Definition of Suitable Review Logic
- Demonstration

- Best practice comparison with automotive sector

This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

Model based potential to validate re-use approaches and enhance model philosophy tailoring to project needs

Status quo

- **Top-down V approach and bottom-up Product Line approach** often meet together in a **less well defined landscape** of **ad-hoc** adaptations of model philosophy and review approach for **re-use** of design artefacts and equipment / subsystems
- These requirements **may drive away** from the overall programmatic optimisation target if **not sufficiently validated up-front against the most open acceptable scenario** of user needs (over-specification)
- **Validation** of bottom-up re-use opportunities are often **very costly** to achieve against top-down requirements **especially across contractual boundaries**

WHAT?

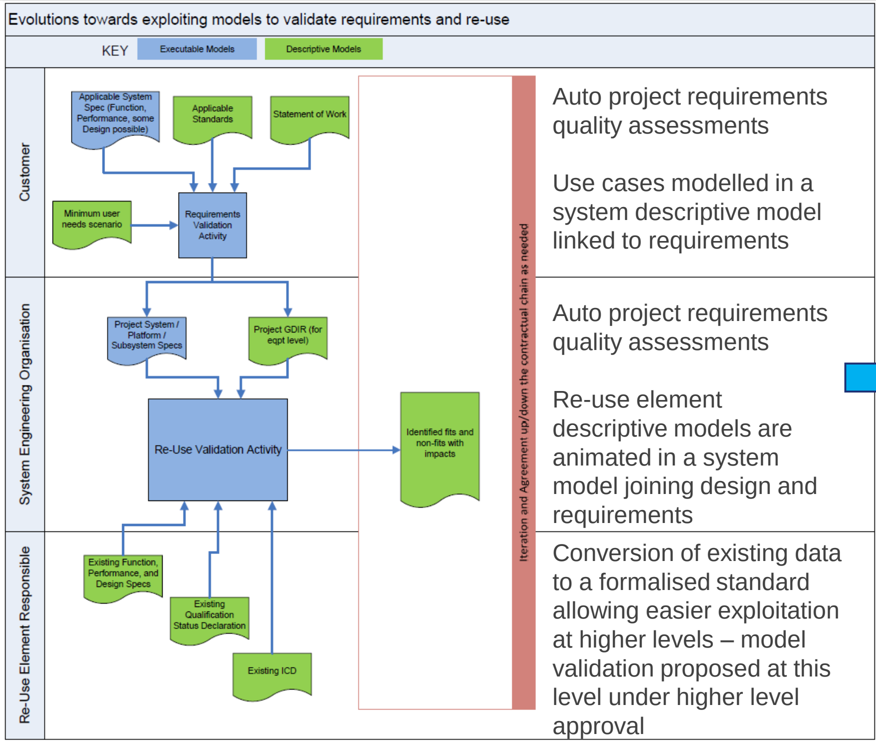
- Focus on **requirement validation** to avoid over-specification, followed by **re-use validation**
- **Develop and exploit** potential of **models** of both requirements & design characteristics, and their interactions throughout the system
- Define **model validation** responsibilities and **tailor the model philosophy**

WHY?

- To **prevent to lose** some re-use opportunities through over-specification
- To **earlier reveal** fits / no fits of the proposed re-use to validated requirements
- To **reduce cost and duration** of the re-use validation phase

HOW?

1. **Executable models** for **requirements validation** against minimum defined set of user needs
   - Formalized modelling of requirements categorised as per ECSS-E-ST-10-06C, and needs as use cases, with auditing of relationships to reveal un-needed reqts
2. **Executable models** for **re-use validation** against the previously validated requirements
   - Function, Performance, Interface, Qualification Status – *tech reqt. related*
   - Verification Content, PA, Industrialisation, Management – *SOW related*
3. **Model based compatible data exchange** across contractual boundaries
   - Standardisation of formalised data models and exchange protocols



- **Minimise** number of **RFDs** against project requirements
- Less **misdirection of effort** against poor quality , duplicated or contradictory requirements
- **Earlier entry** to tailoring of model philosophy on more secure foundations, **with fewer surprises**
- **Lower recurring cost** of validation phases

