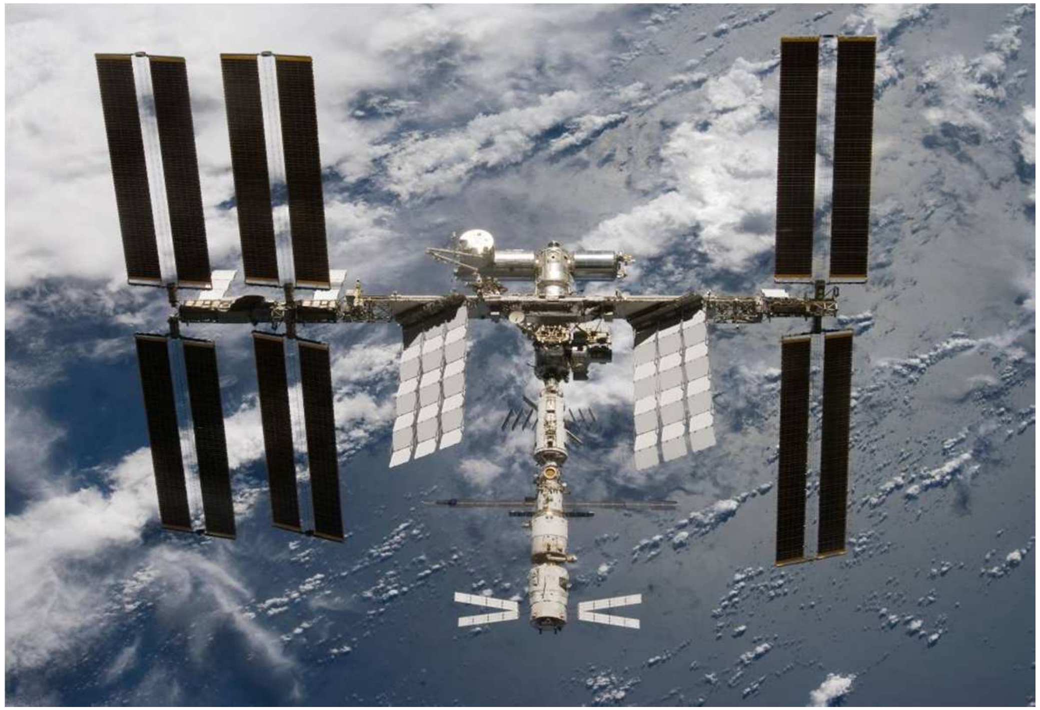
centre de contrôle de toulouse
toulouse control centre

Zoom on ATV Safety (Automated Transfer Vehicle)



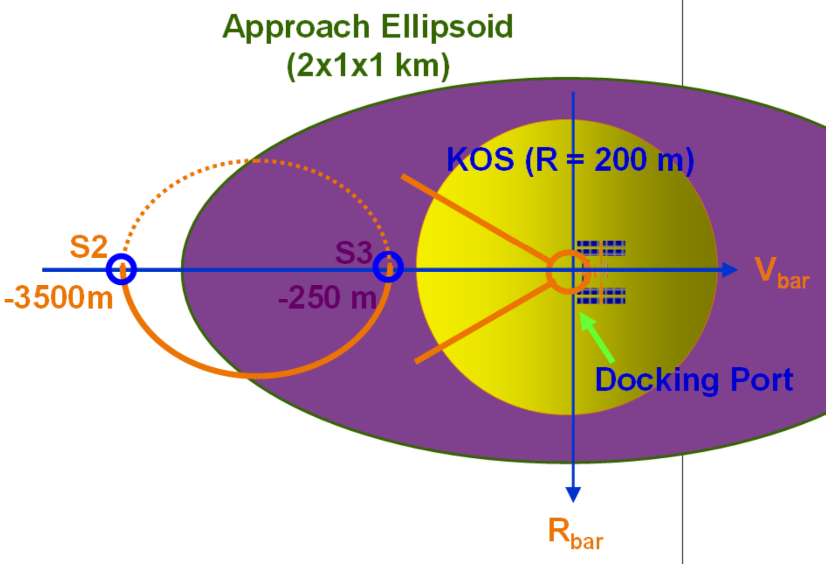
Gérard GALET

04 Juin 2012

Safety requirements / Life on board ISS

High level ISS safety requirements:

- ATV shall be 2 failures safe for ISS and crew safety in proximity or attached to ISS
- In case ATV control is lost, ATV shall not enter:
  - The Approach Ellipsoid (AE) within 24 hours
  - The Keep Out Sphere (KOS) within 4 orbits



ISS and crew safety is ensured by:

- ATV vehicle design
- ATV mission design
- Ground monitoring
- Crew monitoring

Safety impacts on ATV Vehicle design

Redundancy at equipment level and at functional level and managed by FDIR

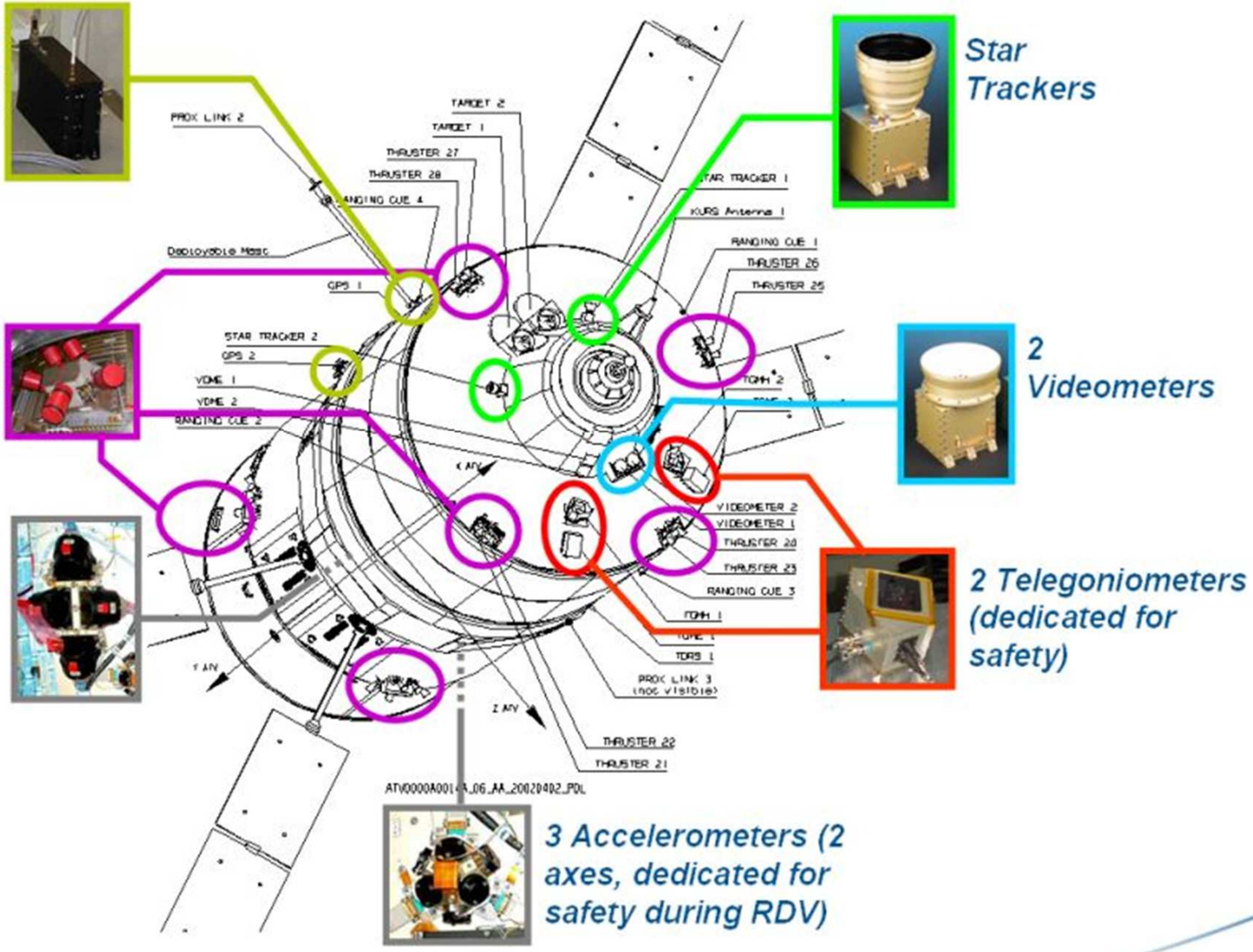
ATV is “flown” by the on-board **Guidance, Navigation and Control (GNC)** system.

