Model-based System and Software Engineering – Future directions

ESTEC, 8 December 2016

A. Jung, M. Verhoef, M. Perrotin (TEC-SWE)

Agenda

- Welcome and logistics
- Background of this workshop
- Purpose of this workshop
- Highlights from the final presentation days
- MBSSE landscape
- Workshop programme
- Audience participation – the “work” part

Background to this workshop (1)

1. Follow-up to the *Future of Compass* workshop (held on 22 November 2015)
   - Participants expressed the need for continuation and follow-up
   - Workshop format (short talks, room for interaction) was appreciated

2. A significant number of MBSE themed studies have been completed in 2016 (all presented at the TEC-ED/SW final presentation days on 6 and 7 December)
   - Model-based Software Development Lifecycle (FPD Dec 2015)
   - Schedulability Analysis Techniques and Tools for Cached and Multicore Processors
   - TASTE Multicore
   - Improvement of the OSRA SCM Model Editor
   - Verification of Computer-Controlled Systems
   - Catalogue for System and Software Properties – CatSY
   - Catalogue for System and Software Properties – CSSP
   - Enabling FDIR design through diagnosability and recoverability analysis
   - Consolidation of COMPASS tools

3. Similar / related MBSE activities are on-going in systems engineering, avionics and AOCS/GNC domains

Background to this workshop (2)

4. Model Based System and Software Engineering (MBSSE) is gaining more and more interest and momentum in the space domain, just a few examples:
   - SECESA / INCOSE
   - ADCSS (i.e. session on Model-Based Avionics in 2016) / DASIA
   - SESP
   - Capella 1.0 release, Clarity-SE consortium
   - SysML v2.0, AADL v2,…
   - Academic communities: MODELS / SAFECOMP / IMBSE / SEFM

5. Scattered landscape: diversity of notations, tools, workflows, different TRL…

6. Heterogeneity: many types of models used for different purposes

7. Diverse community / stakeholders : multi-domain, academia, industry (system integrators, OEMs, services), customers, regulators

Embrace this diversity and openly **identify and discuss challenges ahead**

Purpose of this workshop

We would like to

1. Share our vision on MBSSE, with focus on COMPASS, TASTE and OSRA

2. Showcase experiences gained from MBSSE applications in on-going projects

3. Discuss the potential alignment across different model-based technologies

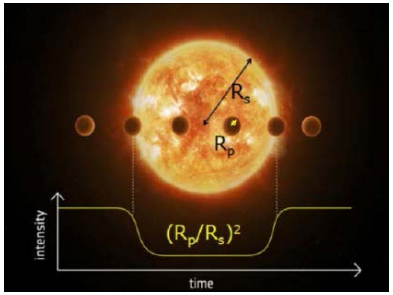
4. Identify opportunities for further collaboration, harmonization and consolidation

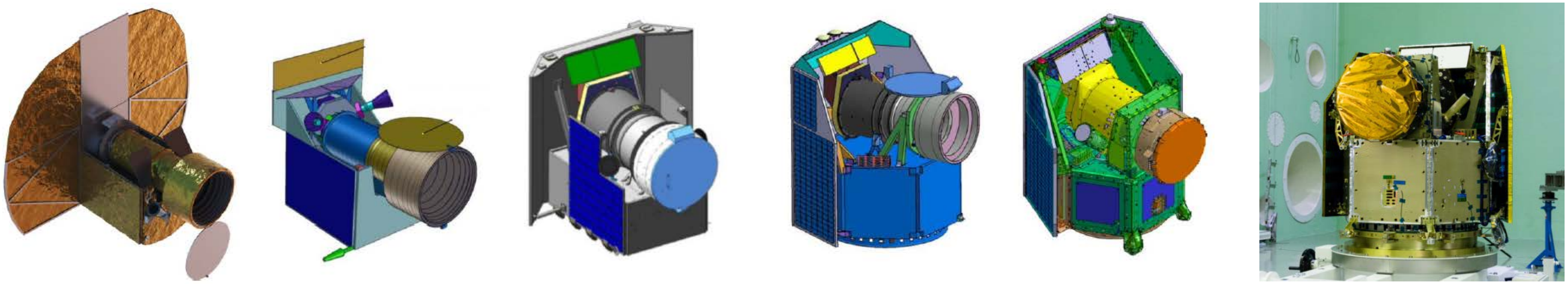
5. Identify next steps for technology exploitation and R&D

