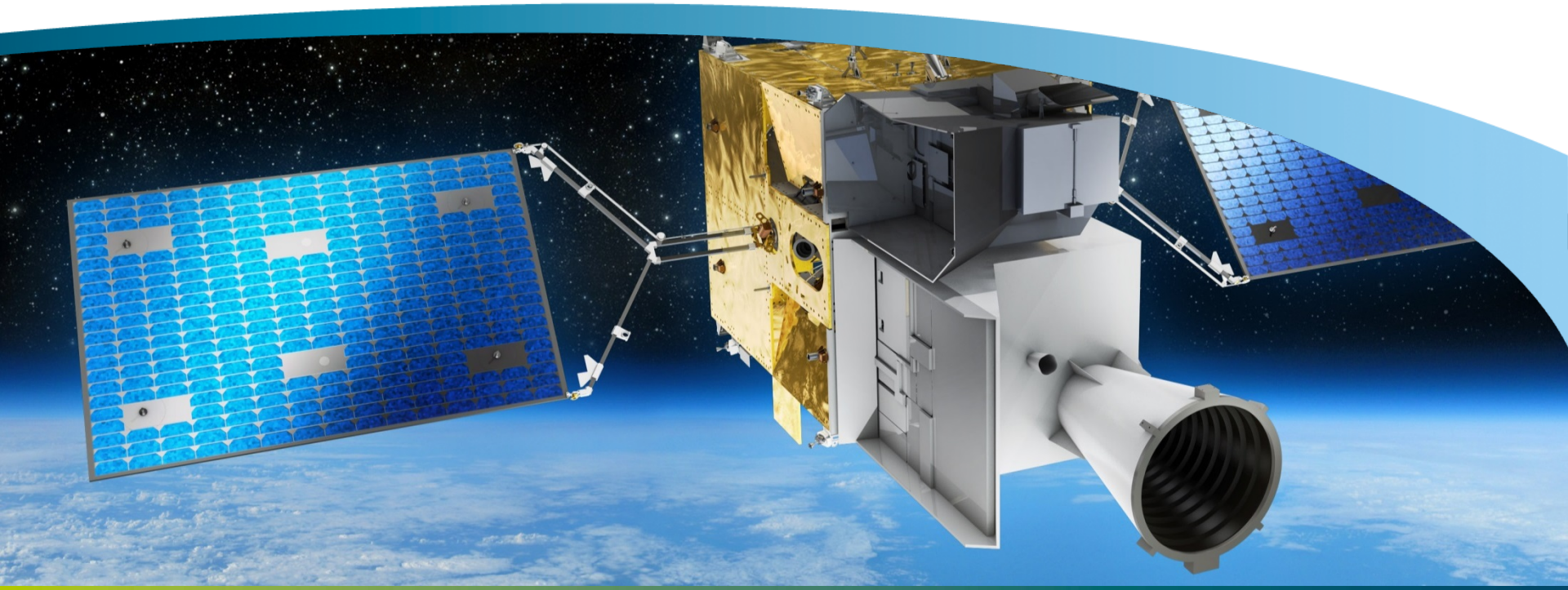
OHB System AG
Massimo Tipaldi
08.12.2016, MBSSE Workshop ESA/ESTEC



SPACE SYSTEMS

Model checking techniques applied to spacecraft mode management

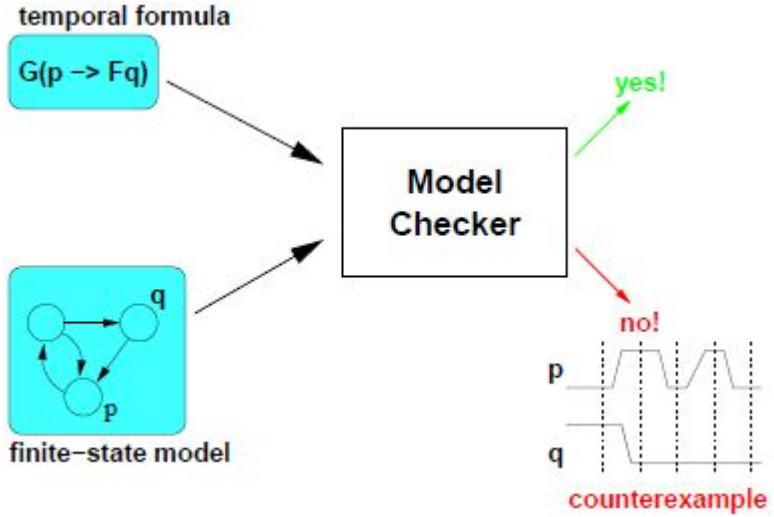
We. Create. Space.

