



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

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016. All rights reserved.



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



Markets Served by THALES

DUAL MARKETS Military & Civil



AEROSPACE



SPACE



**GROUND
TRANSPORTATION**



DEFENCE



SECURITY

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016. All rights reserved.

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

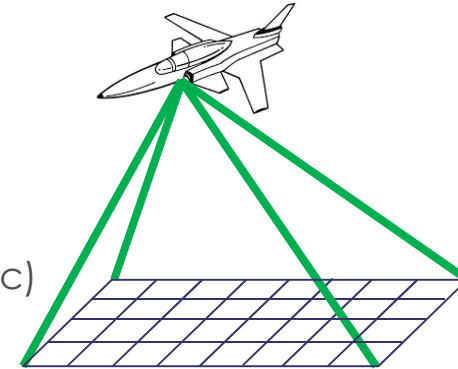
- Hardware platforms: from single processors to multi-core systems
- Real-time constraints: from soft to hard constraints
- Design processes: component-based, functional programming,...

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016. All rights reserved.

Airborne Optronic Systems

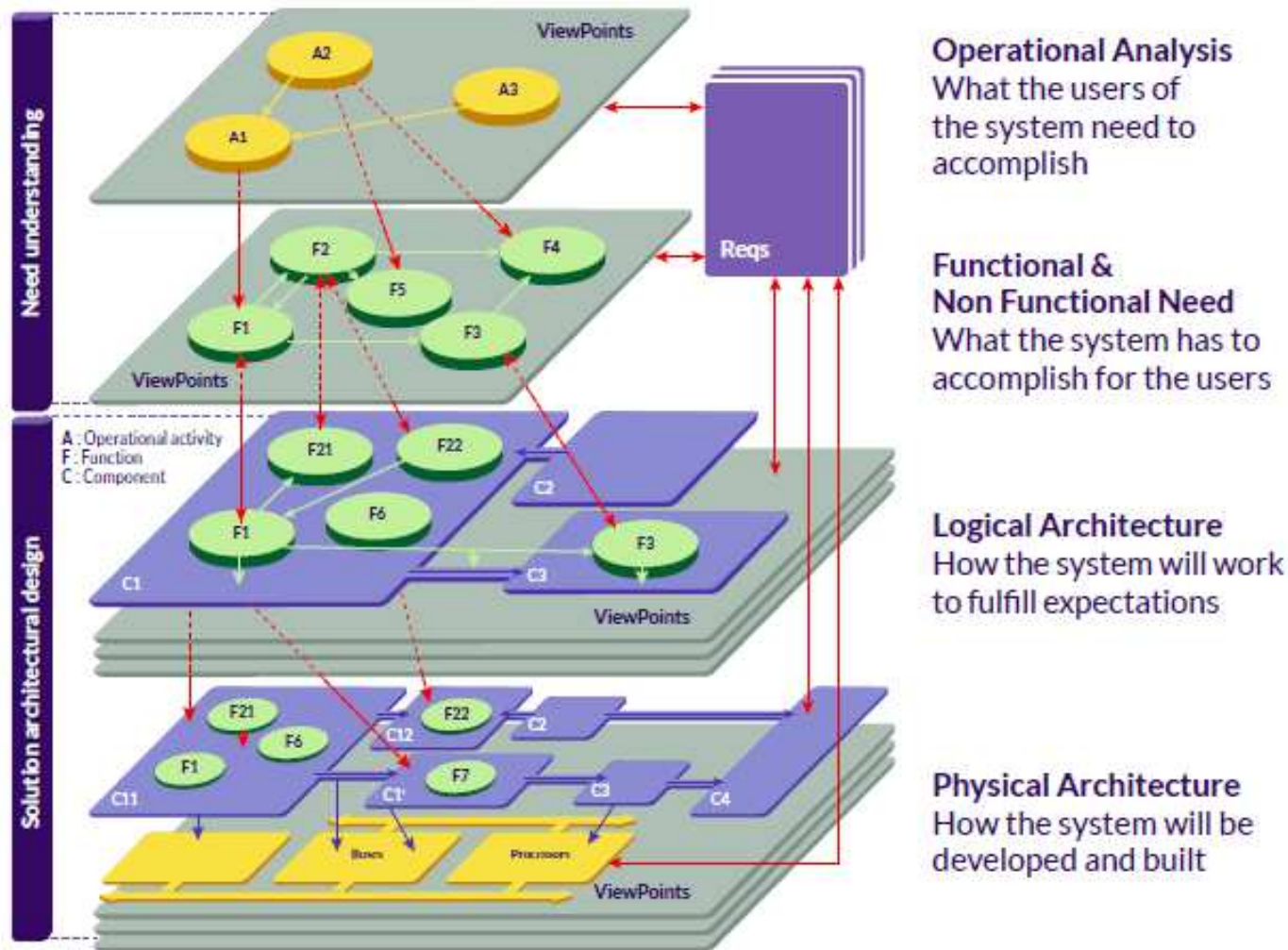
Aerial Video Tracking System (AVTS)

