MOVEP 2012 Tutorial
Safety, Dependability and Performance Analysis of Extended AADL Models

Part 1: Overview

European Space Agency
European Space Research and Technology Centre

RWTH Aachen University
Software Modeling and Verification Group
Thomas Noll

Fondazione Bruno Kessler
Centre for Scientific and Technological Research
Alessandro Cimatti

MOVEP 2012 School; December 7, 2012; Marseille, France

Outline of Tutorial

1. Overview [Noll]
2. System Modeling Using AADL [Noll]
3. Checking Functional Correctness [Cimatti]

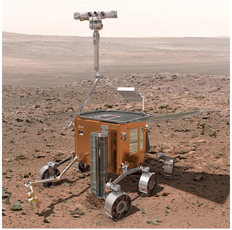
   Coffee Break
4. Safety and Dependability Analysis [Cimatti]
5. Fault Detection, Isolation and Recovery (FDIR) Analysis [Cimatti]
6. Performability Evaluation [Noll]

Contents of Overview

Outline

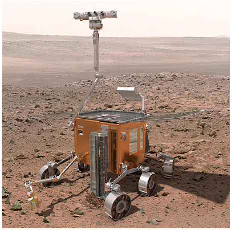
1. Introduction
2. COMPASS Project Overview
3. Industrial Evaluation
4. Conclusion

Domain: Fault-Tolerant Space System Architectures



ExoMars Rover: autonomy

- 4 to 21 min. for radio latency to earth
- infrequent communication opportunities (one or two short sessions per Martian day)



ExoMars Rover: autonomy

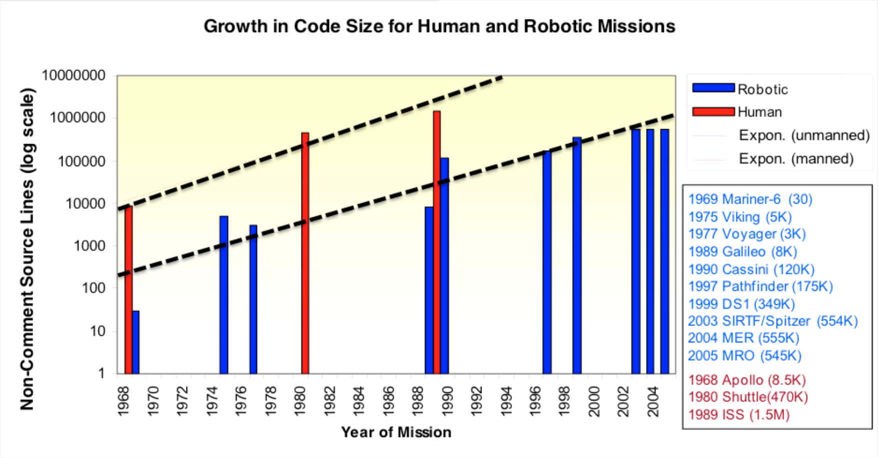
- 4 to 21 min. for radio latency to earth
- infrequent communication opportunities (one or two short sessions per Martian day)

Autonomous Transfer Vehicle (ATV):
autonomy and safety

- fully-automated navigation and docking to ISS
- human-rated requirements for safety (of ISS)

⇒ multi-failure tolerance (1 MLOC of control code)

Spacecraft = Flying Software



NASA Study on Flight Software Complexity (2009)

Extreme Dependability!

Requirements

- Must offer service without interruption for a very long time – typically years or decades
- Faults are costly and may severely damage reputations:
  - Ariane 5 crash in 1996 due to arithmetic overflow
  - Launch failure of recent Phobos-Grunt sample return mission
- "Five nines" (99.999 %) dependability not sufficient

Extreme Dependability!

