



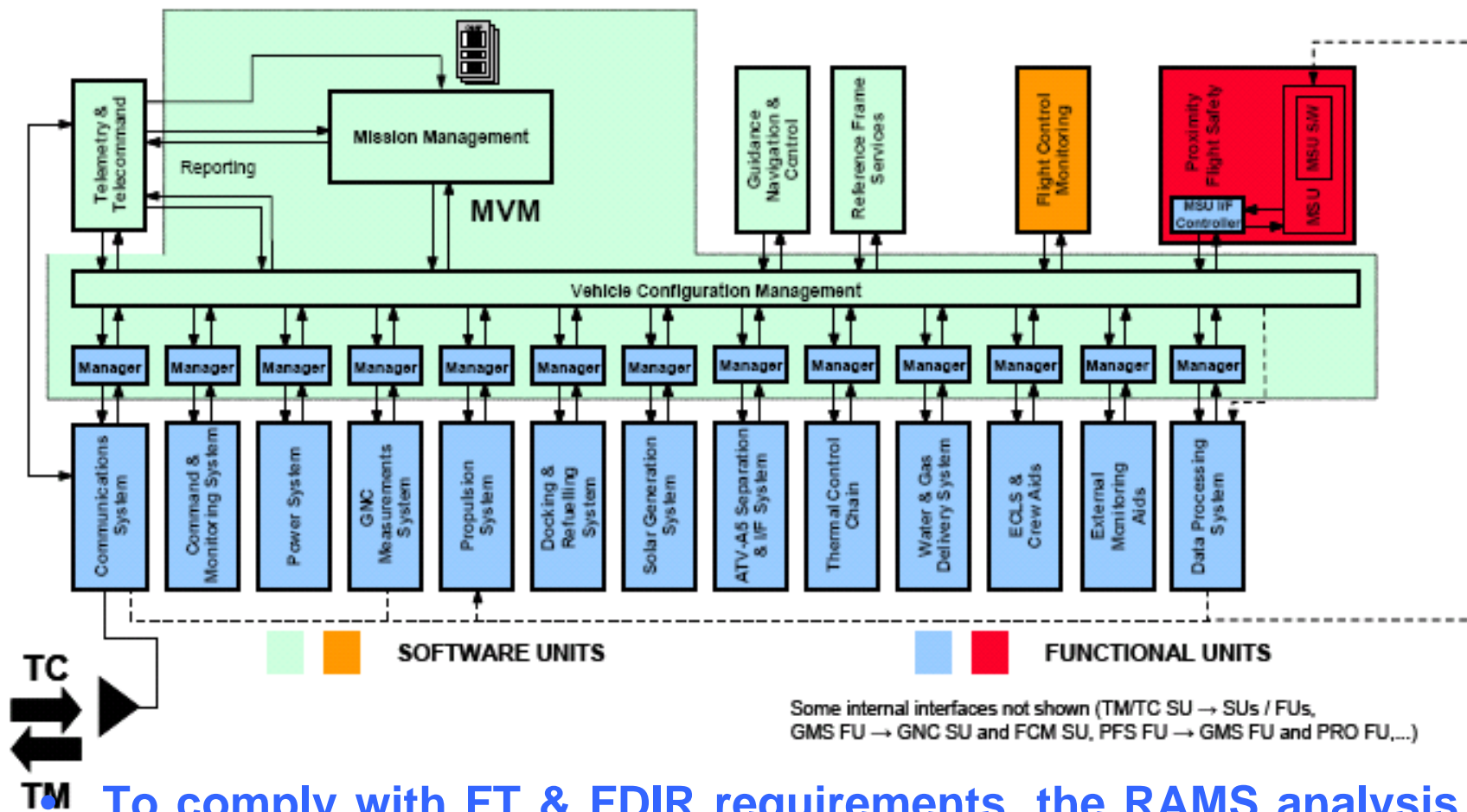
*Françoise Kervégant  
from EADS - Astrium Space  
Transportation*

