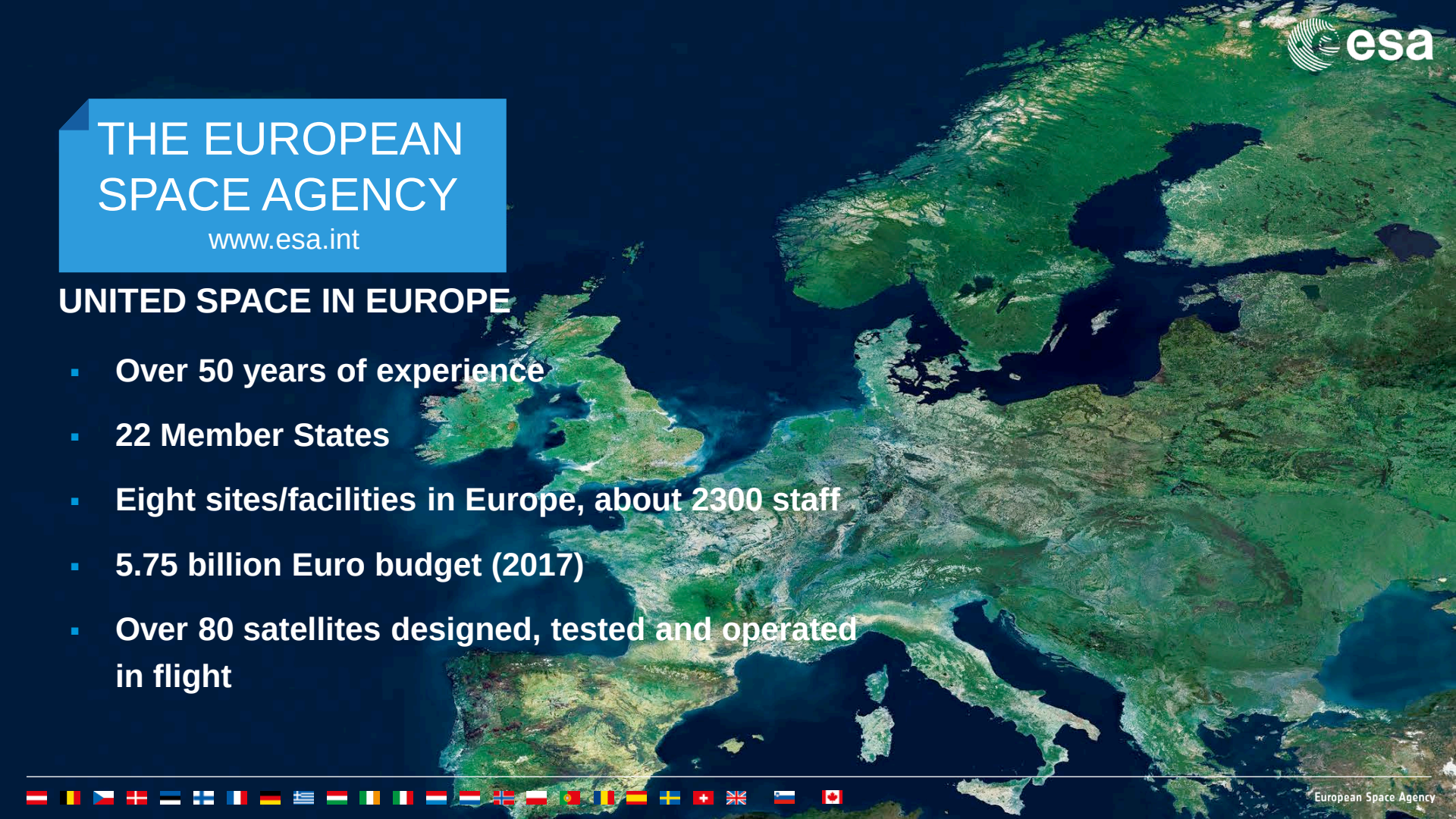
Would any dependability technique have prevented Schiaparelli to land on Mars at 150 m/s?

Jean-Loup Terraillon, European Space Agency



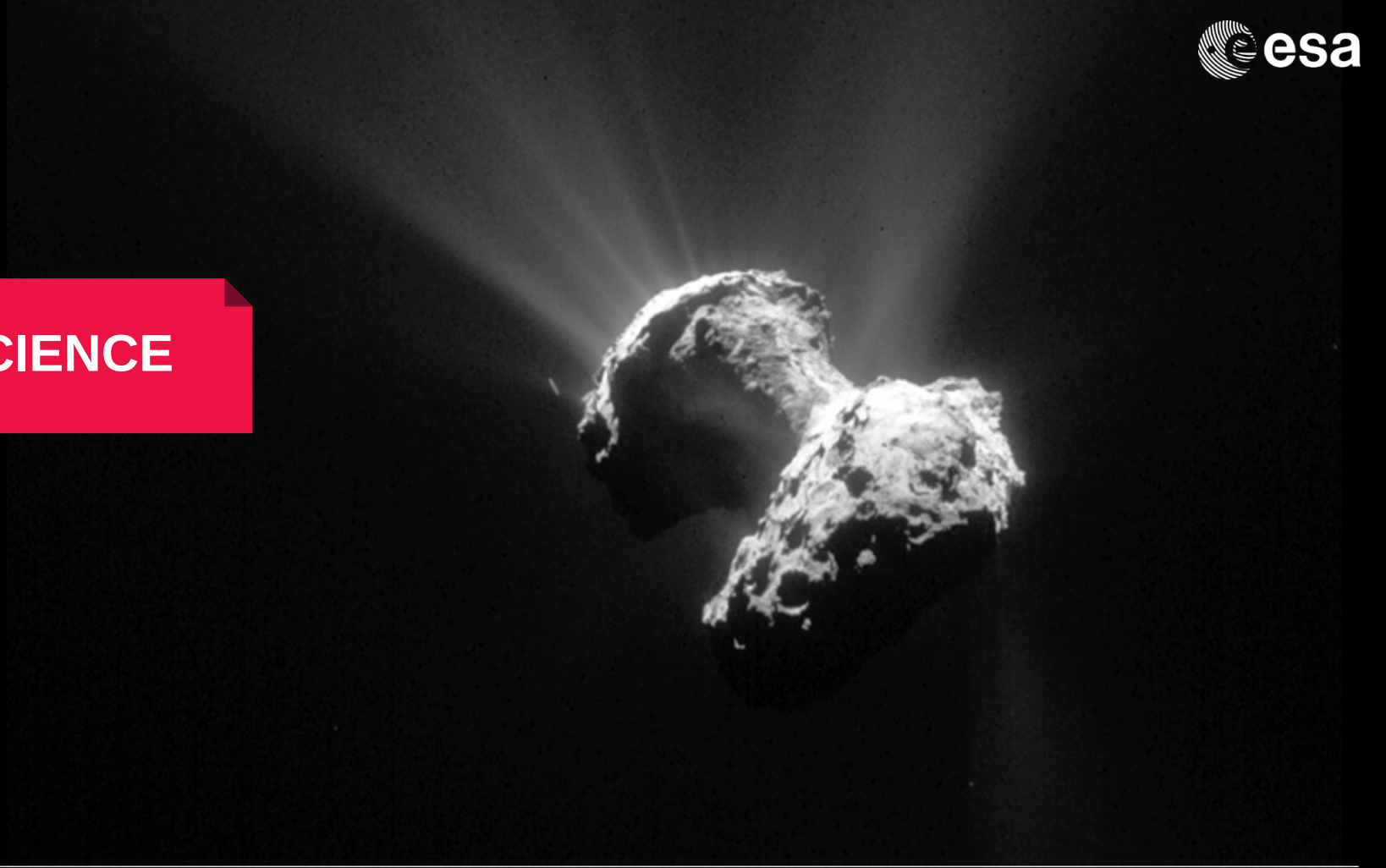
THE EUROPEAN SPACE AGENCY

www.esa.int

UNITED SPACE IN EUROPE

- Over 50 years of experience
- 22 Member States
- Eight sites/facilities in Europe, about 2300 staff
- 5.75 billion Euro budget (2017)
- Over 80 satellites designed, tested and operated in flight

SCIENCE



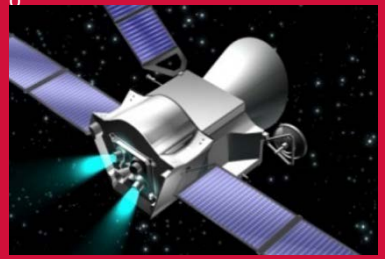
First rendezvous, orbit and soft-landing on a comet

On 6 August 2014, ESA's Rosetta became the first spacecraft to rendezvous with a comet and, on 12 November, its Philae probe made the first soft-landing on a comet and returned data from the surface.

Upcoming missions (1)

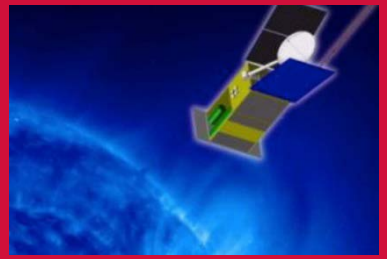
- **BepiColombo** (2018) a satellite duo exploring Mercury (with JAXA)
- **Cheops** (2018) studying exoplanets around nearby bright stars
- **Solar Orbiter** (2018) studying the Sun from close range
- **James Webb Space Telescope** (2018) studying the very distant Universe (with NASA/CSA)
- **Euclid** (2020)
- **JUICE** (2022)
- **Plato** (2024)
- **Athena** (2028)
- **Gravitational wave observatory** (2034)

BepiColombo

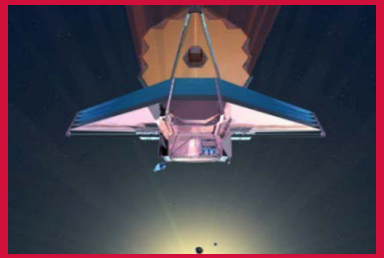


Cheops

Solar Orbiter



James Webb Space Telescope




esa
EARTH
OBSERVATION
European Space Agency

ESA Earth Observation Missions

Colour Code:
Launched
To be launched

Living Planet

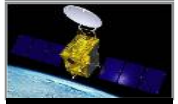
Earth Explorer

Research driven

Core Missions


GOCE
2009-2013


Aeolus
Jun 2018

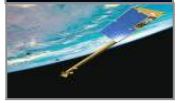

EarthCARE
2019


Biomass
(EE7) 2021

Opportunity


CryoSat-2
8 April 10


SMOS
2 Nov 09


Swarm
22 Nov 13

Fast Track


FLEX (EE8)
2022

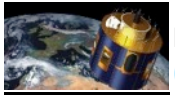
Call EE9 –
Select. for Ph.A
(Nov-2017)

Earth Watch

Operational Service driven
In partnership

Meteorology


Meteosat


MSG - GEO
(1 s/c x 4)


MetOp
1 s/c x 3)


MTG - GEO
(2 s/c x 3)


MetOp SG
(2 s/c x 3)

Copernicus


Sentinel 1 a/b/c/d


Sentinel 2 a/b/c/d


Sentinel 3 a/b/c/d


Sentinel 4 (on MTG)


Sentinel 5 precursor


Sentinel 5 (on MetOp SG)


Sentinel 6 (Jason)

Earth explorers

- **GOCE** (2009–13) studying Earth's gravity field
- **SMOS** (2009–) studying Earth's water cycle
- **CryoSat-2** (2010–) studying Earth's ice cover
- **Swarm** (2013–) three satellites studying Earth's magnetic field
- **ADM-Aeolus** (2017) studying global winds
- **EarthCARE** (2018) studying Earth's clouds, aerosols and radiation (ESA/JAXA)
- **Biomass** (2021) studying Earth's carbon cycle
- **FLEX** (2022) studying photosynthesis

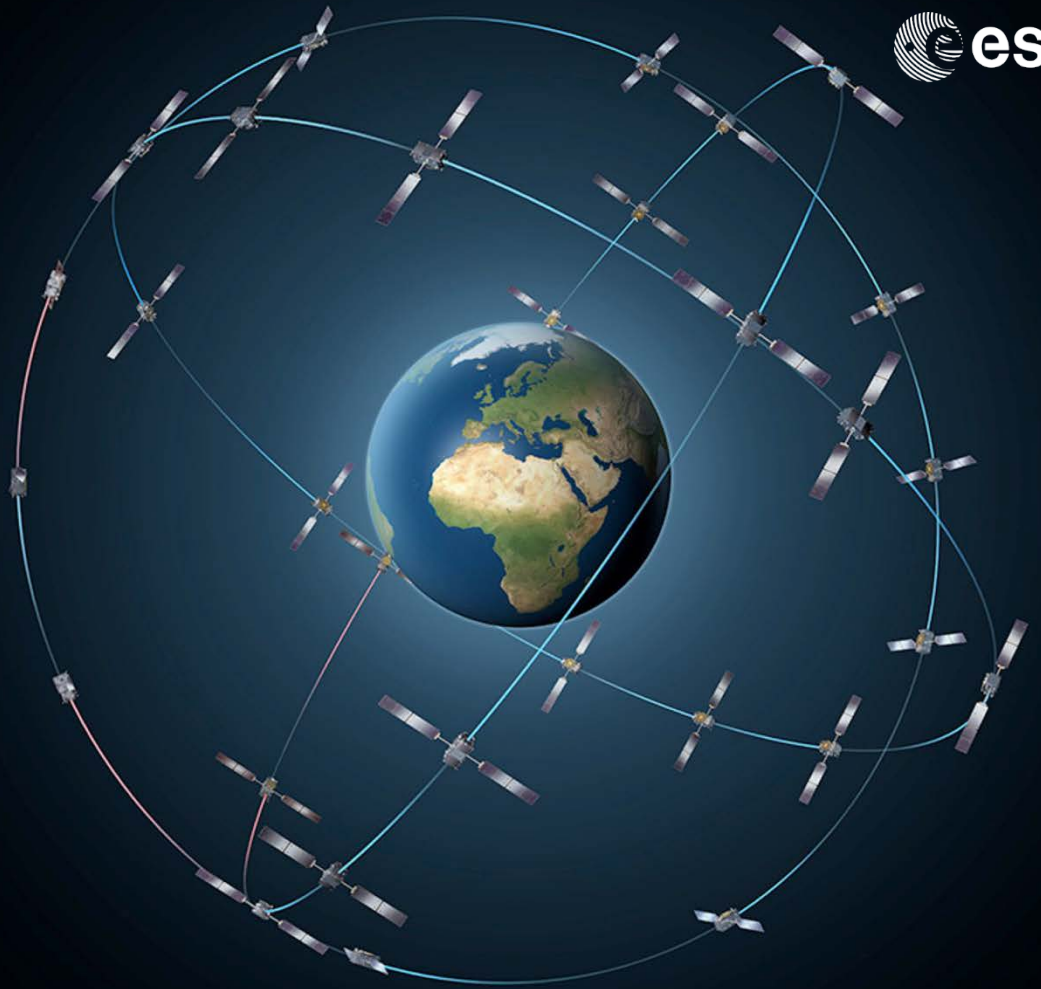
Meteorology

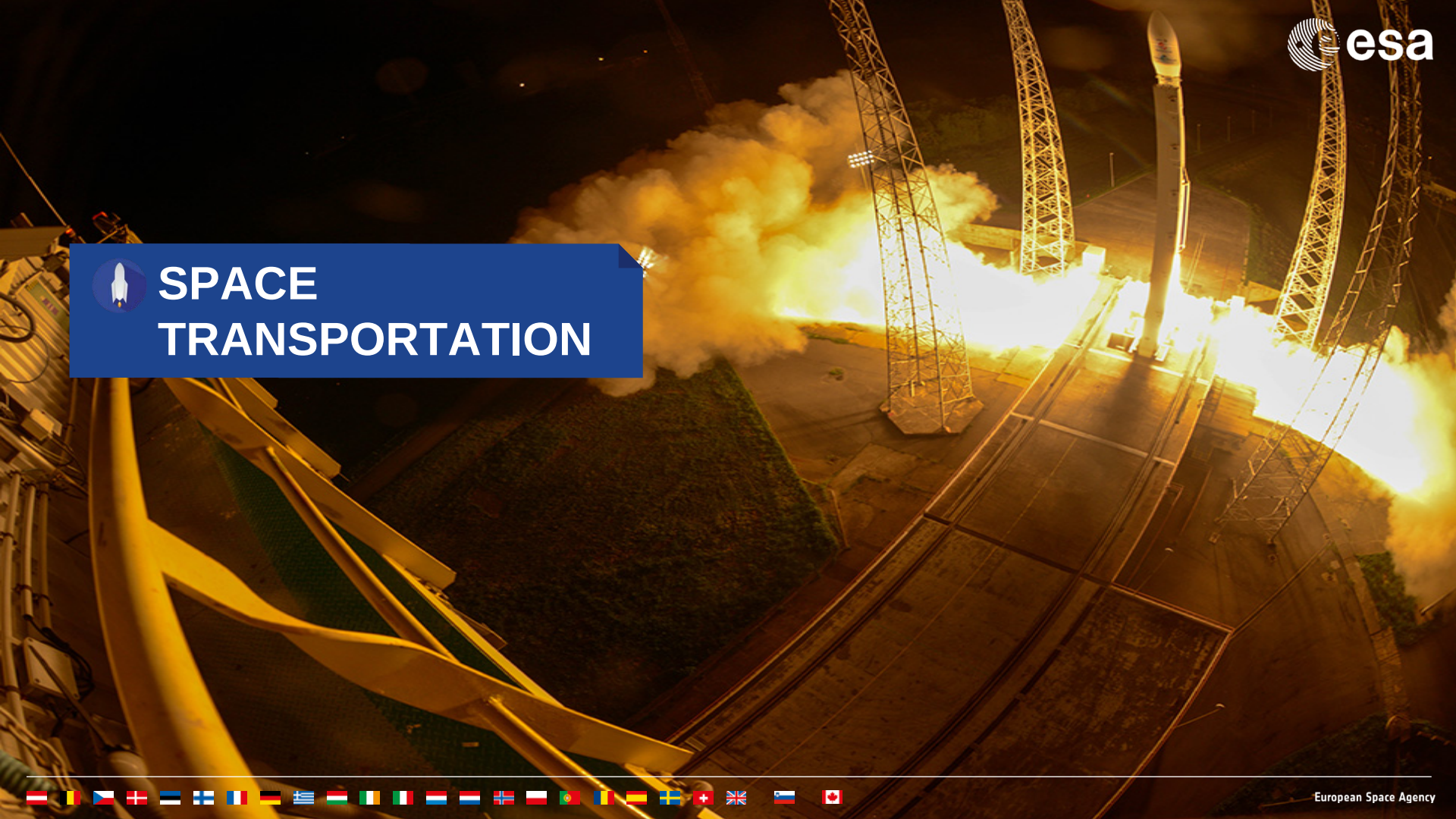
- Meteosat Second & Third generation
- MetOp first and second generation