NOVABASE like life
ScopeSET The Tools Experts
AIRBUS DEFENCE & SPACE

Towards a Dynamic Review Logic through systematic Design & Verification Maturity Assessment and Management

Status quo

- Whilst technology readiness and assessment is generally well treated on a formalised TRL scale with associated thresholds for entry to implementation phase, the emerging **system design maturity** is subject to fewer categories and considered via the classic system reviews PRR, SRR, PDR, CDR, QR, AR.
- These milestones impose a major programmatic environment that **drive project activities**, and **not always in direct synergy with the technical and industrial maturity**, including **non-ideal phasing with unit and software level review cycles**.
- **Reactive adaptation** of the review logic already takes place e.g. delta-reviews, splitting reviews to part 1 and part 2, also renegotiated payment milestones…

WHAT?

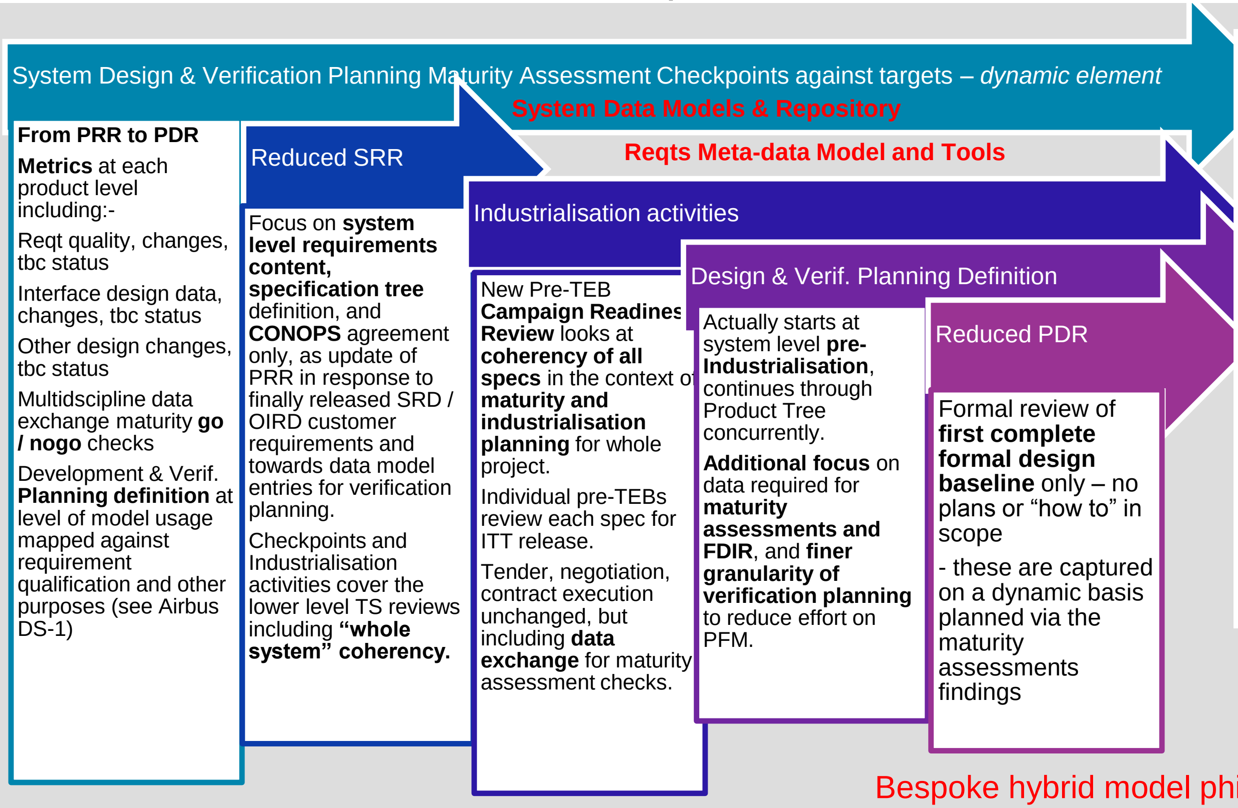
- **Turn the reactive review logic adaptation into a proactive one** with the optimised technical and industrial **maturity evolution planning in the driving seat,** within overall programmatic constraints
- Formulate the **B2CD business agreement** on the **basis of this agreed evolution planning** with **light systematic maturity assessment points**, and a **leaner content and implementation of the classic review cycle**

WHY?