Rendezvous Monitoring and Collision Avoidance

- On-board **Flight Control Monitoring (FCM)**
  - ✦ First level monitoring, using Flight Application Software
  - ✦ Monitors GNC behaviour against thresholds ensuring ISS safety. When thresholds are exceeded → Triggers ESCAPE → Nominal GNC & Propulsion.
  - ✦ **Collision Avoidance Manoeuvre (CAM)** if anomaly detected during departure or ESCAPE
  - ✦ No FTC (Fault Tolerant Computer) reset unless a CAM is triggered

- On-board **Proximity Flight Safety (PFS)** ⇔ **2nd independent spacecraft**
  - ✦ Coarse Monitoring + Monitoring of ATV health (in particular “reset”)
  - ✦ Independent safety chains (power, computer, sensors, actuators, etc.)
  - ✦ Dedicated SW (class A) running on dedicated computers: Monitoring and Safety Unit (MSU)
  - ✦ Always triggers **CAM** ➔ Dedicated system

ATV Measurement Sensors/ Actuators



2 GPS Receivers (2 antennas)

Star Trackers

32 Thrusters

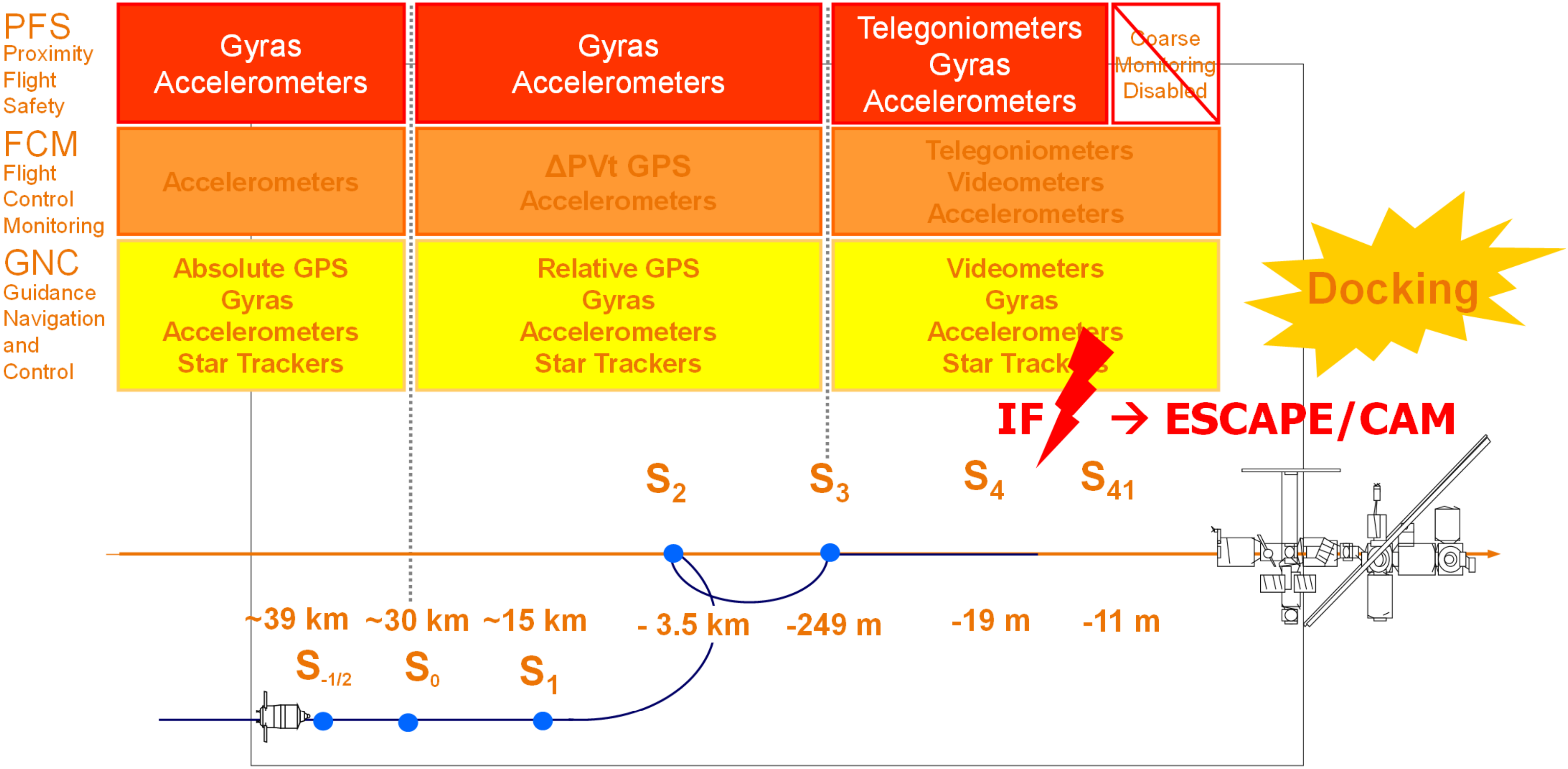
2 Videometers

4 Gyrometers (2 axes)

2 Telegoniometers (dedicated for safety)

3 Accelerometers (2 axes, dedicated for safety during RDV)

Safety impact on ATV mission design



PFS Proximity Flight Safety	Gyras Accelerometers	Gyras Accelerometers	Telegoniometers Gyras Accelerometers	~~Coarse Monitoring Disabled~~
FCM Flight Control Monitoring	Accelerometers	ΔPVt GPS Accelerometers	Telegoniometers Videometers Accelerometers	
GNC Guidance Navigation and Control	Absolute GPS Gyras Accelerometers Star Trackers	Relative GPS Gyras Accelerometers Star Trackers	Videometers Gyras Accelerometers Star Trackers	

Safety is guaranteed by ATV if ATV is within S-1/2 box

Safety is guaranteed by ESCAPE/CAM availability

Safety impact on ground operations (1/2)

To fulfil some requirements, the ground and/or the crew must be in the loop

➔ Operational Control, via OCAD (Operational Control Agreement Document)

OCAD implemented via operational documentation