Global monitoring for environment and security: Copernicus and the Sentinels

- Sentinel-1 – land and ocean services. Sentinel-1A launched in 2014/Sentinel-1B in 2016.
- Sentinel-2 – land monitoring. Sentinel-2A launched in 2015/Sentinel-2B (2017).
- Sentinel-3 – ocean forecasting, environmental and climate monitoring. Sentinel-3A launched in 2016. Sentinel-3B (2017).
- Sentinel-4 – atmospheric monitoring payload (2019)
- Sentinel-5 – atmospheric monitoring payload (2021)
- Sentinel-5 Precursor – atmospheric monitoring (2017)
- Sentinel-6 – oceanography and climate studies (2020)

NAVIGATION

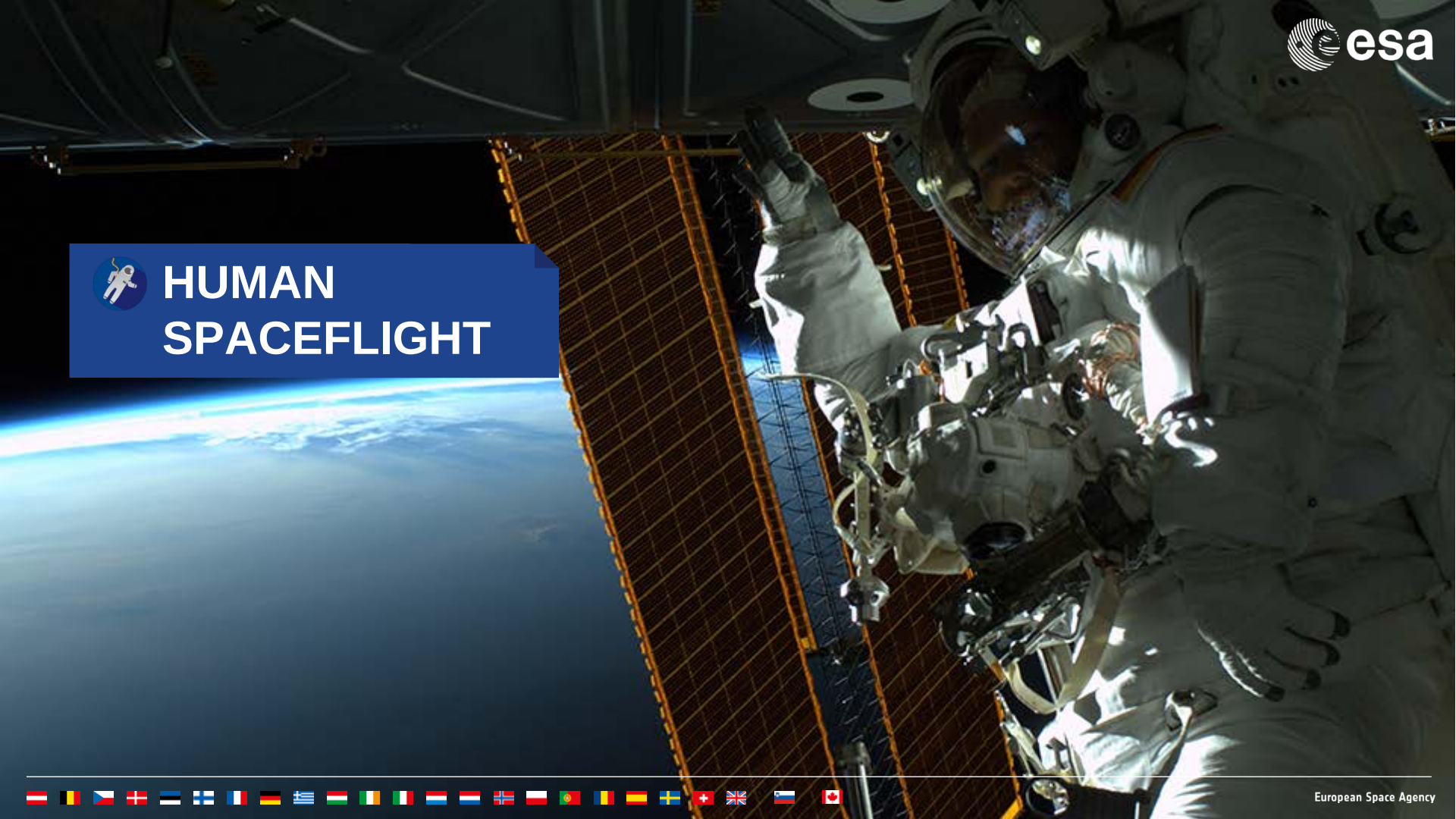



SPACE
TRANSPORTATION

Launchers and technologies of the future: Ariane 6 and Vega C

European Ministers agreed at the Ministerial Council 2014 to develop Ariane 6 and Vega C. These launchers will provide guaranteed access to space for Europe at a competitive price without requiring public sector support for commercial exploitation.

- Ariane 6 – modular three-stage launcher with two configurations, using two (A62) or four boosters (A64);
- Vega C – evolution of Vega with increased performance and same launch service cost;
- Common solid rocket motor for Ariane 6 boosters and Vega C first stage;
- New governance for Ariane 6 development and exploitation allocating increased roles and responsibilities to industry;
- Vega C and Ariane 6 first flights – 2019 and 2020.


HUMAN
SPACEFLIGHT

European Service Module

The European Service Module (ESM) is ESA's contribution to NASA's Orion spacecraft that will send astronauts to the Moon and beyond. The spacecraft comprises the ESM and the US Crew Module.

The ESM resembles ESA's Automated Transfer Vehicle, from which it evolved. Between 2009 and 2014, five Automated Transfer Vehicles delivered supplies to the International Space Station and helped to keep the outpost in orbit.

The first mission for the complete Orion spacecraft will be an unmanned flight to the Moon and back (first launch, 2018)

Next generation: flown and in training

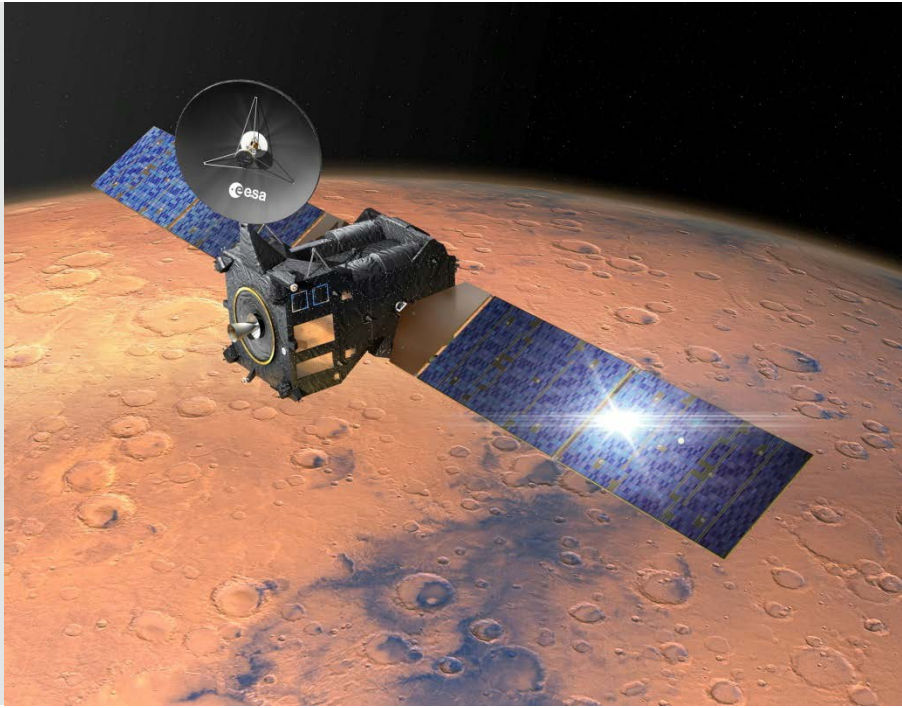
Based at the European Astronaut Centre (EAC), Cologne, Germany:

Luca Parmitano (IT), Alexander Gerst (DE) and Samantha Cristoforetti (IT) flew to the ISS in 2013, mid-2014 and end-2014 respectively. Andreas Mogensen (DK) flew in 2015, Tim Peake (UK) in 2015/16 and Thomas Pesquet (FR) is flying in 2016/17. Matthias Maurer (DE) began training in 2017.

Back: Tim, Andreas, Alex, Luca; front: Samantha, Thomas, Matthias

Robotic exploration

In cooperation with Roscosmos (Russia), two **ExoMars** missions (2016 and 2020) will investigate the martian environment, particularly astro-biological issues, and develop and demonstrate new technologies for planetary exploration with the long-term view of a future **Mars sample return** mission.



Objectives

❑ ExoMars Programme:

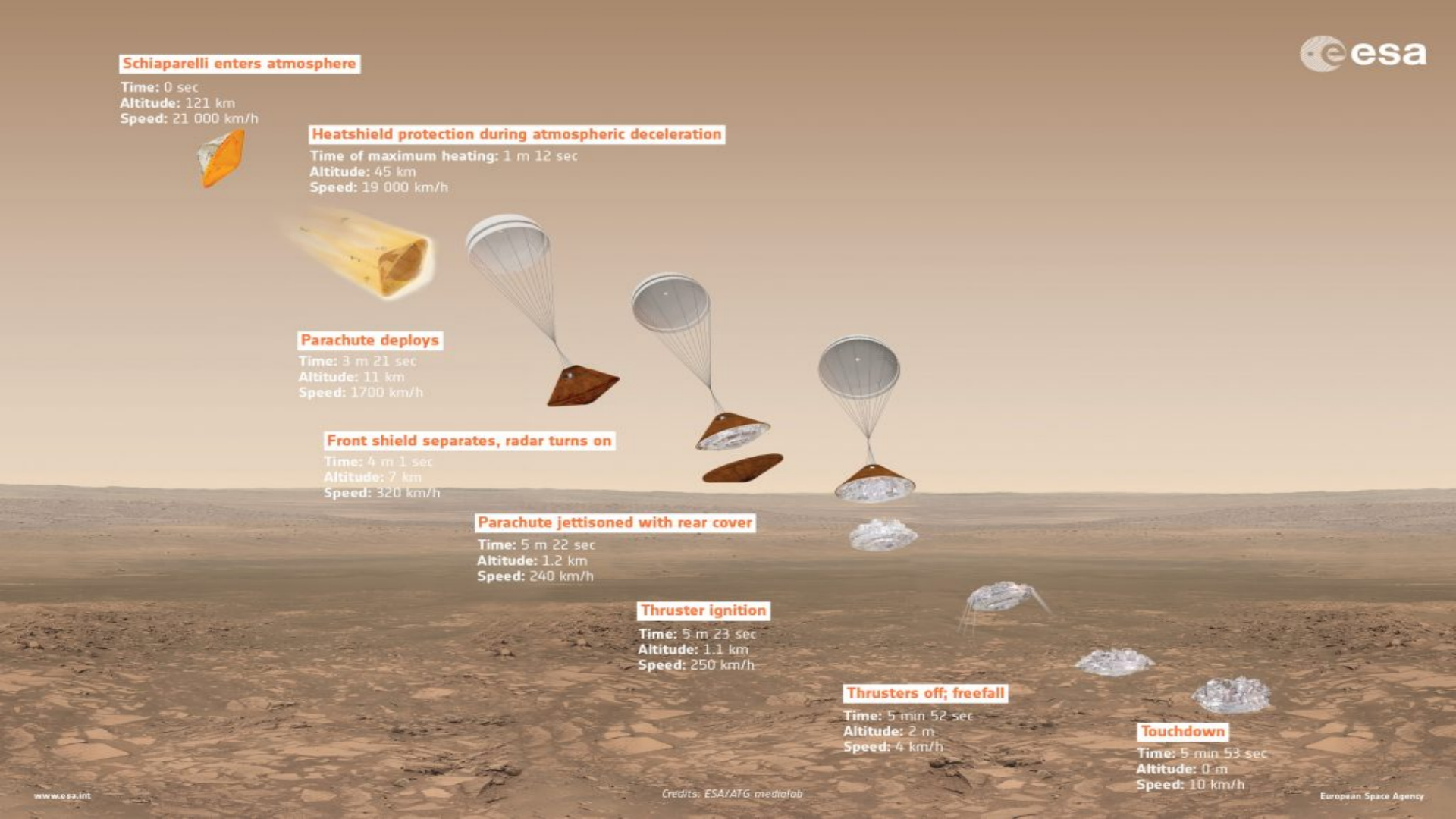
- investigate the Martian environment
- demonstrate new technologies paving the way for a future **Mars sample return** mission in the 2020's

❑ ExoMars 2016:

- provide a **relay orbiter** for landed assets
- search for **signatures** of active biological or geological processes (methane and other trace atmospheric gases)
- test **key technologies** in preparation for ESA's contribution to subsequent missions to Mars