This is a *work*shop: we would like to hear from you

An example: CHEOPS (http://sci.esa.int/cheops/)

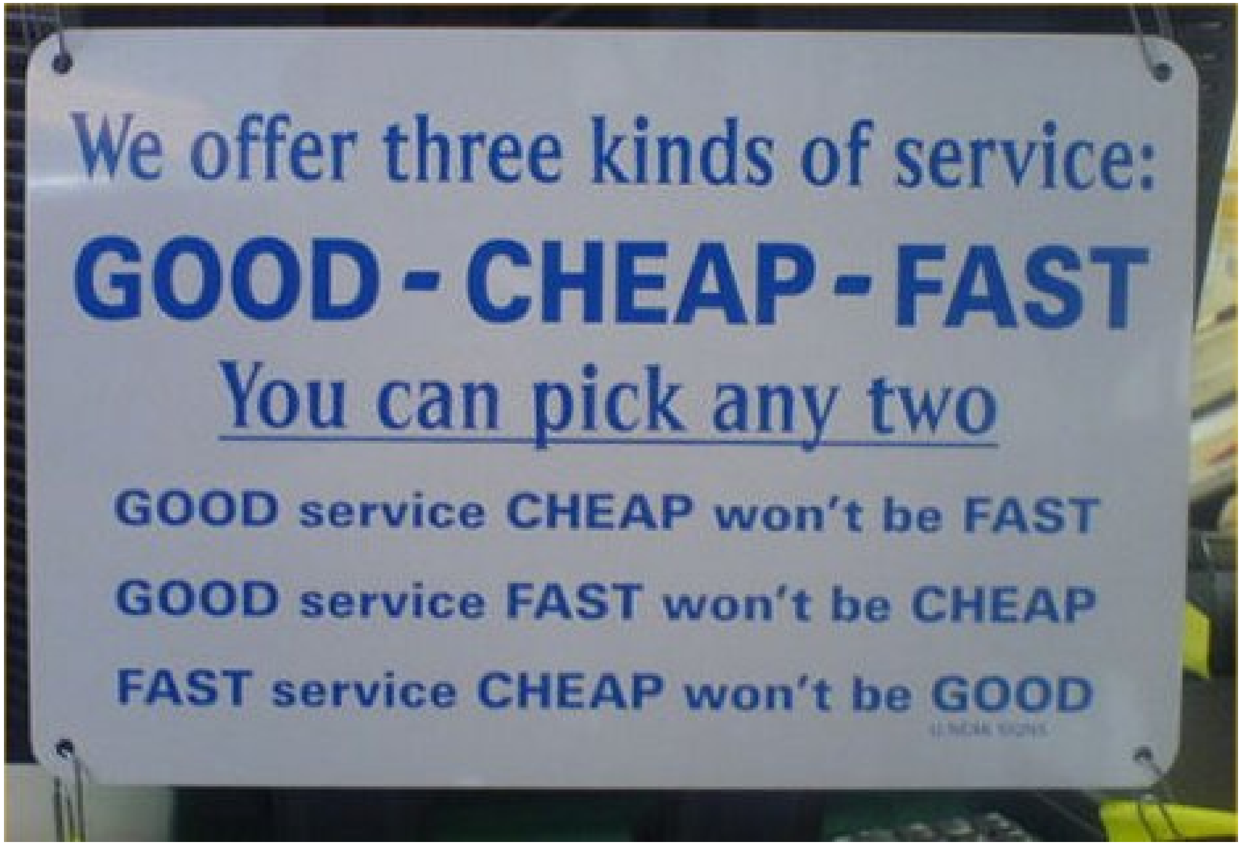
- ESA’s first small class science mission: CHaracterizing ExOPlanet Satellite
- Selected for study Oct 2012, start implementation Feb 2014, launch in 2018
- Tough S-class mission boundary conditions:
    - Development time not exceeding 4 years
    - Small budget: 50 MEuro
- Challenging science: ultra-high photometric precision
- Multi-party collaboration: 10 countries, 20+ contributors
- Compliant to development practices and quality standards





Source: C. Coral van Damme (ESA) – SECECA 2016 keynote

The “faster – better – cheaper” dilemma



We offer three kinds of service:

