System Verification Through the Life Cycle

Final Presentation

S. Willis

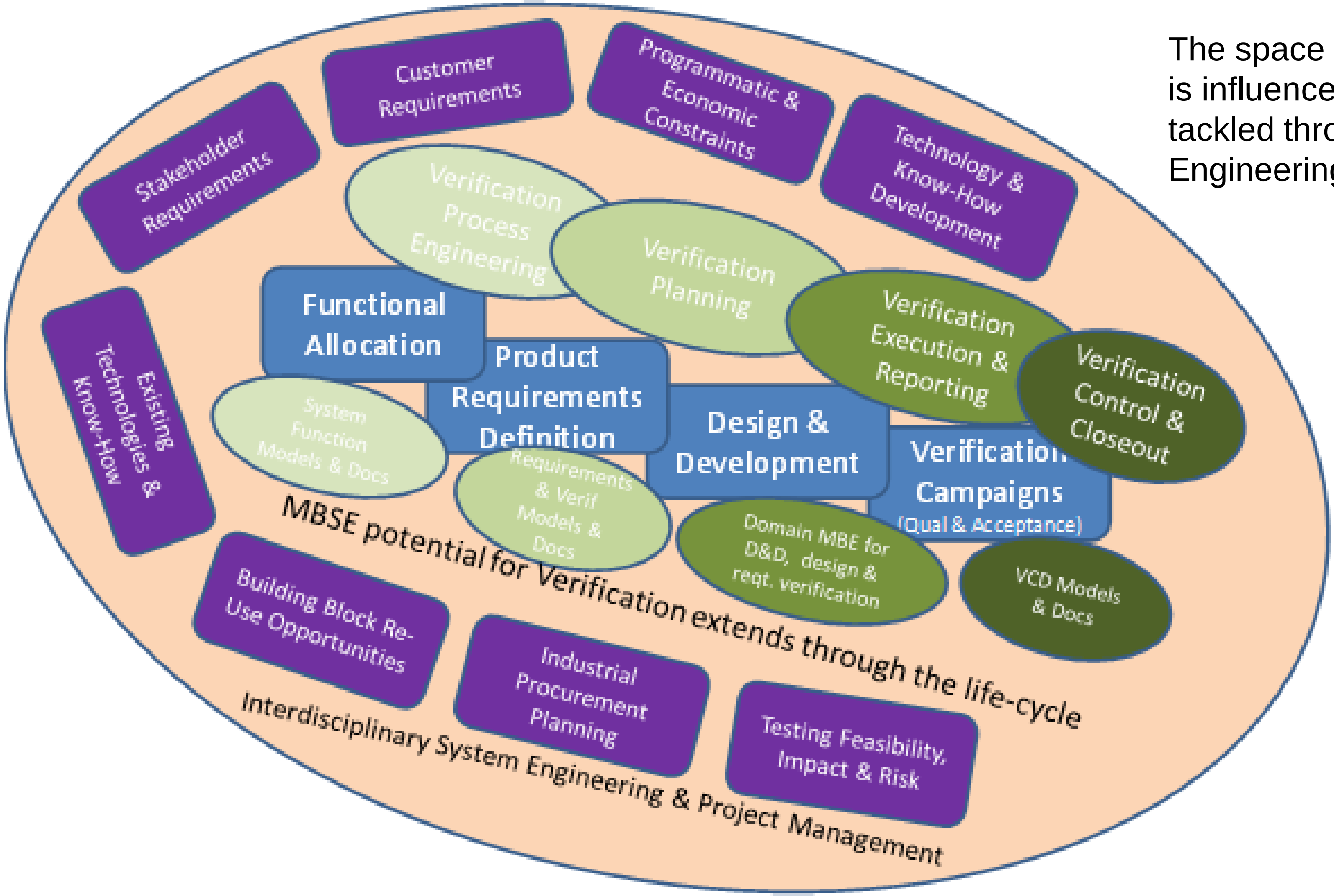
02nd June 2015

NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Introduction – Towards Improved System Verification Practice



The space project development problem is influenced by an array of factors tackled through Interdisciplinary System Engineering & Project Management

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**

Potential of improved virtual models through the lifecycle

Using model based engineering at system level

- There are often lots of quite specific models used within a system design team.
- In this context MBSE refers to a holistic system data model which links specific models in subsystem domains
  - This can be seen as an aggregation of domain specific activities / models through a common infrastructure fed by a common data source.
- This is more often seen on the right hand side of the V model of design and verification (from Phase B onwards).

Describing/defining a system using a modelling language

- Objective is to either to support analyses out of this modelling information, or simply to represent simply and in fidelity the reality.
- This is more often seen on the left hand side of the V model of design and verification (early study phases at system level, requirement definition at software level).

SVTLC – What has been done in the study

Task 1 – Evaluate Suitability of Models for Early Verification

- Real project experience across Science and Earth Observation missions has been critically analysed to determine model usage efficiency towards verification and other added value purposes
- Summary findings allow to identify some incremental model improvements

Task 2 – Define Advanced Model Philosophy

- Focus on hybrid model approach (between QM and PFM, typical Science), whole lifecycle
- 14 new models / nomenclatures proposed with many different identified use cases spread across 6 new model purpose definitions
- System modelling and simulation categorised
- Importance of separation of Qualification and Acceptance, and allocations of Qual on models

Task 3 – Impact of Elements Re-Use

- Examination of re-use state of practice, Industry-Agency workshop findings
- Re-use process definitions and identification of target areas
- Concepts for model-based use cases associated to re-use

Task 4 – Definition of Suitable Review Logic

- examines Readiness / Maturity level indicators to allow dynamic review logic and milestone allocation in the context of the proposed advanced model philosophy
- Industry – Agency Workshop for feedback and iteration

Task 5 – Support Tool Definition & Demonstration

- Extension of capability in Functional Engineering Simulator class to focus on Phase B simulation

Additional Best Practice Comparison with Automotive Sector faciliated by 3DSE Management Consultants

Automotive Best Practice Comparison – Technical Outcome

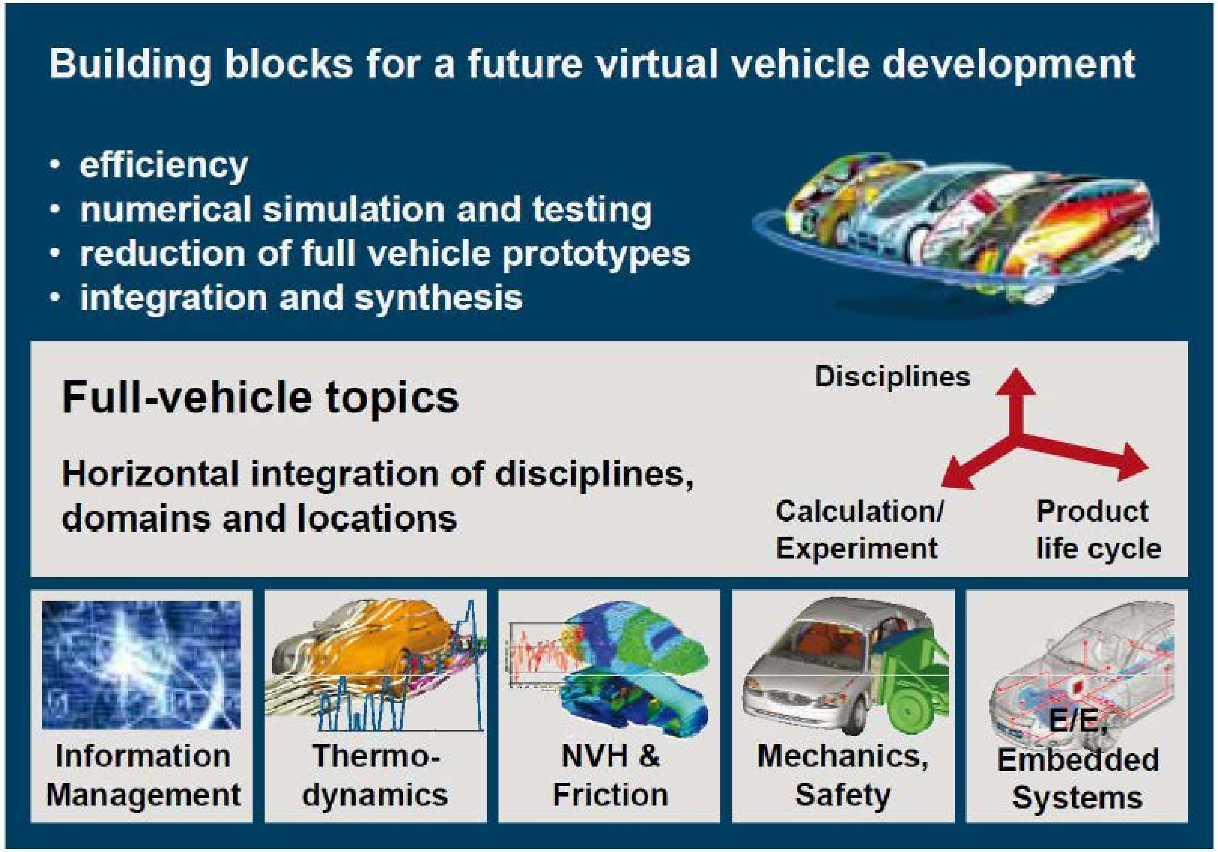
- Automotive focusses on two promising fields
- The reduction of physical prototypes due to cost & time constraints
- The application of new design & verification methods to fill the gap

Virtual Development (more than Verification) is used

- To prove the feasibility of a product and its functions and properties
- For early detection of problems for realization
  - Proof of recovery measures
- To detect relevant factors that drive functions and costs

"Frontloading" is used to support concept development by means of virtual product development, and needs the following aspects

- High integration level even in the first phase of product development
- Efficient methods for layout and functional verification
- Usage of knowledge and experience
- Handling of complexity



Source: Virtual Vehicle Research Center

Making use of Automotive-Space best practice findings

Bottom-up (space approach) vs Top-Down (automotive approach)

- From models evolution to review logic adaptations in Space (bottom-up)
- From a gate logic focussed on maturity targets to the required model developments to achieve it in automotive (top-down)

Automotive "front-loading" equates to Qualification-Acceptance distinction in Space

- How to better "front-load" space projects to allow maximum Qualification off the flight article?

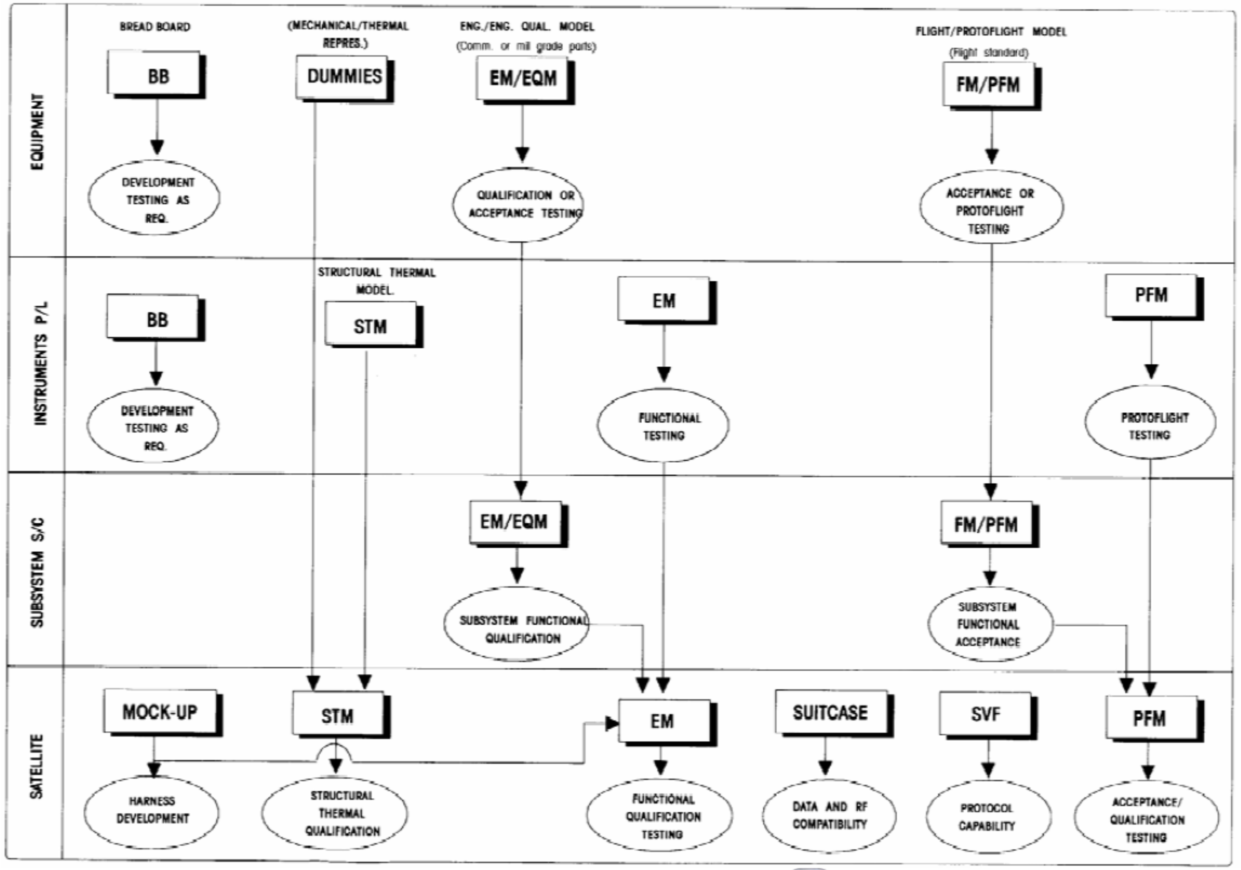
Importance of management of abstraction levels substantiates the need for Functional Engineering Simulator class of tools / executable specifications

Data Management as a core discussion for both industries

Cartography of current models – Model philosophy

Model objective for verification

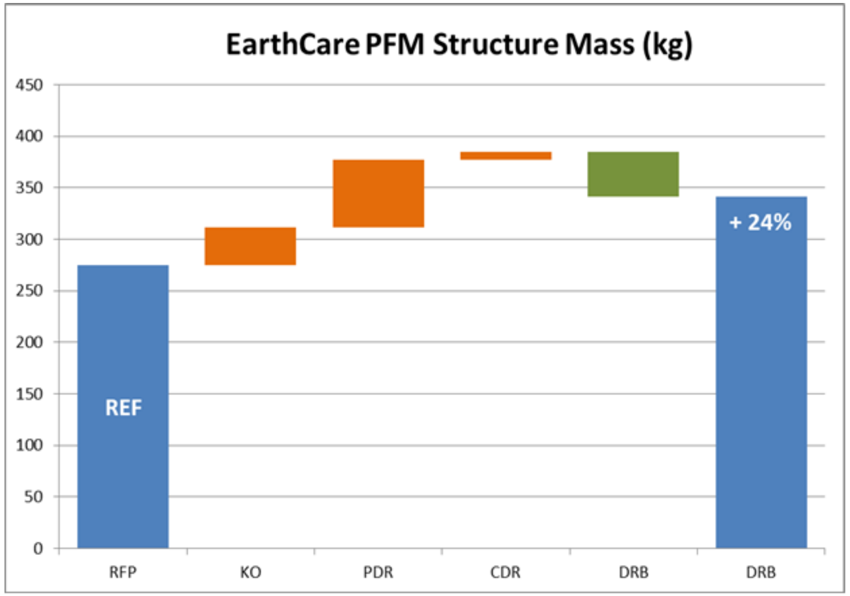
- Based on collection of solutions from several programs (Science, Earth Observation, Navigation, Commercial export)
- Current state of practice of project Models philosophy is well in line with hybrid model summary available in ECSS-E-HB-10-02A figure 5-6
  - Tailoring is done according to project heritage and risk policy assessment, principally wrt :
    - Mechanical / Thermal : SM, STM, spotted models (ex : module QM), none
    - Electrical / Functional : EM in shape, EFM, reduced EFM, none
  - Tailoring is performed as of B2/C/D proposal
    - Pending a robust A/B1 analysis phase
    - Latest for plans at PDR
    - Generally, no change of landscape

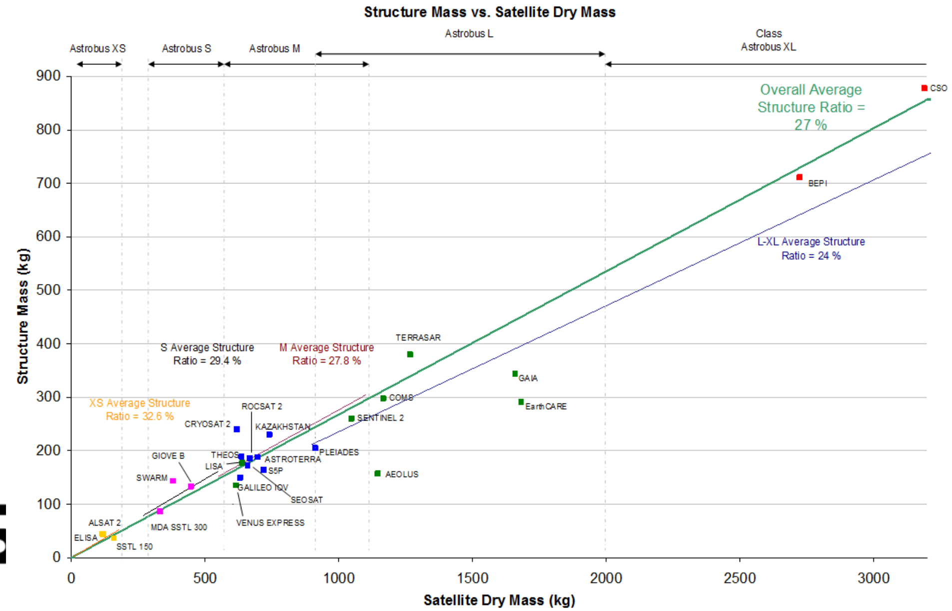


Cartography of current models : Efficiency analysis

Suitability for verification purpose through efficiency KPI (Mechanical Domain)

- Simplified "design KPI" are used as of early phases to de-risk design in mechanical domain
  - Margin policy → design derisking
    - Initial budget + maturity margin
    - DRB mass within margins
  - Mass benchmark → Pre design mass assessment
    - Structure dry mass vs S/C dry mass
    - Payload mass vs S/C dry mass
    - Harness mass vs equipment mass
    - Mass budget (S/C, P/L, harness)
- Experience return and lesson's learnt
  - Adequacy of these early checks to secure design solution, not to validate requirements
  - Acoustic model required in advanced phase
  - µ-vibration issue possibly found late