ExoMars 2016: TGO and Schiaparelli

esa
European Space Agency


Schiaparelli enters atmosphere
Time: 0 sec
Altitude: 121 km
Speed: 21 000 km/h
Heatshield protection during atmospheric deceleration
Time of maximum heating: 1 m 12 sec
Altitude: 45 km
Speed: 19 000 km/h
Parachute deploys
Time: 3 m 21 sec
Altitude: 11 km
Speed: 1700 km/h
Front shield separates, radar turns on
Time: 4 m 1 sec
Altitude: 7 km
Speed: 320 km/h
Parachute jettisoned with rear cover
Time: 5 m 22 sec
Altitude: 1.2 km
Speed: 240 km/h
Thruster ignition
Time: 5 m 23 sec
Altitude: 1.1 km
Speed: 250 km/h
Thrusters off; freefall
Time: 5 min 52 sec
Altitude: 2 m
Speed: 4 km/h
Touchdown
Time: 5 min 53 sec
Altitude: 0 m
Speed: 10 km/h
esa
www.esa.int
Credits: ESA/ATG medialab
European Space Agency

https://youtu.be/s3WCtJt46qU?list=PLHWdbfW26Esa2Reh-2ODRTbcCc5SbFxZM

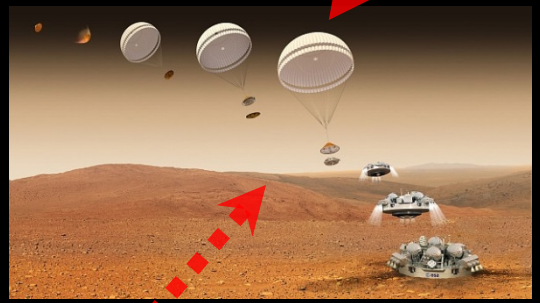
Schiaparelli's descent to Mars.mp4

ESA
TGO

ESA
Mars Express

NASA
MRO

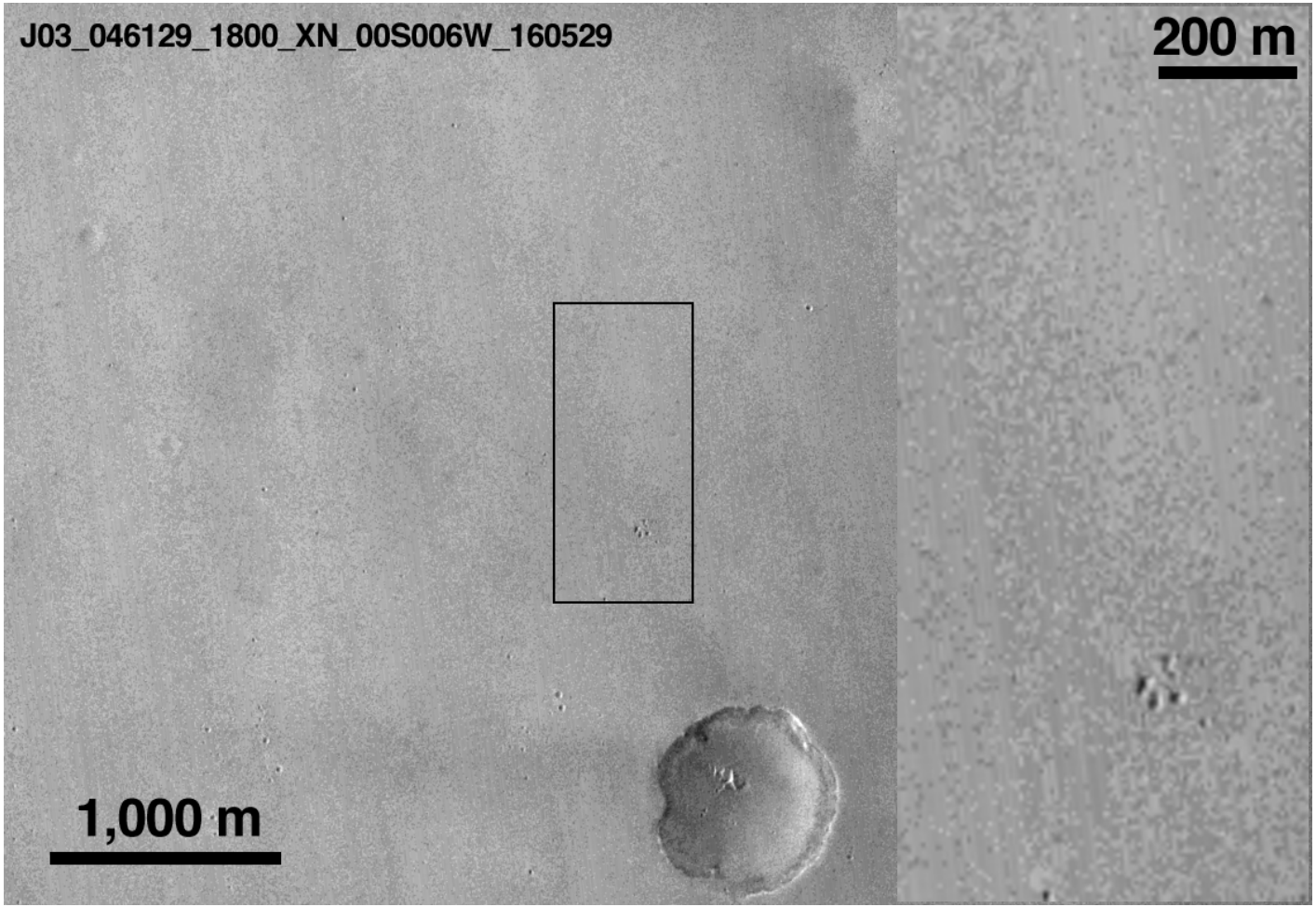
NASA
MAVEN

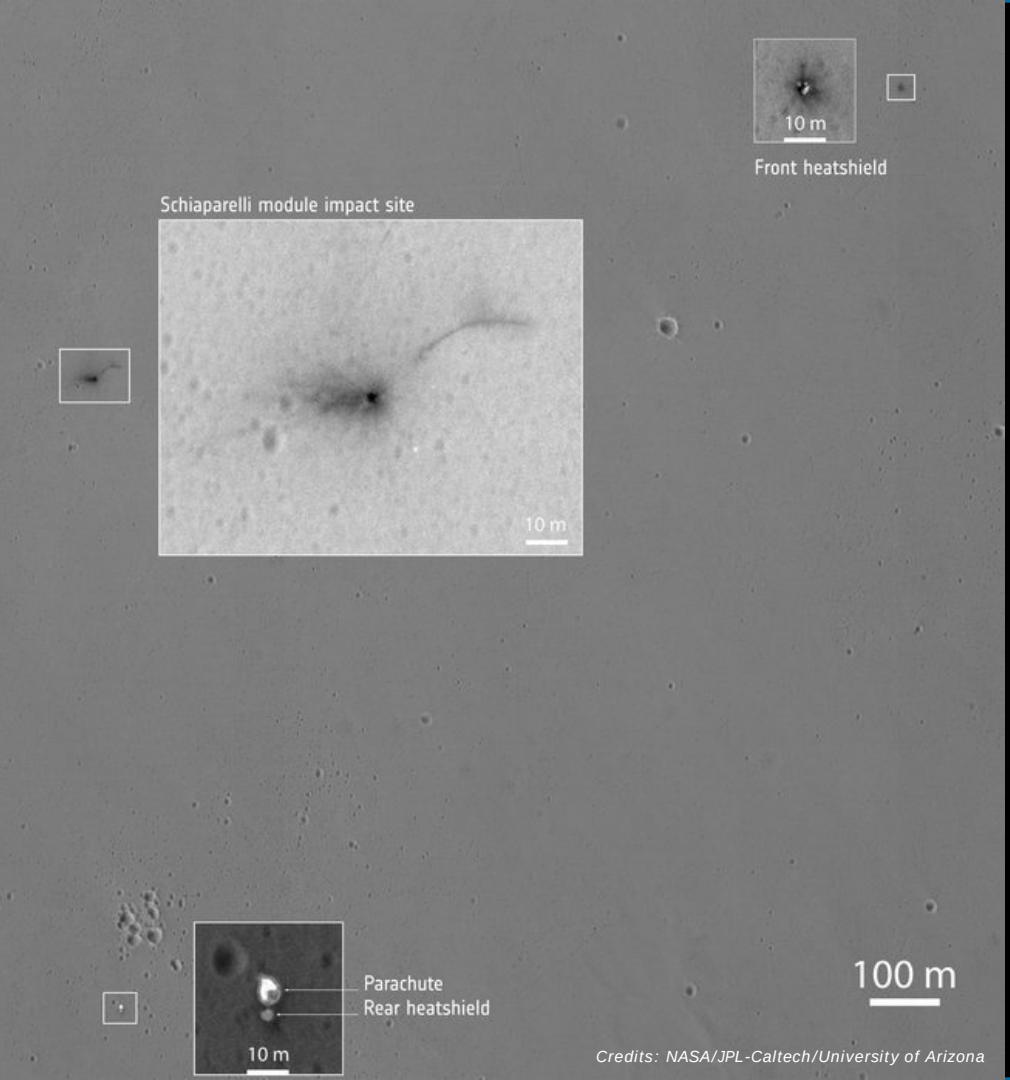


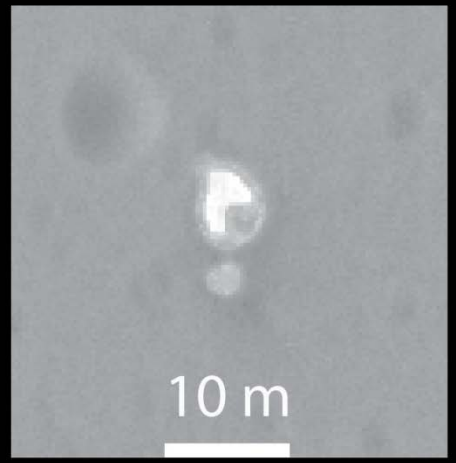
NASA
Odyssey

Press conference…


EUROPE'S NEW ERA OF MARS EXPLORATION
www.esa.int/exomars
#ExoMars
@ESA_ExoMars
esa
Andrea Accomazzo
Don McCoy
ExoMars Program Manager, ESA


J03_046129_1800_XN_00S006W_160529
200 m
1,000 m

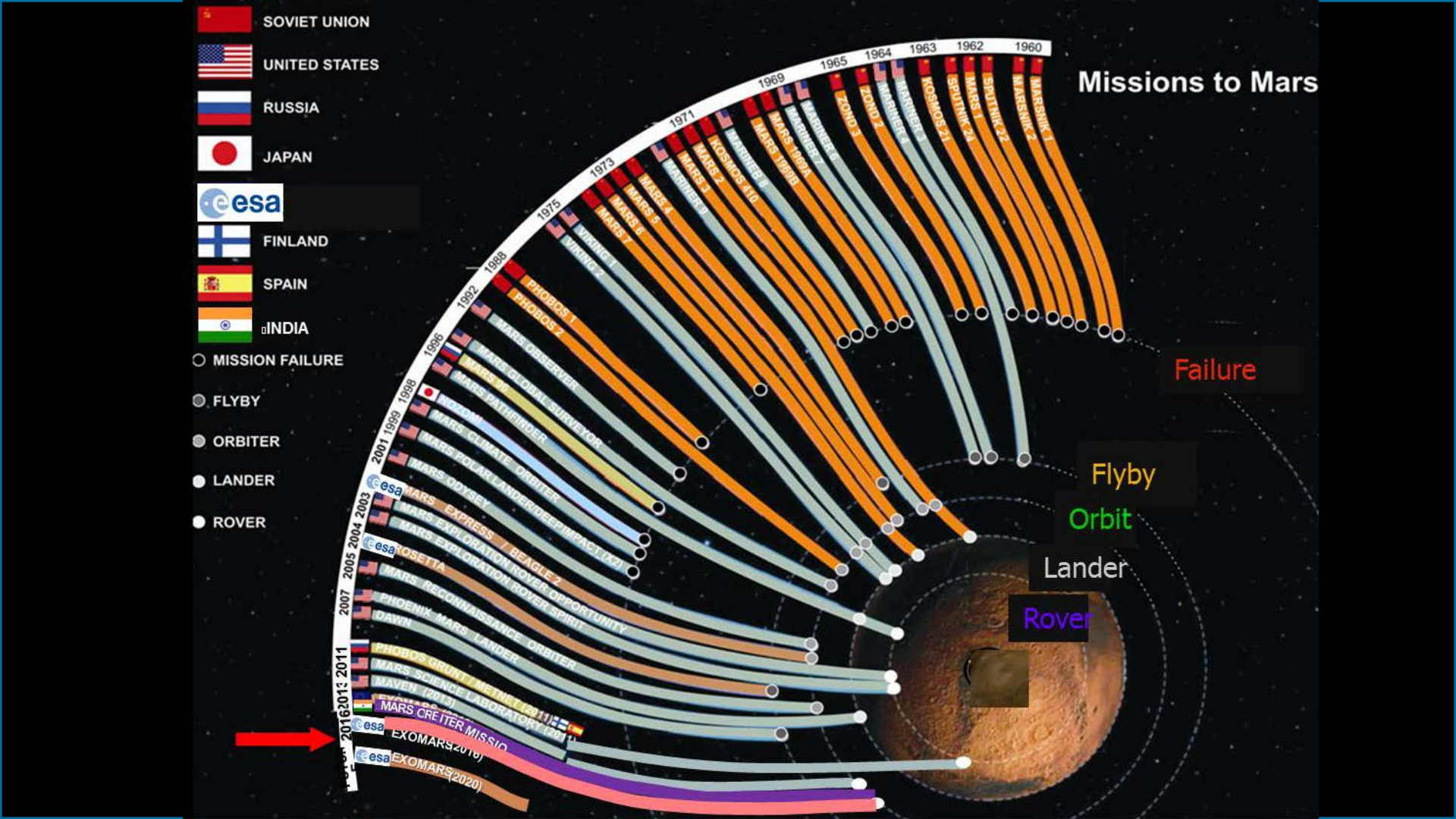




Credits: NASA/JPL-Caltech/University of Arizona

25 Oct

1 Nov


SOVIET UNION
UNITED STATES
RUSSIA
JAPAN
esa
FINLAND
SPAIN
INDIA
MISSION FAILURE
FLYBY
ORBITER
LANDER
ROVER
Missions to Mars
1960
1962
1963
1964
1965
1969
1971
1973
1975
1988
1992
1996
1998
1999
2001
2003
2004
2005
2007
2011
2016
2018
2020
MARSNIK 1
MARSNIK 2
SPUTNIK 22
MARS 1
SPUTNIK 24
KOSMOS 21
MARINER 4
MARINER 5
ZOND 2
ZOND 3
MARS 1969A
MARS 1969B
MARINER 6
MARINER 7
KOSMOS 419
MARS 2
MARS 3
MARINER 8
MARS 4
MARS 5
MARS 6
MARS 7
VIKING 1
VIKING 2
PHOBOS 1
PHOBOS 2
MARS OBSERVER
MARS GLOBAL SURVEYOR
MARS 96
MARS PATHFINDER
NOZOMI
MARS CLIMATE ORBITER
MARS POLAR LANDER/DEEP IMPACT (DS2)
MARS ODYSSEY
MARS EXPRESS / BEAGLE 2
MARS EXPLORATION ROVER OPPORTUNITY
MARS EXPLORATION ROVER SPIRIT
ROSETTA
MARS RECONNAISSANCE ORBITER
PHOENIX MARS LANDER
DAWN
PHOBOS GRUNT / MetNet (2011)
MARS SCIENCE LABORATORY (2011)
MAVEN (2013)
MARS CRETER MISSION
EXOMARS2016)
EXOMARS(2020)
Failure
Flyby
Orbit
Lander
Rover

Anomaly Tree Investigation Findings

- **no anomalies** occurred in the MIMU

- there was **high dynamics motion** experienced during parachute deployment

➔ it was most likely not caused by a specific system or component failure

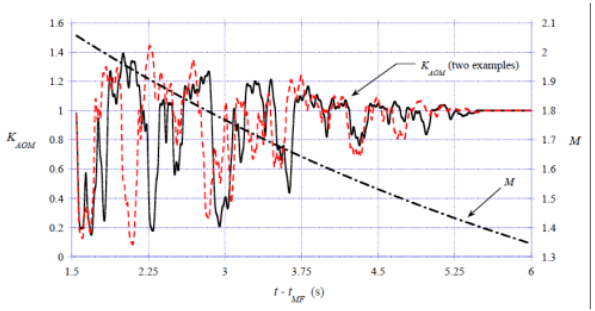
- high rotation rates **saturating** the MIMU at 187.5 º/s during parachute deployment

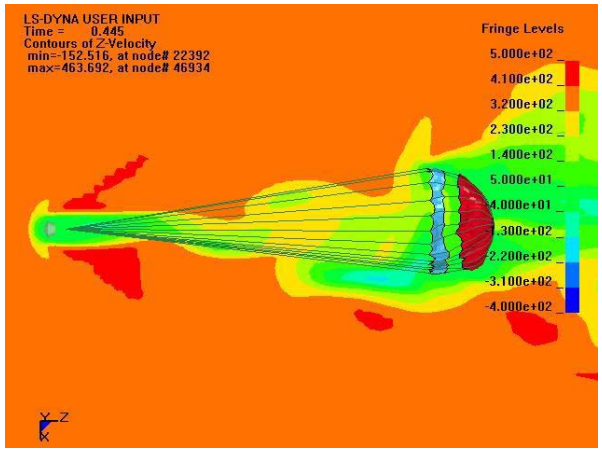
➔ *Saturation flag used to filter IMU overflow*

Root Causes #1/6: parachute

Insufficient conservative modelling of the parachute dynamics which led to expect much lower dynamics than observed in flight

- Does not account for supersonic disturbances
- Predicted Mach [1.88 – 2.07] Real 2.05
- Riser angle higher than expected [9 deg]





$$\bar{V}_R = \frac{2V_{R,mf} - \Delta V_v + \bar{V}_b \Delta t}{2}$$

equation (A2) yields

$$V_{R,mf} = \frac{2\bar{V}_R + \Delta V_v - \bar{V}_b \Delta t}{2}$$

that drag is the principal force acting on the bag during
ring only longitudinal motion

$$\bar{V}_b \approx \frac{-\overline{(C_D S)_b q_w} + g \sin\gamma}{\bar{m}_b}$$

is estimated from

$$V_{R,mf} = \frac{2\bar{V}_R + \Delta V_v - \left[\frac{-\overline{(C_D S)_b q_w} + g \sin\gamma}{\bar{m}_b}\right]\Delta t}{2}$$

APPENDIX

$$V_{R,ls} = V_{R,mf} - \Delta V_v + \frac{-\overline{(C_D S)_b q_w} + g \sin\gamma}{\bar{m}_b}\Delta t$$

Root Causes #2/6 : saturation flag

Inadequate persistence time of the MIMU saturation flag and inadequate handling of MIMU saturation by the GNC

- 1 sec ←→ 15 msec

Root Causes #3/6 : verification

Mishap in management of subcontractors and acceptance of hardware,

- the importance of the persistence of IMU saturation time was under estimated
- It was **not measured** at acceptance and instead believed to be 15 ms.
- It was **not tested** after delivery of the unit
- Instead, a **mathematical model** was used. The mathematical model was done by the User, not by the Supplier. It was not validated by the Supplier.