GOOD - CHEAP - FAST

You can pick any two

GOOD service CHEAP won’t be FAST

GOOD service FAST won’t be CHEAP

FAST service CHEAP won’t be GOOD

caveat: the 4th dimension is missing:
we want more services and service complexity is increasing

Our interest in MBSSE

In order to deal with the time – quality – complexity – cost battle,
we believe that the key is to improve communication

- Among engineering disciplines
- Across the life-cycle phases
- Along the system – subsystem – equipment axis
- Along the customer – system integrator – supplier chain

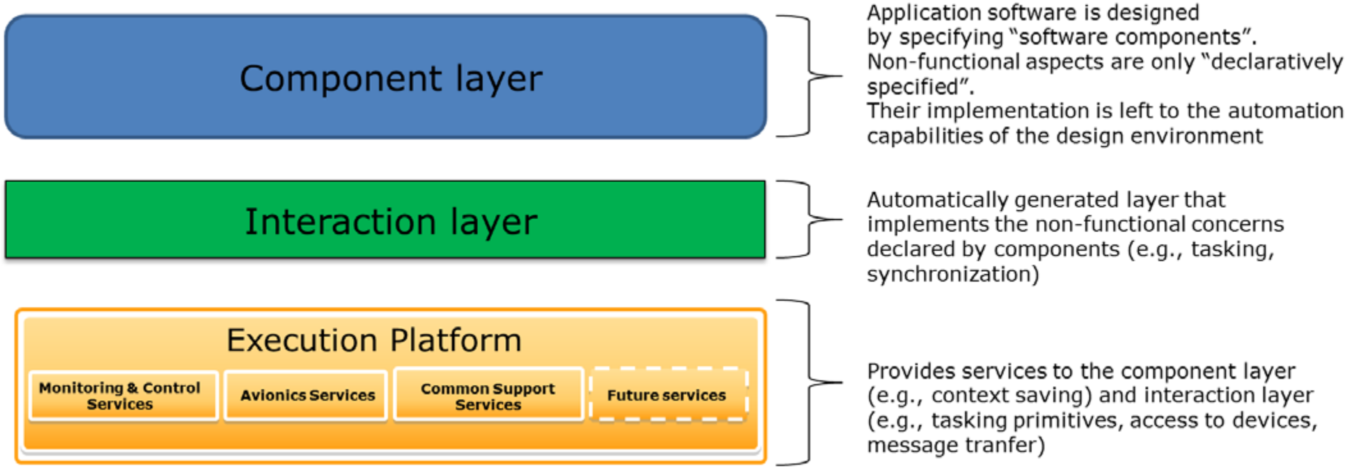
- **Time**: we have to communicate *more often* (iteration, access to consistent data)
- **Quality**: we have to *continuously increase* the *confidence* of the information exchanged
- **Complexity**: we need to be able to *succinctly* communicate (abstraction, depth, purpose)
- **Cost**: we need to *detect / prevent* potential *problems* as *early* as possible

MBSSE addresses these concerns by:

- Providing an explicit notation to create models (abstractions of the real world)
- Providing means to construct and verify the model (internal consistency)
- Providing means to validate models (external consistency)

Vision: move from Informal World (documents, review by [human] inspection)
towards MBSSE World (models, [automated] analysis)

On-board Software Reference Architecture



Application software is designed by specifying "software components". Non-functional aspects are only "declaratively specified". Their implementation is left to the automation capabilities of the design environment

Automatically generated layer that implements the non-functional concerns declared by components (e.g., tasking, synchronization)

Provides services to the component layer (e.g., context saving) and interaction layer (e.g., tasking primitives, access to devices, message tranfer)

- An *agreed* architectural framework for the development of on-board software of future missions
- A development methodology and architectural practices that fit the (software) domain
- Based on the following cornerstone principles
    - Separation of concerns
    - Correctness by construction
    - Composability and compositionality
    - Support for variability
- Full set of training materials (and tools) available (to ESA member states)
- http://savoir.estec.esa.int/ or contact Andreas Jung

SAVOIR
space avionics open interface architecture

Highlights from the Final Presentation Days (1)

- Model-Based Software Development Lifecycle (FPD 2015)
  - Requirements Definition and Analysis Language (AADL annex)
  - User Requirements Notation and Use-case maps