- 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



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

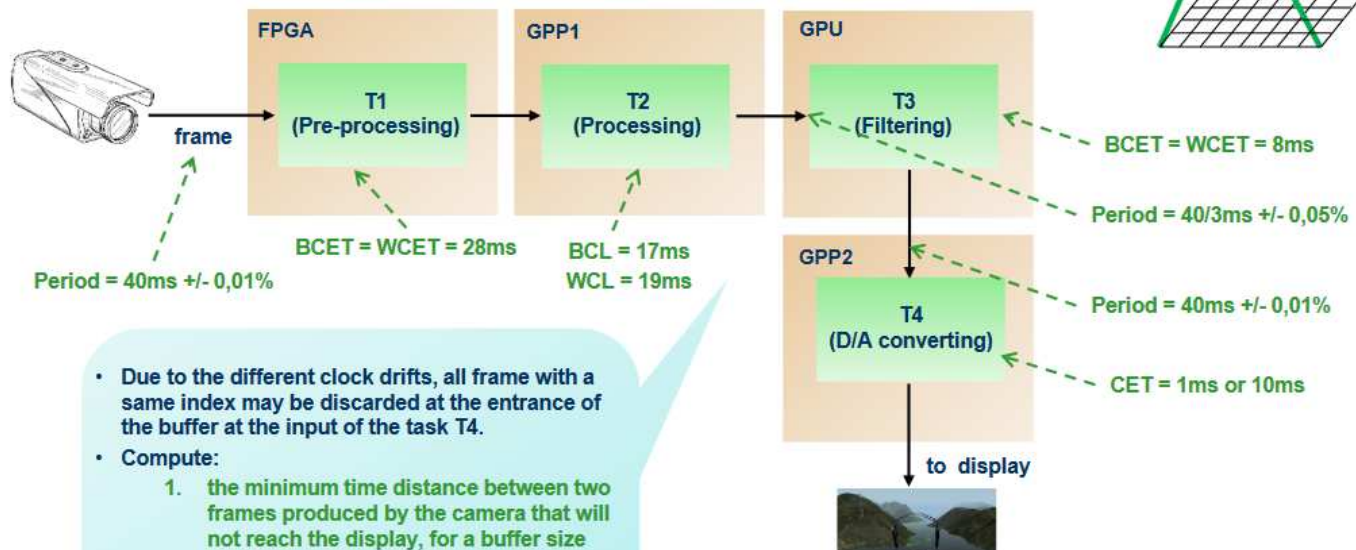
OPEN

AVTS : Timing Performance Design and Verification

Industrial Challenge in WATERS 2015 (consolidated in 2017)

CHALLENGE 1 – VIDEO FRAME PROCESSING

Video frame processing – challenge 1B



> 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"