Root Causes #4/6 : stress

Strong delivery-oriented team

Must-launch in 2016

drawing Bruce Macdonald

nose to the grindstone

nez dans le guidon

Root Causes #5/6 : FDIR

Insufficient approach to FDIR and design robustness;

1. as no such parachute dynamic was expected, there was no consideration of saturation as feared event.
2. initial statement: no redundancy, not Fail-Ops, not Fail-Safe.

- could have been just fail-degraded?
- yes but, anyhow both IMU and Radar are essential to the landing.

➔ RAMS analysis OK w.r.t. known failure or known consequences…

➔ SW FMEA useless: all components critical, no component “failed”

Root Causes #5/6 : FDIR

Risk have been underestimated!

Missing **“what if”, robustness, worst case analysis**

- many **cross check** test possible (acc., ang. rate, altimetry, time, etc.)

➔ fault tolerance in software?

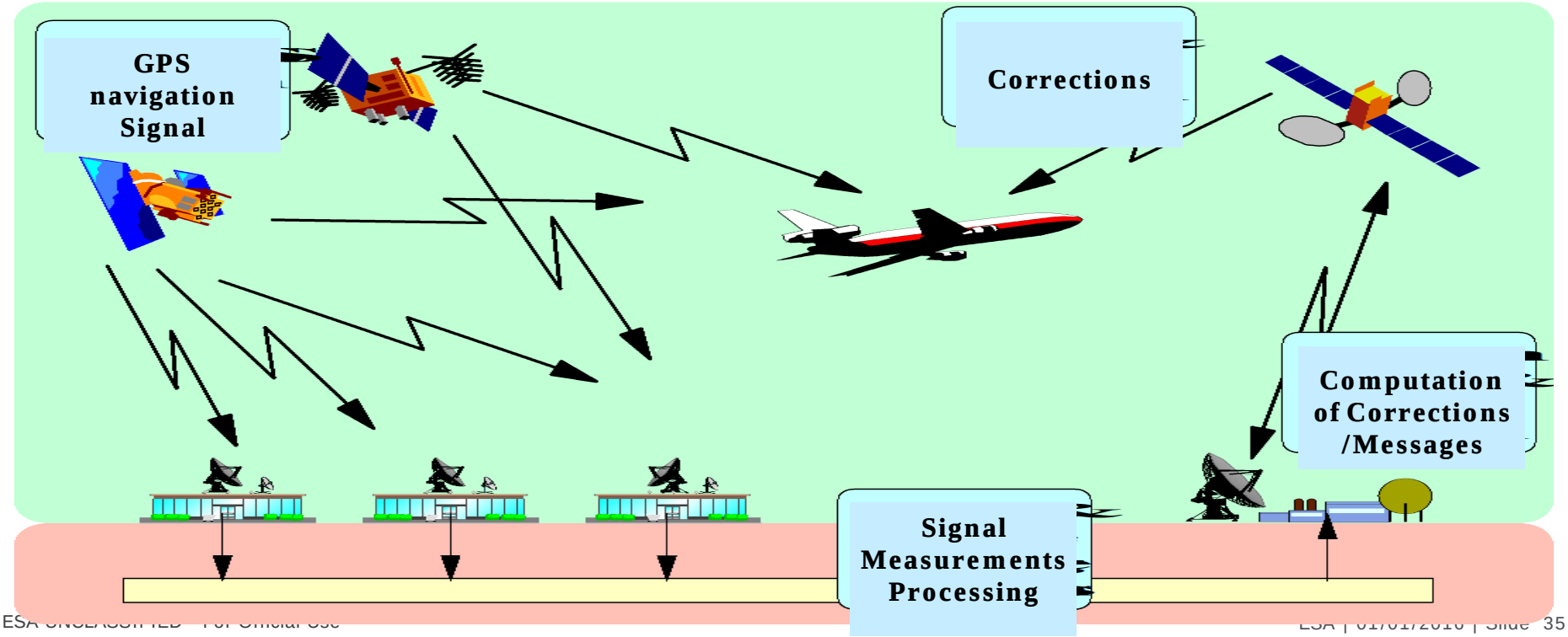
- sensitivity analysis➔ uncertainty ➔ **worst case analysis**

➔ Design robustness, **margins**, software robustness?

THE ESA “RAMS”

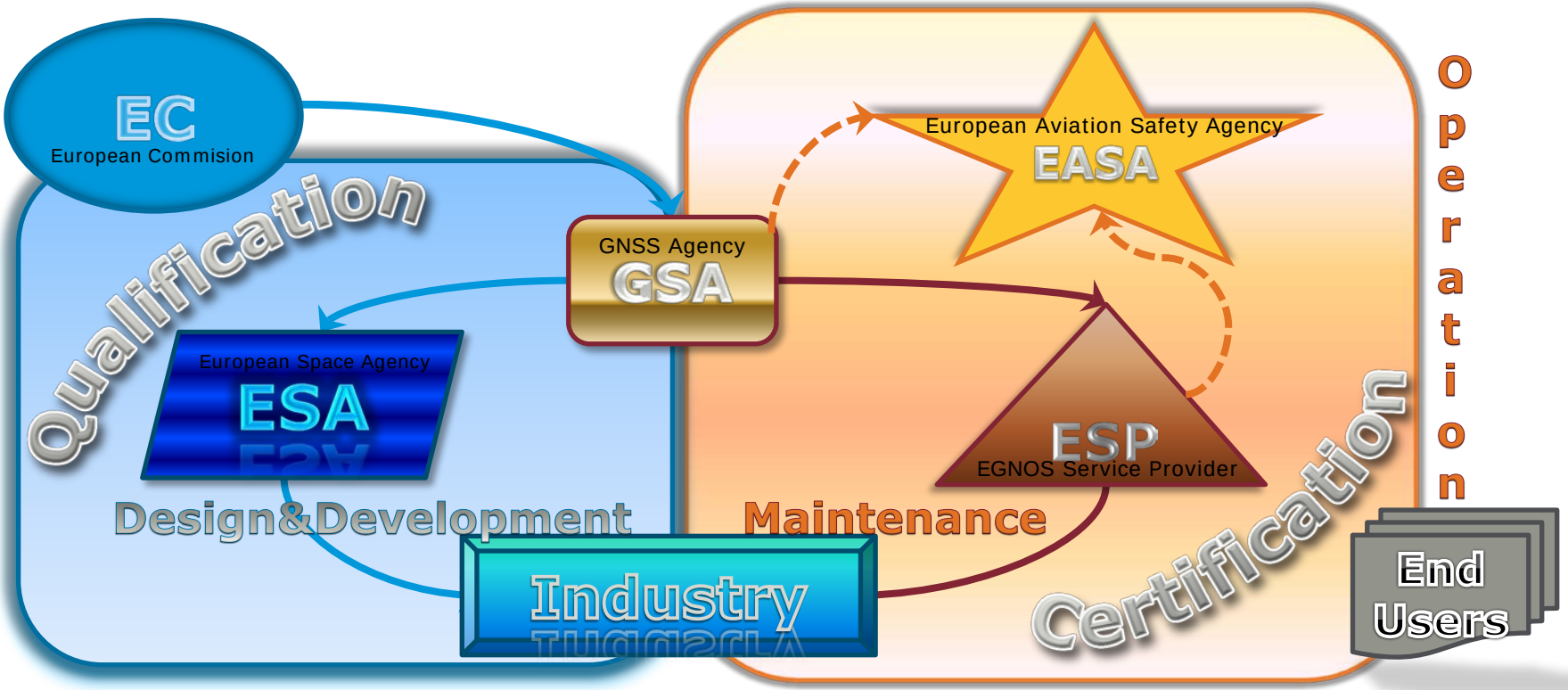
NO CERTIFICATION, BUT QUALIFICATION

EGNOS presentation



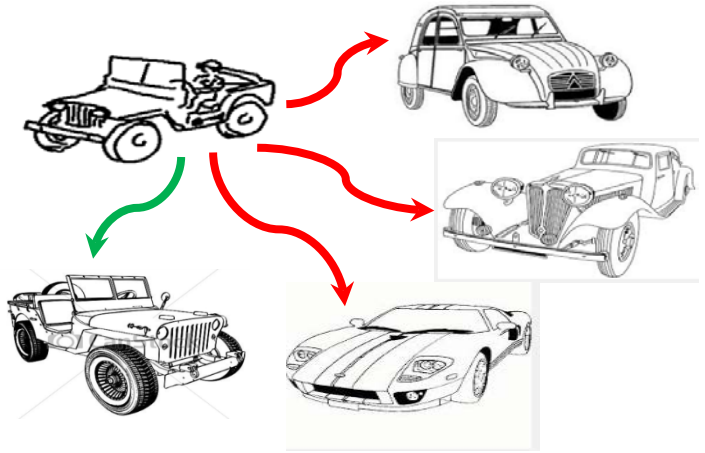
Organisation

Framework Contract – Working arrangement



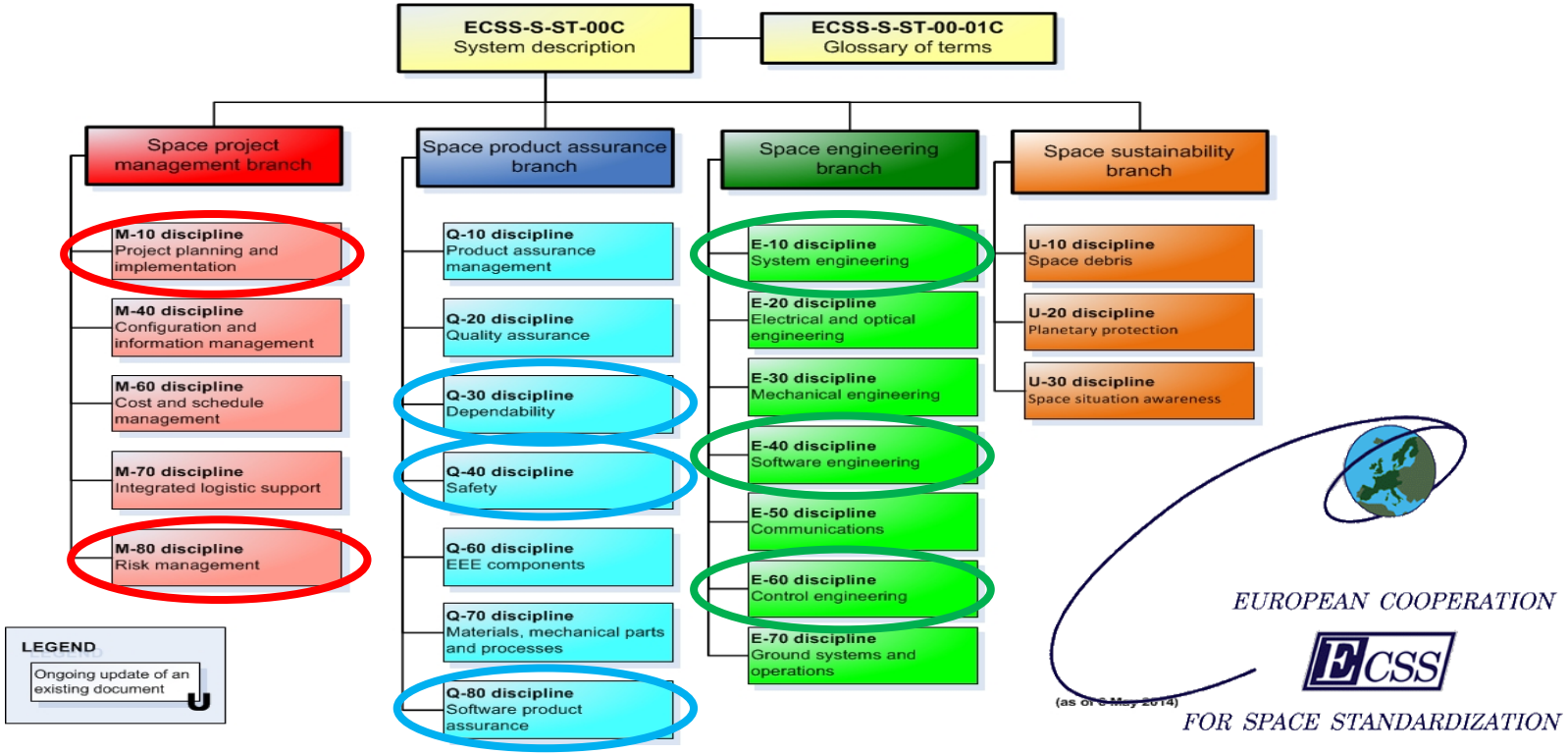
Qualification and Certification

Certification refers to the confirmation **by a recognized body** that an object, person, or organization conforms to required standardised characteristics



Qualification refers to the confirmation **by a customer** that an object conforms to required functionalities and performance according its safety and dependability level need.

128 ECSS standards... www.ecss.nl



Qualification review (ECSS-M-ST-10C)

4.4.3.6.3 Main review objectives – **Qualification review**

• To confirm that the verification process has demonstrated that the design, **including margins,** meets the applicable requirements.

Qualification margin: increase of the environmental, mechanical, electrical, EMC, or operational extremes above the worst case levels predicted over the specified product lifetime for the purpose of design margin demonstration

ECSS-Q-ST-30C: risk reduction

Dependability risk analysis reduction and control shall include the following steps:

1. identification and classification of **undesirable events** according to the severity of their consequences;
2. analysis of **failure scenarios**, determination of related **failure modes**, failure origins or **causes**;
3. classification of the **criticality** of the functions and associated products according to the severity of relevant failure consequences;
4. definition of actions and **recommendations** for detailed risk assessment, risk elimination, or risk reduction and control to an acceptable level;
5. status of risk reduction and risk acceptance;
6. implementation of risk reduction;
7. verification of risk reduction and assessment of residual risks.

NOTE The process of risk identification and assessment implies both qualitative and quantitative approaches.

ECSS-Q-ST-30C: dependability requirements

The dependability requirements shall be included into the technical specifications.

NOTE The technical specifications typically include:

- functional, operational and environmental requirements,
- test requirements including stress levels, test parameters, and accept or reject criteria,
- **design performance margins**, derating factors, quantitative dependability requirements, and qualitative dependability requirements (identification and classification of undesirable events), under specified environmental conditions,
- the identification of human factors and how they can influence dependability during the project lifecycle,
- the identification of external, internal and installation factors that can influence dependability during the project lifecycle,
- **the degree of tolerance to hardware failures or software malfunctions**,
- **the detection, isolation, diagnosis, and recovery of the system from failures and its restoration to an acceptable state**,
- the requirement for the prevention of failures crossing interfaces with unacceptable consequences,
- definition of the maintenance concept,
- maintenance tasks and requirements for special skills,
- requirements for preventive maintenance, special tools, and special test equipment,
- requirements for process and technology margin demonstration and qualification,
- requirement on sampling strategy in serial production and for periodical demonstration of qualification preservation.

ECSS-Q-ST-30C: dependability design

In order to implement dependability aspects into the design, the following approaches shall apply:

1. functional design:

(a) the preferred use of **software designs** or methods that have performed successfully in similar applications

(b) the implementation of **failure tolerance**;

(c) the implementation of **fault detection, isolation and recovery**, allowing proper failure processing by dedicated flight and ground measures, and considering detection or reconfiguration times in relation with propagation times of events under worst case conditions;

(d) the implementation of monitoring of the parameters that are essential for mission performance, considering the failure modes of the system in relation to the actual capability of the detection devices, and considering the acceptable environmental conditions to be maintained on the product.