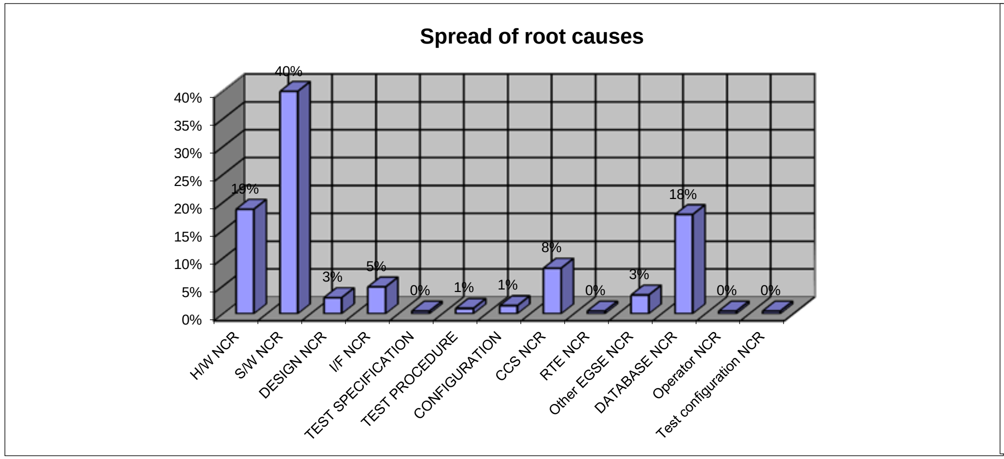


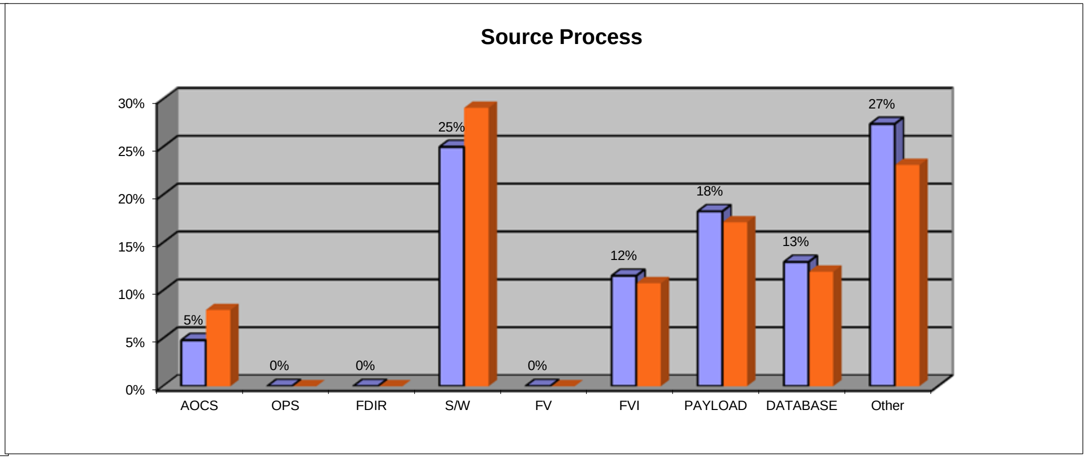


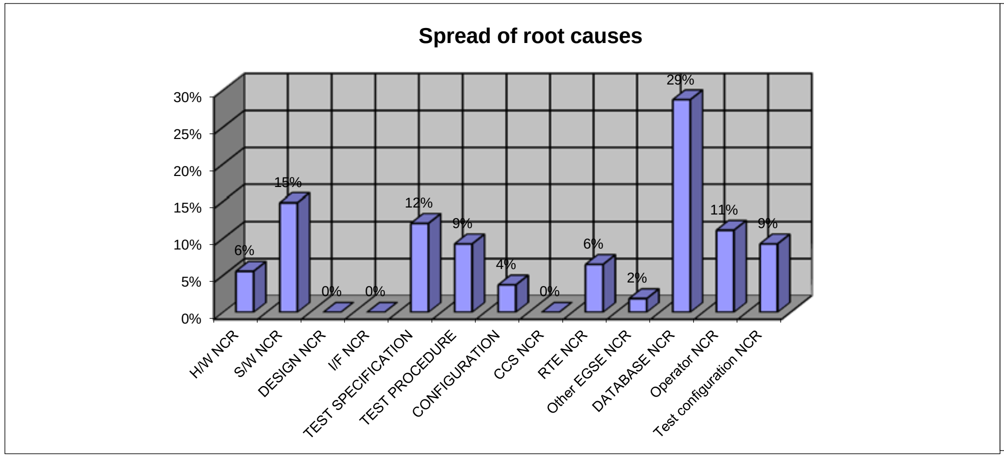
Cartography of current models : Efficiency analysis

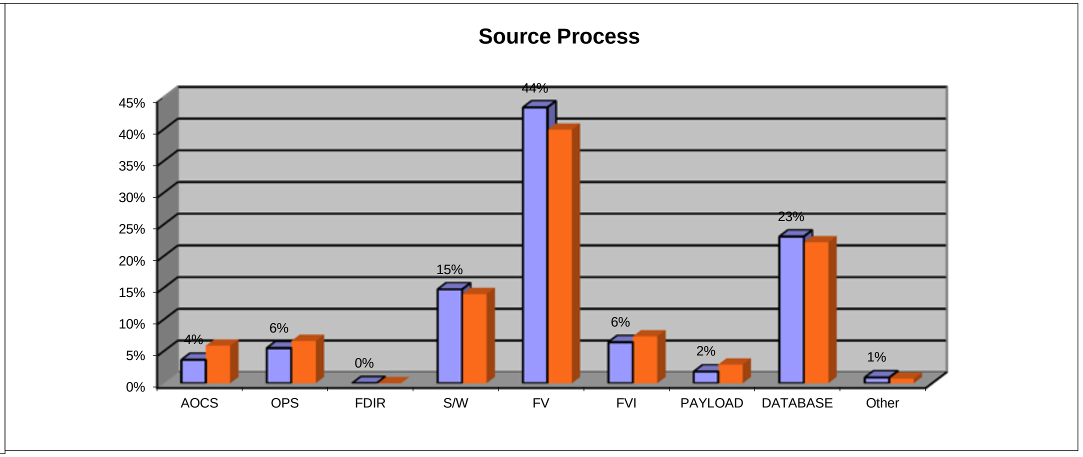
Suitability for verification purpose through efficiency KPI (Functional domains)

- Functional NCR’s KPI synthesis (2 current running programs, close to end of EFM phase) : NCR on EFM phase / NCR + PR on EFM phase







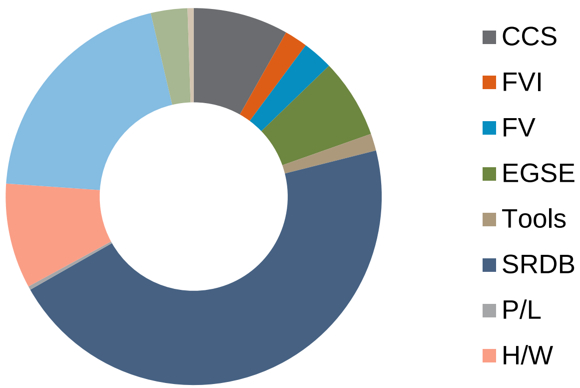


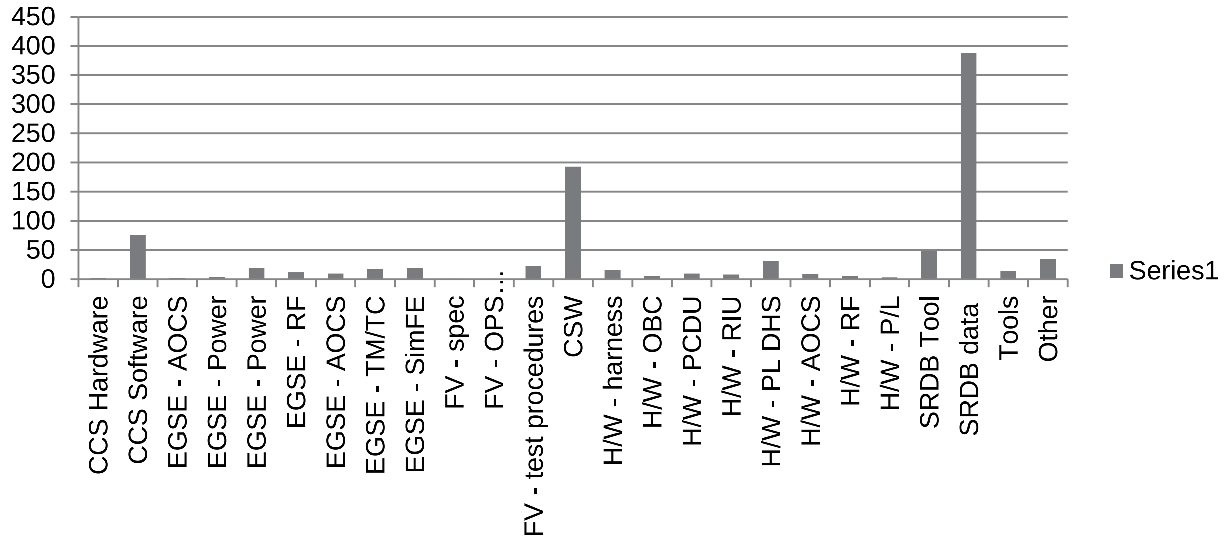
NOVABASE like life · ScopeSET The Tools Experts · AIRBUS DEFENCE & SPACE

Cartography of current models : Efficiency analysis

Suitability for verification purpose through efficiency KPI (Functional domains)

- Functional NCR's KPI synthesis (3rd running program in PFM AIT upfront environments) : NCR on EFM + PFM





NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Cartography of current models : Efficiency synthesis

The whole shows that :

- Verification at equipment delivery can still be improved, most of equipment related issues are found at ambient testing
- Environment testing is not raising too much issues, showing that model philosophy is fairly adequate.
  - Acoustic and Thermal are sometimes at stake
- Data management and S/W maturity (overall : validation of spec + development) is still somehow at stake in our programs, at start of functional testing (this is “somehow” classical), but sometimes up to late in program
  - Some S/W issues are coming from lack of capability to easily represent the design in an effective manner
  - Design complexity (and associated datasets) can be high on autonomous missions
- Some straylight (in testing : as build / as modelled differences), or radiation issues (by analysis when consolidating data) are found late at system level
  - Models or data sheet issues, not methodology or tools
- Dedicated tests and sometime benches are adequately set in place for project critical aspects
  - Radiation testing
  - Magnetic cleanliness
  - Spotted Thermal Models
  - Mock-up for harness routings

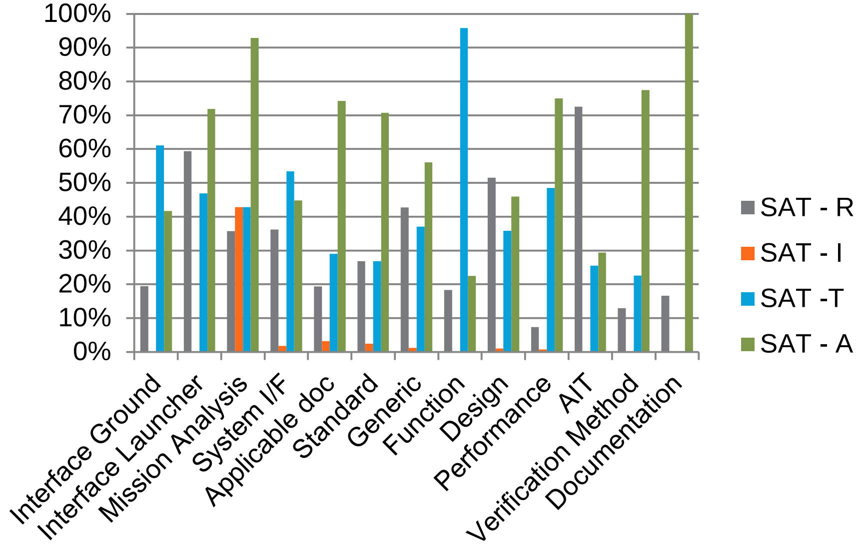
NOVABASE like life

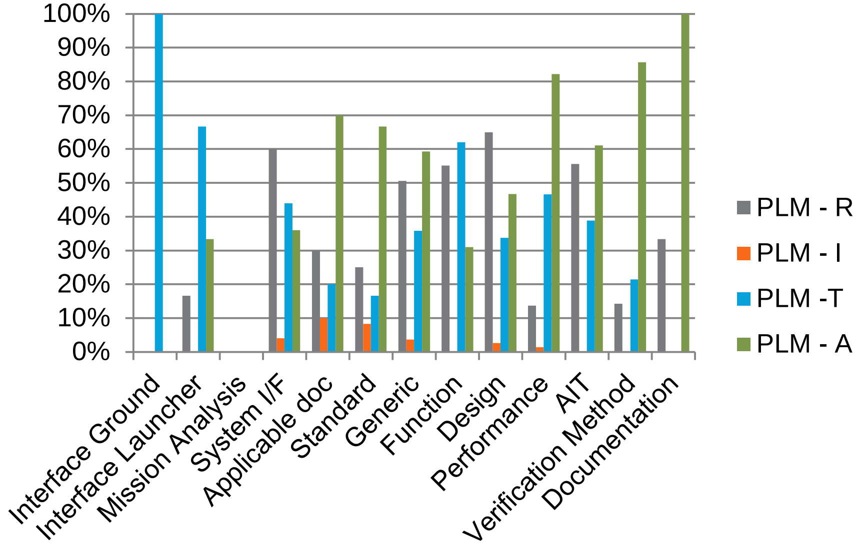
ScopeSET The Tools Experts

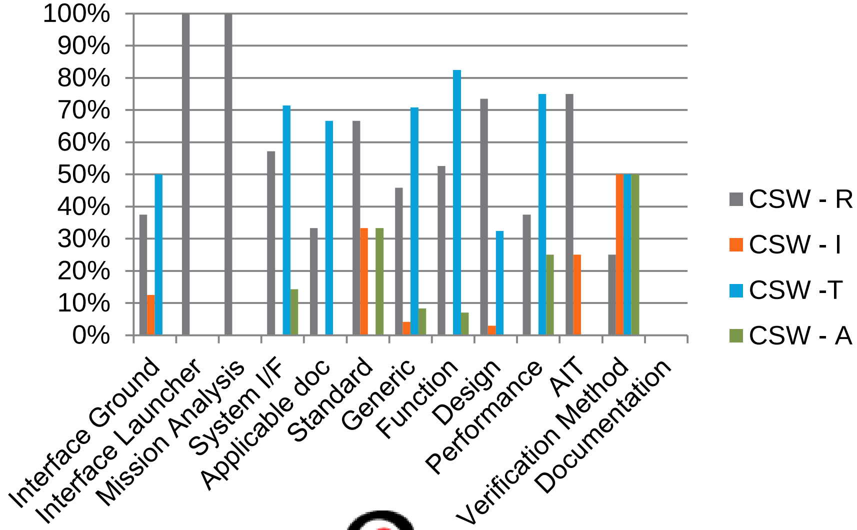
AIRBUS DEFENCE & SPACE

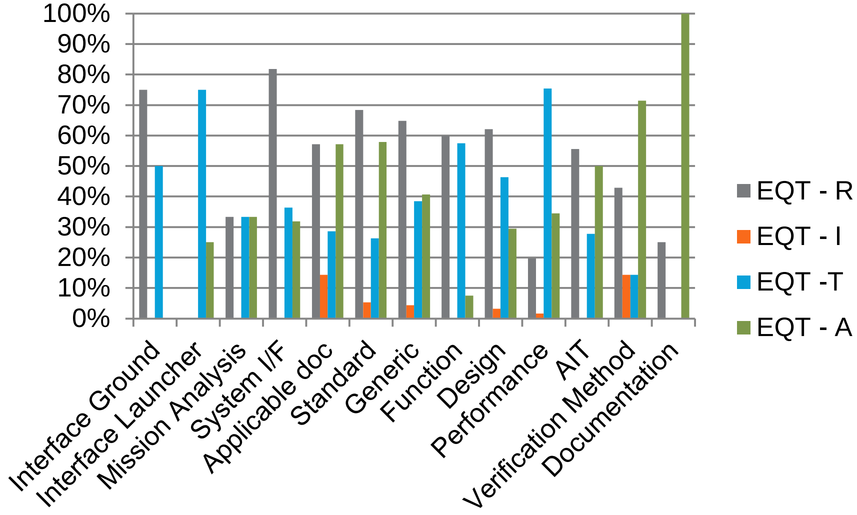
Topology of requirement closure - Overview

Analysis of method per class of requirements from a science project VCD









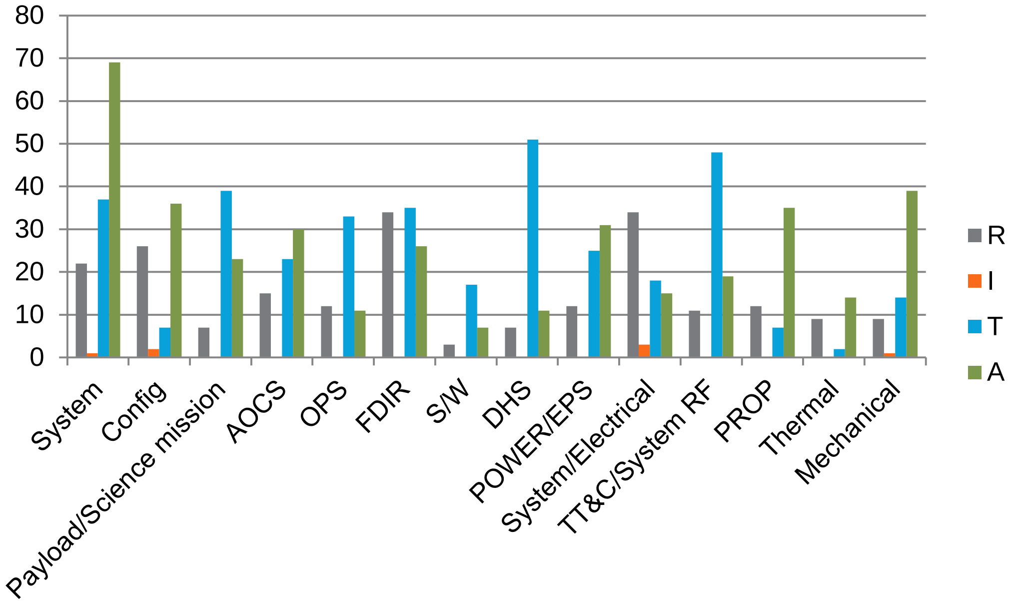
NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Topology of requirement closure - Overview

Analysis of method per source of requirements from a science project VCD



Handling (and sometimes nature) of requirements is quite different between different disciplines

- Analysis is the main axis to consolidate system level
  - Example : radiation, contamination, magnetic, pointing …
- Analysis to consolidate Mechanical / Thermal / Propulsion
  - Example : prediction of environment (BOL / EOL)
- Test to consolidate Electrical / Functional systems & Payloads
  - Example : Functions, performances

NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Mapping of tests phases on benches and verification link

	Simulators	EFM	PFM	FM2…
I&T		AIT Preparation objective Development objective	AIT objective	AIT objective
FFT-W (and RFT)	Debug objective	AIT Preparation objective Functional Design Development and Qualification objective	Specimen Functional Acceptance objective Contributes to VCD	Specimen functional Acceptance objective Contributes to VCD
FFT-Q (open loop)	Debug objective	Functional Design Qualification objective Contributes to VCD	(Back-up in case of representativeness of EFM, Contributes to VCD)	Not applicable
FFT-Q (closed loop)	Functional Design Qualification objective (mission and SW applicative layers) Contributes to VCD	Functional Design Development and Qualification objective (H/W to SW interface, decentralised S/W) Contributes to VCD	Not applicable	Not applicable
PT	Debug objective	AIT Preparation objective Functional Design development and Qualification objective	Specimen Functional Acceptance objective Contributes to VCD	Specimen Functional Acceptance objective Contributes to VCD
MT	Debug objective	AIT Preparation objective Functional Qualification objective Contributes to VCD	Specimen Functional Acceptance objective Contributes to VCD	Specimen functional Acceptance objective Contributes to VCD

Data management strategies and performance budgets consolidation approach

Team Centric Case :

