THALES

Timing Design and Verification of Real-Time Systems with (m,k) Constraints:

Current Practices at THALES

RAFIK HENA
THALES RESEARCH & TECHNOLOGY FRANCE

SOPHIE QUINTON
INRIA GRENOBLE

Outline

Overview of Thales systems

Timing design and verification

- Satellite platform on-board software
- Aerial video tracking system

Conclusion

Thales Profile

Employees

64,000

Global presence

56 countries

Self-funded R&D* 2016

731 million euros

* Does not include therefore R&D undertaken with external funding.

Revenues in 2016

15 billion euros

A balanced revenue structure

Defence **50%** | Civil **50%**

THALES

Markets Served by THALES

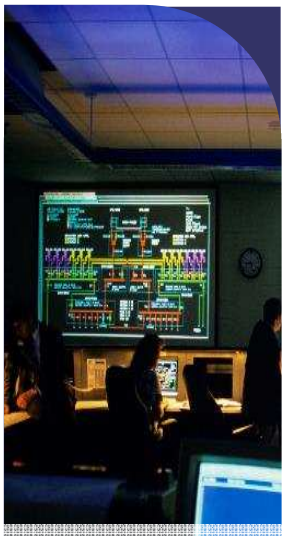
DUAL MARKETS
Military & Civil


AEROSPACE


SPACE


GROUND TRANSPORTATION


DEFENCE


SECURITY

THALES

Worldwide Major Role in…

Air Traffic Management

Satellite platforms

Rail signalling systems

Security for interbank transactions

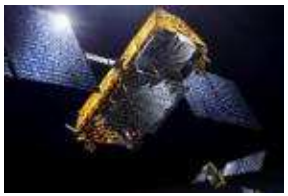
Payloads for telecom satellites

In-flight entertainment and connectivity

Military surface radars

Military tactical radio communications

Commercial avionics



Entire Civil satellites

Airborne optronic systems

Sonars

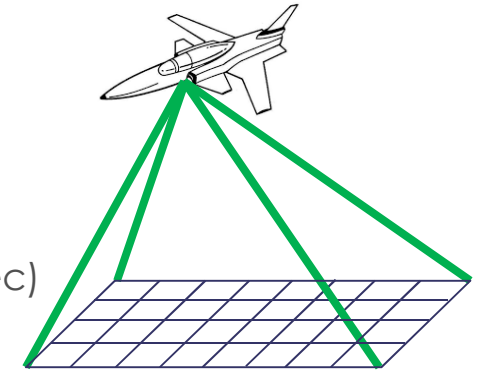
Mainly real-time embedded systems

- Hardware platforms: from single processors to multi-core systems
- Real-time constraints: from soft to hard constraints
- Design processes: component-based, functional programming,…

THALES

Airborne Optronic Systems

Aerial Video Tracking System (AVTS)