- Schedulability Analysis Techniques and Tools for Cached and Multicore
  - Extension of TASTE Interface View
  - Correct-by-construction translation via DOLC to RT-BIP (FPPN)
  - Measurement based WCET analysis to drive mixed-criticality scheduling

- TASTE multi-core
  - Adoption of AADL v3 proposed notion of multi-core in TASTE-DV
  - Adoption of AADL ARINC653 Annex to support TSP in TASTE-DV
  - Implementation support in OCARINA / PolyORB-HIC

- OSRA SCM editor
  - Improved user experience for creating SCM model instances

Highlights from the Final Presentation Days (2)

- Verification of Computer Controlled Systems
  - Systems and avionics modelling using AAML and SDL
  - Software modelling using OSRA SCM and SDL
  - Hardware modelling using SOIS EDS / TASTE

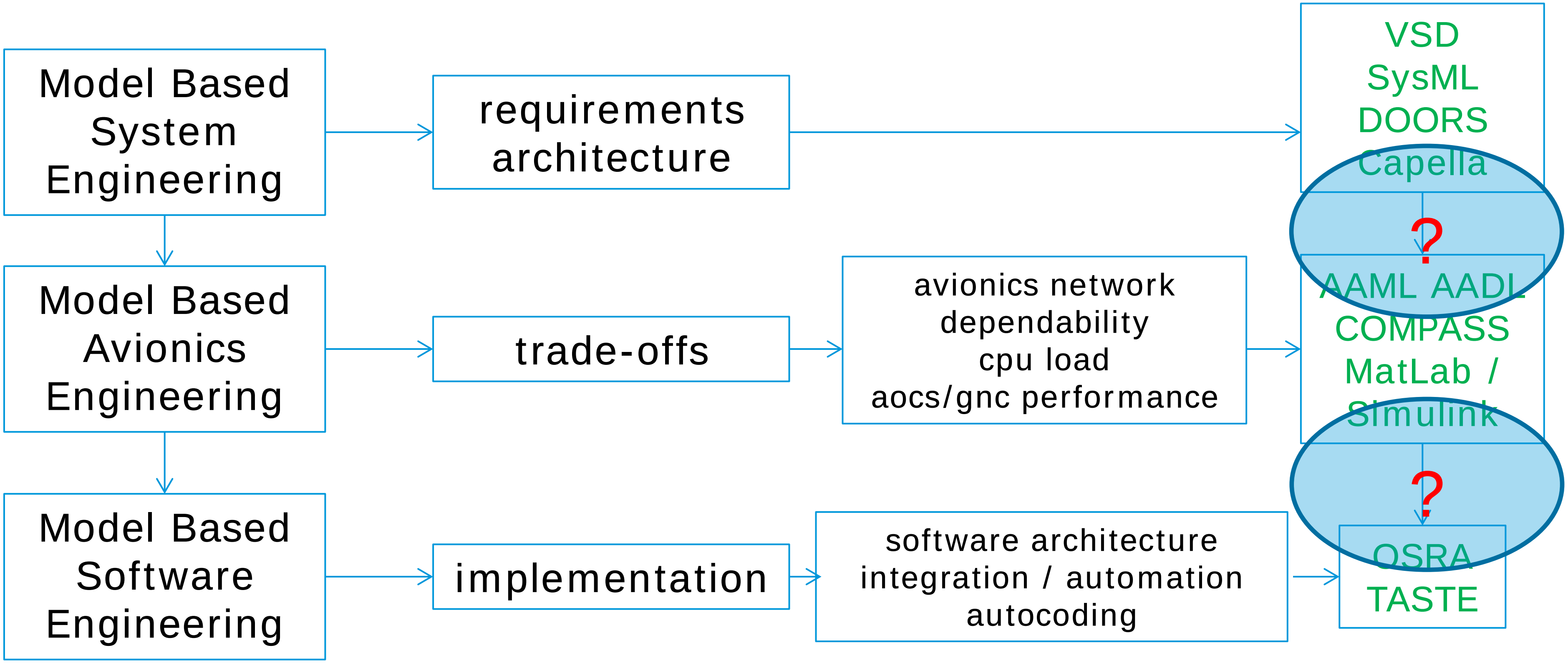
- Catalogue of System Software Properties (2 parallel studies)
  - CSSP: verification of design models against formal properties derived from requirements (using ontologies and boilerplates for requirements capture and property verification using BIP)

  - CATSY: Requirement categorization (contracts, refinement) and property verification using model-checking

- Enabling FDIR design through diagnosability and recoverability analysis
  - Construction and analysis of timed failure propagation graphs

- Consolidation of COMPASS tools
  - Comprehensive tool set for formal analysis of AADL models

MBSE landscape



Model Based System Engineering

requirements architecture

VSD
SysML
DOORS
Capella

?