- To achieve much **greater alignment** of the programmatic, technical , and industrial realities based upon **greater visibility** of the real maturities and risks
- To allow decision-makers to **more systematically** take an informed holistic view on **concrete facts and recognition of unknowns**
- To **reduce consequences** of incorrect maturity assessment e.g. **redesign / rework / retrofit,** and **improve the value added** of the overall review cycle

HOW?

1. **Common team access to a System Engineering environment** built to facilitate rapid and highly accurate multi-discipline data exchange, plus discipline specific views, supporting **design, verification and models configuration** (**to identify regression and change impact**)
   - reduce iteration and cycle times
   - rapid metrics for maturity assessments
2. **tbc is your friend** – allows to make visible what is not really fully mature, and plan to make it mature taking into account **all interactions**
3. Phase B1 outcome includes **definition of system design & verification maturity planning** against which the **checkpoint plan** is made for formulation of **business agreement in Phase B2CD**.
4. **Model sharing across contractual chain** to facilitate requirement, design, and verification reviews, focussed on **key questions** aligned with the above planning



Phase C – maintain **dynamic** checkpoints **as needed** for design and verification planning including test spec definition. **Phase D** shifts to verification implementation and tracking with **earlier close-outs** through cross-model **configuration accounting**

Bespoke hybrid model philosophy project – Phase B is key

NOVABASE like life

Scopeset The Tools Experts

AIRBUS DEFENCE & SPACE

Mapping Model classes with verification objectives to derive Fidelity Requirements on the lifecycle

This document and its content is the property of Astrium [Ltd/SAS/GmbH]. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