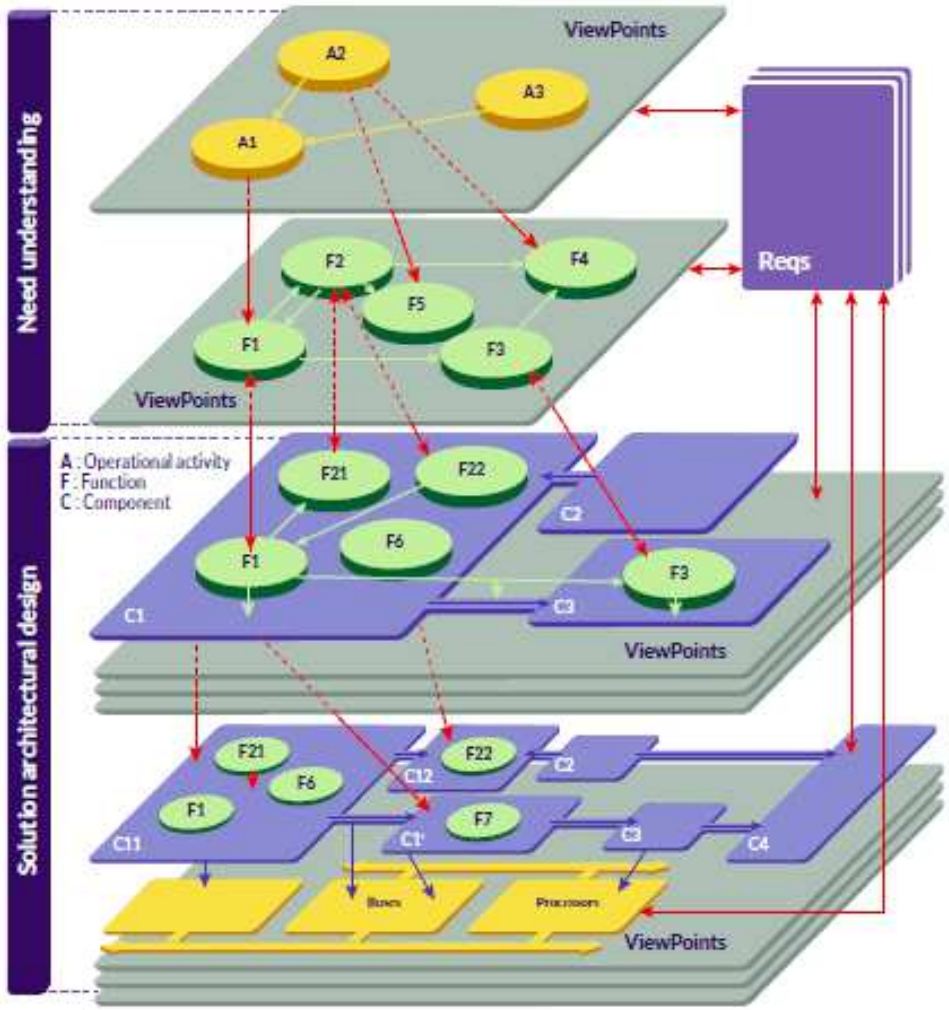


- Aerial video system to detect and track a moving object, e.g. a vehicle on a roadway
  - Track an object over longer time periods
  - Display a high quality video imagery to user (25 images/sec)
  - Embed tracking data into the video (ground speed, distance to tracked object, etc.)
  - Perform motion prediction even if the tracked object is temporarily hidden from view (e.g. the vehicle proceeds in and out of several tree obstructed areas)
  - Calculate new camera angle based on the aircraft sensors data (position, direction and speed, etc..) and the tracked object motion prediction