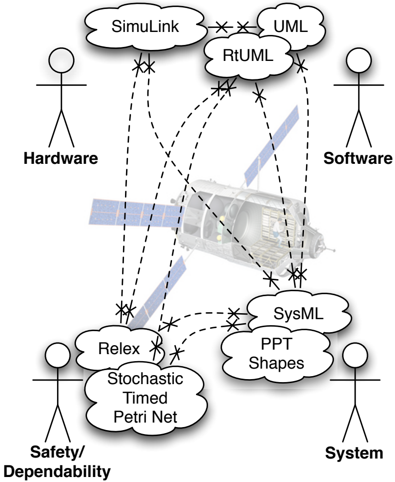
Requirements

- Must offer service without interruption for a very long time – typically years or decades
- Faults are costly and may severely damage reputations:
  - Ariane 5 crash in 1996 due to arithmetic overflow
  - Launch failure of recent Phobos-Grunt sample return mission
- "Five nines" (99.999 %) dependability not sufficient

Challenges

- Rigorous design support and analysis techniques are called for
- Bugs must be found as early as possible in the design process
- Check performance and reliability guarantees whenever possible
- Effect of Fault Detection, Isolation and Recovery (FDIR) measures must be quantifiable

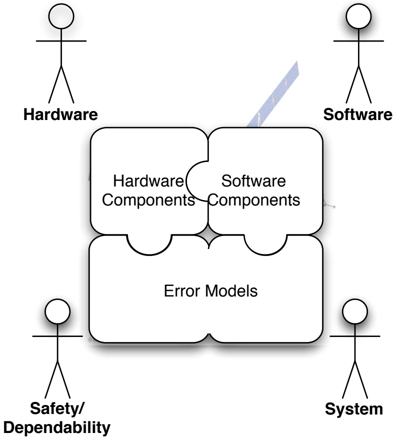
Current Limitations



Limitations

- HW verified independently of SW with exaggerated mutual assumptions
- Safety & dependability analyses isolated from HW/SW models
- Multiple modeling formalisms for different system aspects (e.g. real-time, probabilistic, hybrid)
- No coherent approach to study effectiveness of FDIR

Possible Solutions



Solutions

Combination of

- HW, SW and their bindings +
- real-time, hybrid and probabilistic aspects +
- error models +
- non-nominal modes

in a single integrated model

Outline

COrrectness, Modeling and Performance of AeroSpace Systems

The COMPASS mission

Develop a model-based approach to system-software co-engineering while focusing on a coherent set of modeling and analysis techniques for evaluating system-level correctness, safety, dependability, and performance of on-board computer-based aerospace systems.

The COMPASS mission

Develop a model-based approach to system-software co-engineering while focusing on a coherent set of modeling and analysis techniques for evaluating system-level correctness, safety, dependability, and performance of on-board computer-based aerospace systems.

Derived objectives

1. Modeling formalism: variant of AADL called SLIM (SAE Architecture Analysis and Design Language/ System-Level Integrated Modeling Language)
2. Verification methodology based on state-of-the-art formal methods
3. Toolset supporting the analysis of AADL models
4. Evaluation on industrial-size case studies from aerospace domain

COMPASS Project Partners

Consortium

- RWTH Aachen University
  Software Modeling and Verification Group
- Fondazione Bruno Kessler
  Embedded Systems Group
- Thales Alenia Space
  World-wide #1 in satellite systems
- Ellidiss Technologies
  AADL software tools

Funding & supervision

- European Space Agency

COMPASS Project Phases

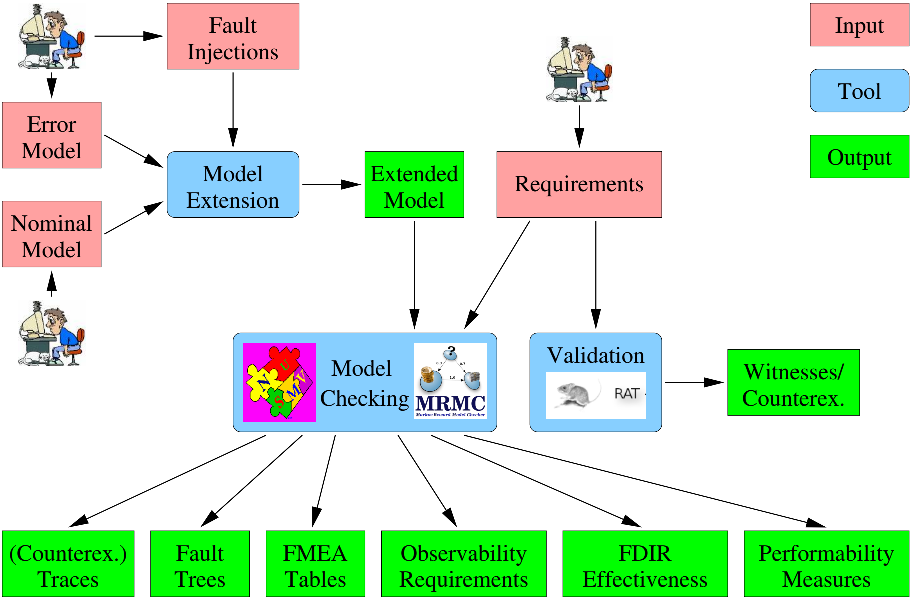
1	Project kick-off	February 2008
2	Language design	
3	Software tool specification + software design document	
4	Formal semantics	October 2008
5	Prototype tool implementation	April 2009
6	Prototype evaluation	
7	Final tool implementation	December 2009
8	Final tool evaluation	March 2010
9	Project extension	until March 2011
10	New projects (NPI, CGM)	until September 2012
11	Other application domains (D-MILS, HASDEL)	since November 2012