*Lars Oliefka, Richard Chase  
from ESA*

# Failure detection and isolation based on FMEA approach for the ATV

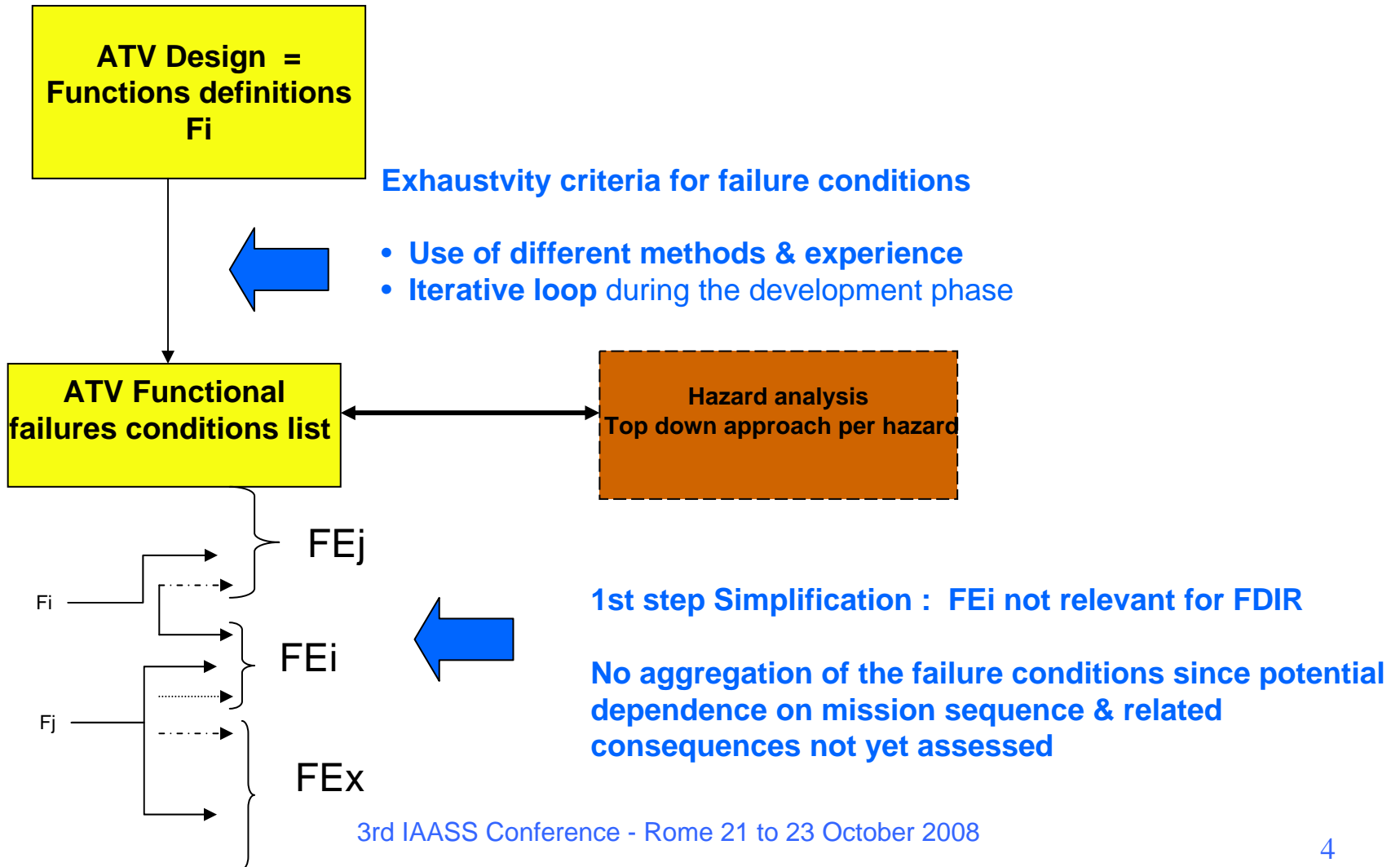
# CONTEXT

- The failure tolerance requirements applicable to ATV system are as follows:
  - 1 FT for mission continuation and critical consequences
  - 2 FT for catastrophic consequences
- As a consequence, it is necessary to detect failures and to perform isolation and recovery (FDIR) adapted to each failure condition.