- Manual approach for system data and SRDB for shared functional data sets (TM/TC, CSW, AOCS, Operations, benches)
  - SRDB Baseline management is handled manually, but consistently within the system teams
    - Links rely on system communication flow
  - Budgeting assumptions are handled manually
    - Data Users are generally the collectors / producers,
    - Traceability of assumptions in budgets is <u>always</u> implemented
    - Checks of assumptions is <u>always</u> performed at system engineer level
- Role & duty of system engineer is then essential
  - Dispatching of information where is needed : requires high skills
  - Mandatory high implication into baseline management
  - Checking is essential at his level : he “is” the baseline
- Asset (claimed by team)
  - Versatility, decentralisation, communication and team integration
- Drawback (as seen from outside)
  - “Team centric approach”, rather than “model centric approach”

Data management strategies and performance budgets consolidation approach

Model Centric case :

- FTM for functional test
  - A tool and process to manage end to end functional testing
    - From spec, …
    - … to procedure …
    - … to configuration …
    - … to supporting report
- Database
  - Engineering Data Repository Plan
    - Use Case Scenarios and Data Flow defined therein
    - Responsibilities expressed
    - A one data one source database and data management view from equipment inputs to system
- DMU
  - Physical and property modelling and data
  - ease of assembly tree planning
  - Formalisation and compliance check with respect to design constraints / requirements
  - Axis to imrove quality of supplier models and integration

Analysis of sensitivity to mission classes

Stable mission (stable thermal environment)

- Lagrange location point where thermal environment are stable (L1, L2)
- Ease thermal design by reducing thermal flux variation
- Stability wrt attitude control shall be considered
- ⇒ stable budgets with margin so no interest into high accuracy models
- ⇒ challenging requirements / low margin can drive modelling needs

Manoeuvring mission

- Earth observation mission
- Highly variable thermal environment (Sun, Earth)
- High interest to dynamic behaviour wrt the thermo-elastic distortion and pointing performance accuracy
- ⇒ Need of correlated models (AOCS, TT&C, Thermal, Power) for early validation and more efficient analysis thanks to valid hypothesis

Telecom mission

- Precise antenna pointing or coverage paths

Survey of engineering tools and models that can be made mature more early in the life cycle

Functional :

- AOCS :
  - Functional AOCS algorithms models already exists for engineering and performance analysis
  - Autocoding of AOCS functional algorithms is now proven as an asset, and is emerging as an operational technique, that will allow to manage transition from A phases models to C/D
- Non AOCS :
  - Room exists for Functional Engineering Simulator in high level languages (AADL, SysML, …), As shown by the return of experiences from projects, despite functional complex designs, OPS-S/W-FDIR baseline are represented as paper document in B early C phases (specifications), preventing :
    - Early validation by use cases (functional simulators / executable specification)
    - Changes impact analysis
  - Enforcing Model Based qualification of functional requirements on the existing model philosphy : workmanship acceptance + model check logic on PFM

Survey of engineering tools and models that can be made mature more early in the life cycle

Mechanical

- Early acoustic models to assess the mechanical environment on large appendix
- Early micro-vibration models for performance assessment and identify weaknesses

Thermal

- Early payload model (dissipation, conductivity, thermo-optical properties) for thermal design architecture
- Verification of S/W thermal control table in a dynamical context

System

- Integrated simplified functional model coupling (sizing, flight domain assessment) : AOCS, Power, thermal, RF for manoeuvring satellites

Main findings on current practice

- **Verification at equipment delivery can still be improved** Most equipment related issues are found at ambient testing

- **Environmental verification fairly adequate from equipment to system level** Sometimes acoustic, thermal, microvibration issues found late
- **Potential for improvement by provision of an adequate acoustic model for large appendages**

- **Some issues** on model usage arising from **absence of correlation with as-built or baselin**e MCI, thermal, straylight, where **as-built geometry is key** to model fine properties

- **Lack of cross-sectorial analysis** Root cause is **lack of data management and configuration capability across disciplines** - “islands of consistent models” (Functional/Mech/Therm)

- **Overall adqeuate approach found for dedicated tests and benches for project critical aspects**
- **Growing model usage to secure AIT preparation, meeting cost/schedule pressure**

Main findings on current practice

We see benefit to **clearly separate** verification purpose at requirement level between **Qualification and Acceptance** in verification planning and VCD tracking (even when mixed on one model i.e. PFM)

Requirement closure mainly driven by aggregation of levels / methods

System level is the preferred place to close requirements for many reasons, industrial set up and interface management being two main ones

Analysis is main axis to consolidate real system level discipline (radiation, contamination, magnetic, pointing…)

- Analysis to integrate and consolidate Mech/Therm/Prop, correlated by test SM/STM/TM not really claimed to close requirements
- Test used to consolidate Elec Func systems and Payloads
- **Testing on PFM by far preferred approach to close functional and design requirements, whereas existing deployed hybrid model approach could support it already**

Main findings on current practice

- **Room exists for a Functional Engineering Simulator in high level languages (AADL, SysML…)** Early validation by use cases of OPS-S/W-FDIR baseline
- Impact analysis on changes

- System models – **better and earlier** differentiation between **qualification and acceptance** activities across the model philosophy for requirement close-out, **simplified functional model coupling** to ease sizing case selection and provide flight domain assessment
- **Early acoustic and micro-vibration models where needed for early feasibility assessment**
- **Verification of S/W thermal control table in a dynamical context**

Model Classes / Verification types terminology

Facility	SCS	MPS	FES	FVT	SVF	MU	FOM	DRE
Name	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
Target System Milestone(s)	SRR, PDR	SRR, PDR, CDR	SRR, PDR, CDR	CDR, FAR	CDR, QR/AR	SRR, PDR, CDR	CDR, FAR	Whole lifecycle
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 types :

- Requirement closure – Verification (REQ)
- Overall Design validation (VAL)
- Detailed design consolidation – breadboarding for risk mitigation (DDC)
- Design or I/F freeze – proof of concept (POC)
- Proof of Architecture (POA)
- AIT or OPS preparation (PREP)

Main Outcomes – Model Fidelity Requirements

Facility	SCS	MPS	FES	FVT	SVF	MU	FOM	DRE
Name	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	POA	POC, REQ	POC	DDC, VAL, REQ	REQ (S/W)	POC, DDC, PREP	DDC, VAL, REQ, PREP	N/A

Main outcomes – New model Philosophy

USE case Name	Model Name	Model type	MBSE Type	Verification type	Model Phasing in life cycle	Model Continuities
Early Verification of Operational concept	Operational Concept Simulator (OCS)	SCS	Type 2	Proof of Architecture (POA)	PDR, early C	CONOPS to be further used in Functional Design Simulator FES
Architectural Design and Mapping	Architectural Design and Mapping Model (ADM)	SCS	Type 2	Proof of Architecture (POA)	PDR	function model and connectivity matrixes of to be further used in Functional Design Simulator FES and as SSS entries to FVI units specification + SE(DB) top level entries
OBSW Design modelling	OBSW Requirement Model (OSRM)	SCS or FES, depending implementation technology	Type 2	Design or I/F freeze – proof of concept (POC)	PDR, Phase C (up to SW PDR)	OBSW Requirement Model to be further used in Functional Design Simulator FES
AOCS-SW MBSE with Auto-coding	AOCS Modes and Control Model (AMCM)	as seen for AOCS a FVT, as seen from SW a SVF	Type 2	For AOCS performances : Requirement closure – Verification (REQ) For AOCS MCL OBSW perimeter : Requirement closure – Verification (REQ) wrt applicable SW requirements and Overall Design validation (VAL) wrt system AOCS design functional requirement For FVI models : Detailed design consolidation – bread boarding for risk mitigation (DDC)	Early C, CDR, AR	link with Functional Design Simulator to be analysed
Functional Design Simulator	Functional Design Simulator (FDS)	FES (FVT for PUS tables ?)	Type 1	For operability issues, OPS modes and procedure architecture Overall Design validation (VAL) For FOP, OPS preparation (PREP) For detailed functional design, Detailed design consolidation – breadboarding for risk mitigation (DDC)	Phase C (SW PDR to SW CDR, EQT CDR – 6 months)	inheritance of CONOPS model from Operational Concept Simulator (OCS) inheritance of function model and connectivity matrixes from Architectural Design and Mapping Model (ADM) inheritance of OBSW Requirement Model from OBSW Requirement Model (OSRM) Link with AOCS Modes and Control Model (AMCM) to be analysed wrt S/W spec, FDIR implementation / operability, as scopes are overlapping. Preliminary Failure model (feared events) to be shared with Failure Mode Model (FMM)

Main outcomes – New model Philosophy

USE case Name	Model Name	Model type	MBSE Type	Verification type	Model Phasing in life cycle	Model Continuities
FDIR & RAMS analyses	Failure Mode Model (FMM)	as seen for FDIR design aspects a FES, as seen from RAMS aspects a FVT	Type 2	For FMECA/HSIA aspects : Requirement closure – Verification (REQ) For FDIR analyses aspects : Overall Design validation (VAL) For FDIR design aspects : evolving from Design or I/F freeze – proof of concept (POC) to Detailed design consolidation – bread boarding for risk mitigation (DDC) in life cycle	PDR, CDR, AR	The Model-Based FDIR Process defined consists in creating an abstract model of the system representing its architecture (hardware, functional) and its behaviour under failure (failure modes propagation, FDIR). Design trade-offs are supported by analysis tools and use of simulation capabilities. Export of model information is used to create design documentation (FMEA/HSIA tables, SW requirements, etc.). The modelling of Failure Modes shall be scalable, from a feared event model to a true failure model fed from units / subsystem FMECA's. The modelling of Failure Modes and effects should be shared with the Functional Design Simulator (FDS) and the Augmented FTM (AFTM)
Power / Thermal sizing	Power Thermal Sizing Simulator (PTSS)	FES	Type 1	Design or I/F freeze – proof of concept (POC)	PDR	Link with SEDB, power budget and TMM.
AOCS/POWER/TT &C/THERMAL management	Flight Domain Verification Model (FDVM)	FES evolving to FVT	Type 1	For FES use case : Design or I/F freeze – proof of concept (POC) For FVT use case : Requirement closure – Verification (REQ) and OPS preparation (PREP)	Early C phase, CDR, AR, Flight operations	Requires TMM, System SVF, Power / energy budget tools, RF budget tools Evolution from FES (used preliminary sizing with simplified models) to FVT (used for verification with hi-fidelity models is pending maturity in life cycle) Inputs to Coupled Thermoelastic analyses (TAB) regarding mission profiles

Main outcomes – New model Philosophy

USE case Name	Model Name	Model type	MBSE Type	Verification type	Model Phasing in life cycle	Model Continuities
Thermal FVT	Thermal FVT (TFVT)	as seen for TCS S/W algos and tables a SVF, as seen from Overall TCS aspects a FVT	Type 1	Requirement closure – Verification (REQ) with correlated TMM Overall Design validation (VAL) / AIT preparation (PREP), upfront TB/TV for algos and Tables Detailed design consolidation - breadboarding for risk mitigation (DDC) for SW in early phases	from SW CDR for algorithms to Phase D (,E) for tables	Coupling of already existing SVF and TMM, evolution of TMM maturity in life cycle, allowing to evolve verification level accordingly
Coupled Thermoelastic Domain analyses	Thermoelastic Analysis Bench (TAB)	FVT evolving to FOM	Type 1	Evolving from Overall Design validation (VAL) to Requirement closure – Verification (REQ)	CDR, FAR	Connection of domain models sharing datasets (FVDM/TFVT, FEM, TMM)
AIT – Augmented reality	Virtual Assembly Model (VAM)	FOM	Type 1	AIT preparation (PREP)	Phase D (PFM / FM AIT)	Plugin on top of GFM, sharing large data sets + proprietary data sets
AIT – Automated Harness verification	Executable EICD (E²)	FOM	Type 1	Overall Design validation (VAL) for Harness AIT preparation (PREP) for Equipment Signals	Phase D (PFM / FM AIT)	Coupling of EICD base (Equipments / system), Harness geometrical routing base (in DMU), GDIR requirements
AIT – Functional Test coverage management	Augmented Functional Test Manager (AFTM)	FOM	Type 1	AIT preparation (PREP)	PDR + 6 months to FAR	Data Repository coupled with shared items of Architectural Design and Mapping Model (ADM) and Failure Mode Model (FMM) for consistency checks
AIT – TV management	TVAC Test Simulator (T²S)	FOM	Type 1	AIT preparation (PREP)	Phase D (PFM / FM AIT)	similar to TVFT, coupling of already existing SVF (actual SIMAIT instance) and TMM (actual TB/TV configuration instance), tailored to the test configuration

Main outcomes – New Data Repository

USE case Name	Model Name	Model type	MBSE Type	Verification type	Model Phasing in life cycle	Model Continuities
Global physical model	Global Physical Model (GFM)	DRE	Type 2	N/A Scope : Extending perimeter of Digital Mock Up (ie geometrical information base) with physical datasets related to system analyses (thermal, power, RF, radiation, contamination…)	Whole life cycle, evolving with baseline knowledge	DRE feeds overall model philosophy Plugin on top of DMU.

NOVABASE like life

ScopeSET The Tools Experts

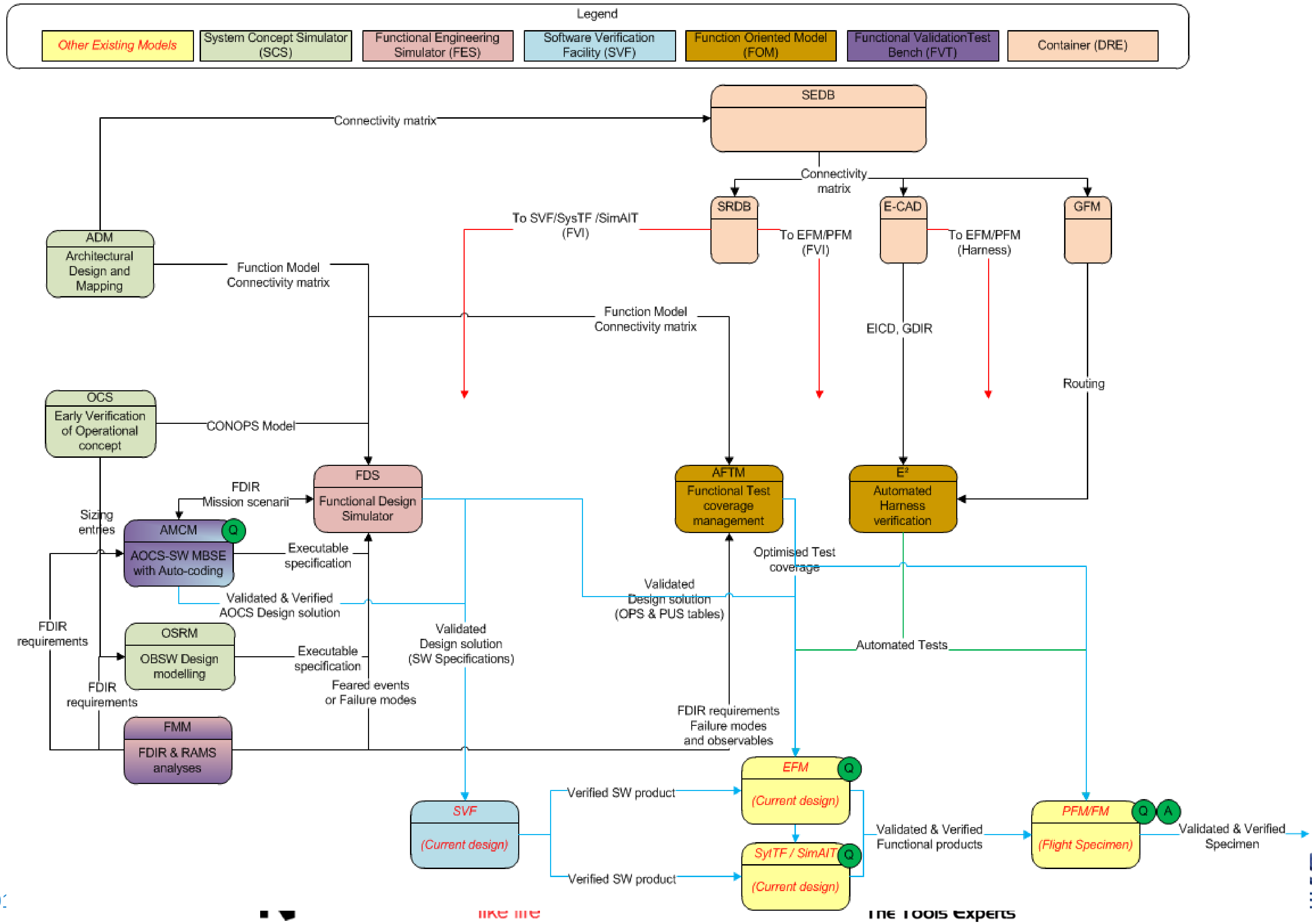
AIRBUS DEFENCE & SPACE

Main outcomes – Qualification & Acceptance

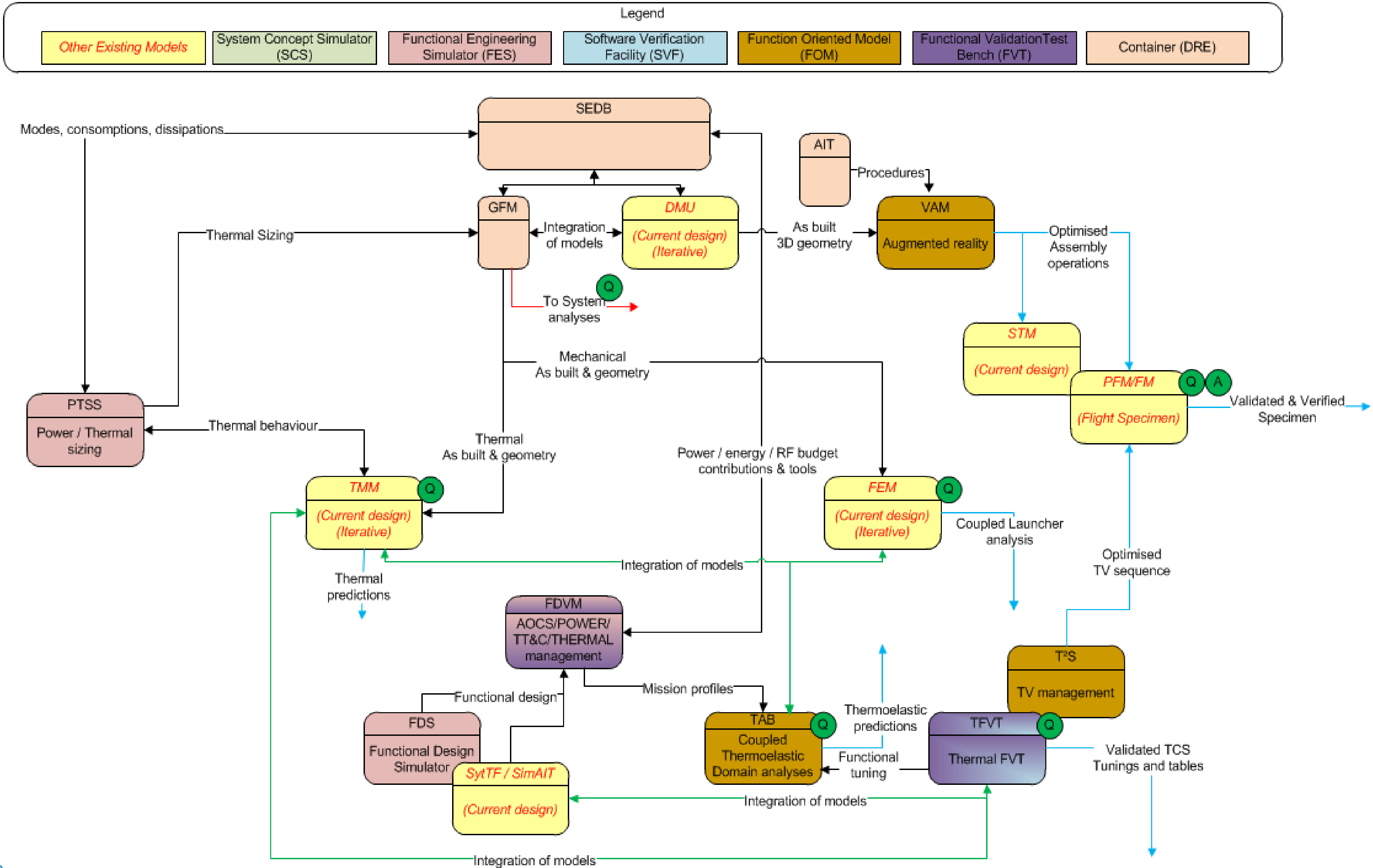
Regarding formal requirements verification aspect, there are really two different objectives to be accounted for : Qualification and Acceptance.