Model Based Avionics Engineering

trade-offs

avionics network
dependability
cpu load
aocs/gnc performance

AAML AADL
COMPASS
MatLab /
Simulink

?

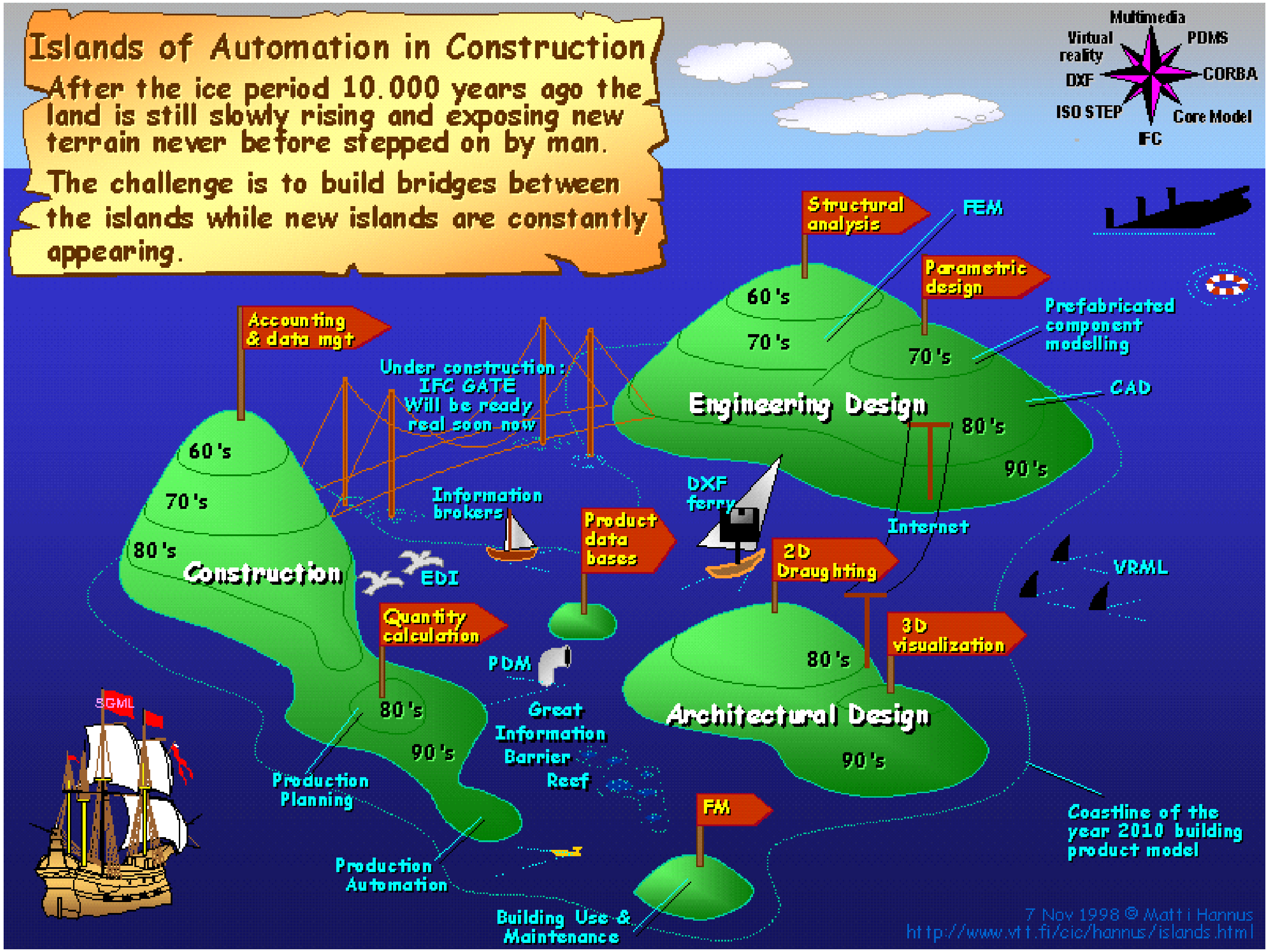
Model Based Software Engineering

implementation

software architecture
integration / automation
autocoding

OSRA
TASTE

We’re not the only ones with this challenge



Islands of Automation in Construction

After the ice period 10.000 years ago the land is still slowly rising and exposing new terrain never before stepped on by man.

The challenge is to build bridges between the islands while new islands are constantly appearing.

Today’s programme (1)

Morning session will focus on model-based system level and avionics modelling

Four solicited talk (20 min each):

1. *Trends in MBSE and experiences with SysML on Euclid* (Metselaar, ESA)
2. *MBSSE used in the Ariane 6 launcher development* (Comery, ASL)
3. *Connecting COMPASS to Capella* (De Ferluc, TAS)