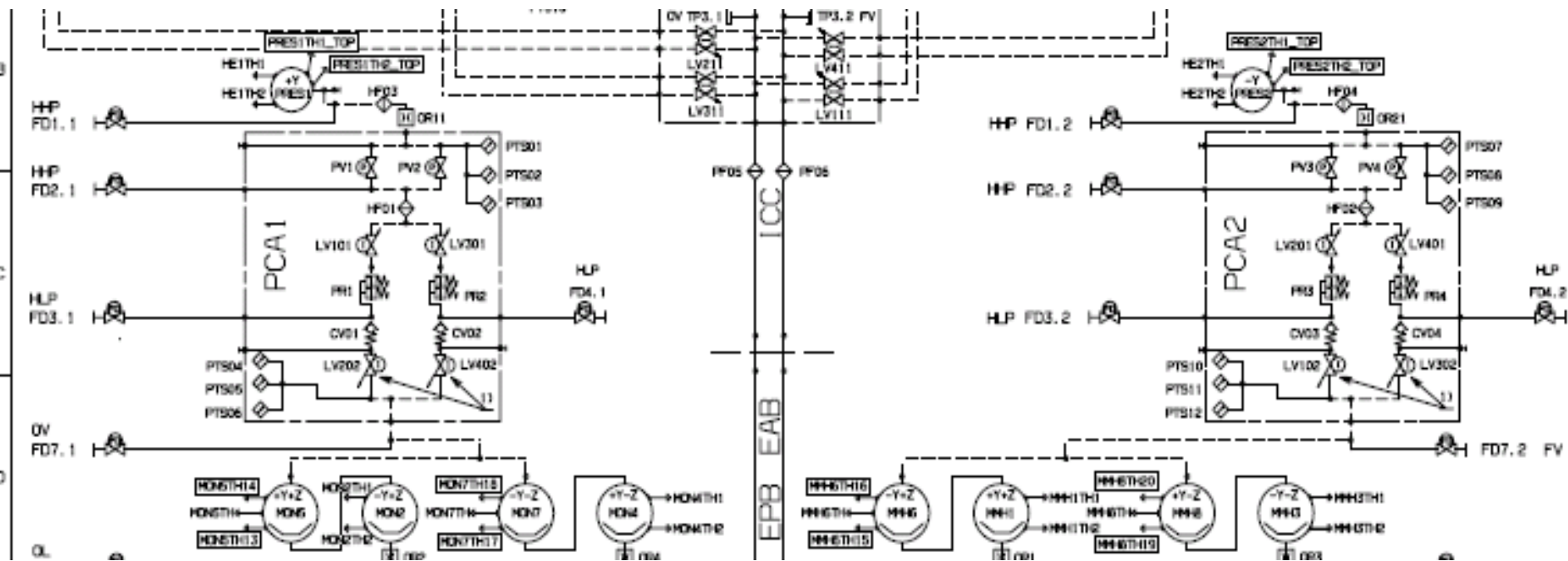
To comply with FT & FDIR requirements, the RAMS analysis was performed based on the Functional breakdown of the ATV and with a step by step approach to manage the complexity .