Agenda

- Background on model checking
- Case study
  - MTG Satellite Mode Management
- Conclusion
  - Benefits and open points

Background on model checking

- Model checking as formal verification method
  - Given a model and a set of properties, it searches for traces of the model that violates the properties (calculated from a set of initial states)
  - Classes of linear time properties: invariants, liveness, safety, deadlocks
- Many model checkers available: JavaPathFinder, NuSMV, SPIN, UPPAAL, *CWB-Concurrency WorkBench (CCS)*



Background on model checking

- *Model based approach*: generating a new system requirement representation:

FROM:

- System-level requirements
- SysML Diagrams
- Lengthy description

TO :

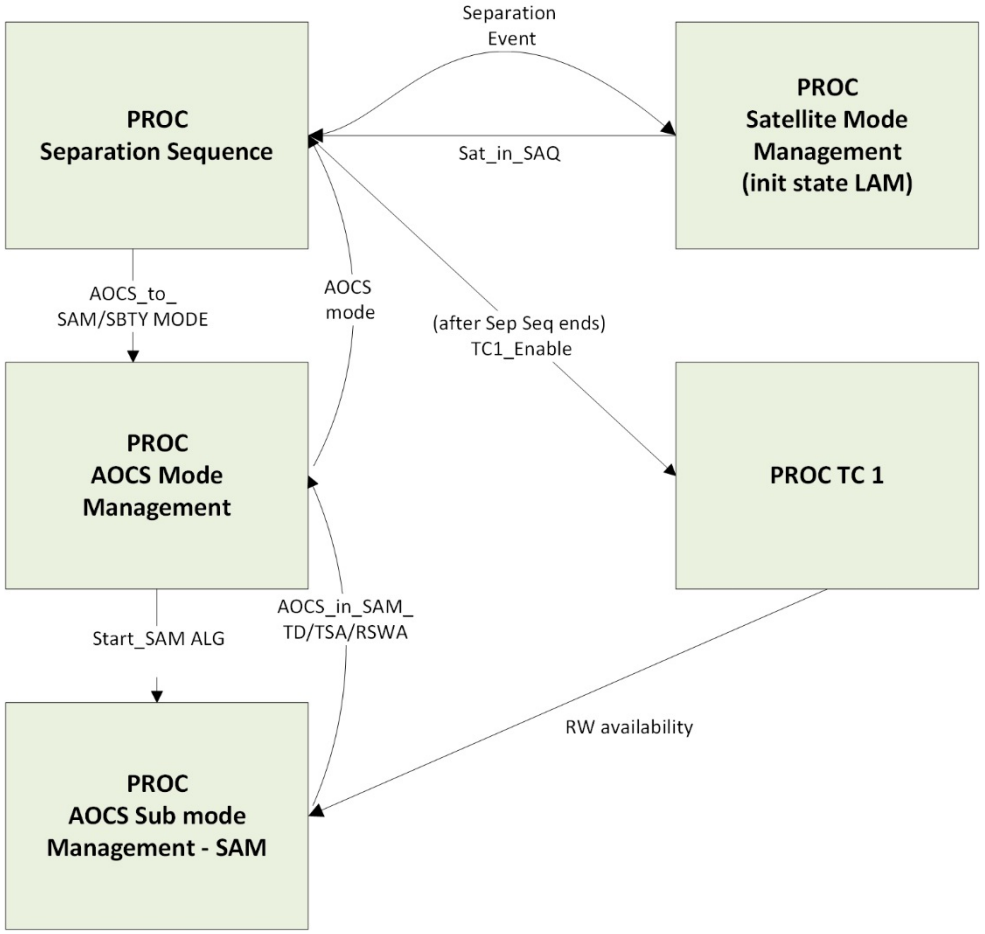
- *Concise and verifiable models* (CCS, Temporal Logic, Petri Nets)

- Use the resulting formal model to *mathematically* calculate system's behaviour for V&V purposes from the early phases of space projects