4. *COMPASS: Future trends and developments* (Bozanno, FBK)

Elevator pitches (5 min each):

- Bassiliades (AUT) - *Ontology-based Requirements Validation*
- Tipaldi (OHB) - *Formal verification techniques applied to Spacecraft Mode Management*
- Bruintjes (RWTH) - *Model Driven Engineering using COMPASS and Simulink*
- Tonetta (FBK) - *CITADEL Adaptive Systems for High-Assurance Protection*
- Cimatti (FBK) - *COMPASS without AADL: towards COMPASS-STAR?*

Discussion session and round-up

Today's programme (2)

Afternoon session will focus on model-based software engineering

Four solicited talks (20 min each):

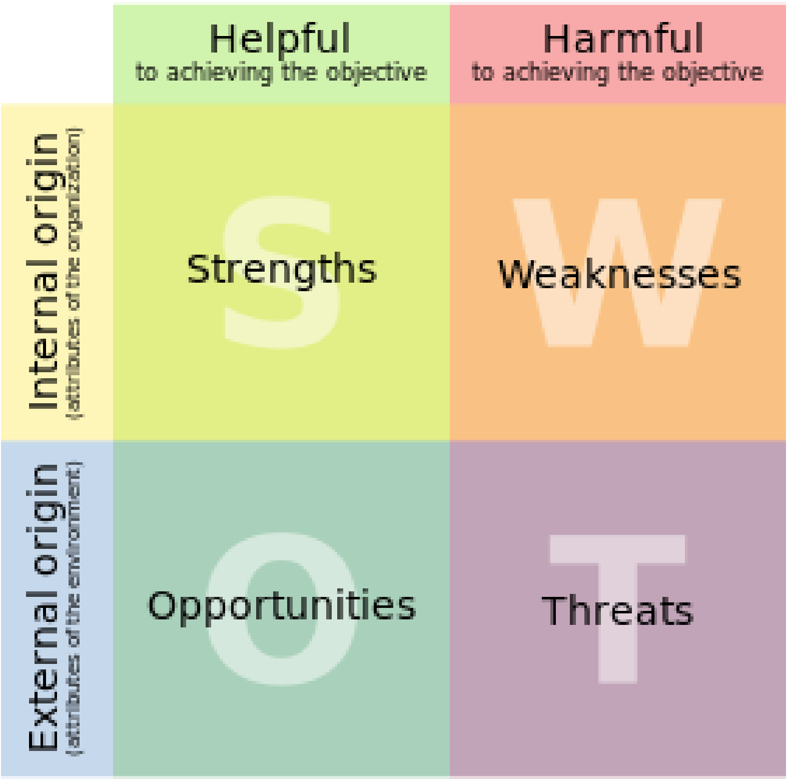
1. Data Modelling on Proba3 ASPIICS payload (Grochowski, N7 Mobile)
2. Mixing Re-Use and Model-Based Development (Pasetti, PnP Software)
3. Space Automation & Robotics General cONtroller (Azkarate, ESA)
4. MBD of an Energy-System Embedded Controller using TASTE (Cavada, FBK)

Elevator pitches (5 min each):