- An accurate differentiation between both aspects in the early requirements engineering phases is a key enabler for an MBSE efficient approach.
- Model solutions oriented towards qualification objectives should be developed incrementally in early stages of the project.
- This allows subsequent focusing of the PFM verification activities towards acceptance of design assembly & workmanship at system level, any needed activity to calibrate / characterize system models with the flight specimen.
- As a fall-back, qualification for areas subject to late as-built evolution or known models representativeness issues needs to be performed on PFM.
- Design qualification test effort shall be done at the right representativeness level, as soon as possible in the program, so as to kill development risks and check interfaces, then functions.
- Acceptance testing shall be limited on the schedule critical paths to regressions with the as-built.

Main outcomes – Animation of models, Elec & Func.



Main outcomes – Animation of models, Thermal



Main outcomes – verification on new philosophy

Thermal example – target MBSE view

	Items to be validated	Analyses	Unit tests (supplier level)	Simulators (SCS / FES)	Function models (FVT / FOM)	S/W Tests (SVF)	TMM / DMU	STM	PFM	FM
nent requirements (system)		Q					Prep	Prep	Prep	A
nent requirements (units)		Prep	Q				Prep			
	Thermal responses (global)	Prep			TB/TV prep on T^2S		Prep	Q_1	Q_2	A
	Thermal responses (local)	Prep			TB/TV prep on T^2S		Prep	Q_1	Q_2	
	Elementary Material Thermal properties	Prep	Q				Prep			
	Elementary component performance	Prep	Prep				Q	Prep	Prep	
ign	Heat pipes sizing			Prep (PTSS)			Q	A	A	
	Radiating surfaces sizing			Prep (PTSS)			Prep	Q_1	Q_2	
	Heating power			Prep (PTSS)			Prep	Q_1	Q_2	
	MLI geometry	Prep					Prep	Q_1	Q_2	A
	Thermal HW geometry	Prep					Prep	Q_1	Q_2	A
	Conductiveness	Prep					Prep	Q_1	Q_2	
	Workmanship							Prep	Q	A
	Heater location	Prep					Prep	Q_1	Q_2	
	Thermistance location	Prep					Prep	Q_1	Q_2	
	Thermal loop definition	Prep					Prep	Q_1	Q_2	
tion lity/	Thermal loop algorithm				Q(TFVT)	Prep		A	A	A
	Thermal loop performance						Prep coupled with correlated DMU	Prep, Q_1	Prep, Q_2	
	Thermal loop thresholds table				Q(TFVT)	Prep		A	A	A
del		Prep			TB/TV prep on T^2S		Q coupled with correlated DMU			

Better use of our models (here TMM geometrical correlation upfront TB/TV)

New proposed model and implications

Main outcomes – verification on new philosophy

Complete diagrams exist for verification logic of each of:-

- DHS
- AOCS
- OPS / FDIR
- Software
- Power
- Electrical System
- TT&C
- Thermal
- Mechanical
- Propulsion

Main outcomes – MBSE cost effectiveness

Cost effectiveness form assets of alternate MBSE approaches can be categorized through different categories :

- Direct costs savings,
- Schedule induced cost

Both categories are themselves split as follows :

- Saving from avoiding non quality engineering impacts in programs : avoid doing errors
- Saving from performing a leaner engineering effort on a given model philosophy : doing the same things slightly differently, but more efficiently
- Saving from implementing a leaner a model philosophy : addressing the things differently

MBSE approaches on programs (new development cases) can be assessed globally at the level of :

- - Few months of schedule on the program critical path (typically 2 to 3).
- - Few M€ of overall engineering / project work effort, when consolidating both the direct effort saving and the valorisation of schedule impacts

Concept Idea 1 – improved model philosophy

- Despite typical usage of a **hybrid model philosophy**, functional and design **system requirement closure** is still dominated on **PFM** with **consequent effort**
- The verification process allows functional requirement **closure** at Qualification stage on **hybrid/EM** models, but this is **not significantly achieved** to date
- Protoflight system testing is therefore a mix of environmental qualification, pure acceptance, and functional qualification **repeat,** adding **schedule** and **cost**
- Issues linked with **design maturity** are seen at design **qualification** stage, principally in **functional** design area
- Formalize a **deeper model terminology** supporting the hybrid model philosophy, linked with model purpose, maturity management and verification objective throughout the lifecycle, from cradle to grave
- Couple the above with the existing verification process through **deeper delineations of verification stages** applied at appropriate Verification Level
- **Reduction of activities** on PFM and therefore schedule/cost saving
- Simpler planning and tracking due to **improved visibility** and **separation of different targets** of effort
- Greater potential to **re-use / standardise** blocks of activities

To be printed in A0

ID <Airbus DS-1> - A new model approach and terminology to support realisation of the full potential of hybrid model philosophies

Status quo

- Despite typical usage of a **hybrid model philosophy**, functional and design **system requirement closure** is still dominated on **PFM** with **consequent effort**
- The verification process allows functional requirement **closure** at Qualification stage on **hybrid/EM** models, but this is **not significantly achieved** to date
- Protoflight system testing is therefore a mix of environmental qualification, pure acceptance, and functional qualification **repeat,** adding **schedule** and **cost**
- Issues linked with **design maturity** are seen at design **qualification** stage, principally in **functional** design area

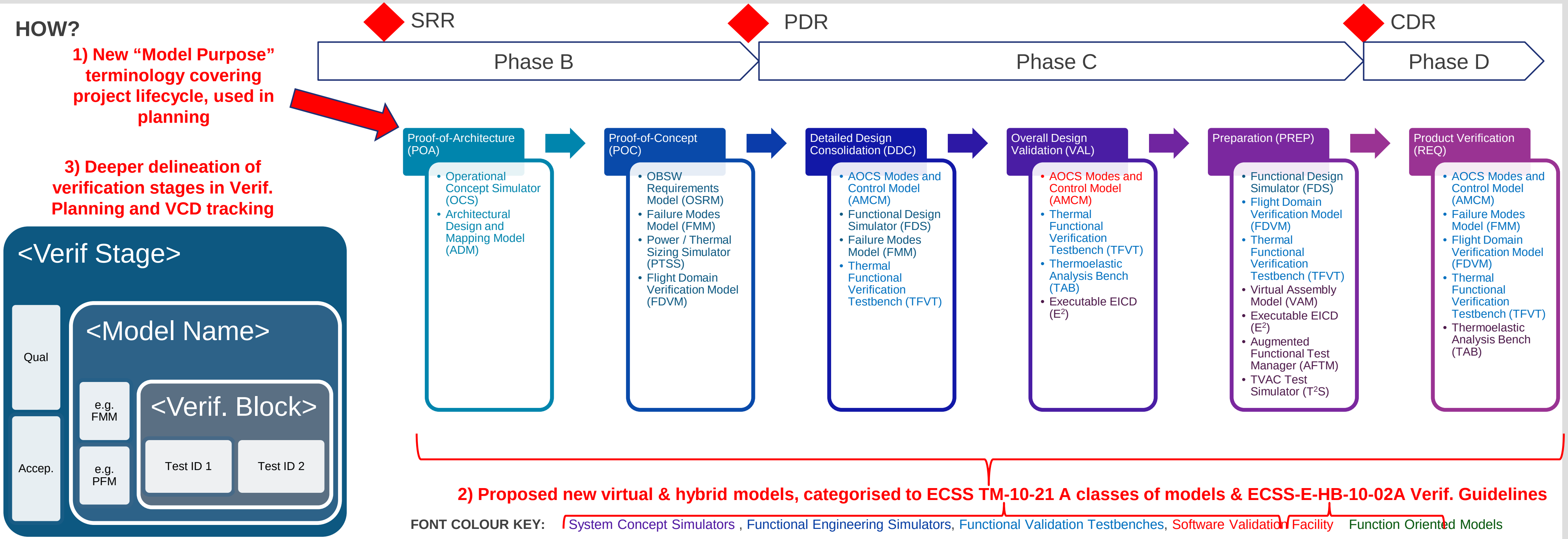
WHAT?

- Formalize a **deeper model terminology** supporting the hybrid model philosophy, linked with model purpose, maturity management and verification objective throughout the lifecycle, from cradle to grave
- Couple the above with the existing verification process through **deeper delineations of verification stages** applied at appropriate Verification Level

WHY?

- **Reduction of activities** on PFM and therefore schedule/cost saving
- Simpler planning and tracking due to **improved visibility** and **separation of different targets** of effort
- Greater potential to **re-use / standardise** blocks of activities

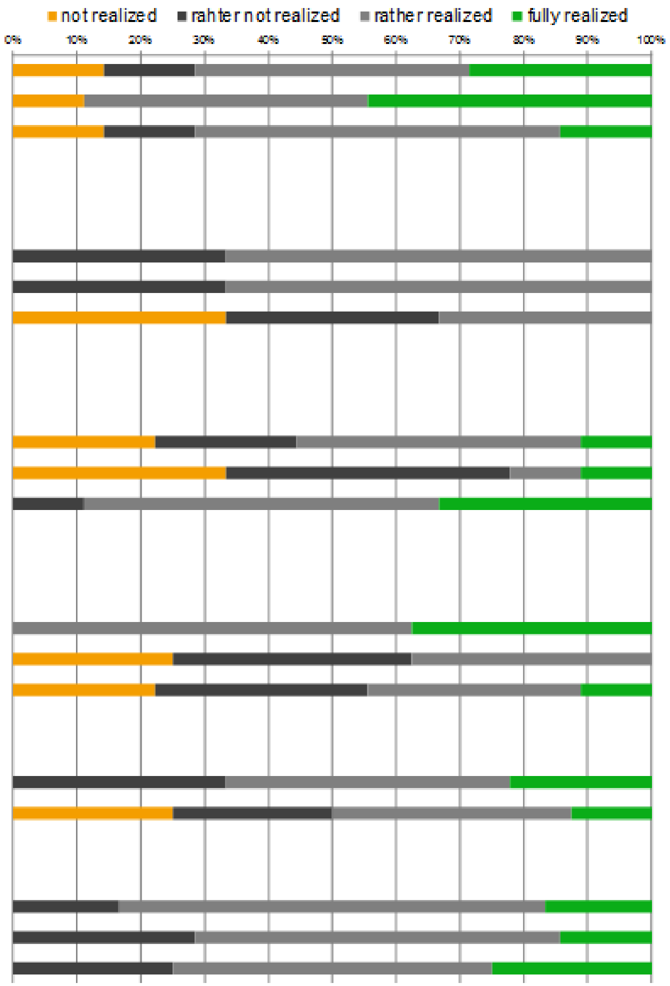
HOW?



Concept Idea 1 – New Model Philosophy

FEEDBACK: Long Term Traffic Light Green – Strengths to build on, Amber – Barriers to Tackle, Red – areas to improve or consider out of scope of concept

	# not realized			# fully realized	Average
effectiveness of specifications					
iterative requirements definition process between customer … will be enabled	1	1	3	2	rather realized
existing solutions can be matched against requirem… early in the … ss	1	0	4	4	rather realized
requirements have appropriate leve… verified mor…	1	1	4	1	rather realized
reuse					
the verification status from re… transferred	0	2	4	0	rather realized
models for reusable … s are validated	0	2	4	0	rather realized
a reference product architecture a… ces can be created	2	2	2	0	rather not realized
evidence and benefits					
the concer… managers and public	2	2	4	1	rather not realized
th… eaper, simpl… quicker	3	4	1	1	rather not realized
… required qu… ined	0	1	5	3	rather realized
co-engineering and organisati…					
speed of communication and access to in… cantly	0	0	5	3	rather realized
every party is clear on its rol… ramework	2	3	3	0	rather not realized
the config… ged efficiently	2	3	3	1	rather not realized
risk orientation					
… sks can be better evaluated and shared	0	3	4	2	rather realized
… not wasted for low risk topics and standards	2	2	3	1	rather not realized
review and verifica… ocess					
… s focus on things that really matter	0	1	4	1	rather realized
re… started early and less document based	0	2	4	1	rather realized
the verification activities can … ccording to type of mission, risks, customer	0	2	4	2	rather realized



Rather realized

Can be compatible

Confirmation of return on investment

Industrial chain implications

Confirmation of risk impact

Rather realized

Task 3: Impact of Elements Re-Use
Task 4: Definition of Suitable Review Logic

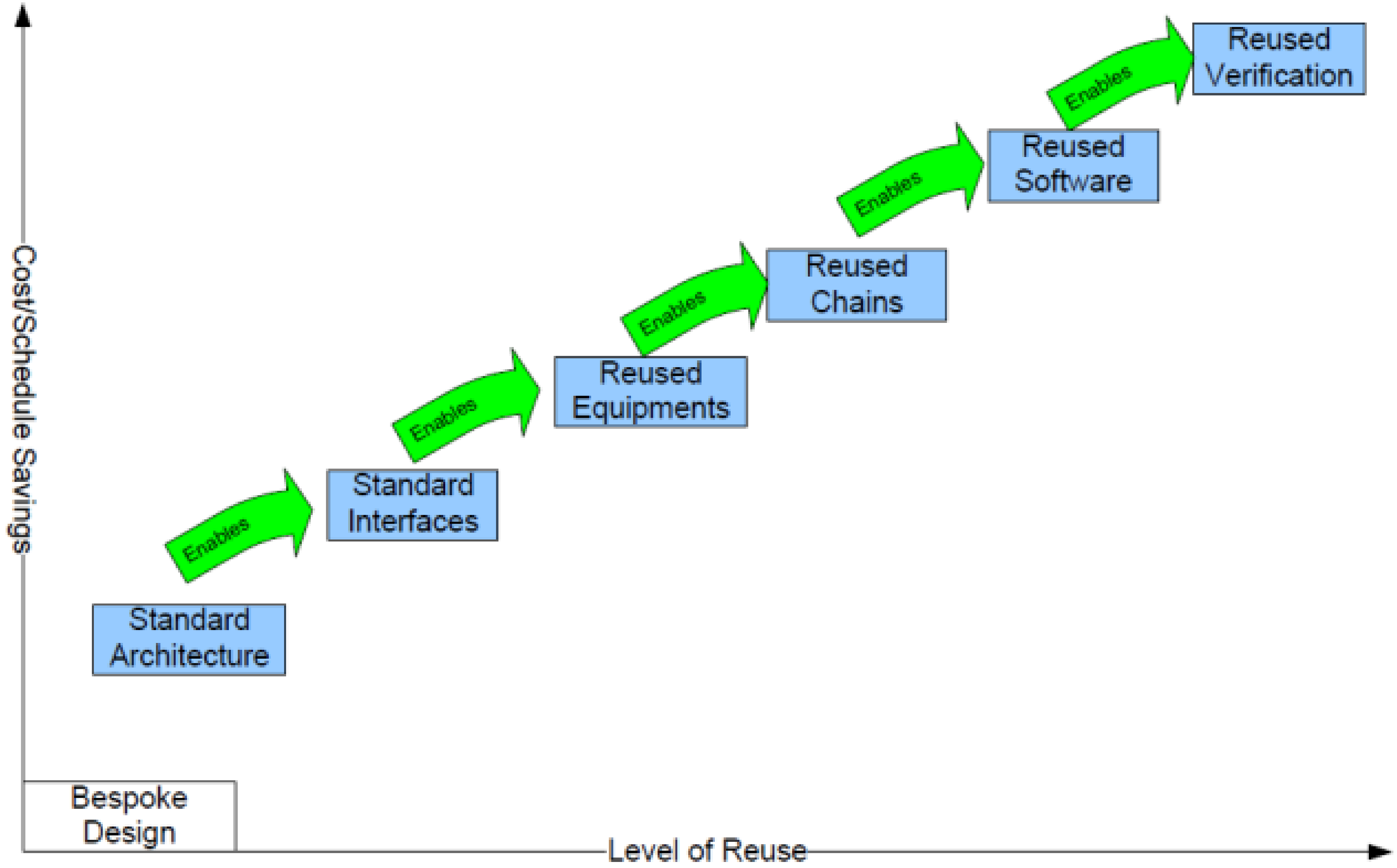
- MLR proposed routes towards an advanced model philosophy for optimised programmatic effort based on
  - Deeper graduation of the lifecycle verification objectives (in their widest sense including development phase objectives) amongst several targets, with associated proposed terminology
  - New virtual & hybrid models categorised to ECSS-E-TM-10-21A classes mapped against use cases and phase
  - Deeper delineation of Verification Stages more rigorously distinguished between Qualification and Acceptance objectives

- The above has maximum potential to realise benefit for hybrid model philosophies (including virtual models) as per Section 5.2.5.3.5 of ECSS-E-HB-10-02A

- Task 3 assesses the impact the use of heritage and the re-use of design artefacts and equipment / subsystems has on the proposed Task 2 model philosophy
  - Examination of re-use state of practice, Industry-Agency workshop findings
  - Re-use process definitions and identification of target areas
  - Concepts for model-based use cases associated to re-use

- Task 4 examines Readiness / Maturity level indicators to allow dynamic review logic and milestone allocation in the context of the proposed advanced model philosophy

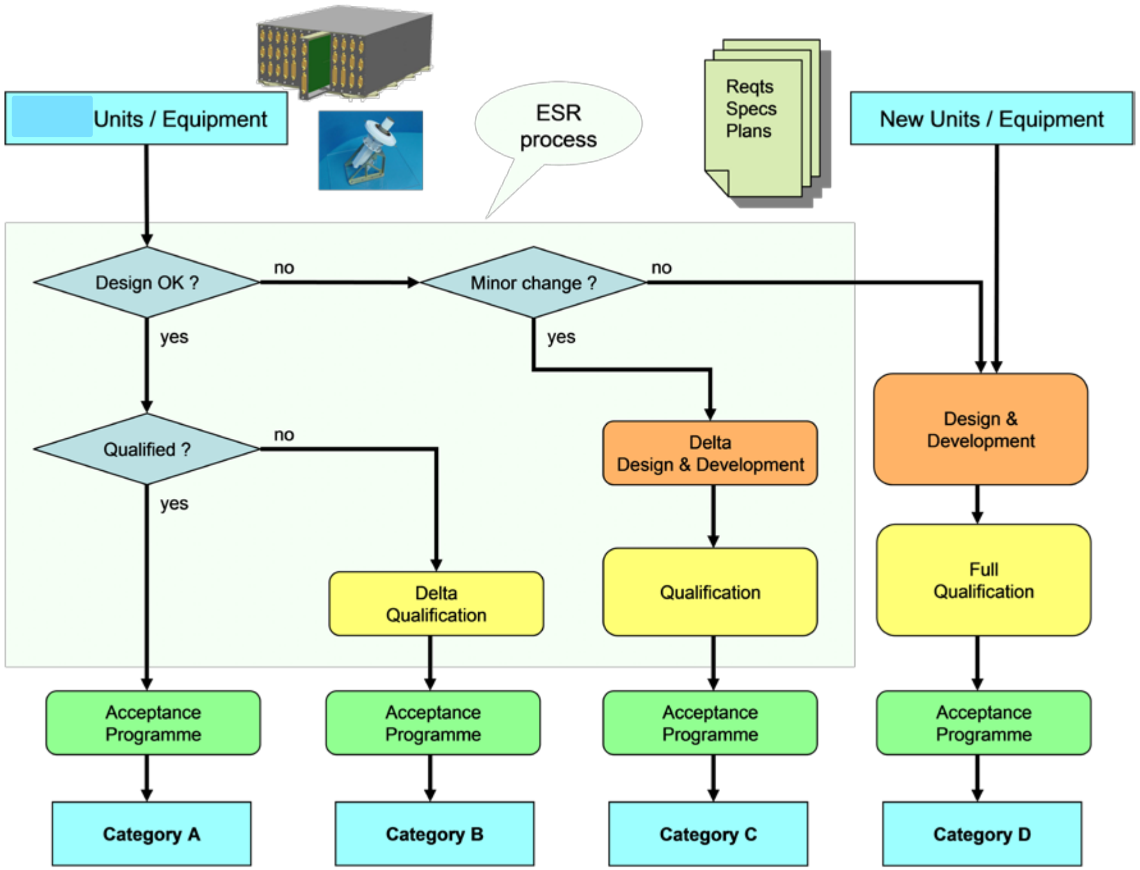
Stepping Stones towards higher degrees of re-use



Existing re-use approaches – ECSS-E-ST-10-02 C categorisation

- On a technical level, actual space product re-use approach is highlighted through the ECSS-E-ST-10-02 C product categorisation according to heritage, and supported by the EQSR, design & development, delta-qualification, qualification, and acceptance verification processes
  - Usually implemented at the level of unit / equipment as per HW/SW matrix, not functional chain / subsystem

Category	Description	Qualification programme
A	Off-the-shelf product without modifications and • subjected to a qualification test programme at least as severe as that imposed by the actual project specifications including environment and • produced by the same manufacturer or supplier and using the same tools and manufacturing processes and procedures	None
B	Off-the-shelf product without modifications. However: It has been subjected to a qualification test programme less severe or different to that imposed by the actual project specifications (including environment).	Delta qualification programme, decided on a case by case basis.
C	Off-the-shelf product with modifications. Modification includes changes to design, parts, materials, tools, processes, procedures, supplier, or manufacturer.	Delta or full qualification programme (including testing), decided on a case by case basis depending on the impact of the modification.
D	Newly designed and developed product.	Full qualification programme.