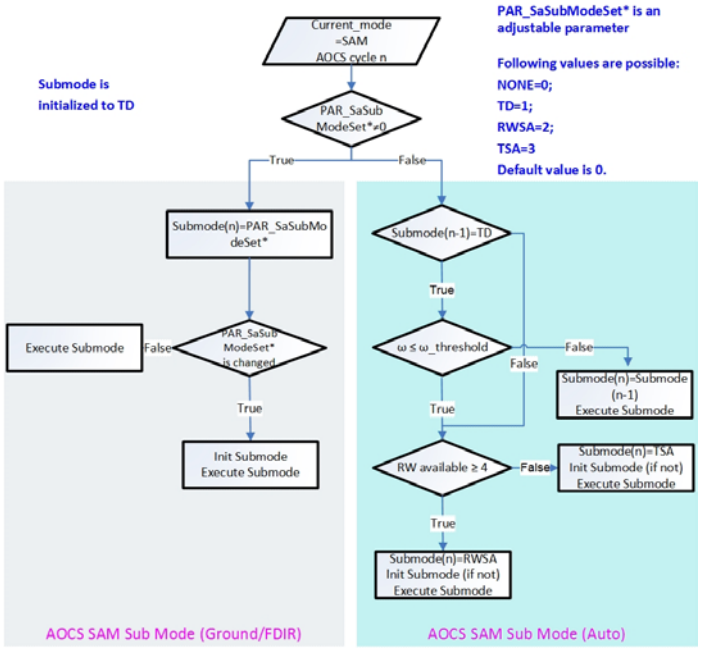
- *CCS (Calculus of Communicating Systems)*
  - Process algebra language for describing communication and concurrent system
  - Expressiveness to describe dynamic behaviors and interactions with simple constructs
  - Operational conditions modelled and verified by enabling suitable actions

Case study: MTG satellite mode management

- LEOP and GEO phases modeled in CCS (Calculus of Communicating Systems):
  - Separation Sequence, including autonomy
  - LEOP State Machine, including FDIR
  - GEO State Machine, including FDIR
  - Ground TCs
  - AOCS State Machine & Sun Acquisition Sub-mode



Case study: MTG satellite mode management




```
proc SAM = (startSamMode.'startSamAlg.SAM)+(reStartSamAlg.SAM)
+(subModeTSAEntering.'subModeTSAOk.SAM)+(subModeRWSAEntering.'subModeRWSAOk.SAM)

proc SAM_ALG = startSamAlg.
(subModeInitAuto.((ThrusterDetFalse.'ThrusterDetFalse.(RWAvail4False.'subModeTSAEntering.SAM_ALG
+RWAvail4True.'subModeRWSAEntering.SAM_ALG))
+ThrusterDetTrue.(OmegaLowerThanTreshFalse.'reStartSamAlg.SAM_ALG+(OmegaLowerThanTreshTrue.
(RWAvail4False.'subModeTSAEntering.SAM_ALG+RWAvail4True.'subModeRWSAEntering.SAM_ALG)))))
+(subModeInitRWSA.RWAvail4True.'subModeRWSAEntering.SAM_ALG)
```

- CCS code snippet from AOCS SAM (Sun Acquisition Mode) Sub-mode

Case study: MTG satellite mode management

- Verified properties:
  - Deadlock-Free
  - Spacecraft Angular Rate > Threshold => AOCS in SAM-TD Mode
  - Spacecraft Angular Rate < Threshold => AOCS in SAM-TSA Mode
  - LEOP Phase ends successfully in nominal case (usage of Reaction Wheels)
  - GEO Spacecraft Mode Transitions
  - Failure mechanism for FDIR L3 & L4

Conclusion

- Model checking as formal method to model and verify system-level requirements and artifacts from the early phases of a project
  - deadlock / race conditions
  - system behavior according to the specs
- Suitable for complex systems and concepts, e.g. spacecraft autonomy
- Further investigation :
  - states explosion problem
  - straightforward creation of models from e.g. SysML diagrams
  - model checking into the ECSS process/product requirements & space project tool chain

OHB System AG
Massimo Tipaldi
08.12.2016, MBSSE Workshop ESA/ESTEC

Thank you!

massimo.tipaldi@ohb.de

santone@unisannio.it

SPACE SYSTEMS

Model checking techniques applied to spacecraft mode management

We. Create. Space.