# Identification of the failure condition and the associated coverage matrix failure / monitoring



# Example : He pressurisation for the Propulsion function

Schematic of the fluidic part



Anomaly	Origins	Diagnostic means	Comments
Lack of pressurant gas on one propellant side	External leakage at the FDV level	<i>Only 1FT covered by design for the FDV interface</i>  <i>Ground monitoring:</i> survey of the pressurant tank pressures	External leakages covered by the design (structure + isolation barriers)
	Filter pollution	<i>Tank pressures:</i> monitoring of the propellant tank pressures according to the nominal operating domain (in line with the operating & qualification engine domain)	Single point failure covered by the ATV-RIBRE-RFW-109
	PR failed in closed or intermediate position	<i>Tank pressure:</i> monitoring of the propellant tank pressures according to the nominal operating domain (in line with the operating & qualification engine domain)	
	HPHFLV of the PCA in a closed or intermediate position	<i>LV status:</i> verification of the correct LV position <i>LV:</i> detection of any short-circuit via the LV Vmonit <i>Tank pressure:</i> monitoring of the propellant tank pressures according to the nominal operating domain (in line with the operating & qualification engine domain)	
Over-pressurisation on one side	Unexpected thermal evolution at the vehicle level	<i>Tank temperatures:</i> monitoring of the level and comparison with the flight predictions	
	Structural failure at the PR level	<i>Tank pressure:</i> monitoring of the propellant tank pressures according to the nominal operating domain (in line with the operating & qualification engine domain)	Limitation of the overpressure time effect by the introduction of the PIProD at the PCA level
	Internal leakage (HPHFLV)		Decision to block the LPHFLV in closed position to deal with the nominal leakage and the thermal expansions
	Overheating at the HPHFLV level (driver short-circuit)		Overpressure of helium caused by LV short-circuit not credible
Inadvertent thrust	External leakage at the FDV level	<i>Only 1FT covered by design (FDV interface)</i>	2FT safety to be covered by the analysis of the maximum thrust disturbance and its consequences

FDIR not needed could potentially improve the design robustness

FDIR needed to cover Failure tolerance

FDIR not needed could potentially improve the design robustness

# Identification of requested reactivity (in Worst case)

Failure condition relevant for FDIR FEi

**validity Matrix = Failures condition \* operational block**

		Operational block	
		T1	Tj
Failure condition			
	FEi		x
		x	

ATV mission = Definition of the operational blocks Ti

Propagation time : Classification High-short-long

Consolidation: Flight hazard scenarii

ATV Severity : Specification for ATV Gri

**Matrix = SEVERITY\*REACTIVITY CLASS**

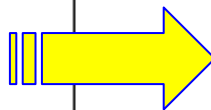
		Operational block	
		T1	Tj
Failure condition			
	FEi	Gr1 High	Gr2 High
			Gr3 long

2nd step Simplification Severity with minor consequence not sizing constraint for FDI

Characterisation & hierachisation of the effects for sizing Severity & reactivity class