- For crew activities → ODF (On-board Data File)
- For ATV-CC
  - Flight Rules (Joint and Internal ATV-CC)
  - Flight Control procedures
  - Monitoring items
  - Flight Dynamics Subsystem monitoring and procedures

Major impacts on ATV-CC design:

ATV-CC architecture: e.g. Redundancy of equipment to ensure continuity of monitoring function and the capability to send urgent commands

ATV-CC Safety Critical SW: e.g. Orbit determination and manoeuvre computation SW are critical ➔ two different algorithms have been implemented for both tasks

Handling of Hazardous Commands: e.g. Implementation of a mechanism to ensure a double check each time a command flagged “hazardous” is to be up-linked

Safety impact on ground operations (2/2)

Examples of specific operations to be performed:

Calculate arrival in S-1/2 box with very high accuracy

GNC monitoring of final approach:

- Continuous monitoring from S-1/2
- To be able to provide GO/NO GO criteria at any hold point
- To be able to detect off nominal situations at any time

Configure the 2nd spacecraft from ground at all hold points

- More than 300 parameters to be calculated
- Safe mechanism to prepare and upload on-board ATV
- Safe verification process

Conclusion on impact of safety on operations

Uniqueness of ATV operations in comparison to most satellite operations regarding safety

- Problem on satellite → “barbecue mode” – no urgent operations
- Problem on ATV → due to safety aspect: critical operations with high reactivity (=> Permanent link is required)

Safety is an integral part of the mission design & execution

- Redundancy + FDIR + FCM + PFS + ATV-CC monitoring + Crew monitoring
- Docking reliability is traded off against safety, but this is the price to pay to be able to rendezvous and dock with the ISS in a safe manner.

=> Major risk = To abort a “non critical” mission !!

Automatic ←=======→ AUTOMATED ←=====→ Assisted