30

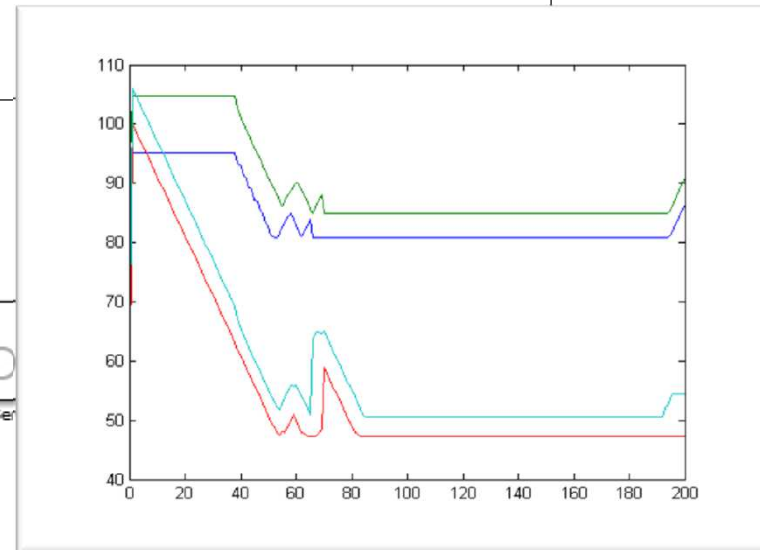
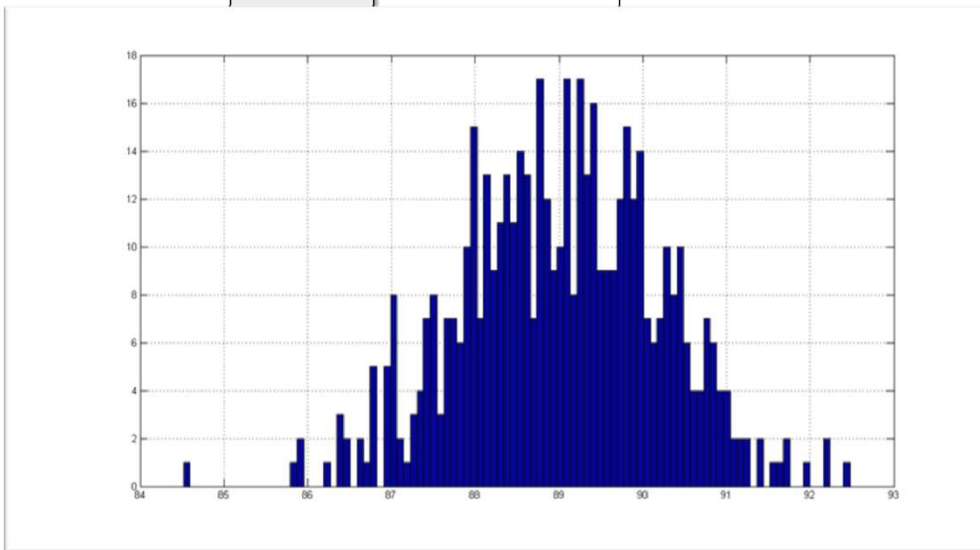
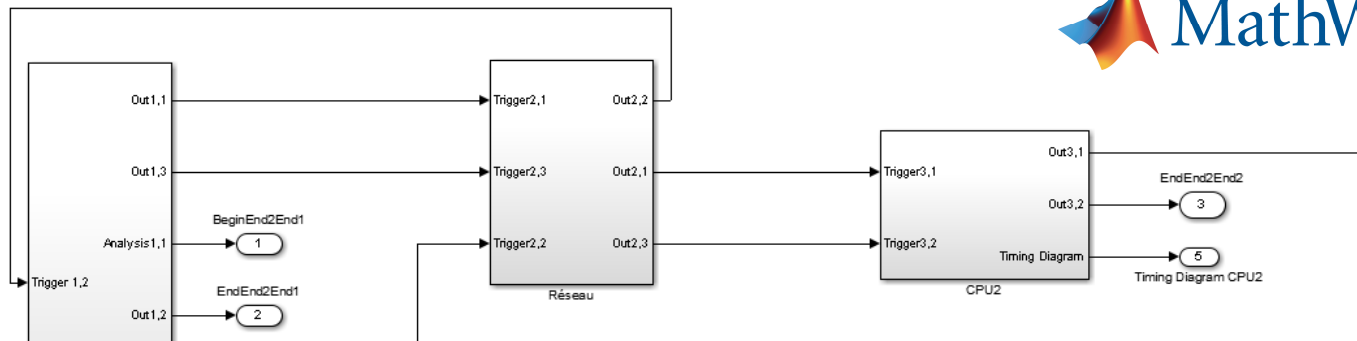
<https://waters2017.inria.fr/challenge/>

OPEN

THALES

AVTS : Timing Performance Design and Verification

Timing verification using simulation with Matlab/SimEvent



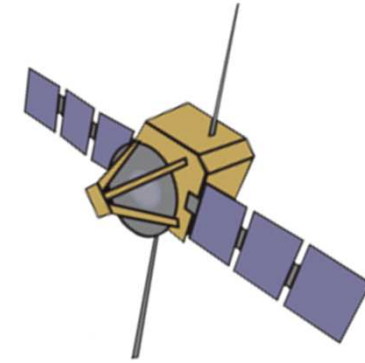
→ No guarantee on (m,k) constraints

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016 All rights reserved.