2. physical design:

ECSS-Q-ST-30C: dependability analysis

Identification and classification of undesirable events

Assessment of failure scenarios

Dependability analyses – methods

- Reliability prediction
- FMEA/FMECA
- Hardware-software interaction analysis (HSIA)
- Contingency analysis
- Fault tree analysis (FTA)
- Common-cause analysis
- **Worst case analysis (WCA)**
- Part stress analysis
- Zonal analysis
- **Failure Detection Isolation and Recovery (FDIR) analysis**

OUR FDIR EXPERIENCE

FDIR in software is a recurrent issue

Difficult **verification** - experimental tuning

➔ cost and delay in integration

It ends up being a **toolbox** to monitor and reconfigure more or less everything.

➔ over design

Still, there are numerous **particular cases** that are discovered when running scenarii.

➔ uncontrolled design

FDIR "**emerge**" from the engineering process by necessity rather than by conscious intention.

➔ no dedicated process, no support tools, difficult verification

FDIR improvements

Consistent and **timely** FDIR conception, development, V&V

Fit-for-purpose FDIR

Coherent, **repeatable** Process and Methodology

- Applicable from early Software and System architectural design
- Coherent with System development lifecycle
- Milestones with measurable FDIR maturity
- Oriented towards Mission and System RAMS requirements

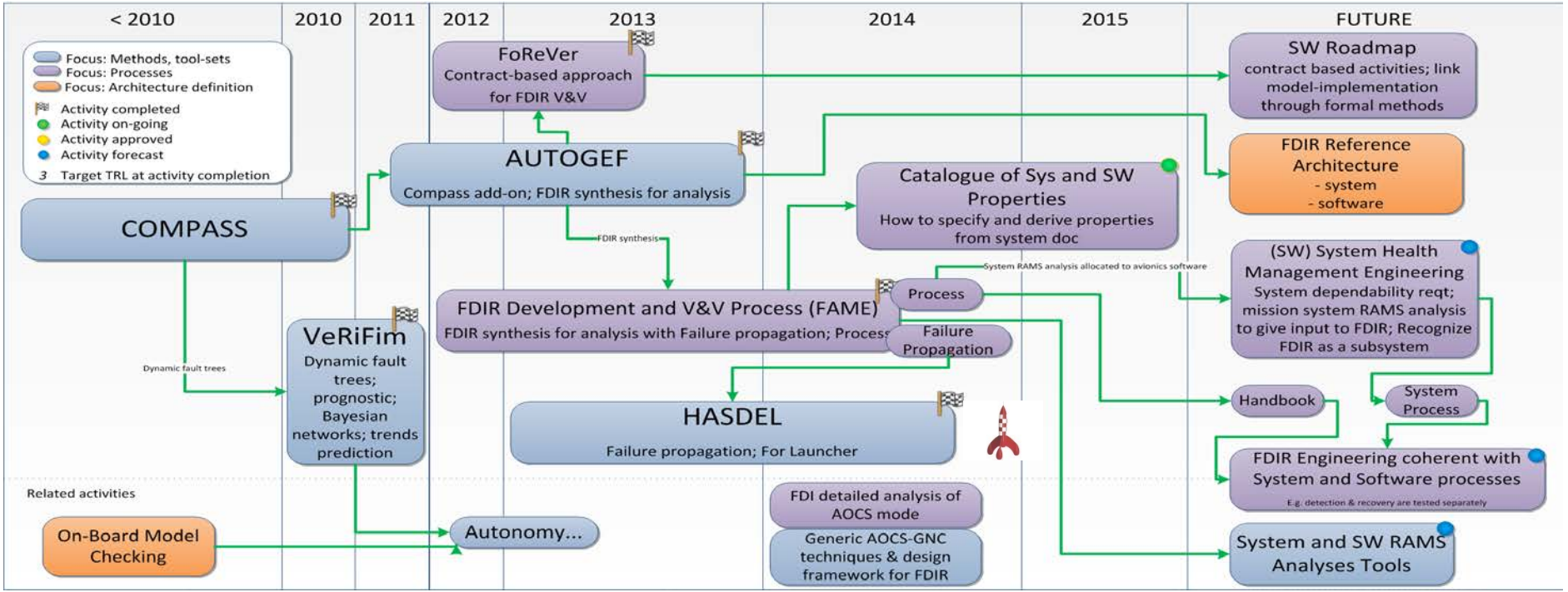
Advanced **modelling** and analysis techniques

- Specification of nominal, erroneous, FDIR behavior
- Automated FTA, FMECA, Failure Propagation and FDIR Analyses

Reference FDIR **architecture**

FDIR as an explicit system discipline

FDIR roadmap of activities



COMPASS Overview

Executed in 2008 – 2010 - 2016

Consortium

RWTH Aachen University (RWTH) – Prime, D

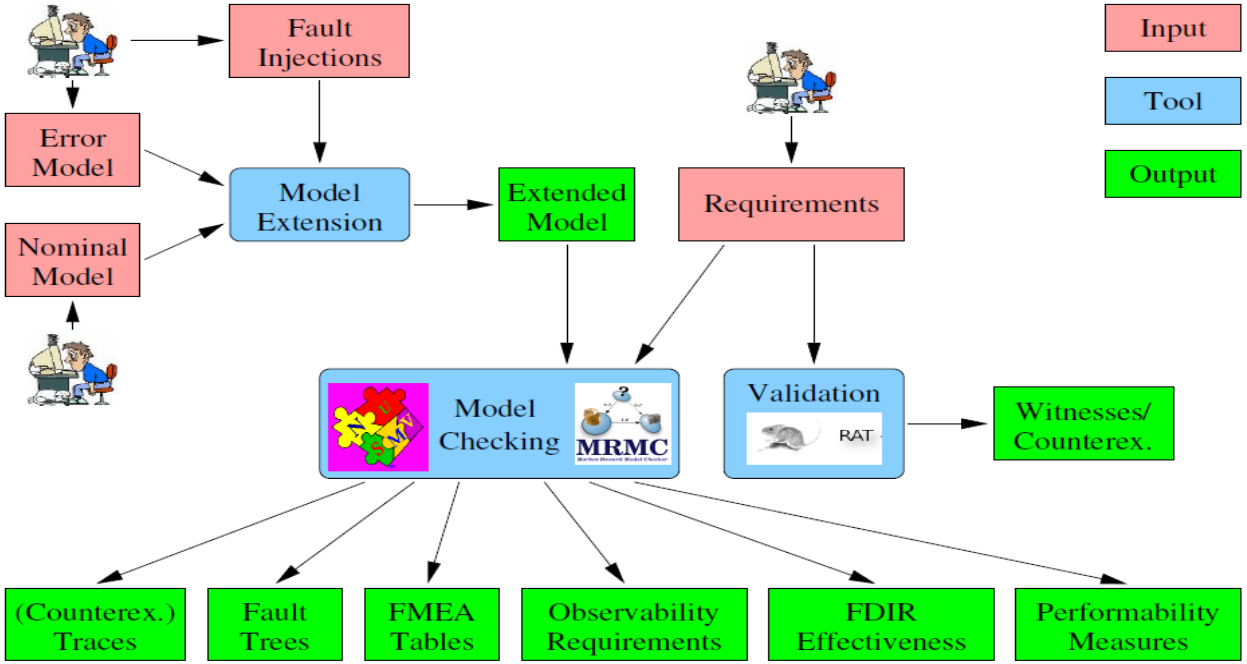
Fondazione Bruno Kessler (FBK), I

Thales Alenia Space (TAS), F

Main objective

Develop a Model-Based approach to System-Software Co-Engineering focusing on a coherent set of modelling and analysis techniques for evaluating System-level Correctness, Safety, Dependability, and performance on On-Board Computer-Based Systems.

COMPASS Tool-set Overview



Questions that COMPASS may reply to

Safety Analysis

Fault Tree Analysis (FTA) : Find the minimal combinations of faults that may cause a top event e.g.: "***Which combinations of faults may cause alarm to be raised***"

Failure Modes and Effects Analysis (FMEA) : Analyze the impact of fault configurations on a set of system properties e.g. "***What are the consequences of a battery failure on the output alarm?***"

FDIR effectiveness analysis

Fault Detection : "***Will given FDIR procedure always detect a fault?***"

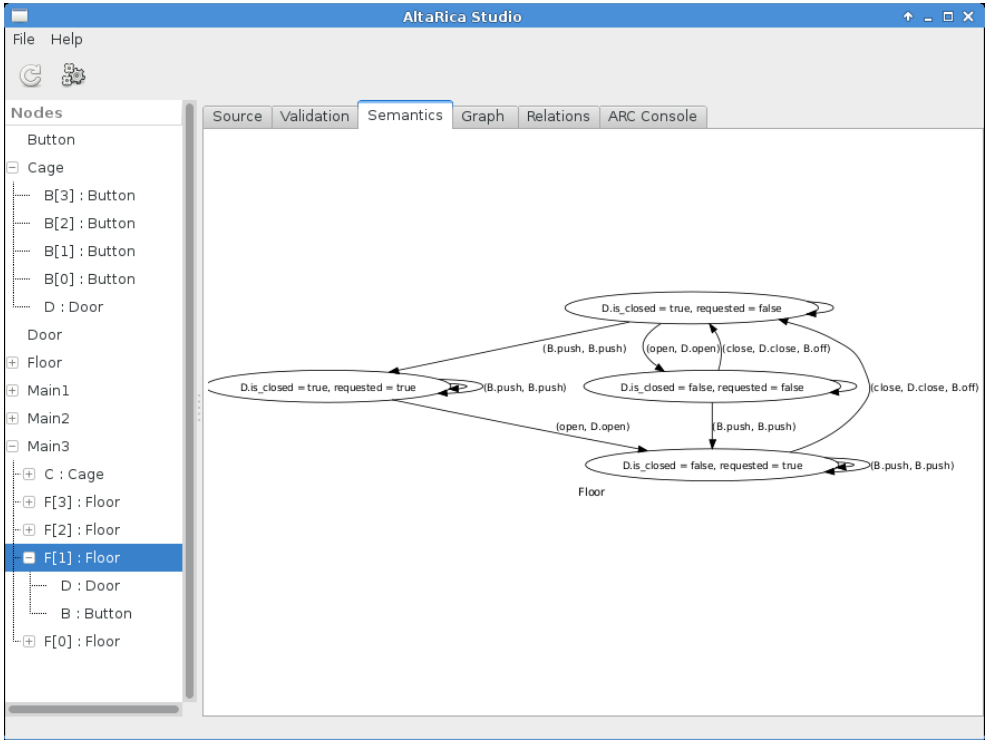
Fault Isolation : "***Will given FDIR procedure identify the fault responsible for an event?***"

Fault Recovery : "***Will given FDIR procedure recover from a fault?***"

Diagnosability Analysis

Diagnosis feasibility : "***Is there a diagnoser for a given property?***"

Diagnoser synthesis : "***Find a good sensors configuration***"



AltaRica Studio

ARC

Several algorithms have been implemented to generate sets of sequences or fault trees according to an unexpected configuration.

A simulator for models decorated with stochastic informations; it permits to evaluate some measure such like MTTF (mean time to failure).

https://altarica.labri.fr/wp/

SIMFIA is a software package that, based on the knowledge and functional analysis of an equipment, product or system, can be used to analyse and simulate its overall behaviour and automate R.A.M.S. studies. SIMFIA integrates a modeling process to simplify its handling.

Thanks to the integration of the AltaRica language, SIMFIA allows fine modeling of the behaviour of a system faced with failures and to obtain automatically relevant information from Monte Carlo simulations. SIMFIA is able to identify all failure combinations that lead to a particular situation (the sequencing of these breakdowns also provides additional precision).

https://www.apsys-airbus.com/en/digital-software-en/#SIMFIA

How do we address it in the Space community?

Who?

***S**pace*

***AV**ionics*

***O**pen*

***I**nterface*

*a**R**chitecture*

Why?

Improve the way we deliver space systems.

Support industrial competitiveness.

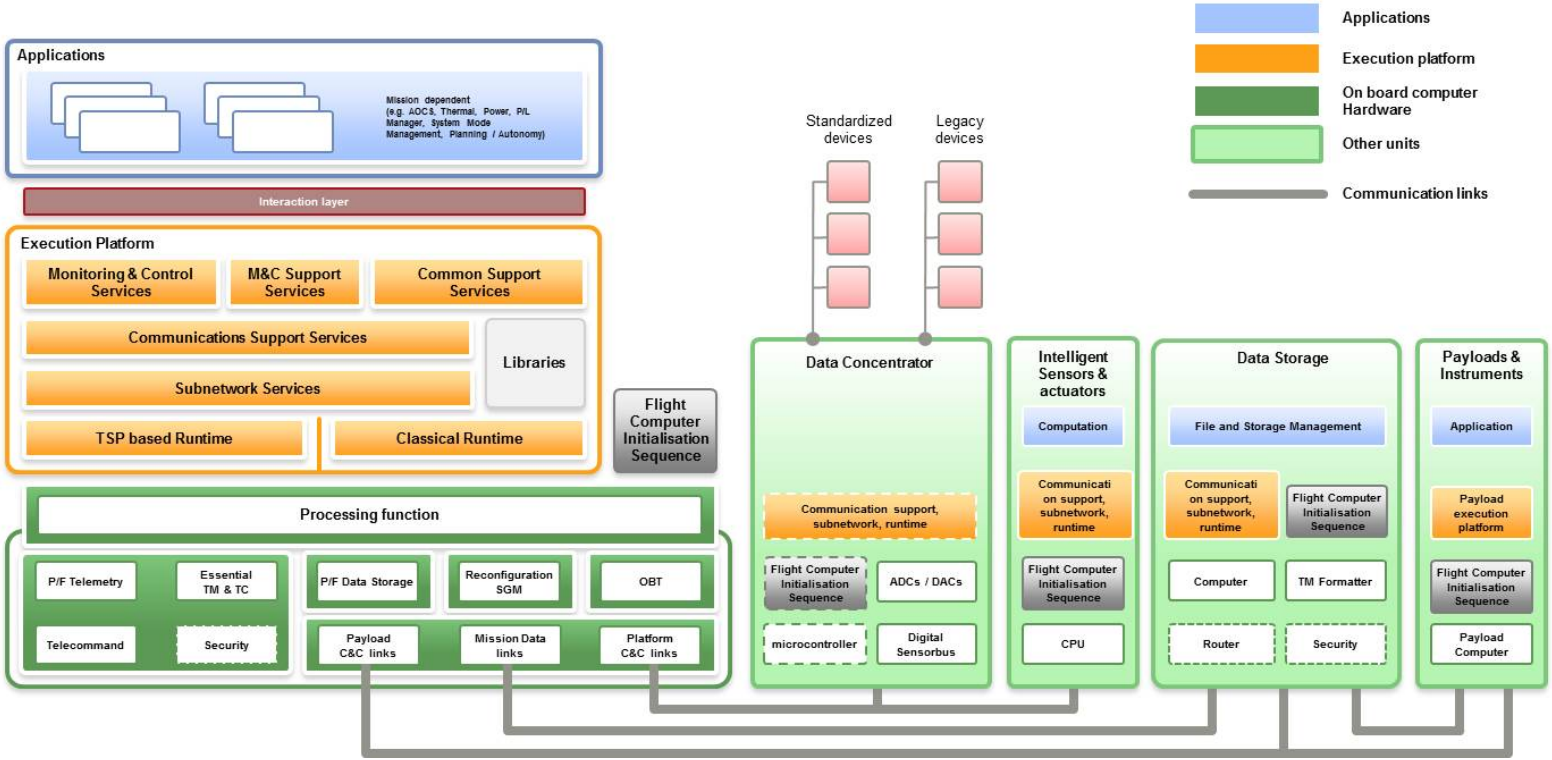
Enhance product orientation.

How?