COMPASS Project Phases

1. Project kick-off — February 2008
2. Language design
3. Software tool specification + software design document
4. Formal semantics — October 2008
5. Prototype tool implementation — April 2009
6. Prototype evaluation
7. Final tool implementation — December 2009
8. Final tool evaluation — March 2010
9. Project extension — until March 2011
10. New projects (NPI, CGM) — until September 2012
11. Other application domains (D-MILS, HASDEL) — since November 2012

Total budget: $\approx$ 900 kEuro; $\approx$ 10 programmers involved at peak times

COMPASS Methodology



Tool Components

NuSMV

- Symbolic LTL and CTL model checker
- BDD- and SAT-based model checking
- SMT-based timed model checking
- Counterexample generation

MRMC
Markov Reward Model Checker

- Model checker for MRMs
- Logics: PCTL and CSL (+rewards)
- Numerical + DES engine
- Bisimulation minimisation

RAT

- Requirements analyser
- Checks logical consistency

FSAP

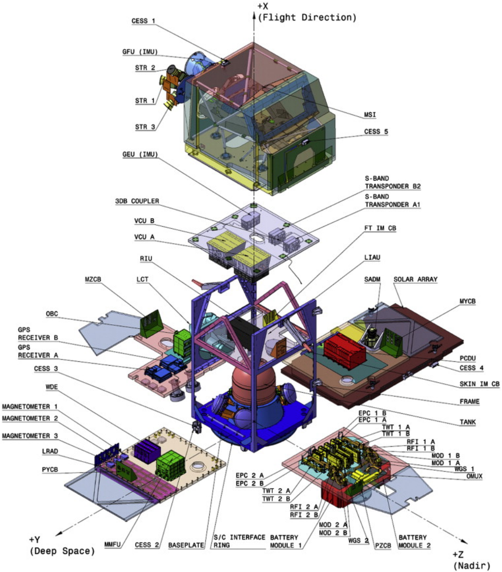
- Safety analyser
- Fault-tree analysis

SigRef

- (MT)BDD bisimulation minimisation
- Models: Markov chains

Outline

Case Study: Platform of [redacted] Satellite
Launches between 2012-2020



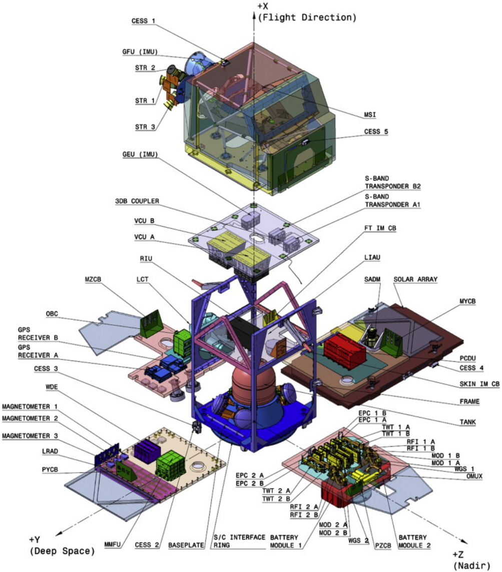
Note: Shown picture is not from the case study

Platform keeps satellite in space, like car's chassis:

- control & data unit,
- propulsion,
- telemetry, tracking & cmd,
- power,
- attitude & orbit control sys,
- reconfiguration modules,
- etc.

Case Study: Platform of [redacted] Satellite

Launches between 2012-2020



Note: Shown picture is not from the case study

Platform keeps satellite in space, like car's chassis:

- control & data unit,
- propulsion,
- telemetry, tracking & cmd,
- power,
- attitude & orbit control sys,
- reconfiguration modules,
- etc.