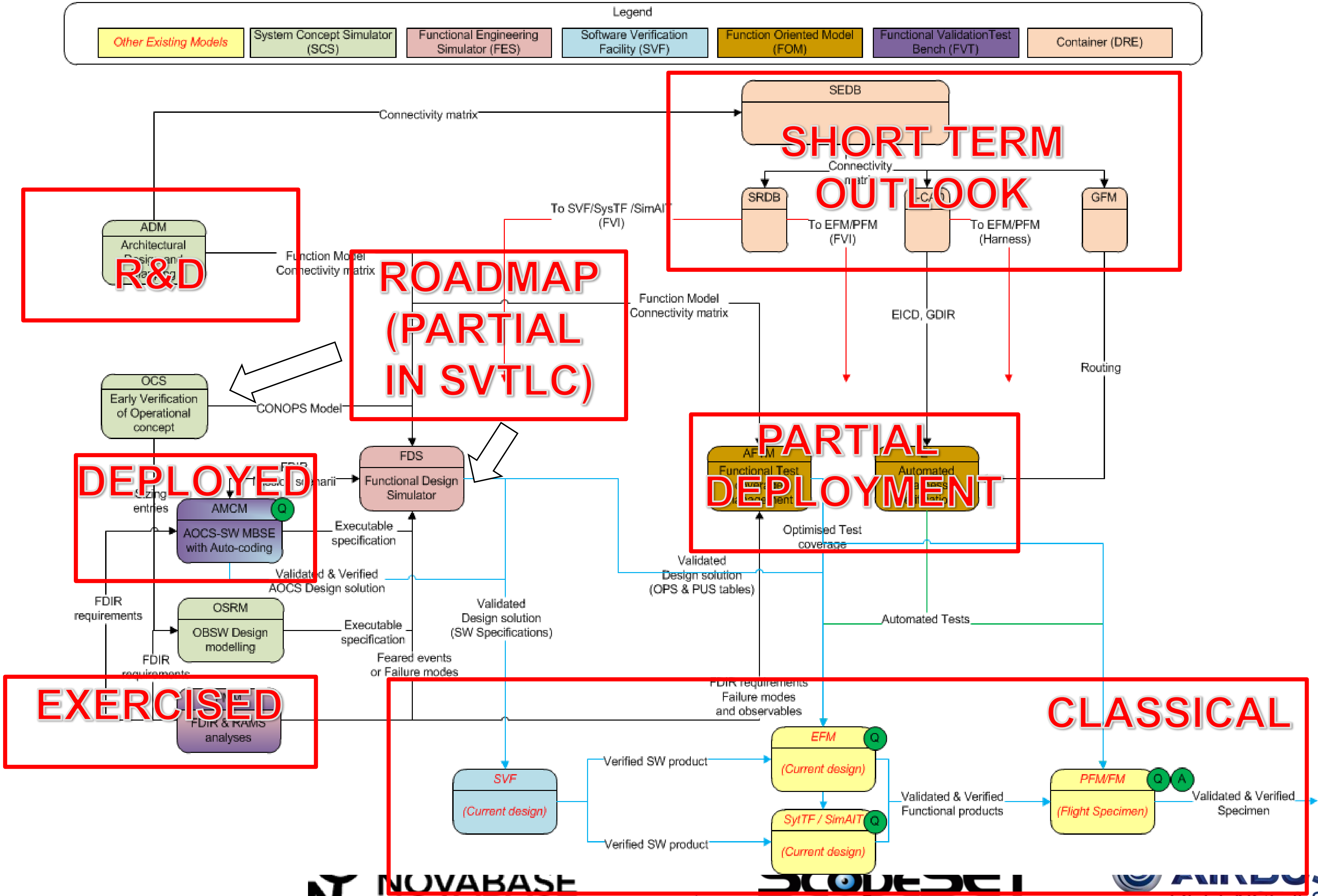
Facility	SCS	MPS	FES	FVT	SVF	MU	FOM	DRE
Name (ECSS-TM-10-21 A)	**System Concept Simulator**	**Mission Performance Simulator**	**Functional Engineering Simulator**	**Functional Validation Test bench**	**Software Validation Facility**	**Mock-Up**	**Function Oriented Model**	**Data repository**
Scope	Functional architecture of the system	Mission product quality	Spotted functional design item(s)	Spotted final design solution	Software Validation	Spotted design item(s) solution	Spotted final design item(s) solution	Spotted final design item(s) solution
System Milestone(s)	SRR, PDR	SRR, PDR, CDR	SRR, PDR, CDR	CDR, FAR	CDR, QR/AR	SRR, PDR, CDR	CDR, FAR	Whole lifecycle
Models Validated Against	Mainly ad-hoc tailored generic models against specifications	PRR Specifications, Design solution at System PDR / CDR	System Specifications and Design solution at System PDR / CDR	System Specifications and Design at System PDR / CDR / FAR	Equipment PDR specifications and Design, Equipment CDR design	PRR Specifications, Design solution at System PDR / CDR	System Specifications and Design at System PDR / CDR / FAR	System Specifications and Design at System PDR / CDR / FAR
Facility Validated Against	Consistency with output from the Concurrent Design Process (if any)	System Specifications (SRR, PDR, CDR)	Real Data/Other Systems (All) System requirements (SRR, PDR, CDR)	Product Under Test (e.g. Breadboard Hardware and Software)	Product Under Test (e.g. Software function) and overall Design solution	Real Data/Other Systems (All) System Specifications (SRR, PDR, CDR)	Product Under Test (e.g. Breadboard Hardware and Software)	As designed / As built