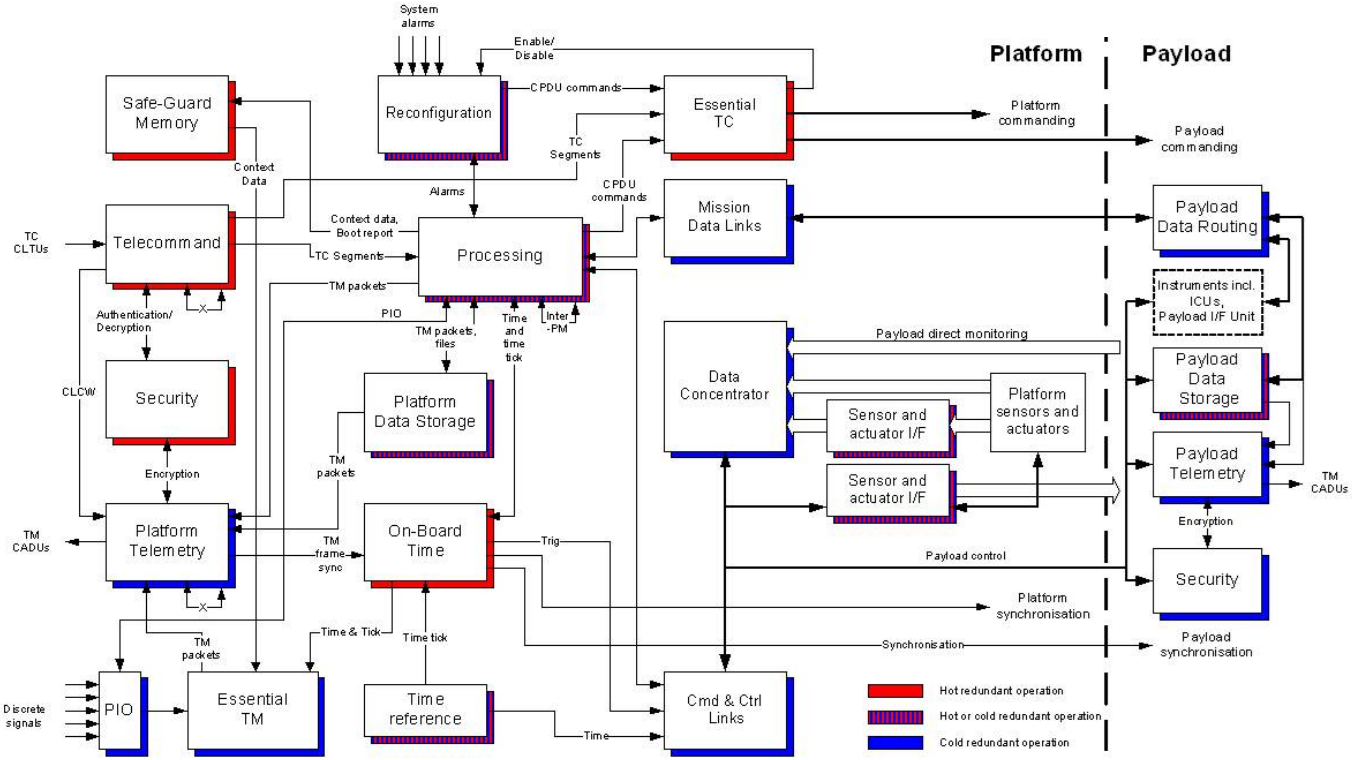
Improve the way we deliver Space Systems (cost & schedule) by

- re-developed **Products / Building Blocks** based on
  - well defined **Specification & Interfaces** based on
    - an agreed **Reference Architecture**

Avionics reference architecture



Avionics functions



http://savoir.estec.esa.int

SAVOIR working groups

SAVOIR FAIRE	Software reference architecture
SAVOIR IMA	Time and Space Partitioning **Finalised**
SAVOIR SAIF	Sensor/Actuator Electrical interface **Finalised**
SAVOIR SAFI	Sensor/Actuator Functional Interface **Finalised**
SAVOIR MASAIS	MAss Storage Access Interfaces and Services
SAVOIR UNION	Functional links
SAVOIR FDIR	Fault Detection, Isolation, Recovery
SAVOIR AUTOCODE	Automatic code generation **New**

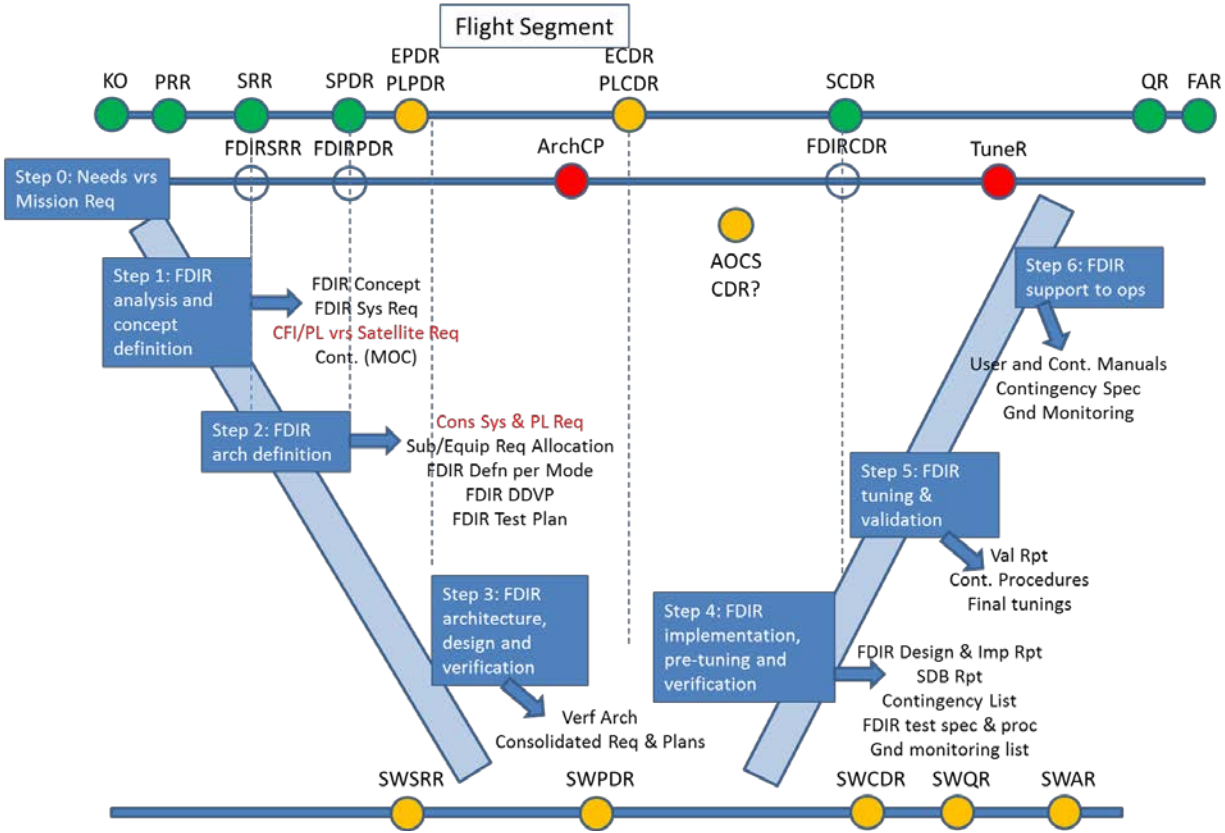
handbook

- Terms & definition
- Overview (strategy, architecture, implementation, requirements)
- Process reference to ECSS-E-ST-10C: 7 steps

  ➔ requirements; concept definition; architecture; detailed design; implementation; validation; operation
- For each step:

  ➔ objective; dependencies; input; output; activities; guideline
- Process per phase
- Relation to other ECSS standards
- List of expected documents
- Template of expected documents

process


Flight Segment
KO
PRR
SRR
SPDR
EPDR
PLPDR
ECDR
PLCDR
SCDR
QR
FAR
FDIRSRR
FDIRPDR
ArchCP
FDIRCDR
TuneR
Step 0: Needs vrs Mission Req
Step 1: FDIR analysis and concept definition
FDIR Concept
FDIR Sys Req
CFI/PL vrs Satellite Req
Cont. (MOC)
AOCS CDR?
Step 2: FDIR arch definition
Cons Sys & PL Req
Sub/Equip Req Allocation
FDIR Defn per Mode
FDIR DDVP
FDIR Test Plan
Step 3: FDIR architecture, design and verification
Verf Arch
Consolidated Req & Plans
Step 4: FDIR implementation, pre-tuning and verification
FDIR Design & Imp Rpt
SDB Rpt
Contingency List
FDIR test spec & proc
Gnd monitoring list
Step 5: FDIR tuning & validation
Val Rpt
Cont. Procedures
Final tunings
Step 6: FDIR support to ops
User and Cont. Manuals
Contingency Spec
Gnd Monitoring
SWSRR
SWPDR
SWCDR
SWQR
SWAR


WORK
IN PROGRESS

SYSTEM , SOFTWARE

SOFTWARE, SYSTEM

SYSTEM, SOFTWARE

SOFTWARE, SYSTEM

(non-)Root Causes Analysis #6/6 : software

The software behaved as expected!

➔ The system defined incomplete expectations…

Contractually OK

➔ But the behavior was not fully adequate…

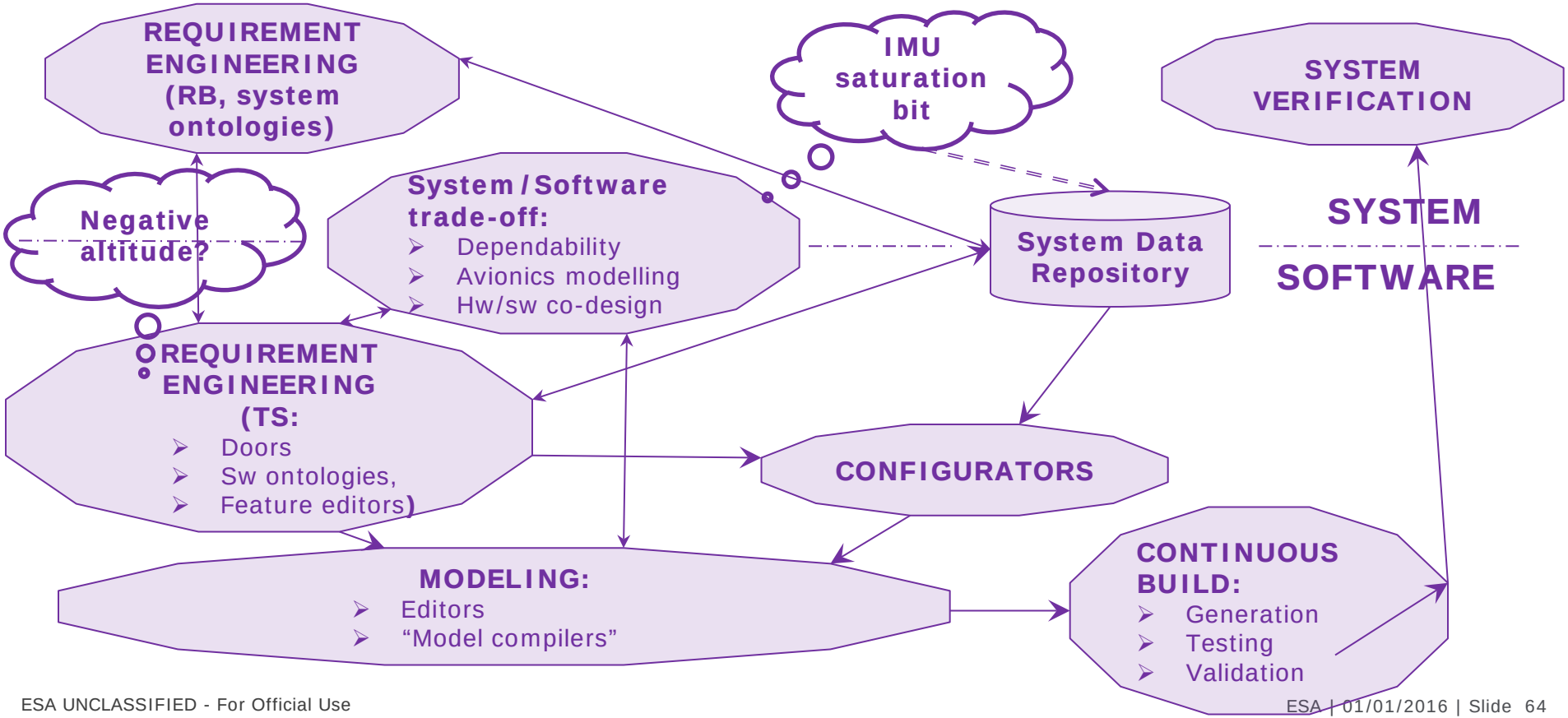
Who checks the software specifications?

➔ Shared between system and software (ECSS-E-ST-40C)

➔ Role of “software architects” in space large system integrators

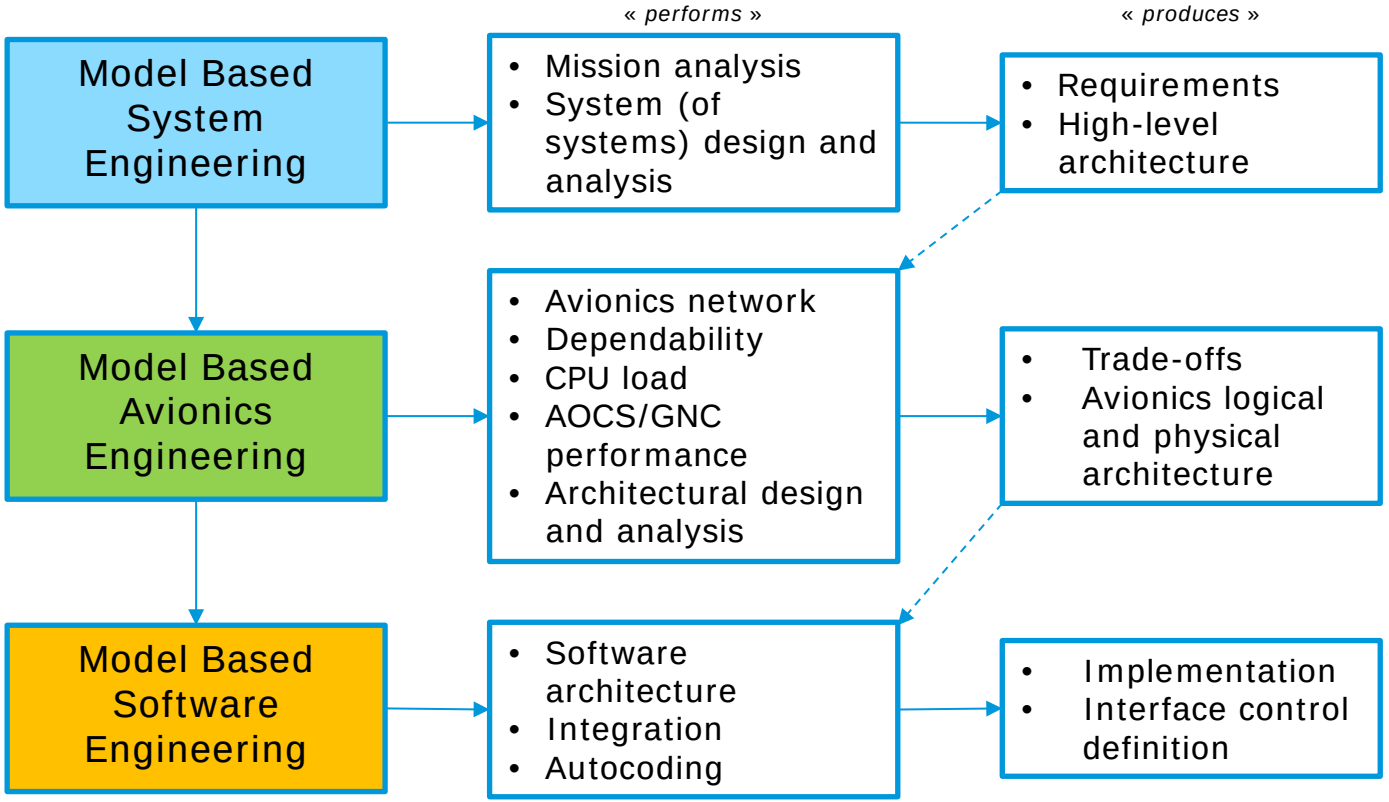
Software engineers are authorized to challenge the requirements (e.g. negative altitude)