- Timing constraints
  - Deadline misses occasionally accepted if video quality is not strongly impacted
    ➔ weakly hard constraints
      – E.g. at least 60 seconds between two successive video frame losses ➔ **"1 out of 1500"**

AVTS : Timing Performance Design and Verification

ARCADIA Methodology



Operational Analysis
What the users of the system need to accomplish

Functional & Non Functional Need
What the system has to accomplish for the users

Logical Architecture
How the system will work to fulfill expectations

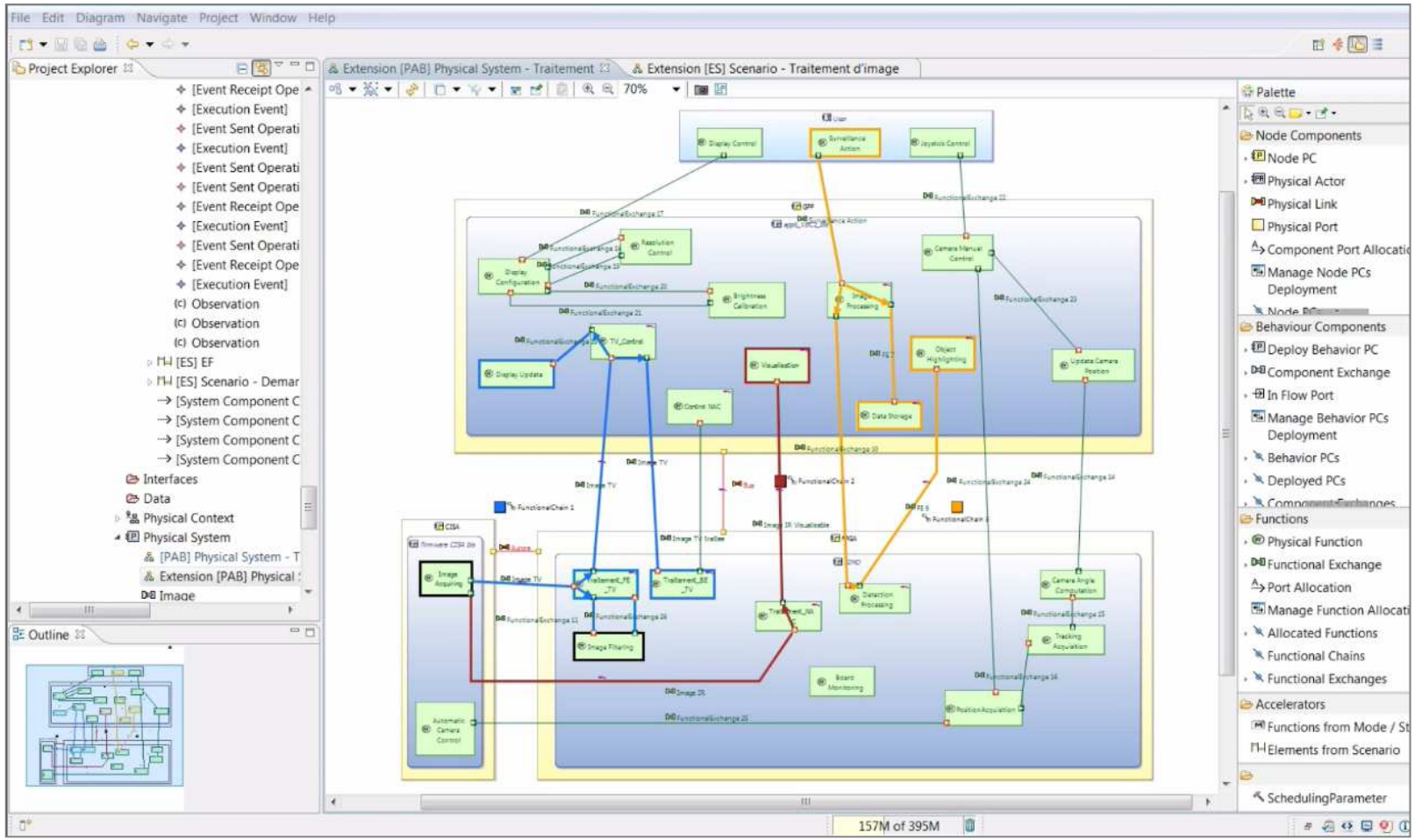
Physical Architecture
How the system will be developed and built