Verified Products	Mission Concept compliance to Requirements Design consistency System performance	Performance of the Mission Product(s)	System functional design & performance validation in the targeted area	Compliance of Product Under Test with system interfaces and design and mission requirements	OBSW Product function Under Test against SW and mission requirements Associated SRDB elements	Pending use case : Architecture/ Configuration / interfaces / operational procedures	Compliance of Product Under Test with system interfaces and design and mission requirements	N/A Feeds ad configures As designed / As built through life cycle
Verification class	**Proof of Architecture (POA)**	**Design or I/F freeze – proof of concept (POC)** **Requirement closure – Verification (REQ)**	**Design or I/F freeze – proof of concept (POC)**	**Detailed design consolidation – bread boarding for risk mitigation (DDC)** **Overall Design validation (VAL)** **Requirement closure – Verification (REQ)**	**Requirement closure – Verification (REQ)** **(for S/W)**	**Design or I/F freeze – proof of concept (POC)** **, Detailed design consolidation – bread boarding for risk mitigation (DDC)** **AIT or OPS preparation (PREP)**	**Detailed design consolidation – bread boarding for risk mitigation (DDC)** **Overall Design validation (VAL)** **Requirement closure – Verification (REQ)** **AIT or OPS preparation (PREP)**	**N/A**

NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Resulting Outlook of models for Electrical & Functional world : vision, continuities, and state of practice in Airbus DS



NOVABASE like life

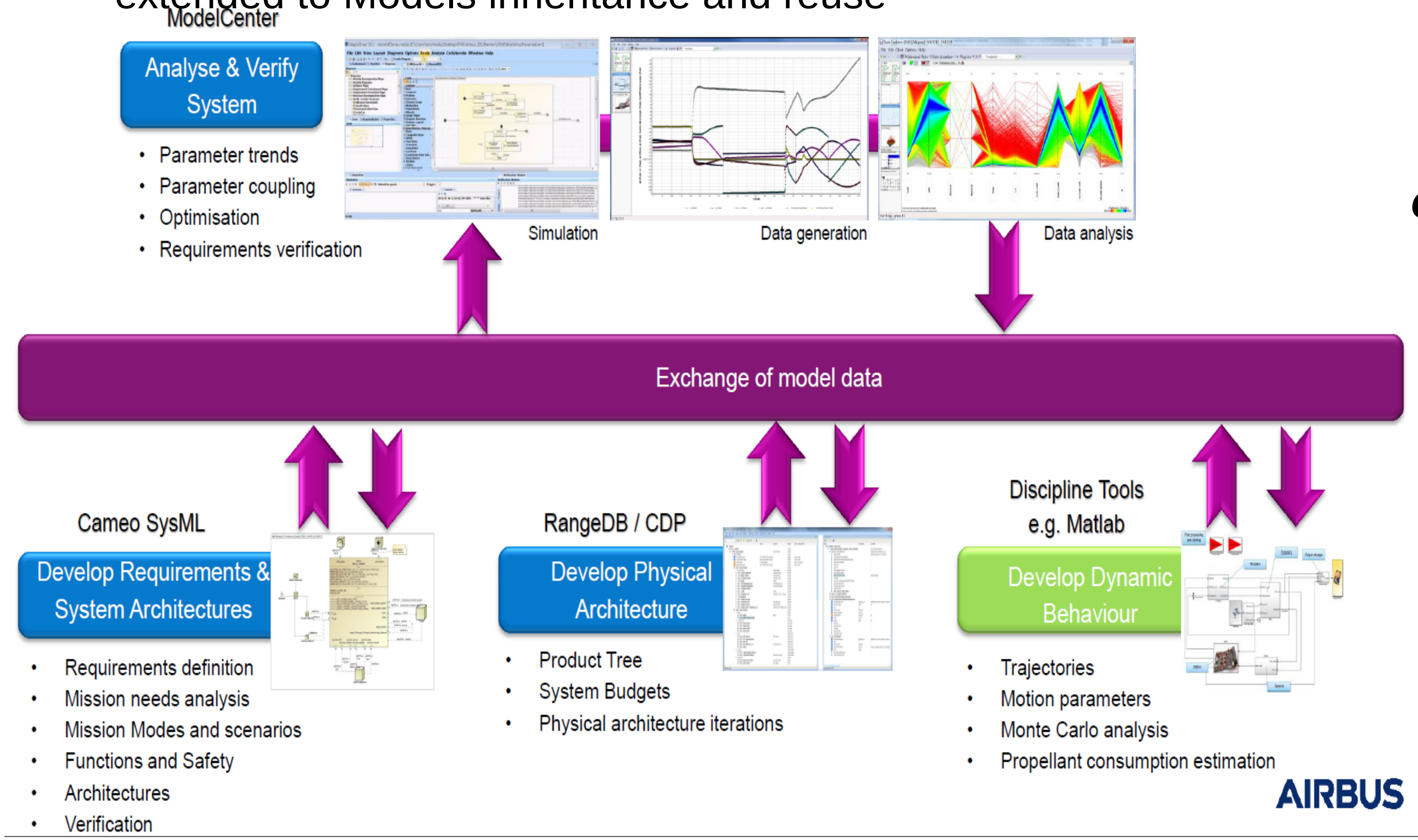
The Tools Experts

AIRBUS DEFENCE & SPACE

This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

Next steps : ADS view on MBSE approach on Avionics

- ❑ Model Based System Verification & Validation relies on Model Based System Engineering
- ❑ Model based Avionics Engineering, Validation & Verification has to be consistent and integrated with:
  - **System Engineering level** (Missions phases and operational scenario, modes and states, physical architecture and equipments)
  - **Avionics functional Engineering** on CONOPS, FDIR, AOCS/GNC, OBSW, Functional Validation & Infrastructure (Simulators and test benches)
  - A strong management of **Data consistency and continuity in a shared and common repository** through the different phases of life-cycle (Phase B/CB/E), different levels of the system (large ground/board system, spacecraft, avionics, equipment & SW), project organization including equipment suppliers - if possible extended to Models inheritance and reuse