	Equipment category				Main purpose
	A	B	C	D	
Equipment Qualification Status Review (EQSR)	X	X			- Verify the acceptability of the equipment specifications, plans, lists with the mission requirements - Assess the qualification status, identify the delta qualification needs - Authorise the procurement and manufacturing activities
Preliminary Design Review (PDR)			X	X	- Verify the compatibility of the design definition and predicted performance with the requirements - Verify the coherency of the lower level constituents specifications with the equipment specification - Review plans and procedures - Review parts list, materials list & processes list - Authorise the equipment development and qualification models manufacturing - Review the production plan and MAIT flow - Review the facilities development plan
Critical Design Review (CDR)			X	X	- Verify compatibility of the detailed design and complete set of analyses with the requirements - Review the development and qualification models test results - Review the FM manufacturing file - Review the manufacturing line qualification - Authorise the equipment FM manufacturing
Manufacturing Readiness Review			X	X	-Status of product definition and requirements, differences with the status of the qualification model, and impacts of these differences; -Status of manufacturing, assembly, inspection and test documentation, differences with the status of the qualification model, and impacts of these differences; -Validation status of manufacturing processes, with particular emphasis on critical processes; -Implementation of dispositions for risk reduction, as defined by risk assessment, into the manufacturing, assembly, integration, inspection and test procedures; -Availability of specified production, measuring and inspection equipment, and calibration status, when relevant; -Cleanliness of facilities, with respect to the specified cleanliness levels; -Facility temperature and humidity with respect to requirements.
Test Readiness Review (TRR)	X	X	X	X	- Review test procedures, test plan and sequences - Verify the readiness of the test equipment - Review as-built configuration
Test Review Board (TRB)	X	X	X	X	- Review test results - Disposition of NCRs - Review equipment documentation
Delivery Review Board (DRB)	X	X	X	X	- Verify that all actions are properly closed - Review completeness of the documentation - EIDP and Certificate of Conformance - Consent to ship

Existing re-use approaches – ECSS-Q-ST-20-10 C off-the-shelf HW

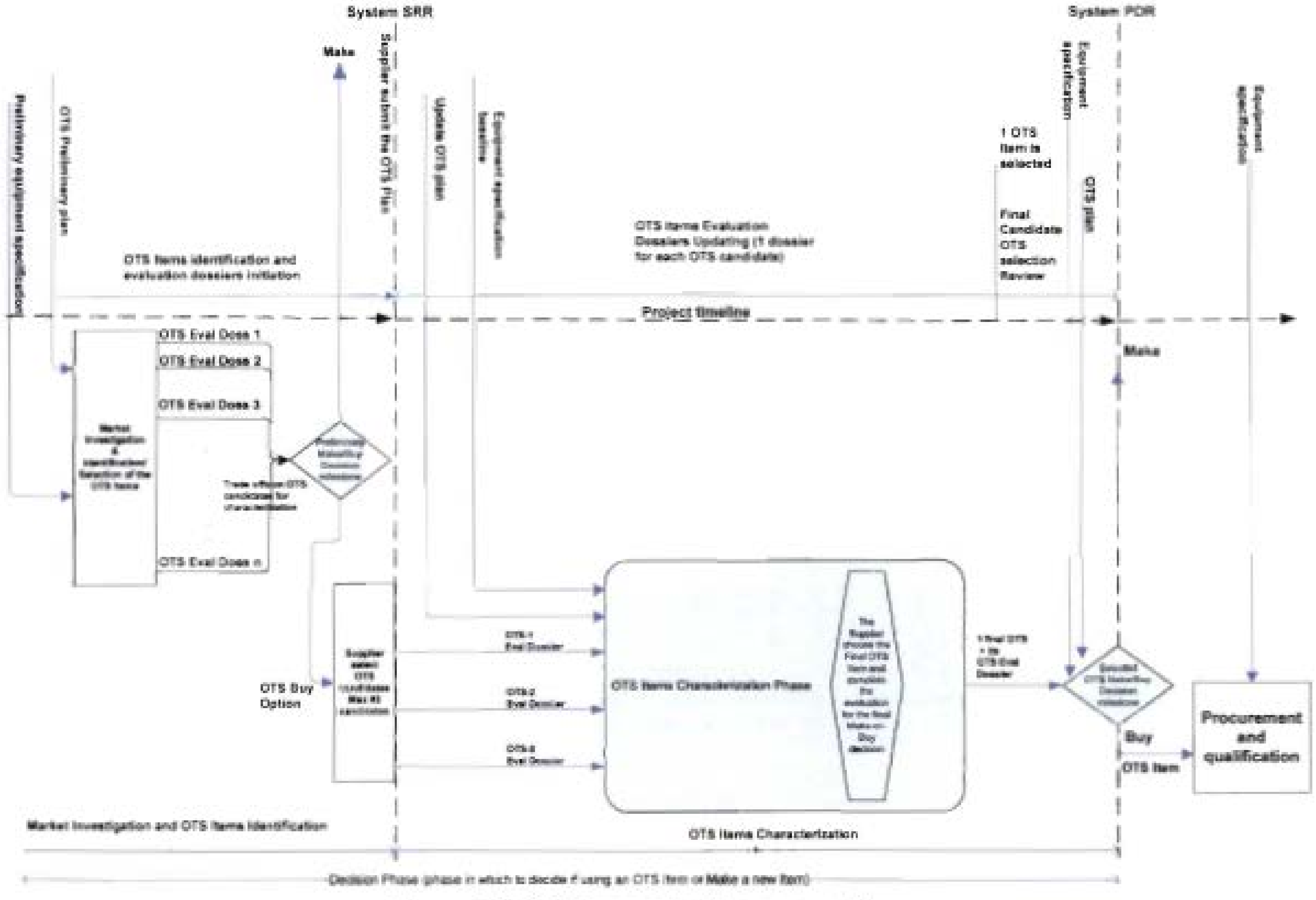


Figure 4-1: OTS items selection process flow

Covers

- Complex OTS items

Does not cover:

- Software OTS
- Items already qualified for space applications
- Pieces, parts and materials

Not specifically addressing re-use of OTS items for the same space application for which they were initially qualified

“Closed” project requirements landscape assumed, document intensive process

A priori - Perceived Obstacles to Re-use

- Existing re-use mainly is at the level of equipment / unit or lower, not functional chain / subsystem
- Over-specification and inflexibility top-down from the target application project
  - Are the project requirements a valid minimum set? Does need to differentiate suppliers at bid drive to overspecify?
- Lack of efficient means to answer the “Design OK?” question in all details responding to the requirements flowed from the top-down
  - Comparison of large numbers of requirements and design against requirements including different origins, wordings, breakdown, assumptions (hidden and explicit)
  - Additional information requests to suppliers immediately reduces the economic benefit of re-use (cost, schedule)
  - Project specific documentation demands
  - More difficult synthesis from various equipments to functional chain level bottom-up, than reverse top-down
- Industrialisation process
  - Open ITT with “supplier neutral” procurement spec misses the opportunity to re-use existing bottom-up unit specifications from the beginning
  - Mindset
    - “Is it as much as I can get” rather than “is it enough”

From analysis of Industry-Agency workshop identified critical success factors, major axes of interest are…

- Requirements Engineering & Validation
- Industrialisation scenarios
- Project process

Requirement Landscapes & Requirements Validation (not System Validation) – i.e. confirmation of the requirements set

The process of establishing a project requirements set progressively moves from an "Open" to "Closed" landscape through Phase 0 and A, and finally B1, with requirements validation marking the transition point. **It is during the "Open" phase** that iteration with potential bottom-up solutions, or at least consideration to rigourously avoid over-specification, **offers the best chance to maximise the opportunity for solution re-use**.

The traditional B2CD "top-down" requirement flow can be considered rather "closed" in the sense that once the requirements are issued, the potential to consider alternative requirement sets is much reduced. Any re-use opportunities not considered or allowed for in the preparation of the requirement set itself will tend to be "locked out" or at least face difficult process to be considered, as described in the "Perceived Obstacles to Re-use".

An example "open" requirement landscape built for re-use on the other hand, **imposes nothing (or much reduced) top-down and examines what can be achieved from assembling available "bottom-up" building blocks**. This could give many options and alternative requirement sets, from which a selection must be made. The "Open" requirement architecture will migrate to a "Closed" one but having been rather driven by re-use. However this approach embarks on a journey with **weakened links to a clear end mission goal (from mission requirements document) and is therefore likely reduced in scope to "special" missions of opportunity**.

It is clear that the requirements validation step (ensuring the requirements set is the right one) is key.

ECSS-E-ST-10-06 C Technical Requirements Specification – extracts and ideas to better align with the Critical Success Factors

4.1 Technical requirements specification purpose and description

The technical requirements specification is a document through which a customer expresses his needs (or those that he is responsible for expressing) and the related environment and constraints in terms of technical requirements.

The technical requirements contained in the TS allow for potential suppliers to propose the best technical and programmatic solutions.

NOTE The intention of the technical requirements specification is not to assume or refer to specific solutions.

The TS is the technical reference for the qualification of the design and for the acceptance of the end product.

In that scope, the technical requirements contained in the TS are subject to the agreed change process defined in the business agreement. They are attainable and verifiable.

NOTE The change process itself can change in between project phases (Phase 0, A, B, C/D).

How to measure the "solution free" aspect, with the aim of avoiding over-specification?

How to enter assessment of pre-existing building blocks against the TS?

ECSS-E-ST-10-06 C lists 12 types of technical requirements – these can be further simplified into fewer categories for assessment of both the TS itself and of possible re-use solutions to it

6.2 Identification of types of technical requirements

6.2.1 Introduction

The differing types of technical requirements contained in the TS are as follows

- functional requirements,
- mission requirements,
- interface requirements,
- environmental requirements,
- operational requirements,
- human factor requirements,
- (integrated) logistics support requirements,
- physical requirements,
- product assurance (PA) induced requirements,
- configuration requirements,
- design requirements,
- verification requirements.

NOTE These different technical requirements are called "user related functions" and constraints in EN 1325-1.

Proposed layering of ECSS-E-ST-10-06 C requirements types to allow easier visibility of true purpose for TS Process Assessment Step

Solution Free Product Reqts

- Function
- Performance
- Interface

Solution Specific Product Reqts

- Design solution requirements
- Physical requirements
- Configuration requirements

Assurance Requirements

- Verification reqts
- Design process, rules, margins
- PA Induced reqts

Solution Free : Function, Performance, Interface can be derived from many of the existing ECSS-E-10-06 C requirement types

F

…derived from
- Functional
- Mission
- Environmental
- Human Factors
- (I)LS
- PA Induced (RAMS)
- Operational

P

…derived from
- Functional
- Mission
- Environmental
- Human Factors
- (I)LS
- PA Induced (RAMS)
- Operational

I

….derived from
- Interface
- Mission
- Human Factors
- (I)LS
- PA Induced (RAMS)
- Operational

The remaining ECSS-E-10-06 C types are mapped as follows:-

Physical Requirements, Configuration Requirements -> Solution Specific Product Requirements

Design Requirements -> split amongst Solution Specific Product Requirements & Assurance Requirements

PA Induced Reqts, Verification Requirements -> Assurance Requirements

Distinction of Design Requirements into Solution Specific or Assurance type

6.2.12 Design requirements

Requirements related to the imposed design and construction standards such as design standards, selection list of components or materials, interchangeability, safety or margins.

NOTE For example "The receiver shall use a phase-lock loop (PLL)".

Design solution requirements

Design process, rules, margins

Making use of this further Requirements Engineering effort – where and how in the existing TS Process from ECSS-E-ST-10-06C

Steps F1.2 & F1.8 steps at Phase 0 and Phase A respectively, state *"The customer structures, classifies and justifies individual technical requirements".*

Proposal: use these steps to correctly express and structure the existing requirement types according to solution free, solution specific, or assurance category

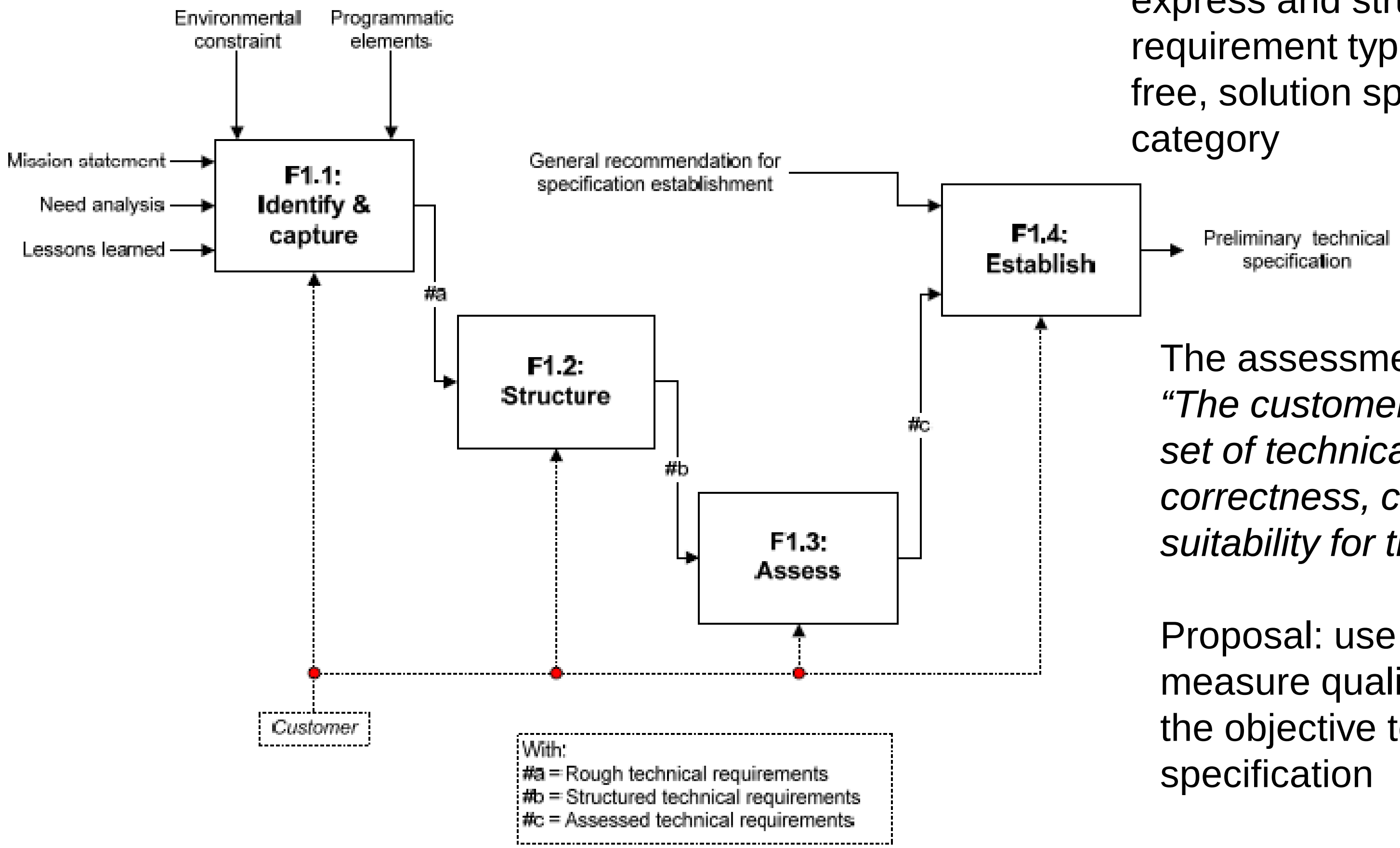
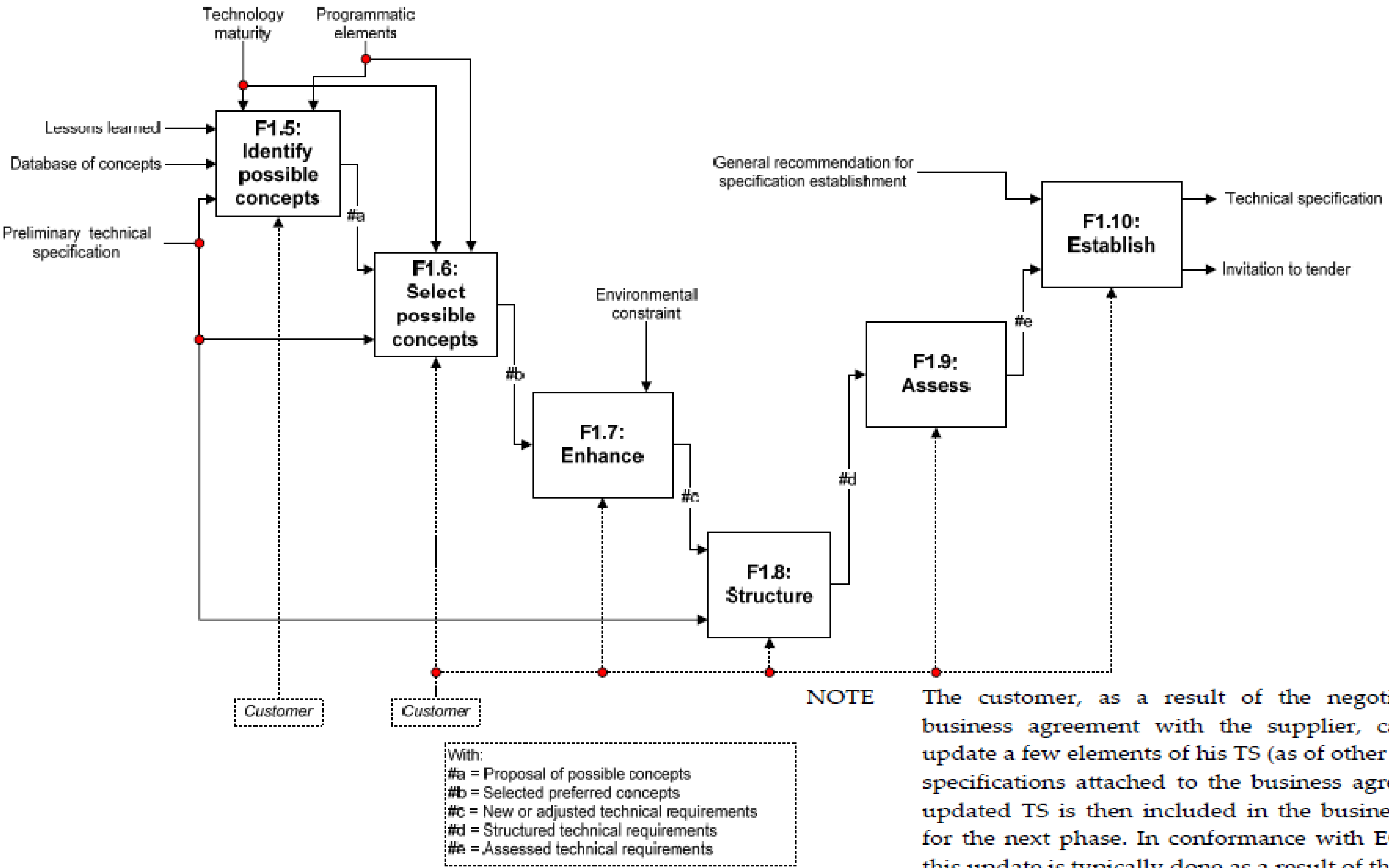