https://www.polarsys.org/capella/resources/Datasheet_Arcadia.pdf

THALES

AVTS : Timing Performance Design and Verification

AVTS design model in CAEPLLA

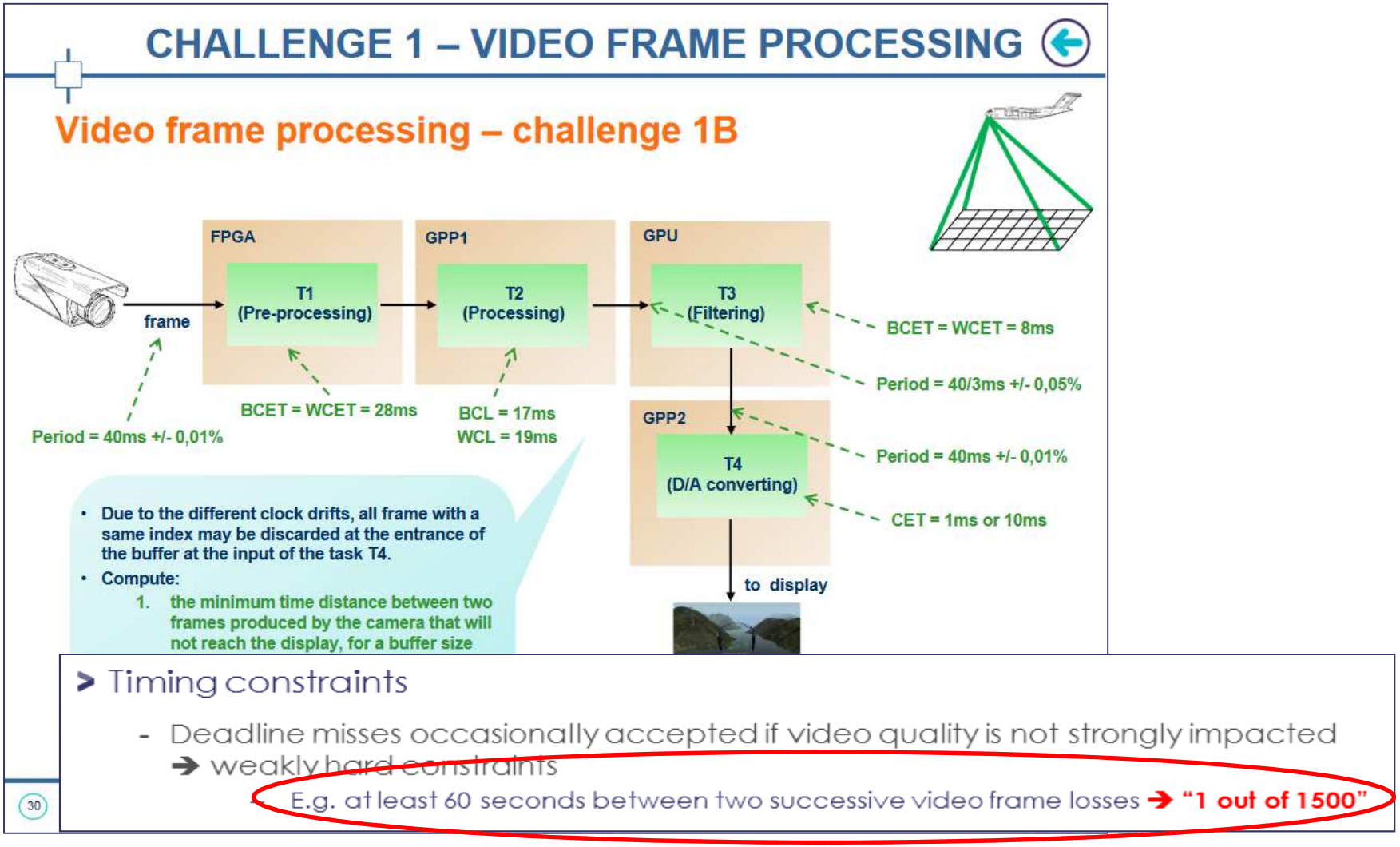


https://www.polarsys.org/capella/

THALES

AVTS : Timing Performance Design and Verification

Industrial Challenge in WATERS 2015 (consolidated in 2017)