System Failure	Severity - wo FDIR -with FDIR	Contributed by Failure Mode		FDIR					
		ID Failure Report (Item) Failure Description	Time to Syst. Effect	Internal Prevention	Observable symptoms	Time to Detect ion	ATV FDIR	Time to Rec over y	System FDIR
<p>PCA-3</p> <p>Degraded or loss of H<sub>2</sub> flow rate at valve -PR assembly</p> <p>See ATV-AS-TN-1554 §5.3</p>	<p>wo FDIR</p> <p>CAT</p> <p>with FDIR</p> <p>Minor</p>	<p>ID PCA3-1 : Mechanical failure of HPLV, PR, CV LPHFLV blocking device in closed position (including partially open).</p> <p>FE1 - Incomplete or failed closed of HP HF LV ( 2 per PCA in parallel )see PRSS FMECA(8) FM 9.2</p> <p>FE2 - Incomplete or failed in closed position of regulator pressure ( one per PCA branch) see PRSS FMECA(8) FM 10.4</p> <p>FE3 - Reduced flown through regulator see PRSS FMECA(8) FM 10.6</p> <p>FE4 - Flow stability disturb on regulator see PRSS FMECA(8) FM 10.7</p> <p>FE5-undue closed position LPHF LV on PCA due to mechanical failure on blocking device see PRSS FMECA(7) FM 12XX</p> <p>FE6-CV blocked in closed position see PRSS FMECA(8) FM 11.2 drawing ref TBD</p>	<p>short term depend ing on thrusters actuation and pressur e level</p>	<p>Design :</p> <p>C1- Risk due obturation due to pollution causes see PCA-2.</p> <p>C2-mechanical failure of HPLV, PR, CV in closed, LPHFLV blocking position (including partially open).see PCA-1</p> <p>- Blocking device on LPHF LV qualification wrt functional performance and qualification of mounting process</p> <p>C3 Obstruction due to potential He/propellant freezing:</p> <p>The CV acts as a barrier against the propellant vapour migration- The potential freezing condition has been assessed taken into account mission profile</p> <p>Operational control :</p> <p>- see ID PCA2-2</p> <p>- Control for blocking device integration</p>	<p>In case of on-board anomaly on PCA low pressure (propellant tank) monitoring :</p> <p>PRO_AN_MON_1; PRO_AN_MON_3; PRO AN MMH 2; PRO_AN_MMH_4</p> <p>The PTS low pressure algorithm implemented on board is compatible with failure sensors.see PCA 4</p> <p>The Acquisition is done through redundanted and independent CMU ( dedicated bus communication and power)</p>		<p>Based on the anomaly MVM triggered an alarm PRO_AL_PRESS_ i=1 to 4</p> <p>For justification of the threshold compatibility with thrusters qualification and reactivity - see See ATV-AS-TN-1554 §5.3.4</p>		<p>The reconfiguration differs pending mission phase are justified in ATV-AS-TN-1554 §5.3.4</p>