Figure 5-1: Process to establish the preliminary TS in Phase 0

The assessment steps F1.3 & F1.9: *"The customer assesses the entire set of technical requirements for correctness, consistency and suitability for the intended use"*

Proposal: use these steps to also measure quality of the TS against the objective to avoid over-specification

….ECSS-E-ST-10-06 C Phase A process, and later TS updates



NOTE The customer, as a result of the negotiation of the business agreement with the supplier, can decide to update a few elements of his TS (as of other requirements specifications attached to the business agreement). This updated TS is then included in the business agreement for the next phase. In conformance with ECSS-M-ST-10, this update is typically done as a result of the SRR.

Figure 5-2: Process to establish the TS in phase A

Moving from equipment re-use to functional chain or higher re-use (avionics, platform…), the impact is seen as reduced system activity

Statistics out of a LEO Satellite level VCD, where avionics level re-use and PFM mech/thermal/prop philosophy is used

Total 812 reqts	At SY Level	At SS Level	At EQ level
Total per Level	384 (47%)	358 (44%)	88 (11%)
…includes T	79 (21%)	310 (87%)	35 (40%)
…includes A	83 (22%)	25 (7%)	7 (8%)
…includes I	5 (1%)	1 (< 1%)	0 (0%)
…includes R	247 (64%)	43 (12%)	54 (61%)
Verif shared with lower level	29 (8%) with SS	8 (2%) with EQ	N/A
Verif shared on all 3 levels	3 (<1 %)		

47% of requirements require a Verif Method at SY level, compared to….

81% for a Science observatory

64% for a Science multi-payload

…..and a large proportion at SY level are Review of Design…(228 = 59% are exclusively R)

Functional Chain, Avionics and Platform re-use still require the need to manage multi-discipline interaction and performance margins

- To validate the re-use up front in Phase B, and to adapt specific sizings where needed e.g. array, radiator, payload data handling, the performance of each chain and overall system performance interaction needs to be modelled well
- The potential for reuse is improved if margin philosophy is realistically adapted for the maturity of the information
- Where core avionics & functional based re-use is strong and adapation is in power/thermal/RF/data-handling performance domains, a strong role for Power Thermal Sizing Simulator (PTSS) and Flight Domain Verification Model (FDVM) from Task 2 is seen

Evaluation of Industry-Agency Workshop Concept Airbus DS-3 related to Task 3 Impact of Elements Re-use

This concept seeks to equip European space projects to more fully exploit the growing potential of equipment, subsystem, and module level re-use to meet top-down system requirement definitions. It has particular growing potential towards Earth Observation missions, although not exclusively, and can be considered case-by-case for application for missions of interest.

The concept aims to bridge the difficult gap between top-down requirements definition arrived at considering the classical V-cycle project lifecycle, and the bottom-up product line approach, in the middle landscape of significant design artefact re-use (either of product line or non-product line artefacts).

The approach is to develop and exploit the potential of models of both requirements and design characteristics, and their interactions throughout the system, in order to allow to focus first on requirement validation (to avoid over-specification) and then re-use validation (to secure the design solution). This should then lead to earlier identification of an increased number of re-use opportunities, and reduced cost and duration of the re-use validation phase.

To be printed in A0

ID <Airbus DS-3> 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?

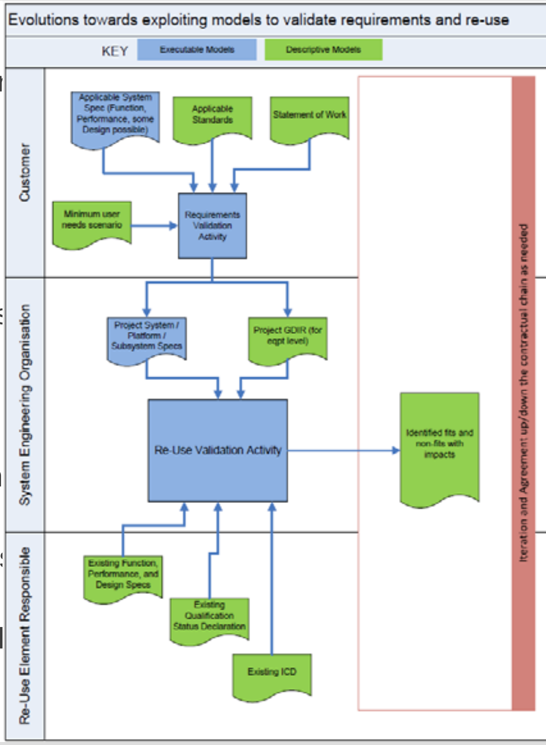
- Focus on **requirement validation** to avoid over-specification, followed by **re-use validation**
- **Develop and exploit** potential of **models** of both requirements & design characteristics, and their interactions throughout the system
- Define **model validation** responsibilities and **tailor 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 validatio** 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** agains 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** acros contractual boundaries
   - Standardisation of formalised data model exchange protocols



Auto project requirements quality assessments

Use cases modelled in a system descriptive model linked to requirements

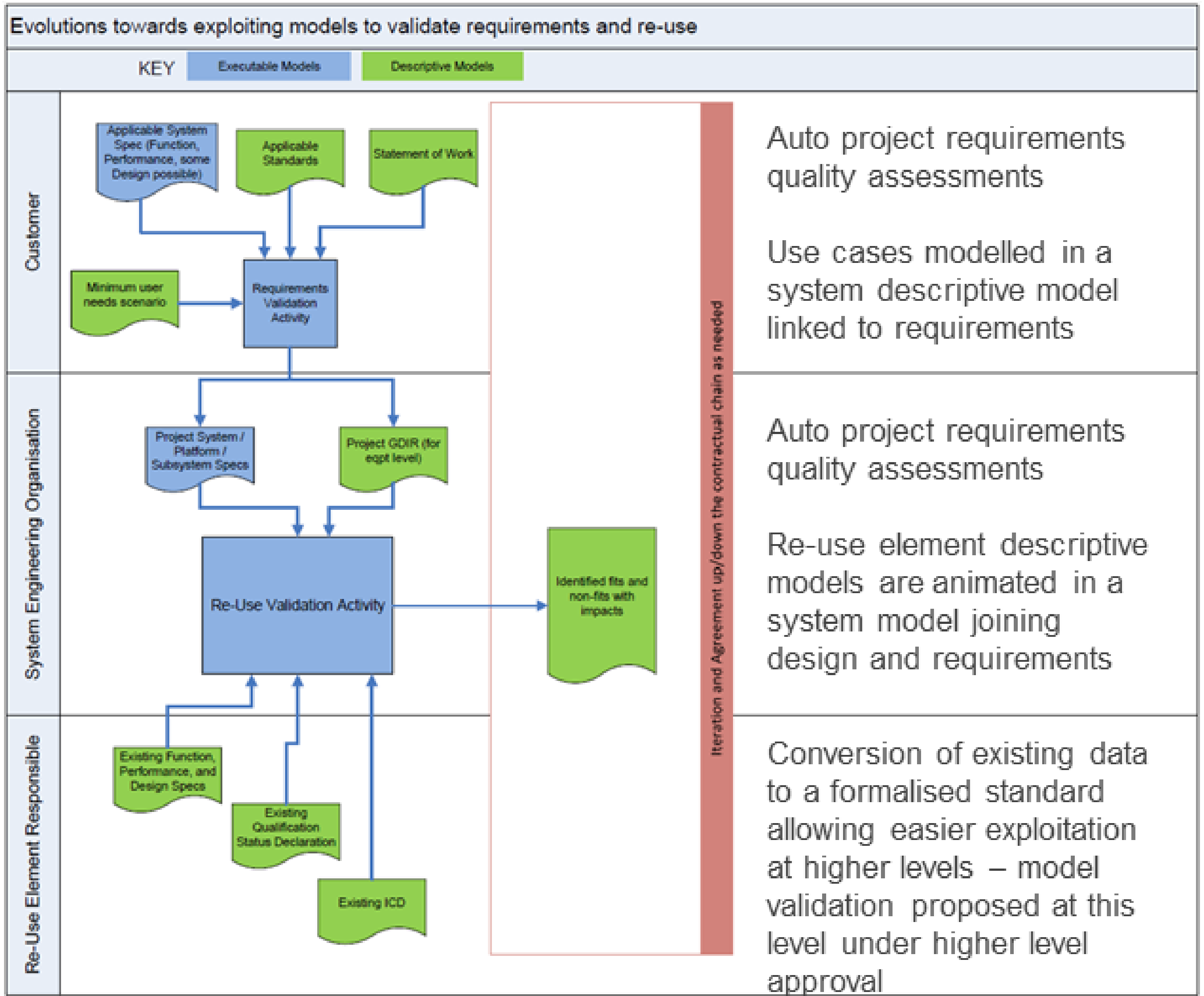
Auto project requirements quality assessments

Re-use element descriptive models are animated in a system model joining design and requirements

Conversion of existing data to a formalised standard allowing easier exploitation at higher levels – model validation proposed at this level under higher level approval

- **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

Zoom on Airbus DS-3 Concept Diagram



FEEDBACK: Long Term Traffic Light Green – Strengths to build on, Amber – Barriers to Tackle, Red – areas to improve or consider out of scope of concept

Concept Evaluation for System Verification - Summary of eva... ...eets per concept

(Airbus DS-3) Model based potential to validate re-use ... ...enhance model philosophy tailoring to project needs

Concept of reqt validation from bottom-up – mindset?

Recognised to achieve the central aim

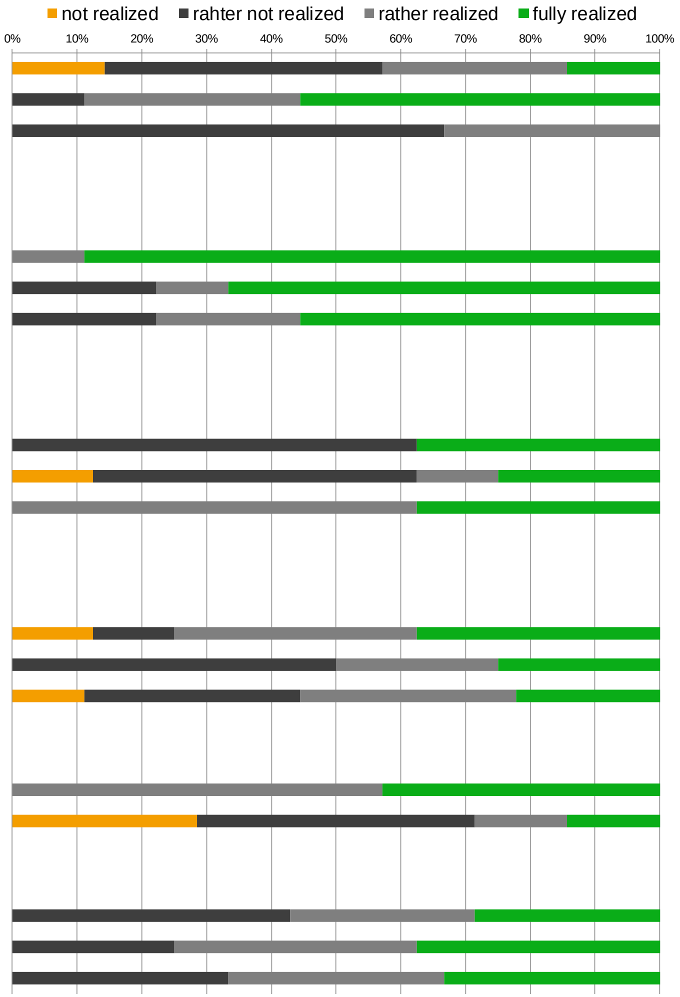
Attractive to project stakeholders

Concept is built to work across contractual boundaries

Allows risk avoidance by up-front validation of concepts

Supporting means towards extending Airbus DS-2 aims in re-use scenarios

		...alized		# fully realized	Average
effectiveness of specifications					
iterative requirements definition process between custom...		3	2	1	rather not realized
existing solutions can be matched against requiremen...	0	1	3	5	rather realized
requirements have appropriate lev... d ca... ...ectively	0	6	3	0	rather not realized
reuse					
...s from reused systems can be transferred	0	0	1	8	fully realized
...s for reusable products/components are validated	0	2	1	6	rather realized
... product architecture and strong interfaces can be created	0	2	2	5	rather realized
evidence and benefits					
the concept ... ...gers and public	0	5	0	3	rather realized
...per, simpler and quick...		4	1	2	rather realized
...e required quality is m...		0	5	3	rather realized
co-engineering and organisation					
speed of communication and ... significa...			3	3	rather realized
every party ... contractu...				2	rather realized
...s can be...			3	2	rather realized
risk orientation					
...d and shared	0	0	4	3	rather realized
resour... ...d standards	2	3	1	1	rather not realized
review and verification process					
... matter	0	3	2	2	rather realized
...based	0	2	3	3	rather realized
the verification activit... ...omer	0	3	3	3	rather realized



NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

Feedback details : individual points to highlight

effectiveness of specifications

	# not realized			# fully realized
iterative requirements definition process between customer and supplier will be enabled	1	3	2	1
existing solutions can be matched against requirements already early in the process	0	1	3	5
requirements have appropriate level and can be verified more effectively	0	6	3	0

Addressed through further requirements validation proposals

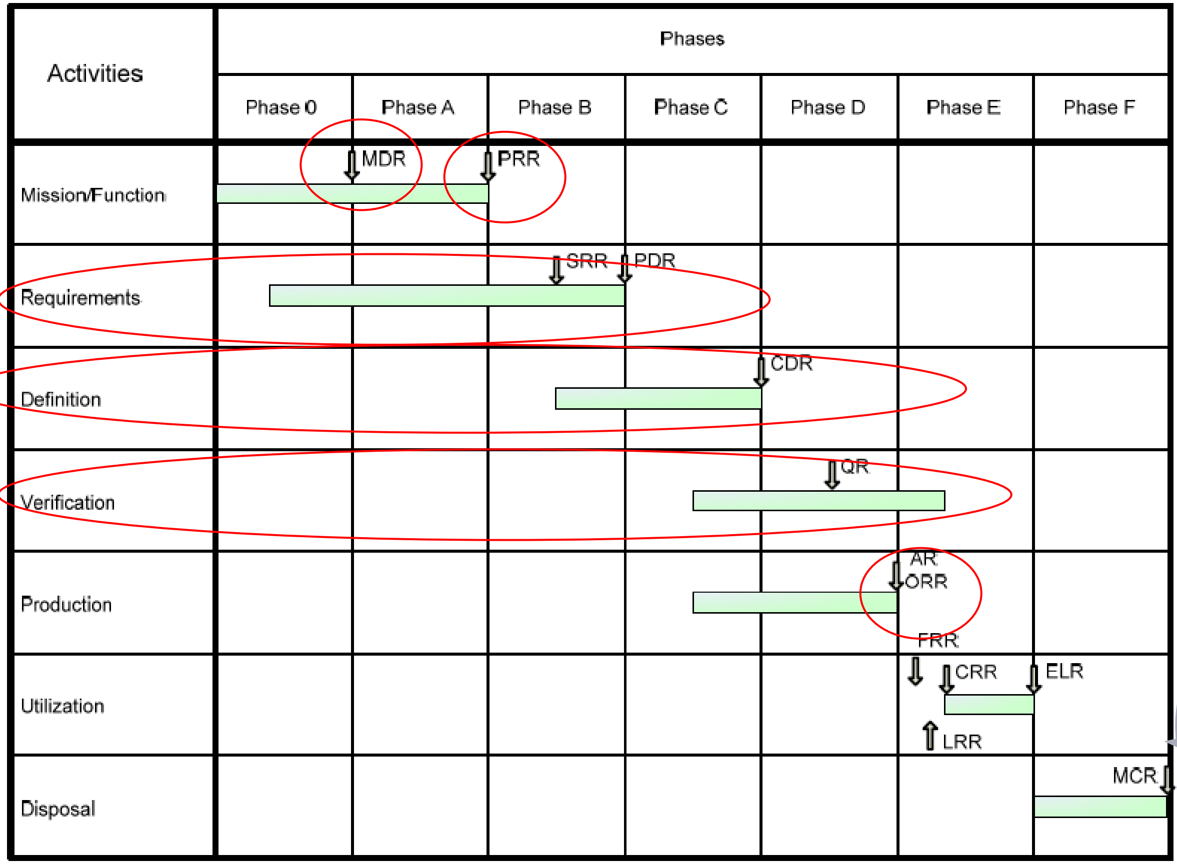
evidence and benefits

the concept will be easily sellable to project managers and public	0	5	0	3
the new approach seems to be cheaper, simpler and quicker	1	4	1	2
the required quality is maintained	0	0	5	3

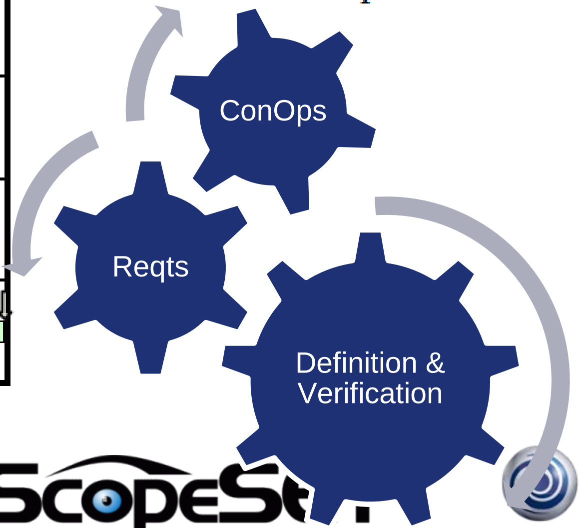
Fully recognised as a barrier to tackle

Task 4: Definition of Suitable Review Logic – Overview of “as-is”