System - Software relationship

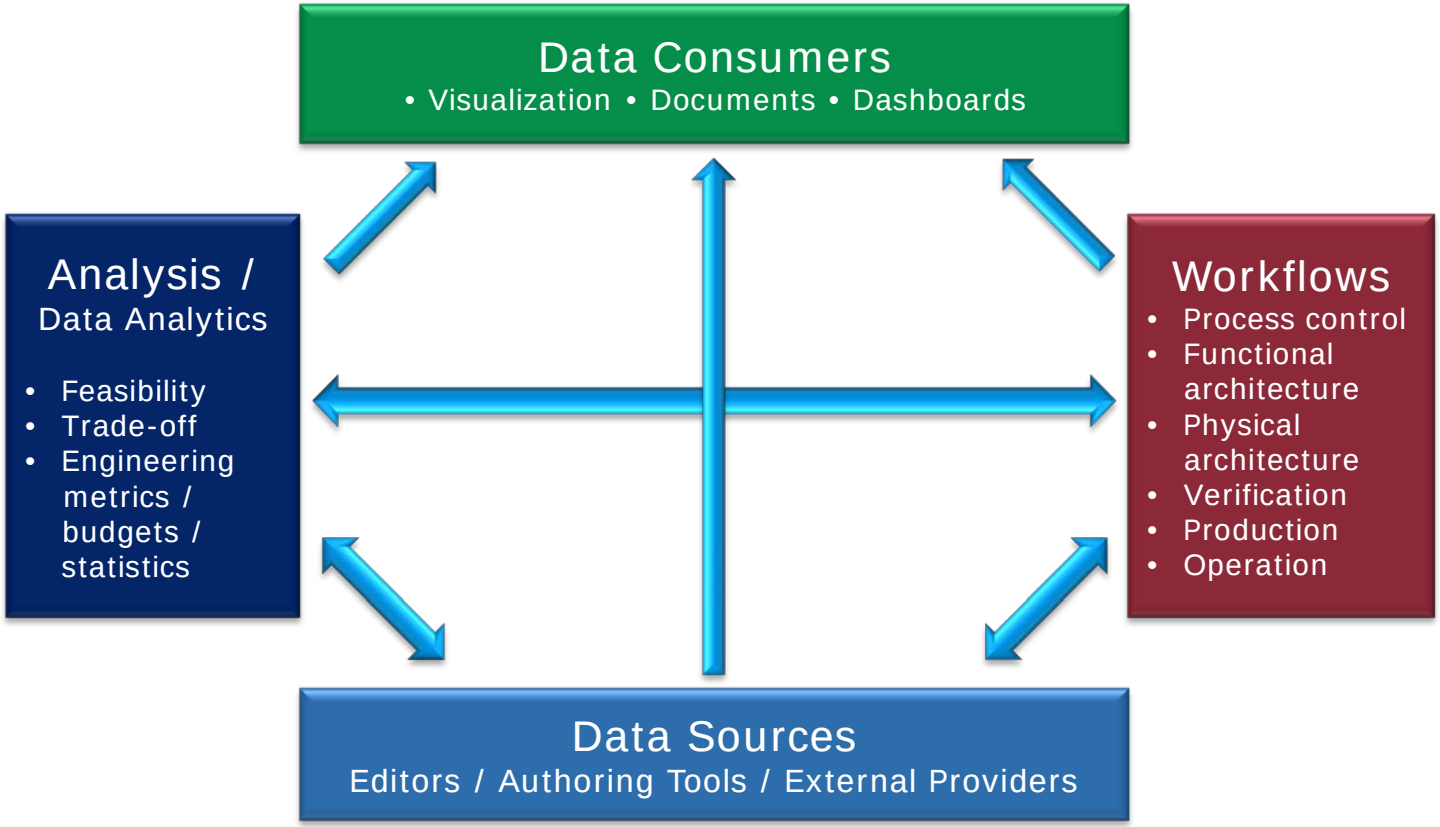


MODEL BASED AVIONICS

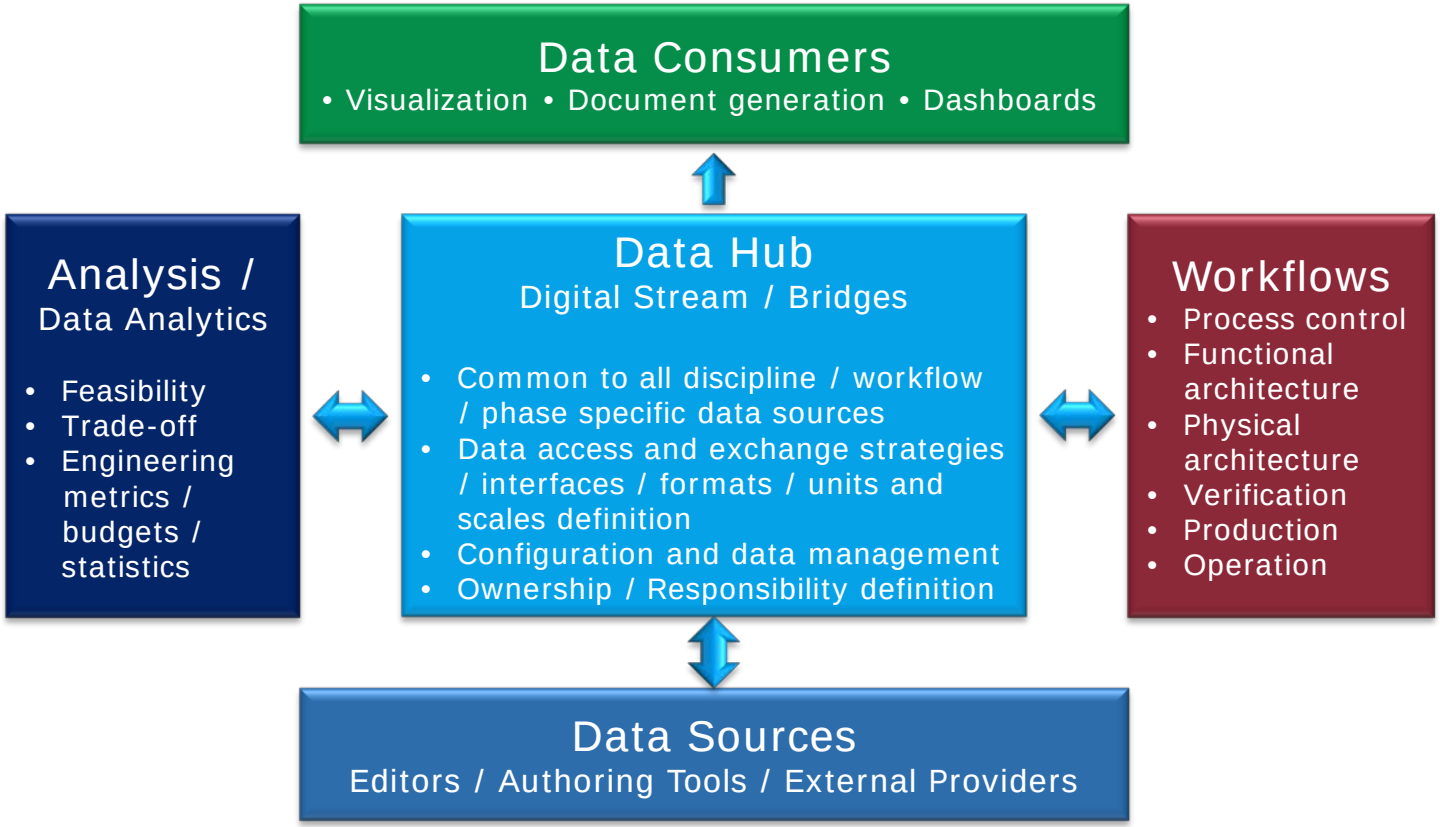
From System to Avionics



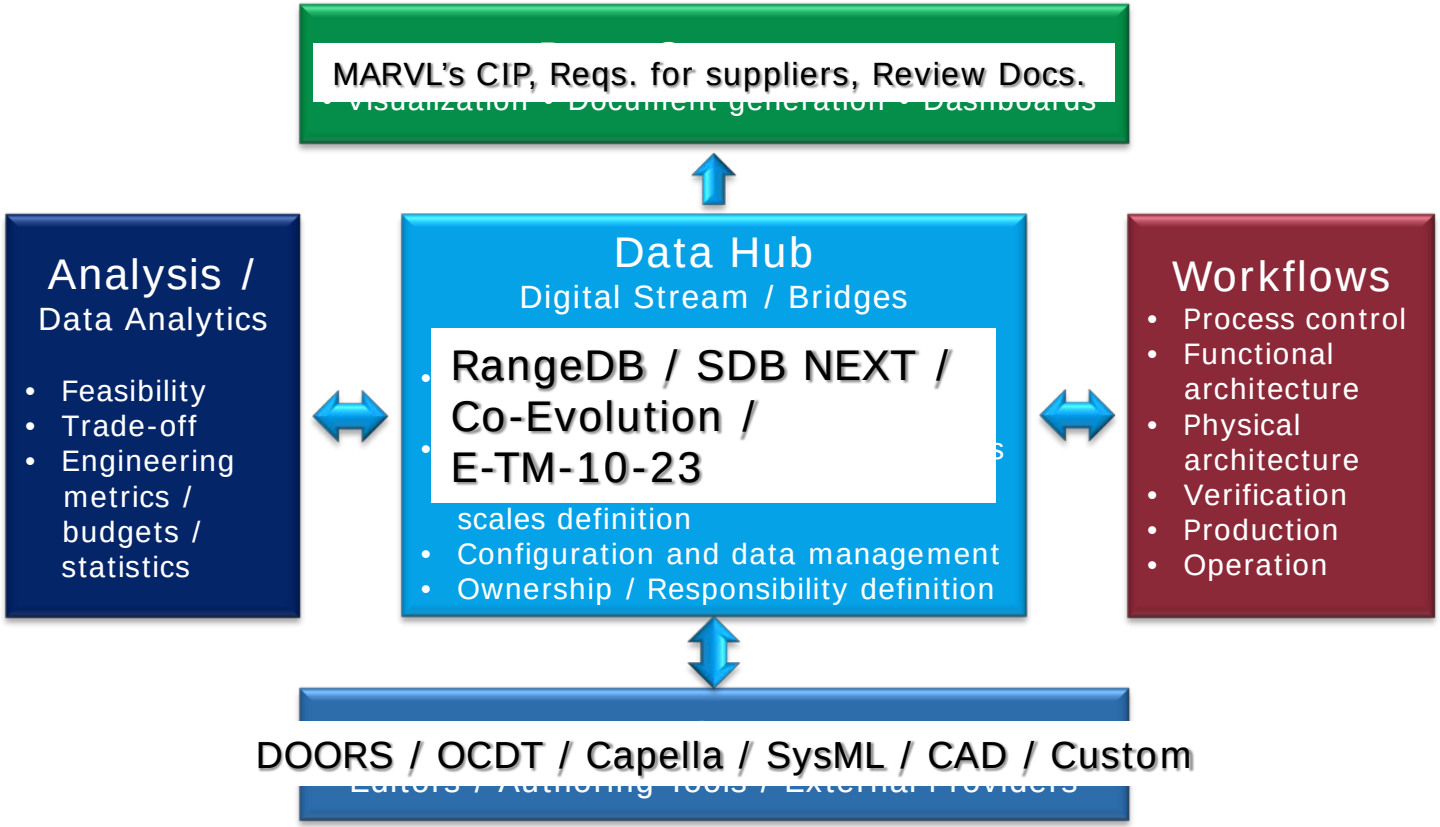
Systems Engineering - After



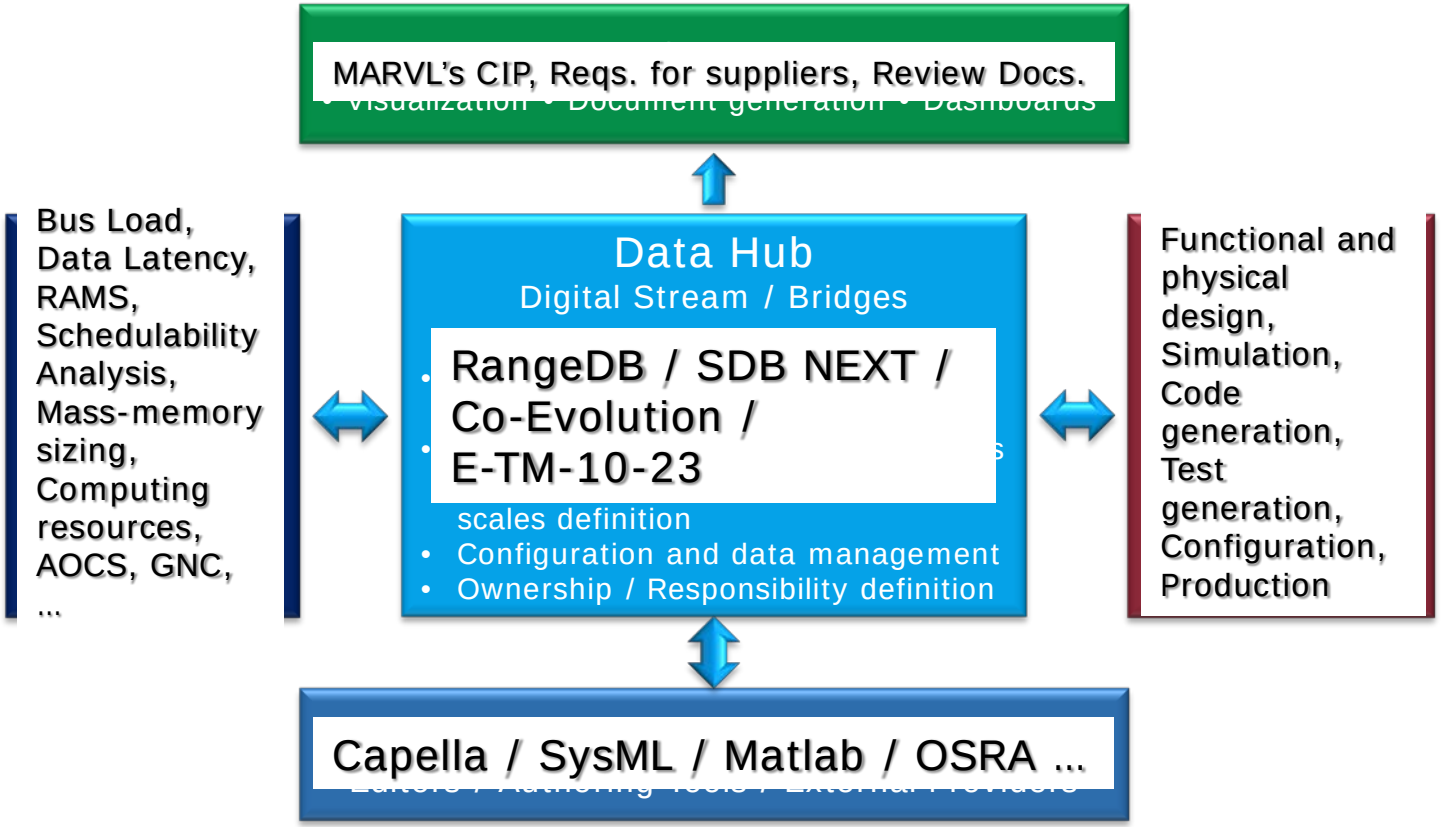
Systems Engineering - After



From System to Avionics

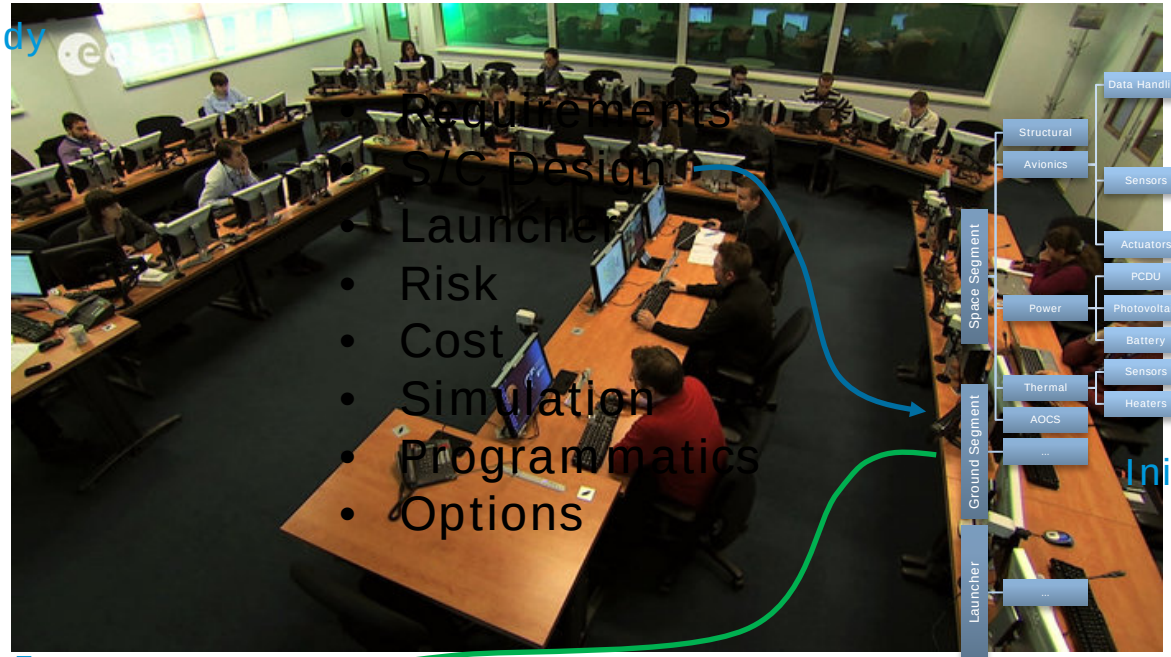


From System to Avionics



Use Case

Initial Study

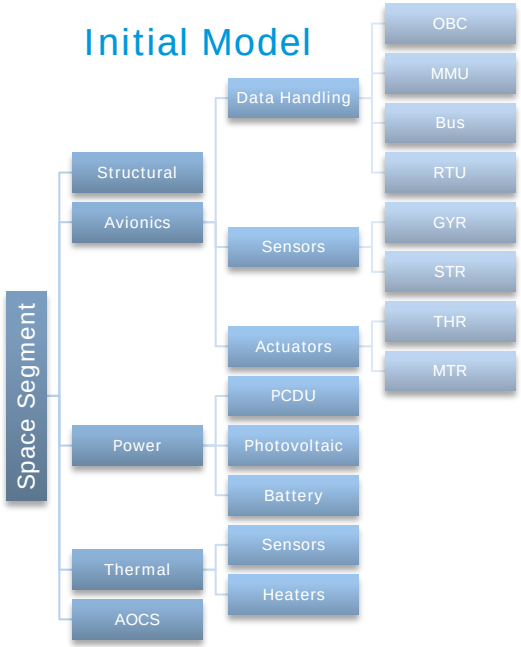


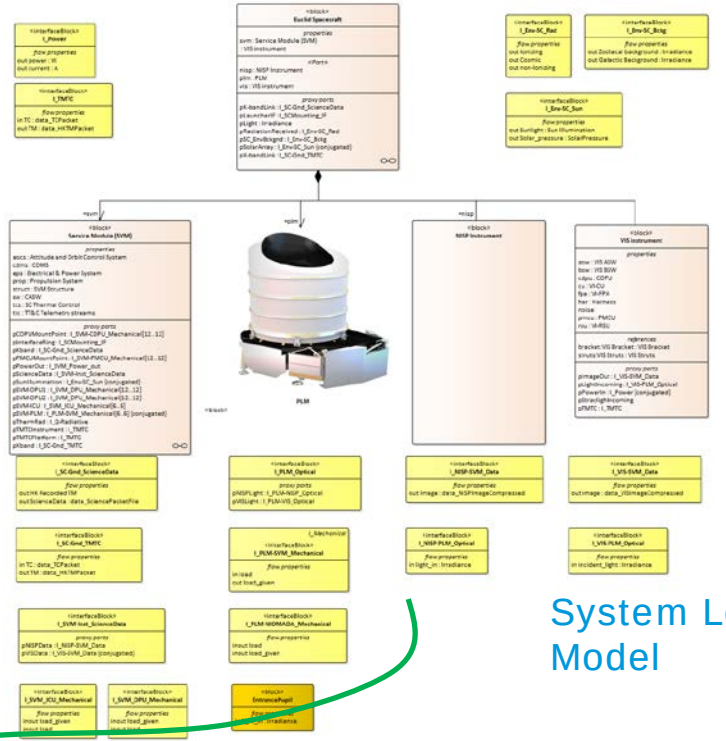
Initial Model

0 A B C D E F

Use Case

Initial Model

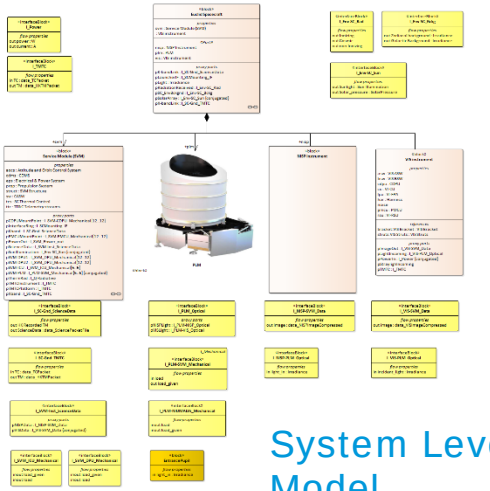




System Level Model

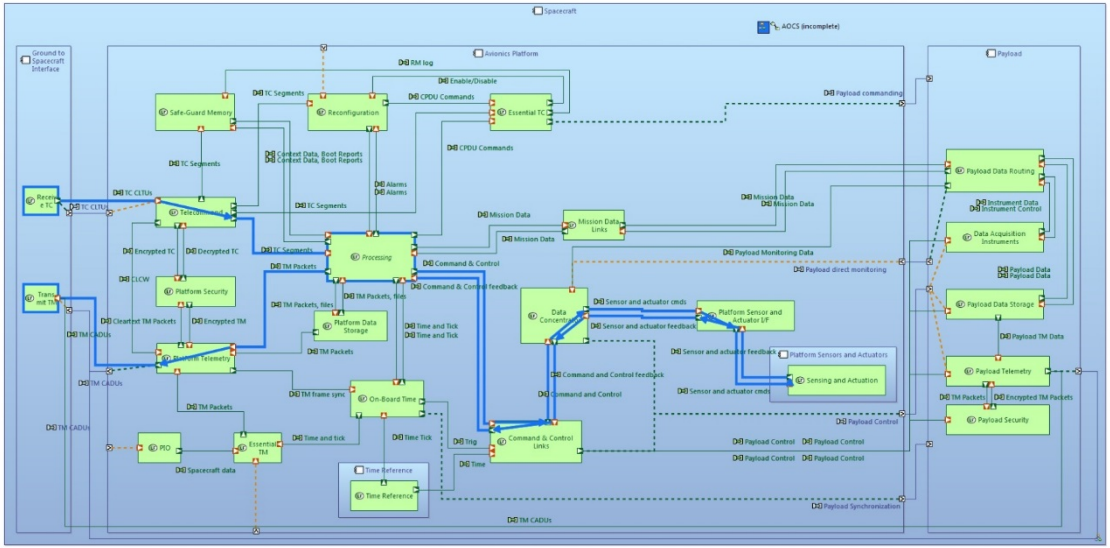
0 A B C D E F

Use Case



System Level Model

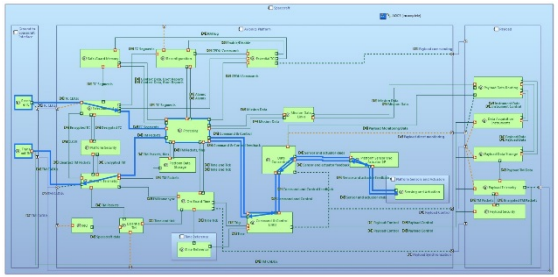
Logical Architecture

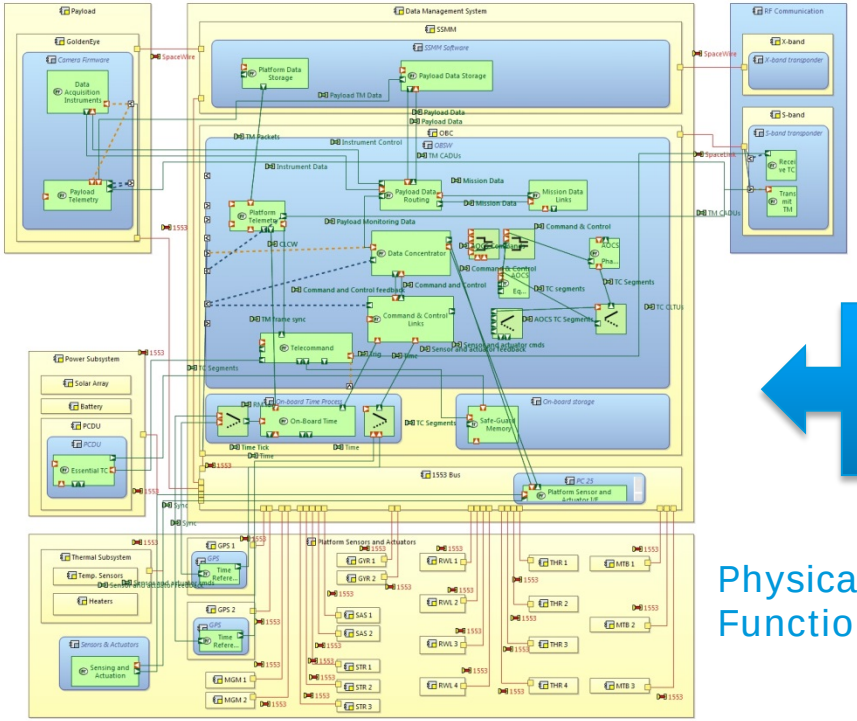


0 A B C D E F

Use Case

Logical Architecture



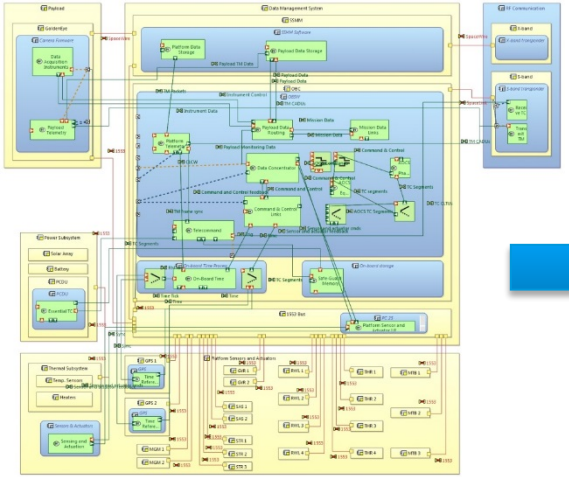


Analysis / Tradeoff

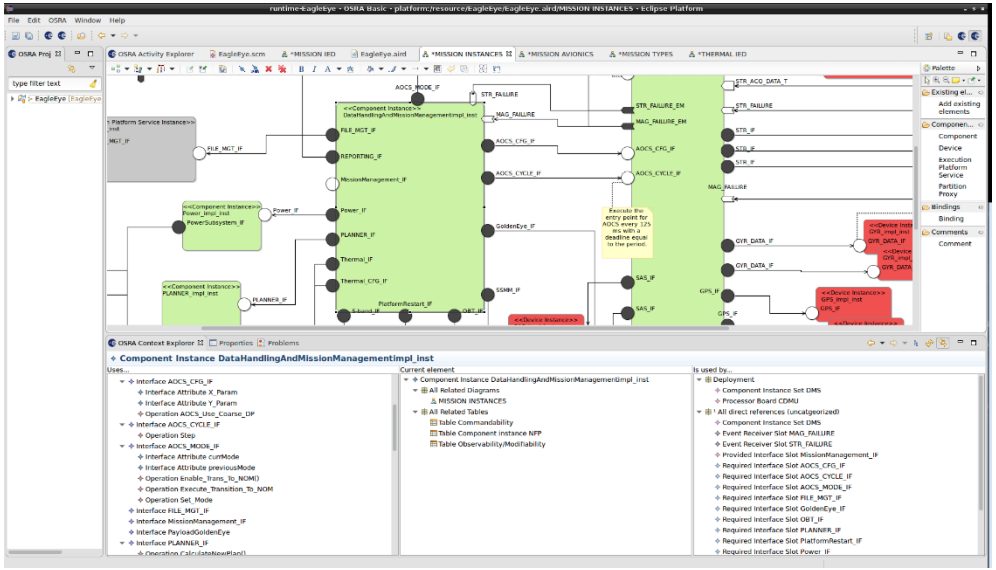
Physical Architecture / Function Allocation

0 A B C D E F

Use Case



Physical Architecture

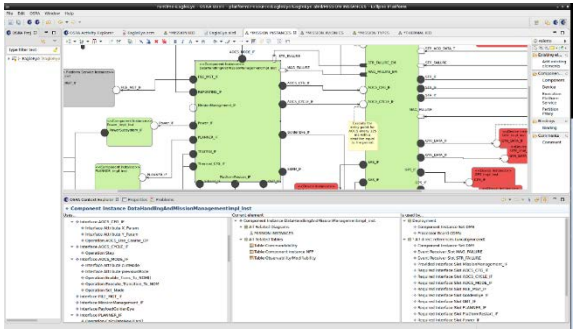


Software Architecture

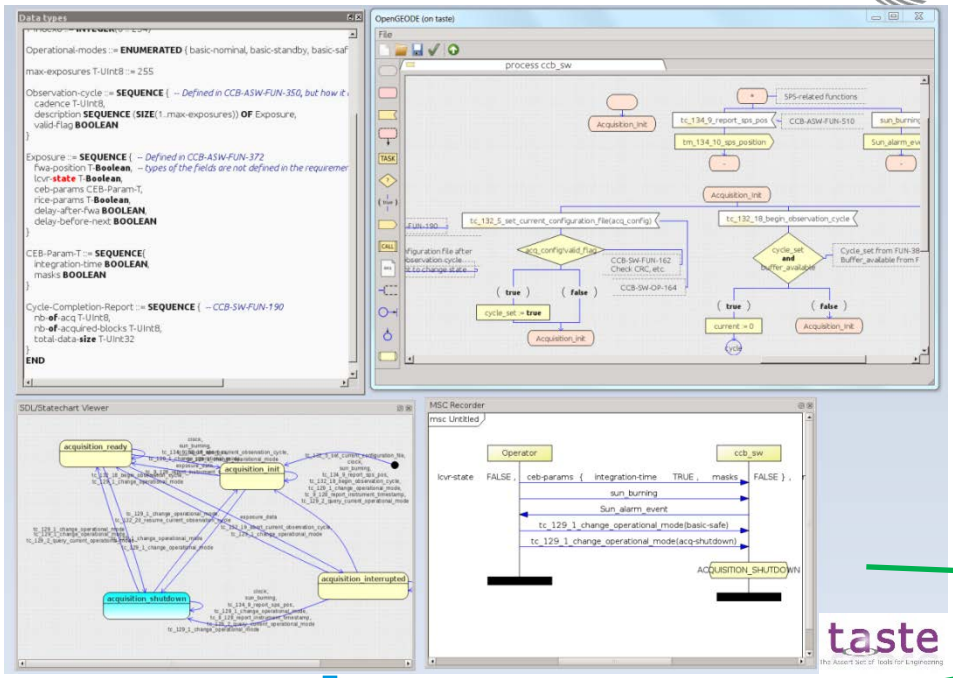
0 A B C D E F

Use Case

SW Implementation / Deployment



Software Architecture



0 A B C D E F

Perspective

Maybe software is not so bad

BUT **system software co-engineering** is essential

AND with model based and digital continuity, the system is now represented in software

So software techniques must propagate in **models** and in **system**!

From

Software Reliability Engineering

to

(model-based) Software (-system) Reliability Engineering?

Another big issue around the corner

From ADCSS2017 [http://adcss.esa.int]

- Hardware integration is costly => powerful computer, all in software