Specification and validation of the FDIR performance

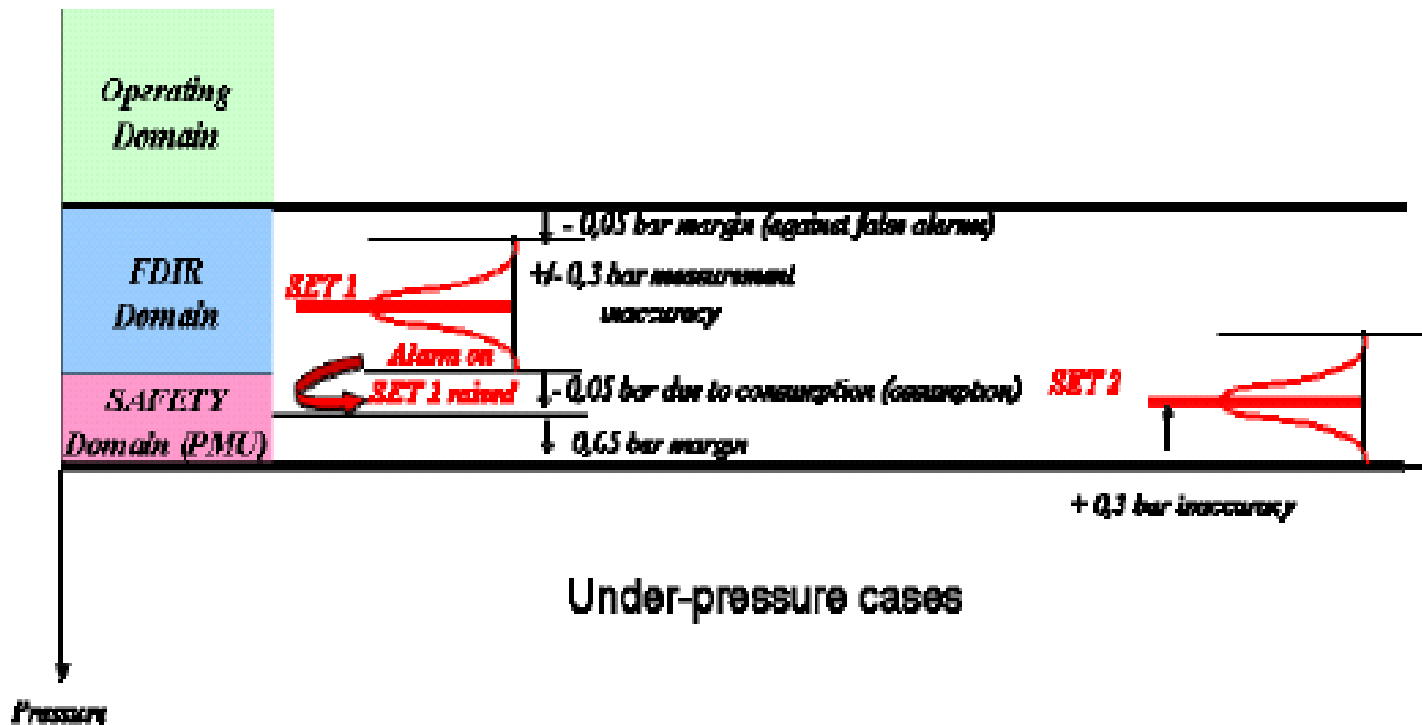


Case to cover	Feared Event	Reactivity Need	Monitoring Specification
Lack of pressurant gas on one propellant side ( <i>FDIR_PRO_ANO_10</i> )	Consequences at the thruster level: <ul style="list-style-type: none"> <li>× Shrapnel effect</li> <li>× Burn-through</li> </ul>	Detection and isolation of the problem to be performed before over-passing the engine qualification box (medium reactivity as the pressure decrease is driven by the propellant consumption)	<p><i>Logic:</i> Over or under pressure detected as soon as the couple (MON pressure, MMH pressure) over-passes the FDIR set 1 (see figure 14.1)</p> <p><i>Constraint:</i></p> <p>For the over-pressure case, reactivity between the FDIR set 1 over-passing and the definitive isolation of the PR failure (via the HPHFLV) to be lower than 3 s (hypothesis considered in [RD3-05] for the PRSS qualification box building)</p> <p><i>Algorithm specification :</i></p> <p>IF (PMON;PMMH) outside the FDIR set 1 box as defined in figure 14.1, current active PCA's failed</p> <ol style="list-style-type: none"> <li>3) Isolate the PCA's via closure of the correspondent HPHFLV</li> <li>4) Inactivate the FDIR set 1 and replace it by the FDIR set 2 during all the recovery process</li> <li>5) Replace FDIR set 2 by set 1 as soon as the (PMON,PMMH) couple is back inside the FDIR set 1 box</li> </ol> <p><b>FDIR SET 1</b> = Limits of the operating domain without failure (corresponds to the nominal operating domain + measurement inaccuracy + margins against the false alarms. When reached, a PCA failure has occurred)</p> <p><b>FDIR SET 2</b> = Corresponds to the extreme points which could be reached during the isolation process taking into account a triggering of the isolation process at the failure detection limit</p>
Over-pressurisation on one propellant side ( <i>FDIR_PRO_ANO_11</i> )	Explosion of the propellant tank (MDP over-passed)	Detection and isolation of the problem to be performed before over-passing the tank MDP and	