ECSS-M-ST-10C Rev 1 is the reference for project phase breakdown and objectives, including review objectives



- Phase 0 - Mission analysis/needs identification
- Phase A - Feasibility
- Phase B - Preliminary Definition
- Phase C - Detailed Definition
- Phase D - Qualification and Production
- Phase E –Utilization
- Phase F – Disposal



Review objectives are based on an idealised V-model

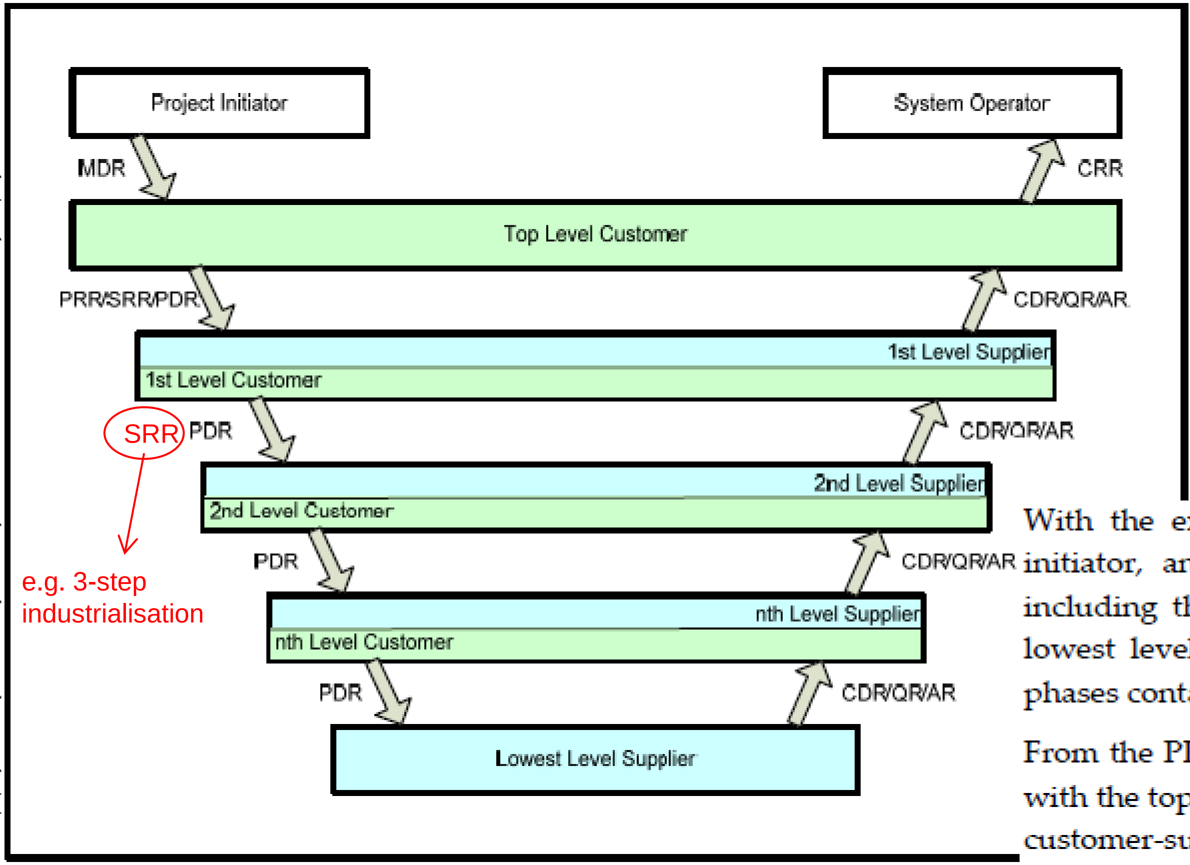


Figure 4-4: Review life cycle

When industrial or technological realities present non-ideal phasings with respect to the V, reactive adaptations take place, with strong need for maturity, configuration accounting, change control, and regression management

With the exception of the MDR which normally involves only the project initiator, and the top level customer, all other project reviews up to and including the AR are typically carried out by all project actors down to the lowest level supplier in the customer-supplier chain involved in the project phases containing these reviews.

From the PRR to the PDR, the sequence of the reviews is "top down", starting with the top level customer and his top level supplier, and continuing down the customer-supplier chain to the lowest level supplier. From the CDR to the AR, the sequence of reviews is reversed to "bottom up", starting with the lowest level supplier and its customer and continuing up through the customer-supplier chain to the 1st level supplier and the top level customer. This so called "V model" is illustrated in Figure 4-4.

Review objectives analysed, leading to Concept 2

To be printed in A0

ID <AIRBUS DS-2> Towards a Dynamic Review Logic through systematic Design & Verification Maturity Assessment and Management

Status quo

- Whilst technology readiness and assessment is generaly 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 indutrial 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

System Design & Verification Planning Maturity Assessment Checkpoints against targets – *dynamic element*

System Data Models & Repository

Reqts Meta-data Model and Tools

From PRR to PDR

Metrics at each product level including:-

Reqt quality, changes, tbc status

Interface design data, changes, tbc status

Other design changes, tbc status

Multidscipline data exchange maturity **go / nogo** checks

Development & Verif. **Planning definition** at level of model usage mapped against requirement qualification and other purposes (see Airbus DS-1)

Reduced SRR

Focus on **system level requirements content, specification tree** definition, and **CONOPS** agreement only, as update of PRR in response to finally released SRD / OIRD customer requirements and towards data model entries for verification planning.

Checkpoints and Industrialisation activities cover the lower level TS reviews including **"whole system" coherency.**

Industrialisation activities

New Pre-TEB **Campaign Readines Review** looks at **coherency of all specs** in the context of **maturity and industrialisation planning** for whole project.

Individual pre-TEBs review each spec for ITT release.

Tender, negotiation, contract execution unchanged, but including **data exchange** for maturity assessment checks.

Design & Verif. Planning Definition

Actually starts at system level **pre-Industrialisation**, continues through Product Tree concurrently.

Additional focus on data required for **maturity assessments and FDIR**, and **finer granularity of verification planning** to reduce effort on PFM.

Reduced PDR

Formal review of **first complete formal design baseline** only – no plans or "how to" in scope

- these are captured on a dynamic basis planned via the maturity assessments findings

Bespoke hybrid model philosophy project – Phase B is key

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**

like life

The Tools Experts

DEFENCE & SPACE

Zoom on Airbus DS-2 Phase B Lifecycle

System Design & Verification Planning Maturity Assessment Checkpoints against targets – *dynamic element*

From PRR to PDR

Metrics at each product level including:-

Reqt quality, changes, tbc status

Interface design data, changes, tbc status

Other design changes, tbc status

Multidscipline data exchange maturity **go / nogo** checks

Development & Verif. **Planning definition** at level of model usage mapped against requirement qualification and other purposes (see Airbus DS-1)

Reduced SRR

Focus on **system level requirements content, specification tree** definition, and **CONOPS** agreement only, as update of PRR in response to finally released SRD / OIRD customer requirements and towards data model entries for verification planning.

Checkpoints and Industrialisation activities cover the lower level TS reviews including **“whole system” coherency.**

Industrialisation activities

New Pre-TEB **Campaign Readiness Review** looks at **coherency of all specs** in the context of **maturity and industrialisation planning** for whole project.

Individual pre-TEBs review each spec for ITT release.

Tender, negotiation, contract execution unchanged, but including **data exchange** for maturity assessment checks.

Design & Verif. Planning Definition

Actually starts at system level **pre-Industrialisation**, continues through Product Tree concurrently.

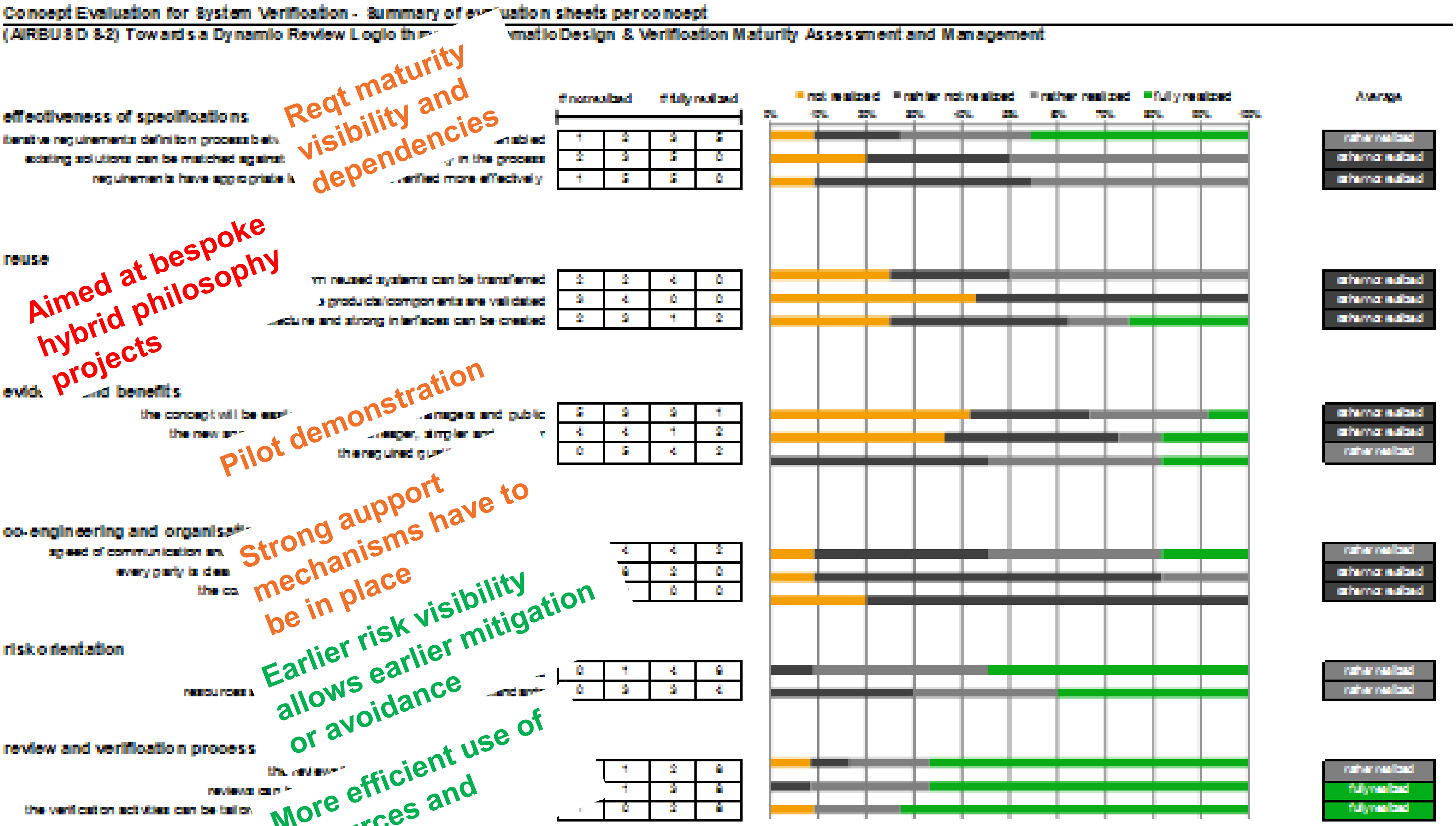
Additional focus on data required for **maturity assessments and FDIR**, and **finer granularity of verification planning** to reduce effort on PFM.

Reduced PDR

Formal review of **first complete formal design baseline** only – no plans or “how to” in scope

- these are captured on a dynamic basis planned via the maturity assessments findings

FEEDBACK: Long Term Traffic Light Green – Strengths to build on, Amber – Barriers to Tackle, Red – areas to improve or consider out of scope of concept



Reqt maturity visibility and dependencies

Aimed at bespoke hybrid philosophy projects

Pilot demonstration

Strong support mechanisms have to be in place

Earlier risk visibility allows earlier mitigation or avoidance

More efficient use of resources and attention

NOVABASE like life

ScopeSET The Tools Experts

AIRBUS DEFENCE & SPACE

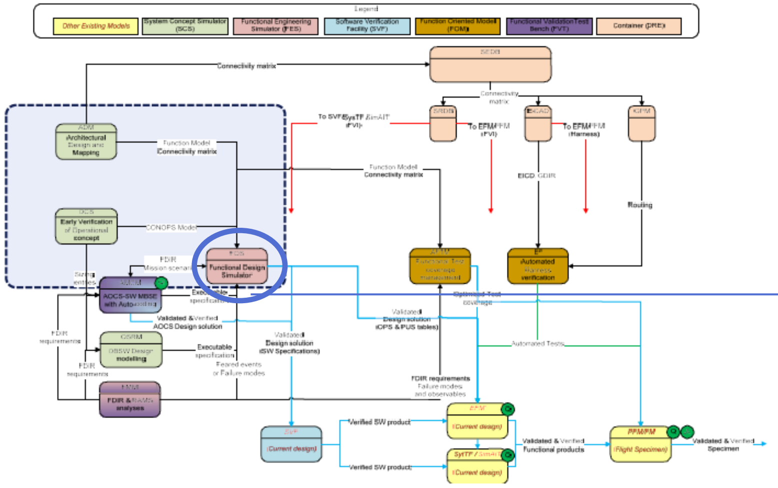
Airbus-DS2 Phase B Review Concept Summary

In summary the concept was found to have major potential to achieve big improvements in space project practice, and does not have to be tackled in a series way - improvements can be piloted from two ends in parallel (re-focussing of effort to core value adding activities at major reviews in phase BCD, and using an improved system engineering environment to improve the maturity evolution planning in phase B1). Nor do such pilots have to wait for standardization evolution (at least not in principle, although the environment infrastructure aspect would benefit from this).

A major constraint to fully realize the technical, programmatic and industrial alignment at stake was considered to be Agency constraints on budget spend per calendar year. It was also identified that two different projected maturity evolution plannings, and consequently resulting review logics with timings, for the same project coming from parallel A/B1 contracts then make it difficult for the Agency to construct a B2CD ITT which allows fair and open competition whilst still containing a realistic single planning. On the other hand it is noted that the concept does not revolutionise the existing major review logic, but seeks to put in place sufficient visibility of real maturity evolution that the review logic timing is planned to have most value-adding effect at least incurred effort. In this respect, the ITT task could be changed from finding “best proposal to meet the reference planning”, to finding “best proposal of a reference planning to achieve the end goal”.

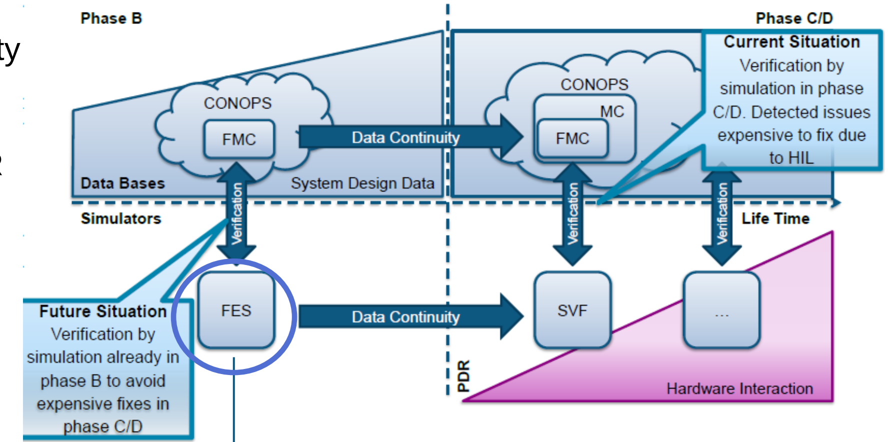
FES demonstrator into higher level project perspective

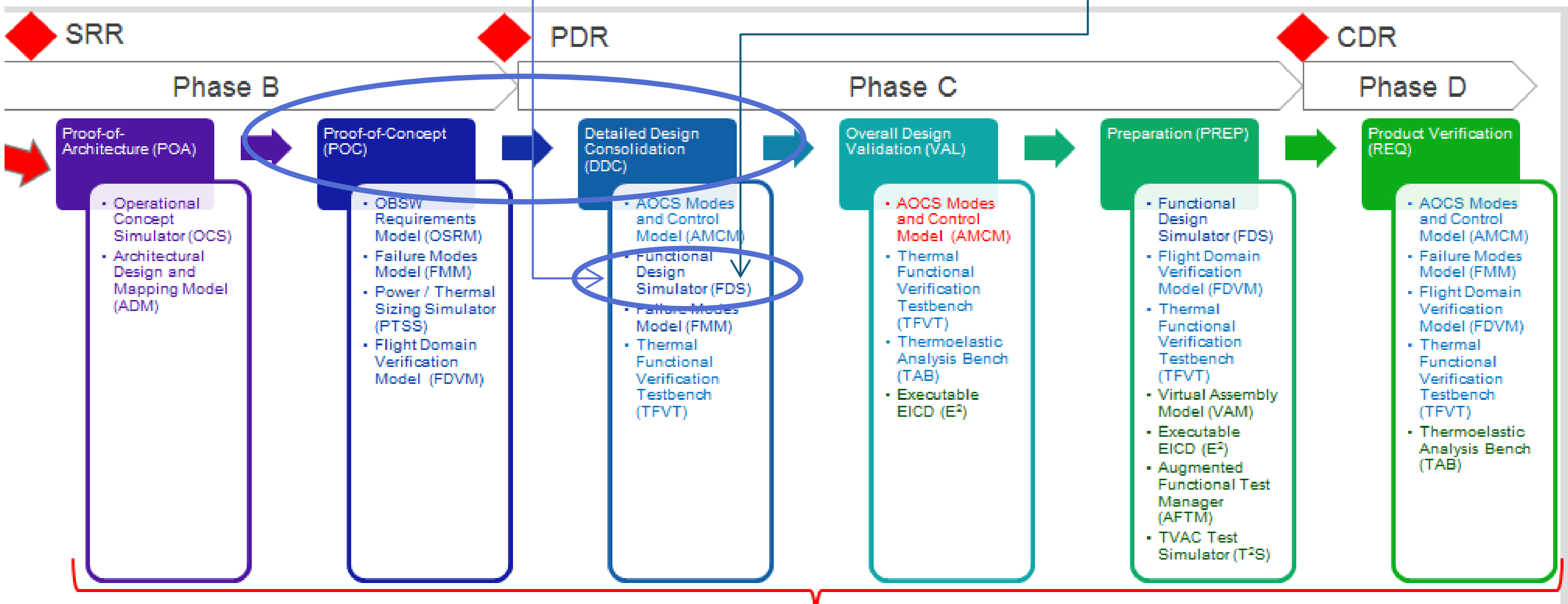
SVTLC – Models in the Lifecycle of Functional Domains



- Modelling packets and operational procedures, verify the CONOPS
- data & model continuity supporting early verification for risk reduction around PDR