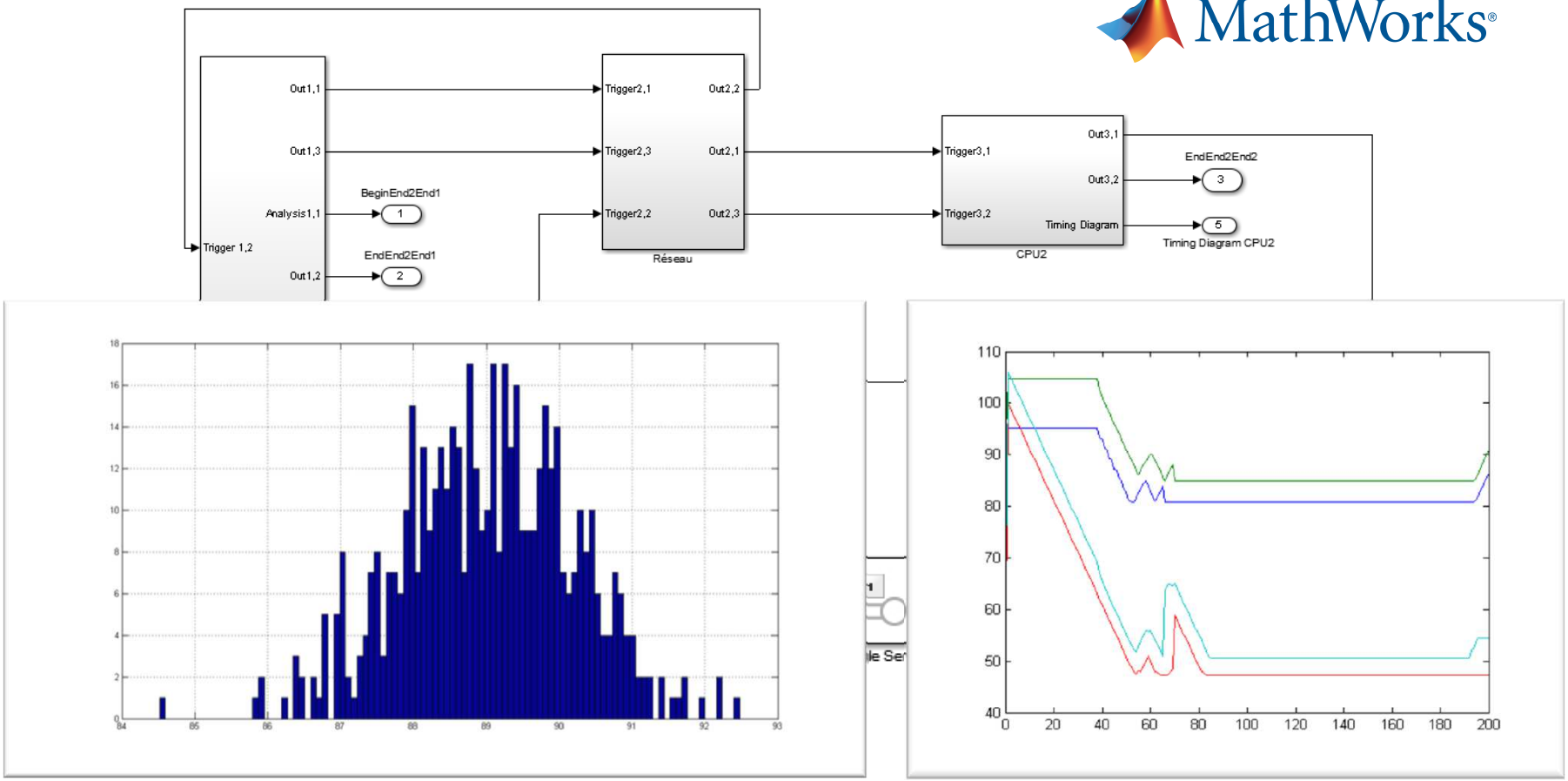


https://waters2017.inria.fr/challenge/

THALES

AVTS : Timing Performance Design and Verification

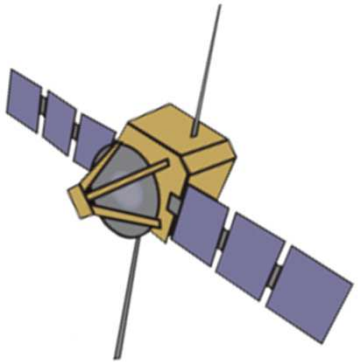
Timing verification using simulation with Mathlab/SimEvent



➔ **No guarantee on (m,k) constraints**

Satellite Platforms

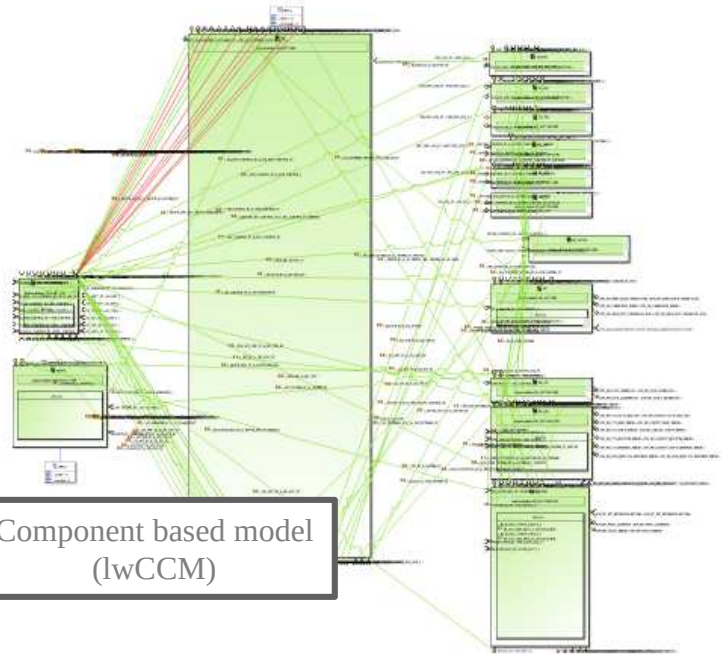
Satellite Platform On-Board SoftWare (OBSW)



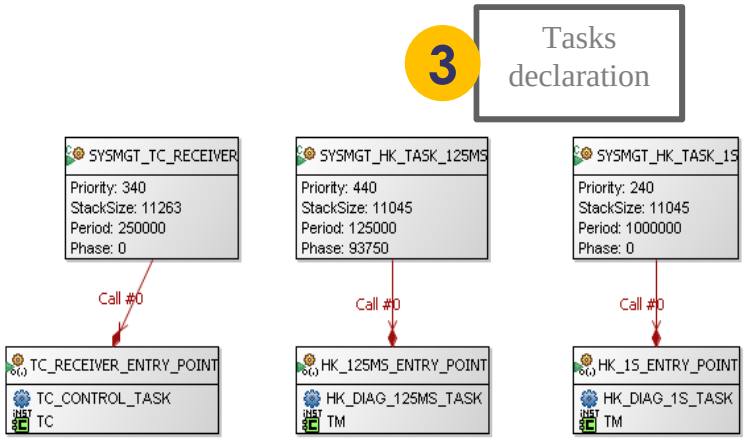
- Implements all major functions to govern the satellite and ensure proper execution of the mission
  - Attitude and orbit control (AOC)
  - Thermal control
  - Power control
  - Management of the ground/board interface
  - System status monitoring
  - Failure detection and system recovery
- Timing constraints
  - Always meet the deadline in any conditions ➔ hard constraints
  - Deadline misses occasionally accepted if mission is not endangered ➔ weakly hard constraints
    - E.g. the AOC task may miss 1 cycle every 8 ➔ **"1 out of 8"**
- Resources constraints
  - Limited choice of space-certified processors that can resist to the sustained radiation exposure (e.g. ESA's LEON processors)