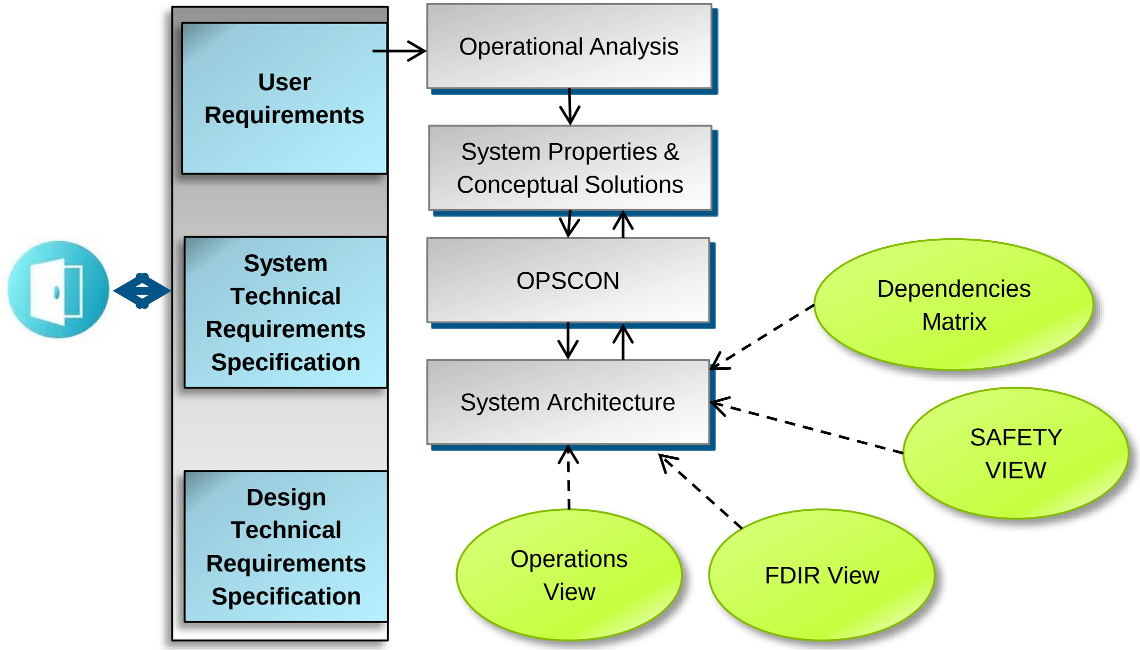


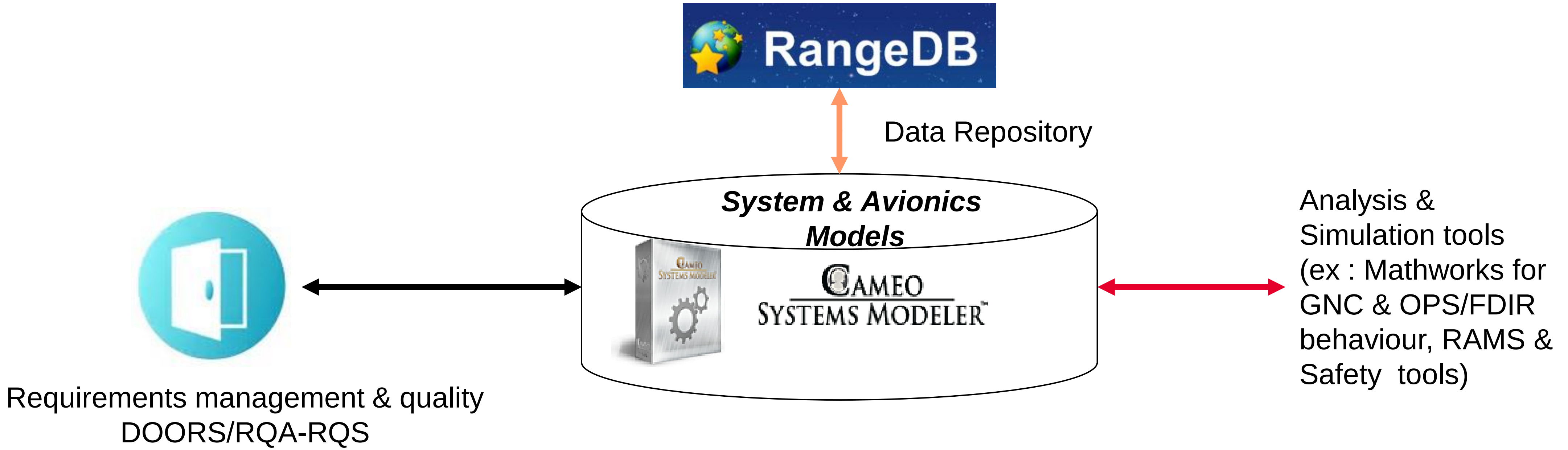
On ESA e.Deorbit Phase B1 project, an MBSE approach based on federated and executable models has been implemented for supporting the generation of requirements and system architectures

AIRBUS

Next steps : ADS view on MBSE approach on Avionics Modelling engineering approach from Systems to Avionics FES

Now we are evaluating methodology and tools integration to "connect" avionics disciplines modeling and analysis tools to the system framework including RANGE-DB Data repository & DOORS for requirement management





AIRBUS

Next steps : ADS view on future Mission needs and advanced Avionics DDV Process

❑ Space systems verification through models will face two major stakes in next decade especially on Avionics and Functional systems

❑ **New mission needs and new avionics architectures** are more demanding in early validation through simulation & model-based approach supporting increasing complexity

- Mini or mega constellations ➔ several spacecraft to be controlled and maintained at same time, sharing of C&C on ground /on-board systems
- More autonomous spacecraft ➔ reducing ground system effort and/or mission constraints,
- Several spacecraft/systems in close cooperation ➔ composite spacecraft, in-orbit servicing or manufacturing with robotic sub-systems

❑ **New Avionics Design , Development & Validation step on efficiency** (cost, schedule & risks)

- More reuse ➔ better product family formalisation with early maturity assessment & product line management along the lifecycle
- Reduction of HWIL models and intensive use of numerical models ➔ more virtualization and digitalization
- Less documents and more shared models with collaborative environments
- More life-cycle flexibility with agility and dynamic approach in reviews and verification activities
- Data continuity, baseline management and models are key

Thank you for your attention

Questions ?

AIRBUS