↑  
Qualification per test requested

Detection – reactivity and isolation specifications →

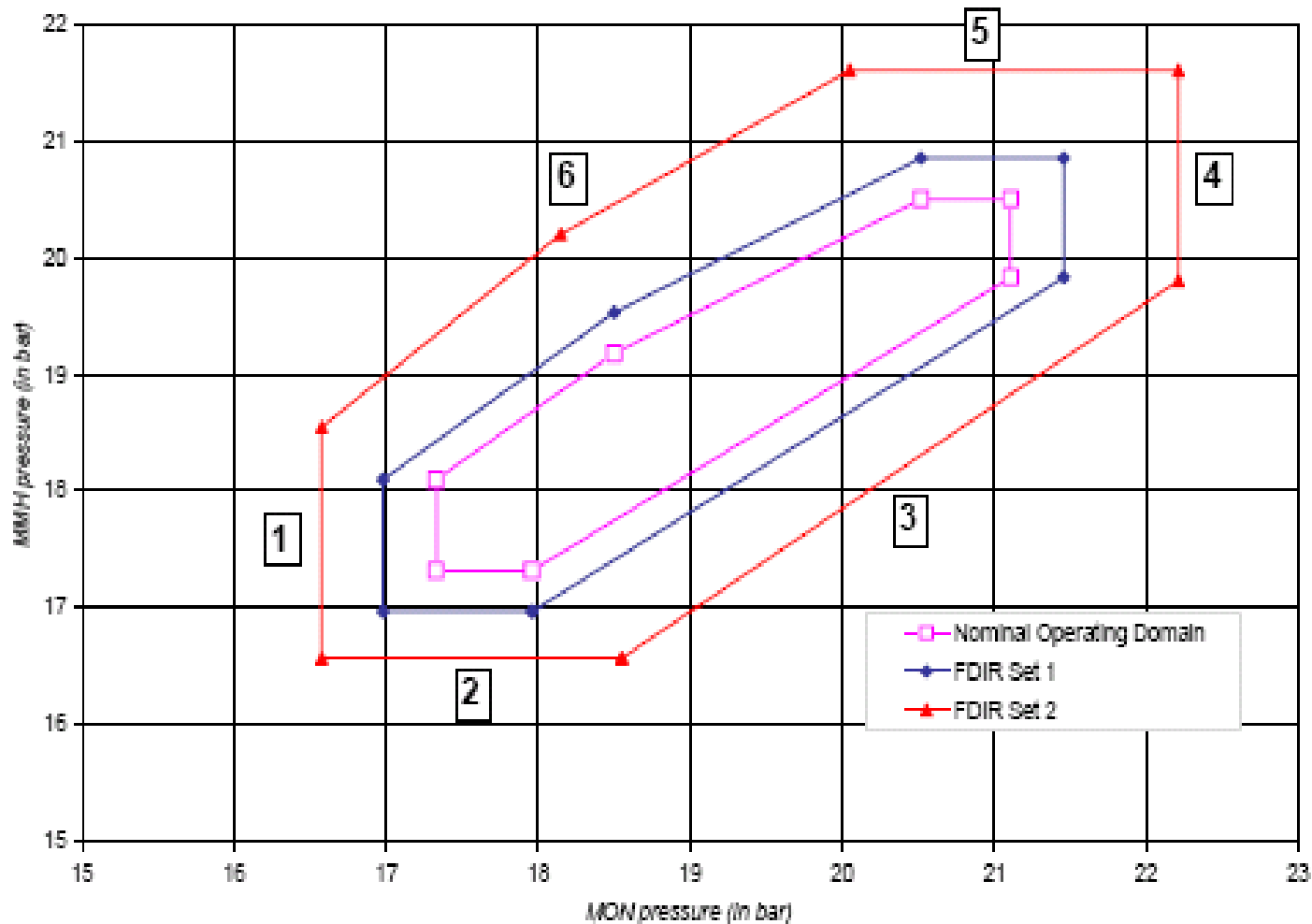
# Thruster Box Definitions



# Example :

## He pressurisation for the propulsion

Propellant Tank FDIR - Definition of the monitoring thresholds sets



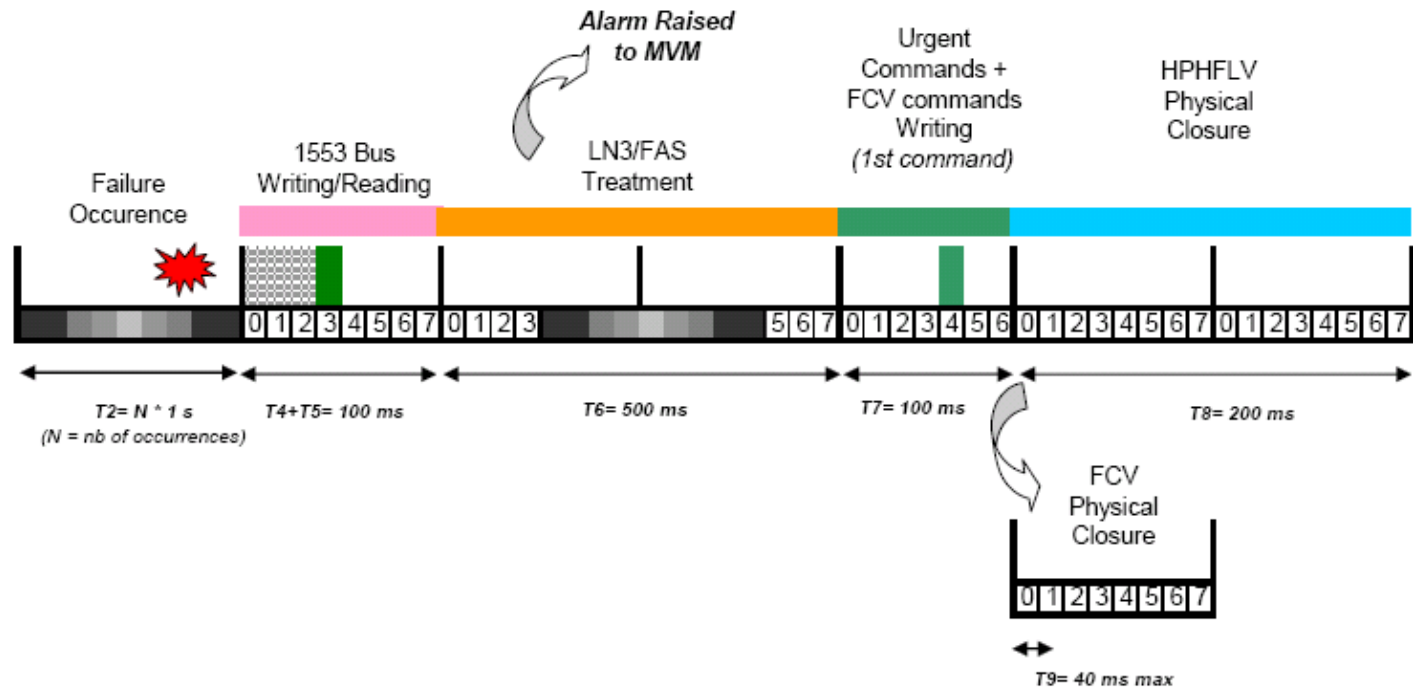


Figure 14.6 – Reactivity (from detection to isolation) for the PCA PTSXY monitoring

This document is the property of ASTRIUM SPACE TRANSPORTATION and shall not be communicated to third parties and/or reproduced without prior written agreement. Its contents shall not be disclosed. © - ASTRIUM SPACE TRANSPORTATION - 2007

## Last step .. Qualification & validation tests

- Validation test campaigns have been completed for each element of FDIR required to provide Failure Tolerance:
  - validation of the reactivity for detection and isolation,
  - validation of the threshold,
  - validation of the recovery plan
- In flight experience with ATV JV has demonstrated the correct reaction of the FDIR.

**On-board FDIR design**

**→ 770 anomalies**

**Function context**

**Vehicle context**

200 alarms  $\times$  1st/2<sup>nd</sup> failure  $\times$  80 vehicle modes

**32 000 cases of recovery to be analysed**



**20 000 relevant cases according to the mission phase**



**300 recovery actions**

# Pressure failure condition Jules Verne flight