THALES

Satellite OBSW: Timing Performance Design and Verification

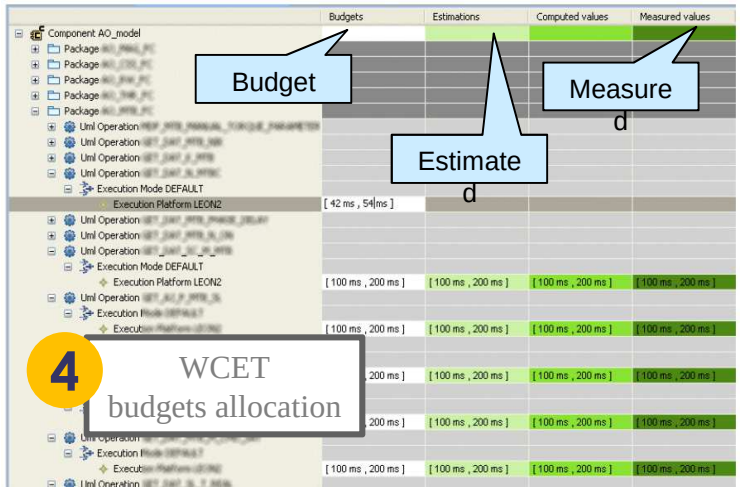


1 Component based model (lwCCM)




```
PRODUCER.IMPL.EXECUTE_PROD_FUNCTIONS :
  scenario NOMINAL {
     call PRODUCER.IMPL.DF.NOM. EXEC_NOM_DATA_FILTERING
     call PRODUCER.IMPL.DP.NOM. EXEC_NOM_DP
  }
  scenario COARSE_PRECISION {
     call PRODUCER.IMPL.DP.COARSE. EXEC_COARSE_DP
  }
  scenario ERROR {
     call PRODUCER.IMPL.DF.NOM. EXEC_NOM_DATA_FILTERING
     call PRODUCER.IMPL.DP.NOM
     raise EVENT.PRODUCER_FAIL
  }
```

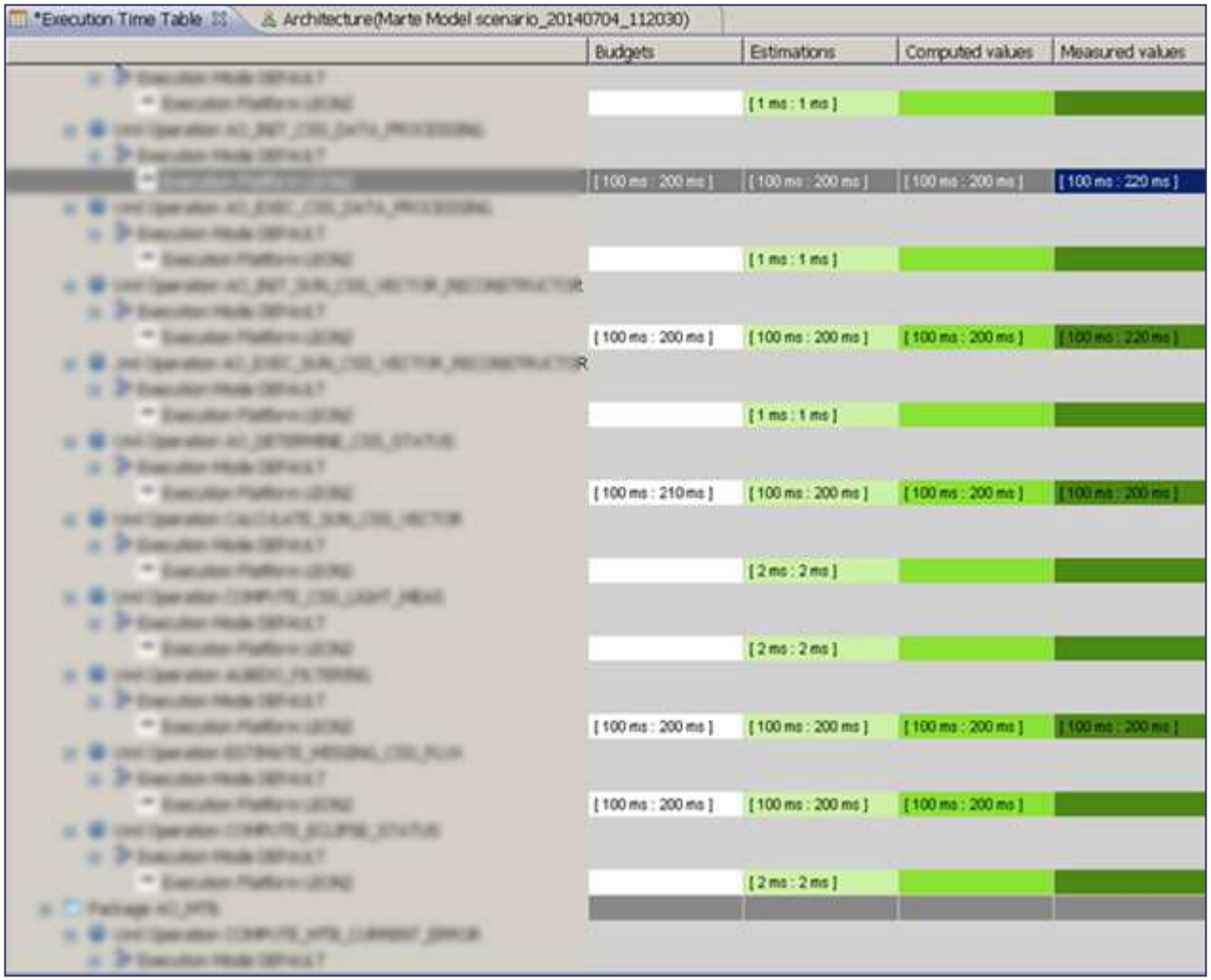
2 Definitions of call sequences and modes