Fault Detection, Isolation, Recovery (FDIR):

- redundancies + recovery,
- compensation algorithms,
- failure isolation schemes,
- omnipresent in satellite

AADL Model of Satellite Platform

Verification & validation objectives

- Ensure that nominal and degraded conditions are correctly handled by FDIR system
- Ensure that performance and risks are within specified limits

AADL Model of Satellite Platform

Verification & validation objectives

- Ensure that nominal and degraded conditions are correctly handled by FDIR system
- Ensure that performance and risks are within specified limits

Model characteristics

✓ Functional	LOC (w/o comments):	3831		
✓ Probabilistic	Components:	86	Error models:	20
✓ Real-time	Ports:	937	Recoveries:	16
✓ Hybrid	Modes:	244		

State space of nominal behavior: **48,421,100** states

AADL Model of Satellite Platform

Verification & validation objectives

- Ensure that nominal and degraded conditions are correctly handled by FDIR system
- Ensure that performance and risks are within specified limits

Model characteristics

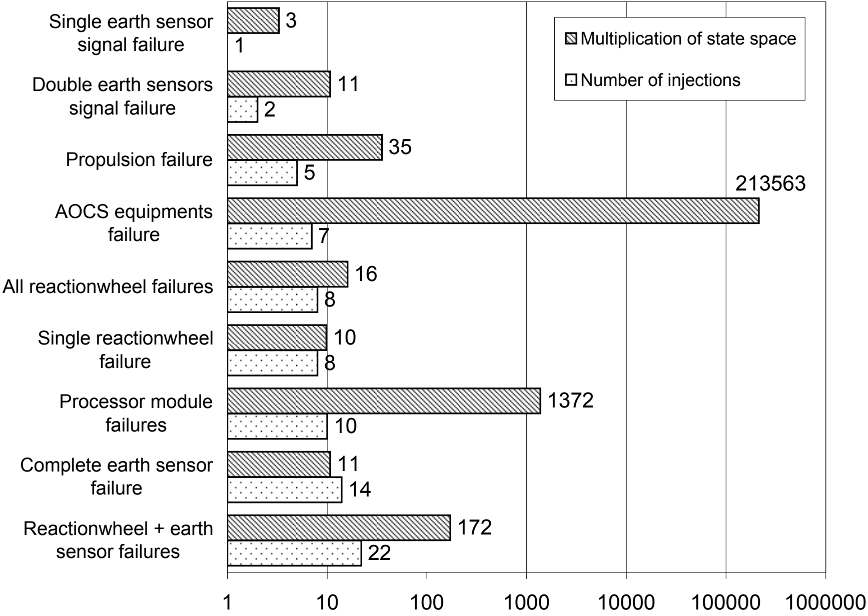
✓ Functional	LOC (w/o comments):	3831		
✓ Probabilistic	Components:	86	Error models:	20
✓ Real-time	Ports:	937	Recoveries:	16
✓ Hybrid	Modes:	244		

State space of nominal behavior: **48,421,100** states

Requirement metrics

- Functional properties: 42
  (25 propositional, 2 absence, 1 universality, 14 response)
- Probabilistic properties: 2 (1 invariance, 1 existence)

State Space Growth by Fault Injection



Outline

Epilogue

Achievements

- Component-based modeling framework based on AADL
- Novelties: dynamic reconfiguration, hybridity, error modeling, ...
- Automated correctness, safety, and performability analysis
- Industrial evaluation by third-party company showed maturity

Trustworthy aerospace design = AADL modeling + analysis

Epilogue

Achievements

- Component-based modeling framework based on AADL
- Novelties: dynamic reconfiguration, hybridity, error modeling, ...
- Automated correctness, safety, and performability analysis
- Industrial evaluation by third-party company showed maturity

Trustworthy aerospace design = AADL modeling + analysis

Further information

- General approach (Yushstein et. al, IEEE SMC-IT 2011)
  (Bozzano et. al, ACES-MB 2009)
  (Bozzano et. al, SAFECOMP 2009)
- AADL model checker (Bozzano et. al, CAV 2010)
- Thales case studies (Bozzano et. al, ERTS^2 2010)
- ESA satellite case study (Esteve et. al, ICSE 2012)
- Tool download at http://compass.informatik.rwth-aachen.de/