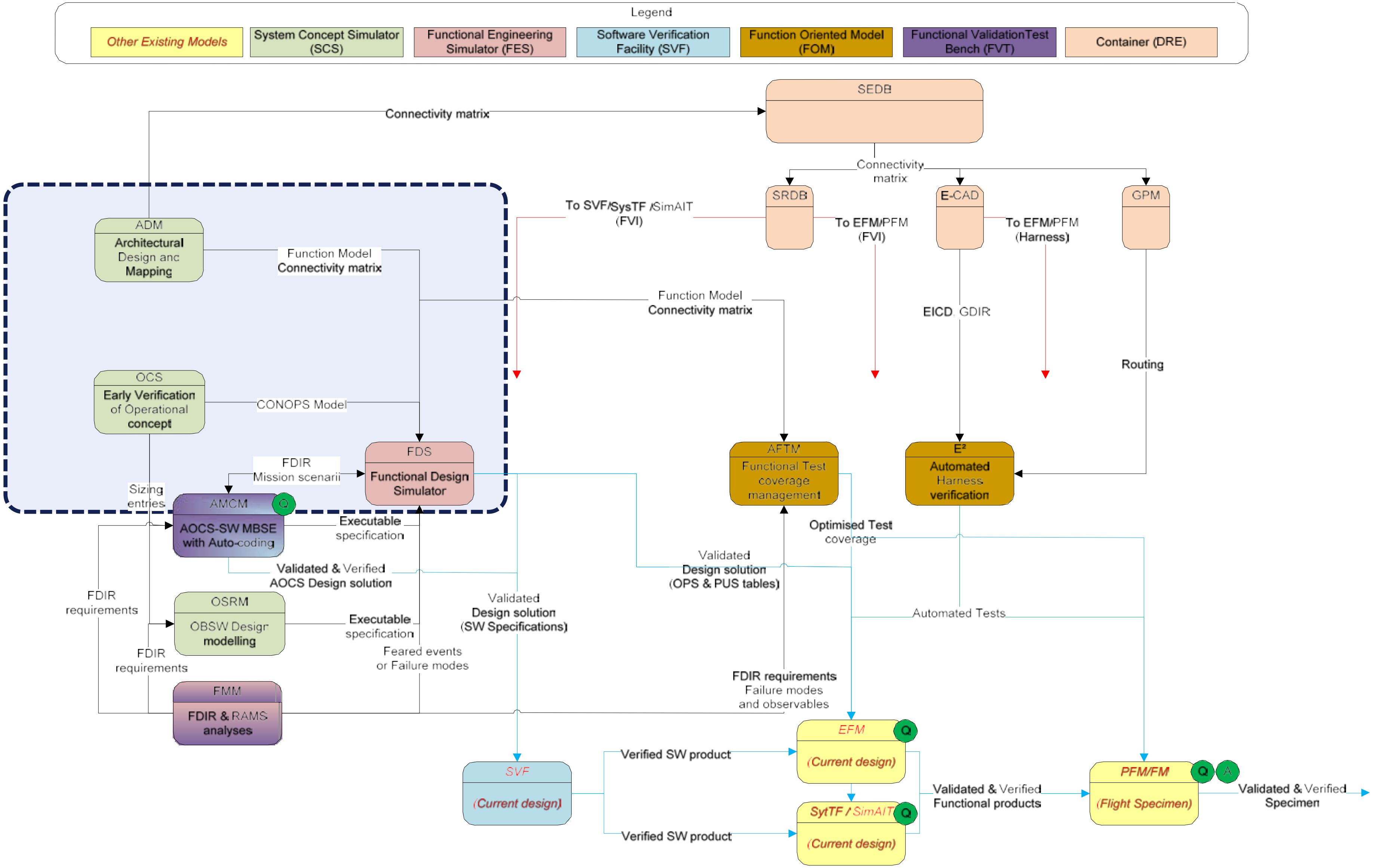
Use the FES to Verify Concept of Operations Already Before PDR



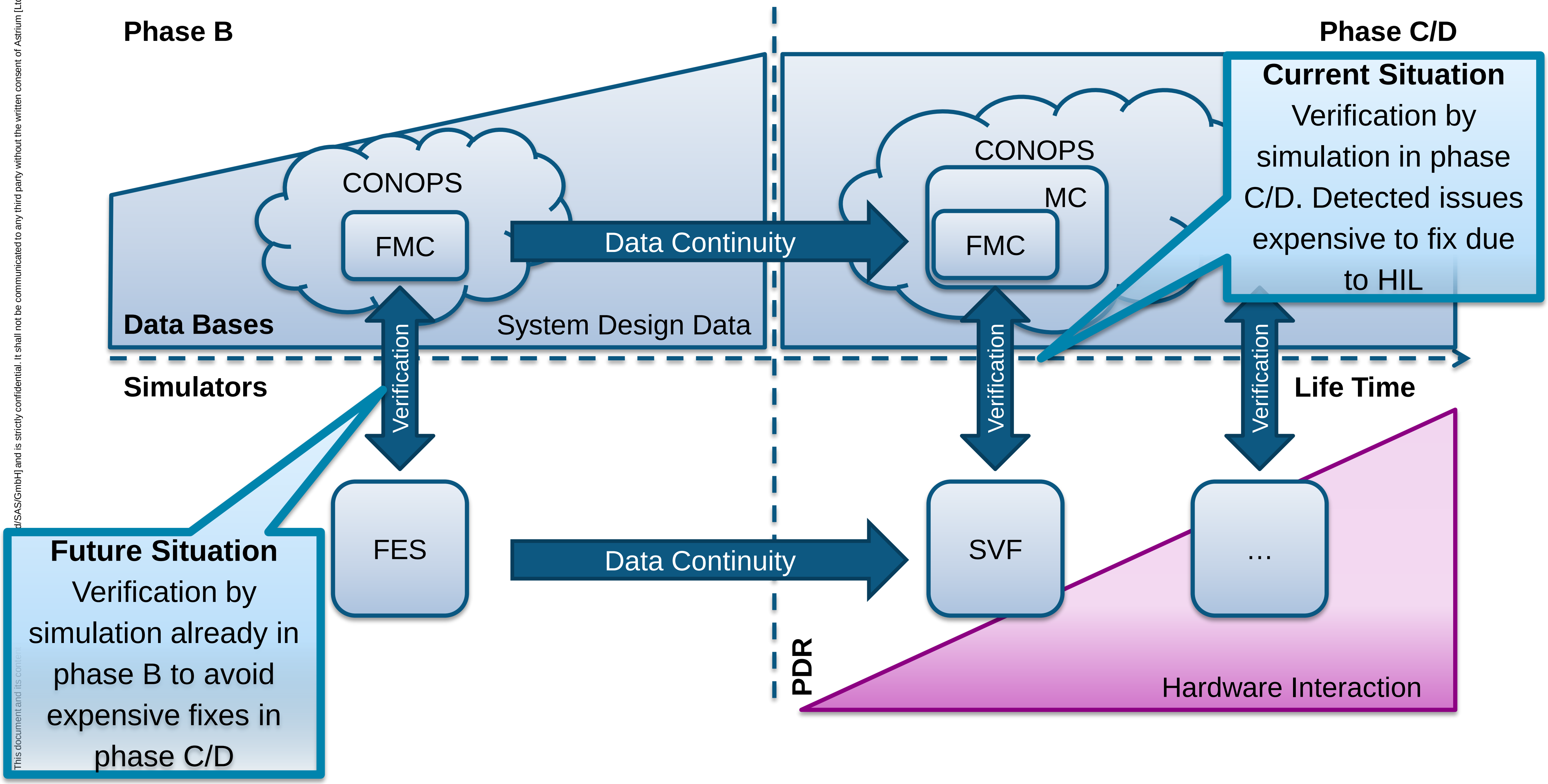


2) Proposed new virtual & hybrid models, categorised to ECSS TM-10-21 A classes of models & ECSS-E-HB-10-02A Verif. Guidelines

SVTLC – Models in the Lifecycle of Functional Domains



Use the FES to Verify Concept of Operations Already Before PDR



SVTLC Functional Design Simulator Objectives and Output

Functional Engineering Simulator as tool in FDS use case

- Validate system functional design and performance in targeted area
- Functional model to be a tool capable to identify and perform impact changes analysis
  - Inputs/outputs of this model should be a partial TM/TC list

Objectives of Functional Engineering Simulator

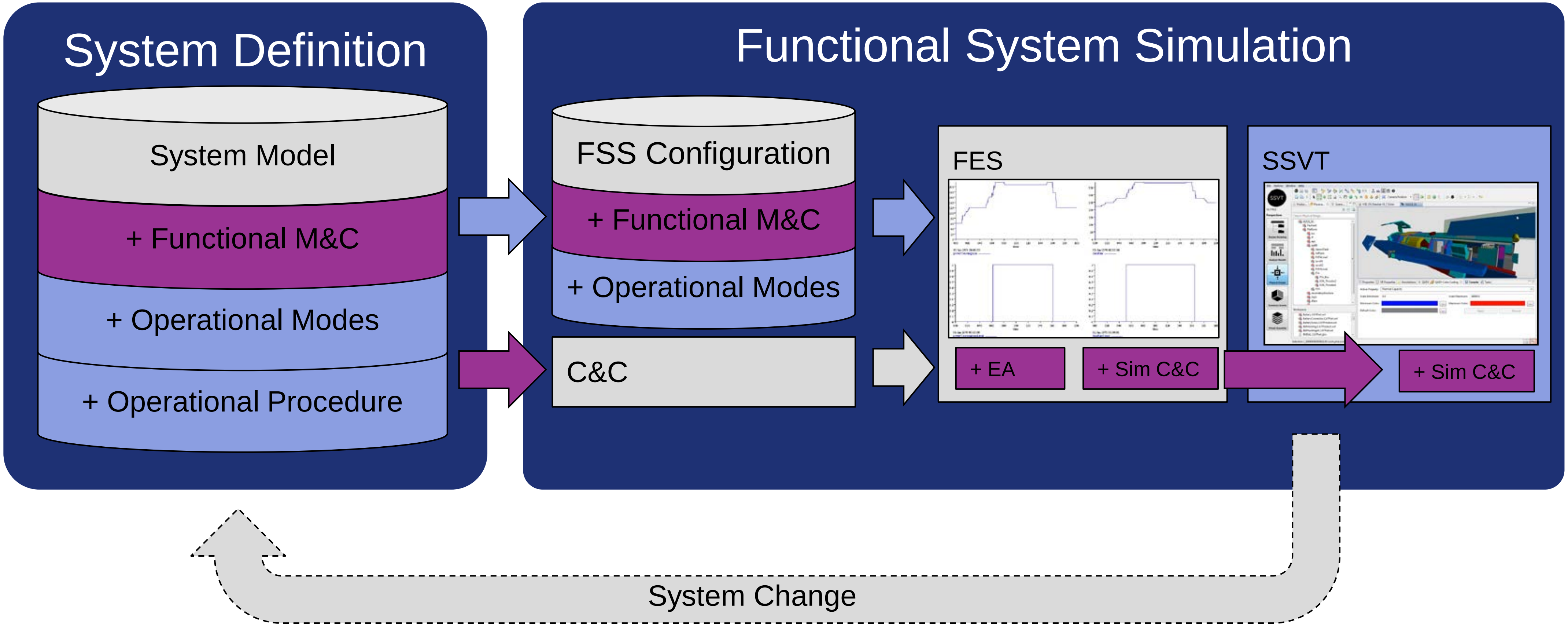
- Multi domain early validation of functional design
  - on board to on ground function mapping (OPS / SW) and FDIR implementation
- Early freeze of operability ICD's
- Maturity increase upfront detailed development in OPS/SW/FDIR implementation
  - Using "executable specifications of design"

Desired/targeted outputs of Functional Engineering Simulator

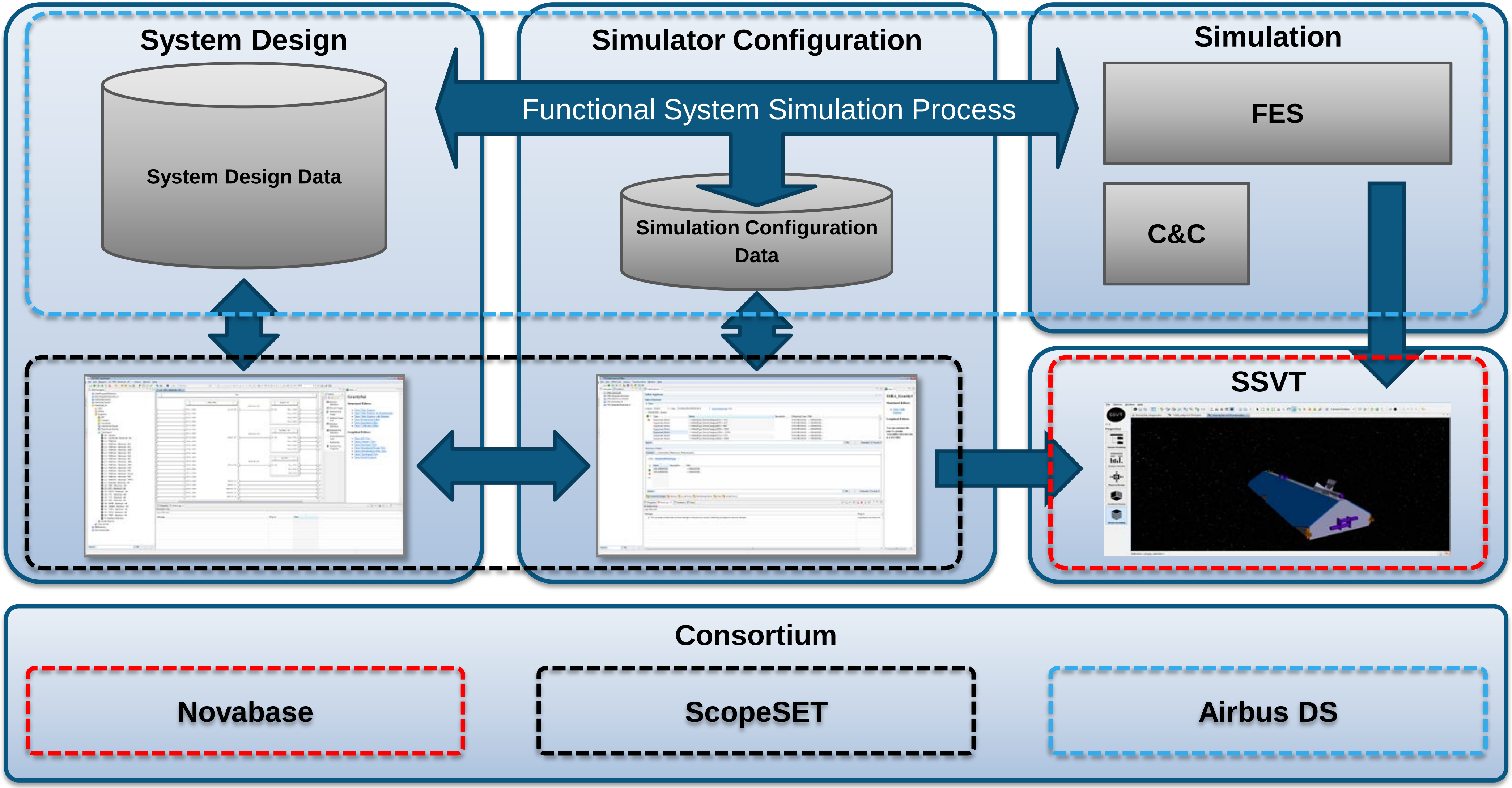
- Operational decomposition into modes
- On board to on ground function mapping
- OPS procedure architecture & demonstration of detailed operability
- Draft PUS tables
- Buffer management e.g. concerning data rate limits
- Impact analysis when managing changes, knowledge capture and operational management of very complex functional systems.

FSS in SVTLC – Architecture Overview and Enhancements

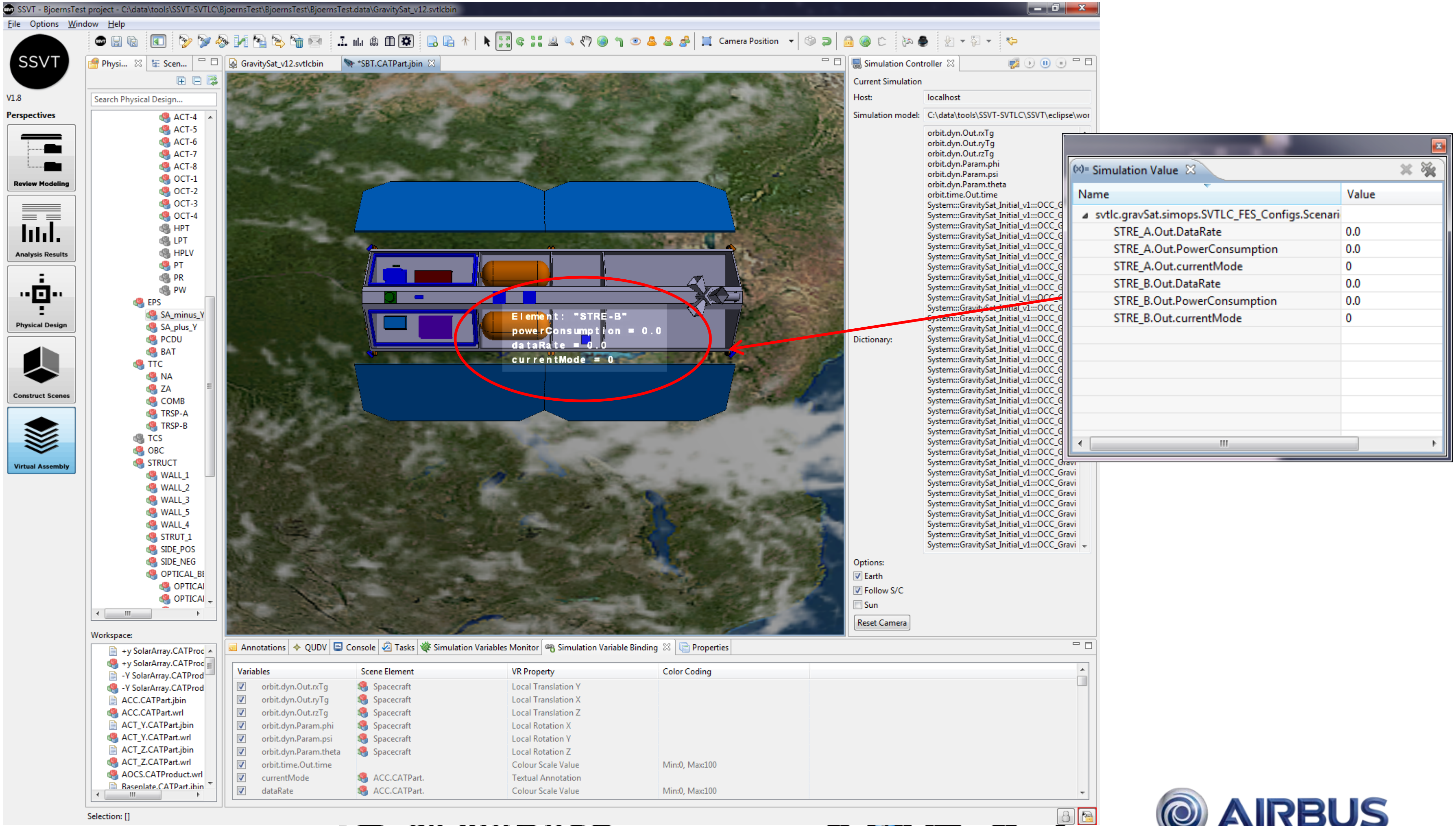
Existing / Present / Complete Part
Modifcation / Adaption / Integration of Existing Part
Development / Implementation of New Part



Data, Tools, Processes to uses System Data for Simulator Configuration



Scenario 1 – SSVT showing Simulation States (STRE_B Off)



End of Presentation