THALES

Satellite OBSW: Timing Performance Design and Verification

Execution time values

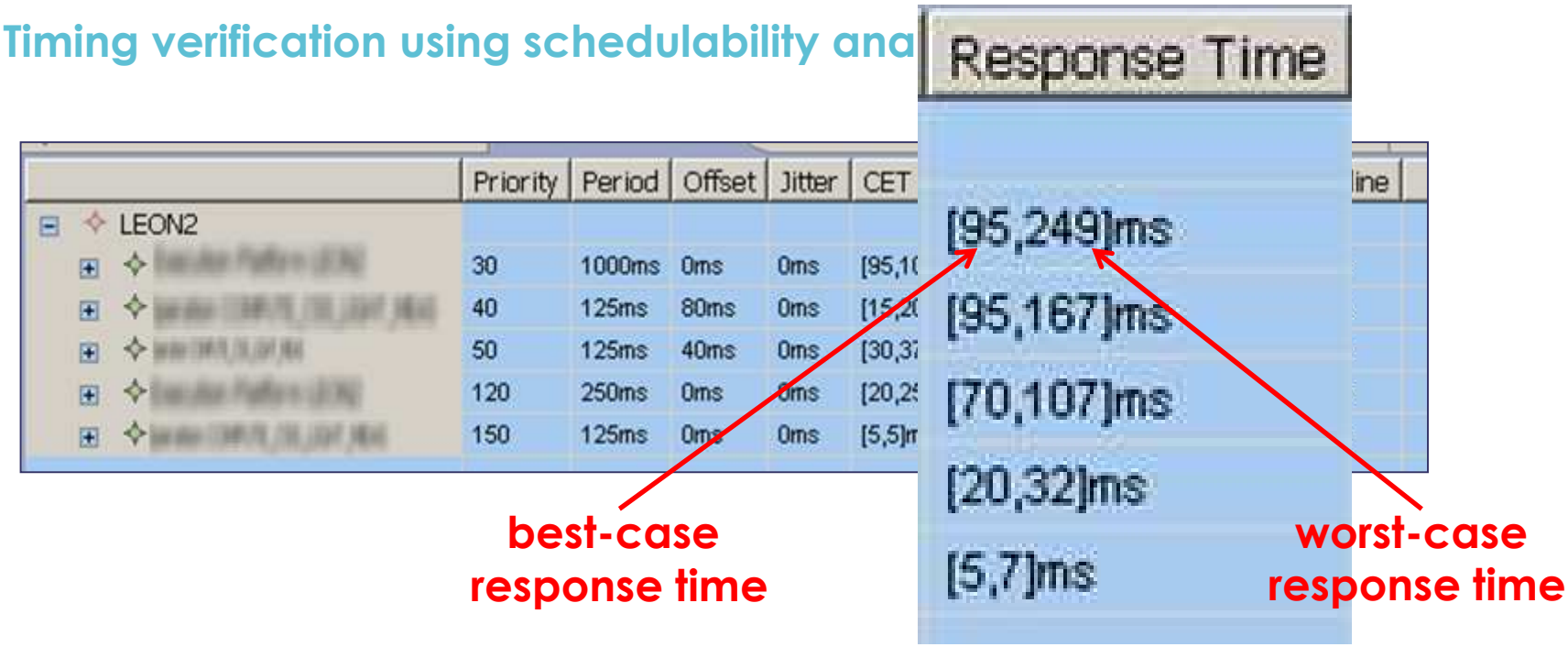


OPEN

THALES

Satellite OBSW: Timing Performance Design and Verification

Timing verification using schedulability ana

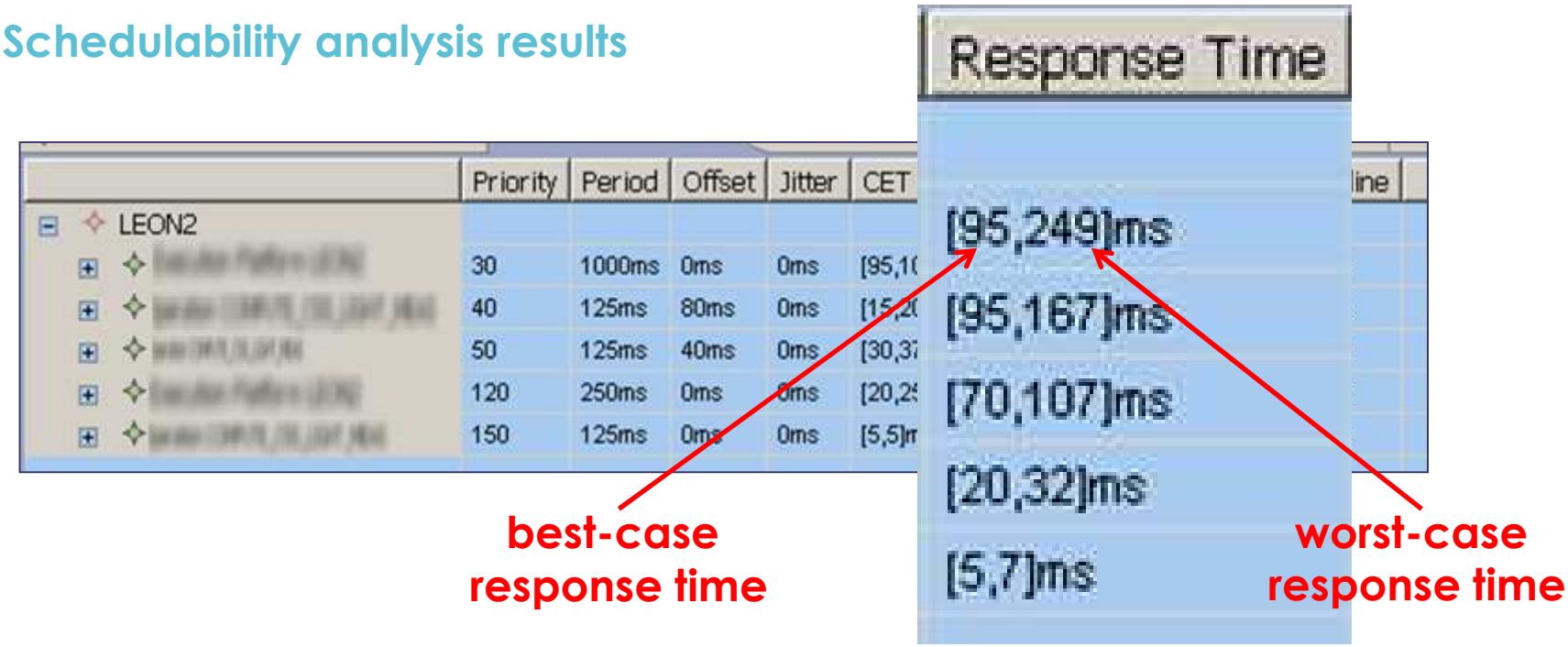


- Timing constraints
  - Always meet the deadline in any conditions ➔ hard constraints
  - Deadline misses occasionally accepted if mission is not endangered ➔ weakly hard constraints
    - E.g. the AOC task may miss 1 cycle every 8 ➔ **"1 out of 8"**

THALES

Satellite OBSW: Timing Performance Design and Verification

Schedulability analysis results



> Timing constraints

- Always meet the deadline in any conditions ➔ hard constraints
- Deadline misses occasionally accepted if mission is not endangered ➔ weakly hard constraints
  - E.g. the AOC task may miss 1 cycle every 8 ➔ **"1 out of 8"**

➔ **Pessimistic guarantee on (m,k) constraints**

THALES

Satellite OBSW: Timing Performance Design and Verification

Impact on resources budgeting

Conclusion