Satellite Platforms

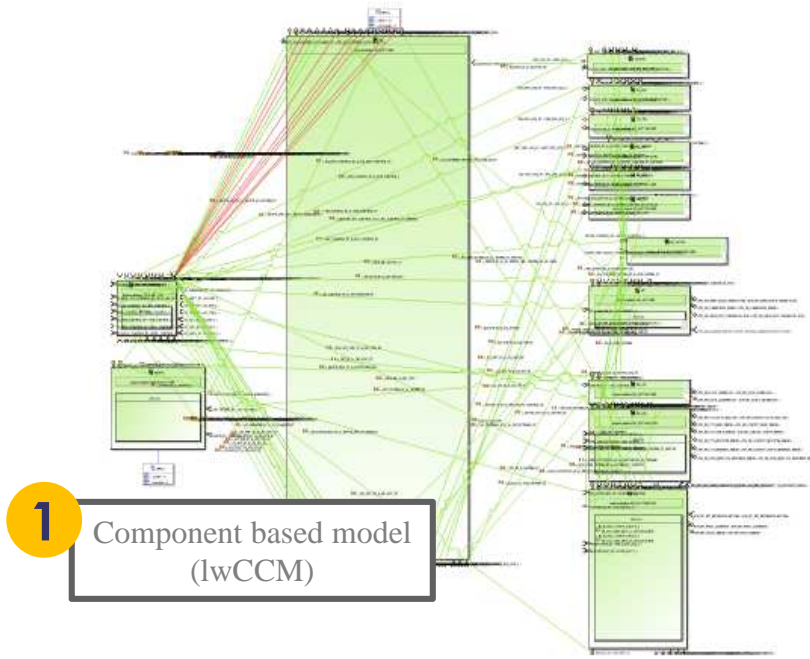
Satellite Platform On-Board SoftWare (OBSW)

- 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)



Satellite OBSW: Timing Performance Design and Verification

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016 All rights reserved.

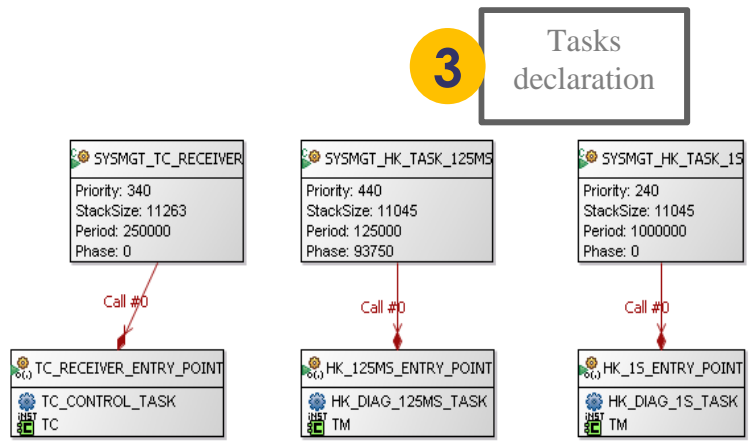


1 Component based model (lwCCM)

```

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. EXEC_NOM_DP
  raise EVENT.PRODUCER_FAIL
}
    
```

2 Definitions of call sequences and modes



3 Tasks declaration

Component AO_model	Budgets	Estimations	Computed values	Measured values
Package AO_1964_PC				
Package AO_1700_PC				
Package AO_1848_PC				
Package AO_1895_PC				
Unl Operation #0P_000_PARAMETER				
Unl Operation #0T_000_000				
Unl Operation #0T_000_000				
Unl Operation #0T_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[42 ms , 54ms]			
Unl Operation #0T_000_PARAMETER_00001				
Unl Operation #0T_000_000_000				
Unl Operation #0T_000_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]
Unl Operation #0T_000_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]
Unl Operation #0T_000_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]
Unl Operation #0T_000_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]
Unl Operation #0T_000_000_000				
Execution Mode DEFAULT				
Execution Platform LEON2	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]	[100 ms , 200 ms]
Unl Operation #0T_000_000_000				