- Schlingloff (Frauenhofer / FOKUS) - Model-based design and tools for space applications
- Wortmann (OHB) - A Model Based and Domain Specific Development Environment
- Jacobs (Topic) - How dynamic is TASTE?
- Toom (IB-Krates) - QGen as a qualifiable code generation backend for TASTE

Discussion session and round-up

Audience participation – SWOT analysis (1)



	Helpful to achieving the objective	Harmful to achieving the objective
Internal origin (attributes of the organization)	Strengths	Weaknesses
External origin (attributes of the environment)	Opportunities	Threats

Topics that may inspire or challenge you:

1. (re-)use of existing technologies versus "inventing something new"
2. technology push versus market pull
3. open versus proprietary standards
4. how to (better) organize the community
5. how to leverage existing results
6. how to achieve MBSSE adoption
7. How to learn from MBSSE outside space?
8. open source versus commercial offerings
9. open access data versus IP protection
10. WHAT CAN YOU DO CONTRIBUTE?

Caveat: the talks are meant to provoke / inspire; specific (constructive) comments are always appreciated but focus on future directions were possible

https://en.wikipedia.org/wiki/SWOT_analysis

Audience participation – SWOT analysis (2)

- Challenge: number of workshop participants has by far exceeded our expectations!
  - Presenters: please stick to your allocated time slot
  - Participants: short questions during / after talks please (use coffee and lunch breaks)

- Discussion / brainstorm sessions
  - Write CONCISE and READABLE on provided post-it notes, use KEYWORDS ONLY
  - Use the talks as inspiration, feel free to raise additional topics or concerns

  - Step 1: put your post-it notes to any of 4 categories (10 min / also use coffee breaks)

  - Step 2: discuss one category in your designated group (20 min)
    (you will discuss the opposing viewpoint in the afternoon)
    - Group the responses – try to find commonalities
    - Discuss: draw some conclusions / define potential actions

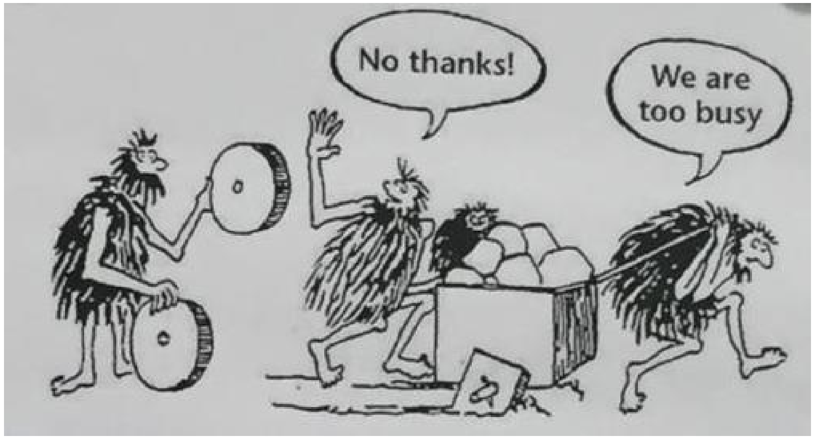
	AM	PM
S	1	4
W	2	3
O	3	2
T	4	1

  - Step 3: plenary presentation per category with Q&A (5 min each)

- Post-workshop follow-up (updated COMPASS roadmap, summary report on SWOT analysis)

Let’s get the show on the road and the ball rolling!

ENJOY THE WORKSHOP



Workshop follow-up

- High-level round-up (Jean-Loup Terraillon) at 17:30
- Input to on-going MBSE harmonization discussion (lead by Joachim Fuchs)
- We will collect the post-it memo's and share the inputs with all workshop participants via e-mail and the workshop web-site (slides will be put on-line too)
- We will try to make a first iteration on the consolidations (reflecting the discussions) and seek interaction with the audience (white paper? questionaire? webex?)
- We will consider concrete follow-up to this workshop in 2017
  you can registers for announcements at https://lists.estec.esa.int/lists/
- Other opportunities to meet and discuss in 2017:
  - SESP (Conf on Simulation and EGSE for space programmes) 28-30 March http://esaconferencebureau.com/2017-events/17c01
  - DASIA
  - Final Presentation Days 2017 (May)
  - SAFECOMP/IMBSA/SEFM (Sept)
  - ADCSS ← likely contender for workshop follow-up (Oct)