- ASIC/FPGA crisis

➔ **Software & Microelectronic Reliability Engineering**

AND SCHIAPARELLI?

Recommendations

- Improvement of the multibody parachute model
- Verification of all sub models and their parameters
- Robustness of the system design (what if, robustness, deterministic WCA, FDIR, degraded cases, parametric and sensitivity analysis)
- “Robust and reliable sanity checks shall be implemented in the on-board S/W to increase the robustness of the design”
- Acknowledge disturbed dynamic and design GNC accordingly
- Improve telemetry
- Improve procurement process

Results of the Demonstration

Successfully demonstrated elements

- Separation from TGO
- Detection of Martian atmosphere
- Detection of parachute deployment time and subsequent deployment and inflation
- Parachute behaviour (with obviously limited understanding)
- Jettison of front shield
- Operations of Radar Doppler Altimeter
- Back shell and parachute separation
- RCS priming and operation
- Interplanetary navigation and targeting (touch down very close to centre of error ellipse)

Elements not demonstrated

- Back shell and parachute avoidance manoeuvre
- Retro-propelled descent to drop point
- Free fall survival from drop point

ExoMars 2020

ESA's ExoMars **rover** will be launched in 2020.

Roscosmos will be responsible for the 2020 descent module and surface platform, and provides Proton launchers for both missions.

Both partners will supply scientific instruments and will cooperate closely in the scientific exploitation of the missions.

Videos

http://www.esa.int/esatv/Videos/2016/10/ExoMars_Science/ExoMars_2020_Rover_mission

http://www.esa.int/spaceinvideos/content/view/embedjw/465664


Landing is blxxdy
difficult