4 WCET budgets allocation

OPEN

Satellite OBSW: Timing Performance Design and Verification

Execution time values

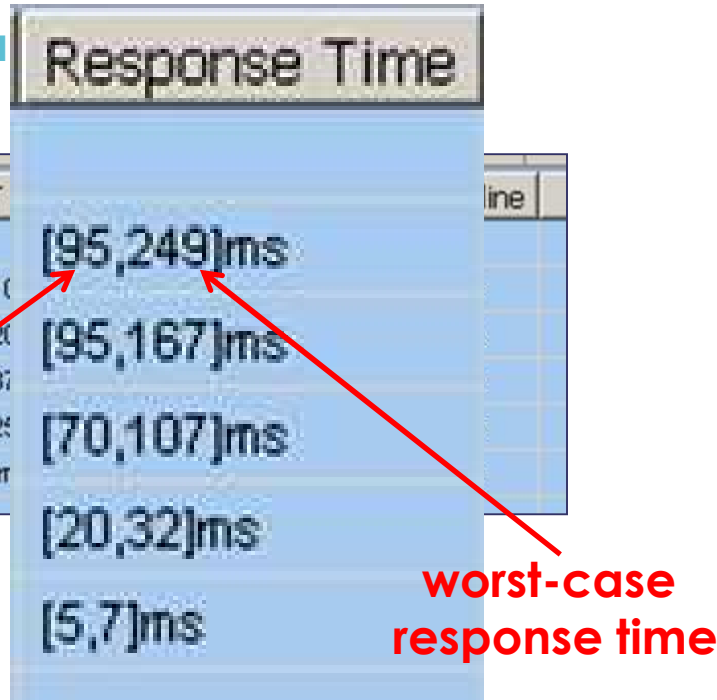
*Execution Time Table		Architecture(Marte Model scenario_20140704_112030)			
		Budgets	Estimations	Computed values	Measured values
+	Execution Mode DEFAULT		[1 ms : 1 ms]		
+	Execution Platform (209)				
+	Int Operation AC_2007_200_DATA_PROCESSING				
+	Execution Mode DEFAULT				
+	Execution Platform (209)	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 220 ms]
+	Int Operation AC_2007_200_DATA_PROCESSING				
+	Execution Mode DEFAULT		[1 ms : 1 ms]		
+	Execution Platform (209)				
+	Int Operation AC_2007_200_VECTOR_RECONSTRUCTOR				
+	Execution Mode DEFAULT				
+	Execution Platform (209)	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 220 ms]
+	Int Operation AC_2007_200_VECTOR_RECONSTRUCTOR				
+	Execution Mode DEFAULT		[1 ms : 1 ms]		
+	Execution Platform (209)				
+	Int Operation AC_2070000_200_STATUS				
+	Execution Mode DEFAULT				
+	Execution Platform (209)	[100 ms : 210 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]
+	Int Operation CALCULATE_SUM_200_VECTOR				
+	Execution Mode DEFAULT				
+	Execution Platform (209)		[2 ms : 2 ms]		
+	Int Operation COMPUTE_200_LIGHT_PATH				
+	Execution Mode DEFAULT				
+	Execution Platform (209)		[2 ms : 2 ms]		
+	Int Operation AUBO_2070000				
+	Execution Mode DEFAULT				
+	Execution Platform (209)	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]
+	Int Operation ESTIMATE_POSITION_200_PLAN				
+	Execution Mode DEFAULT				
+	Execution Platform (209)	[100 ms : 200 ms]	[100 ms : 200 ms]	[100 ms : 200 ms]	
+	Int Operation COMPUTE_ESTIMATE_STATUS				
+	Execution Mode DEFAULT				
+	Execution Platform (209)		[2 ms : 2 ms]		
+	Package AC_209				
+	Int Operation COMPUTE_209_CALLBACK_PACKAGE				
+	Execution Mode DEFAULT				

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016 All rights reserved.

Satellite OBSW: Timing Performance Design and Verification

Timing verification using schedulability and

	Priority	Period	Offset	Jitter	CET	line
LEON2						
+	30	1000ms	0ms	0ms	[95,10]	
+	40	125ms	80ms	0ms	[15,2]	
+	50	125ms	40ms	0ms	[30,3]	
+	120	250ms	0ms	0ms	[20,2]	
+	150	125ms	0ms	0ms	[5,5]	



**best-case
response time**

**worst-case
response time**

> 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"

Satellite OBSW: Timing Performance Design and Verification

Schedulability analysis results

	Priority	Period	Offset	Jitter	CET	Response Time
LEON2						
+	30	1000ms	0ms	0ms	[95,10]	[95,249]ms
+	40	125ms	80ms	0ms	[15,2]	[95,167]ms
+	50	125ms	40ms	0ms	[30,3]	[70,107]ms
+	120	250ms	0ms	0ms	[20,2]	[20,32]ms
+	150	125ms	0ms	0ms	[5,5]	[5,7]ms

best-case response time

worst-case response time

> 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

Satellite OBSW: Timing Performance Design and Verification

Impact on resources budgeting

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016. All rights reserved.

Conclusion

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2016. All rights reserved.

