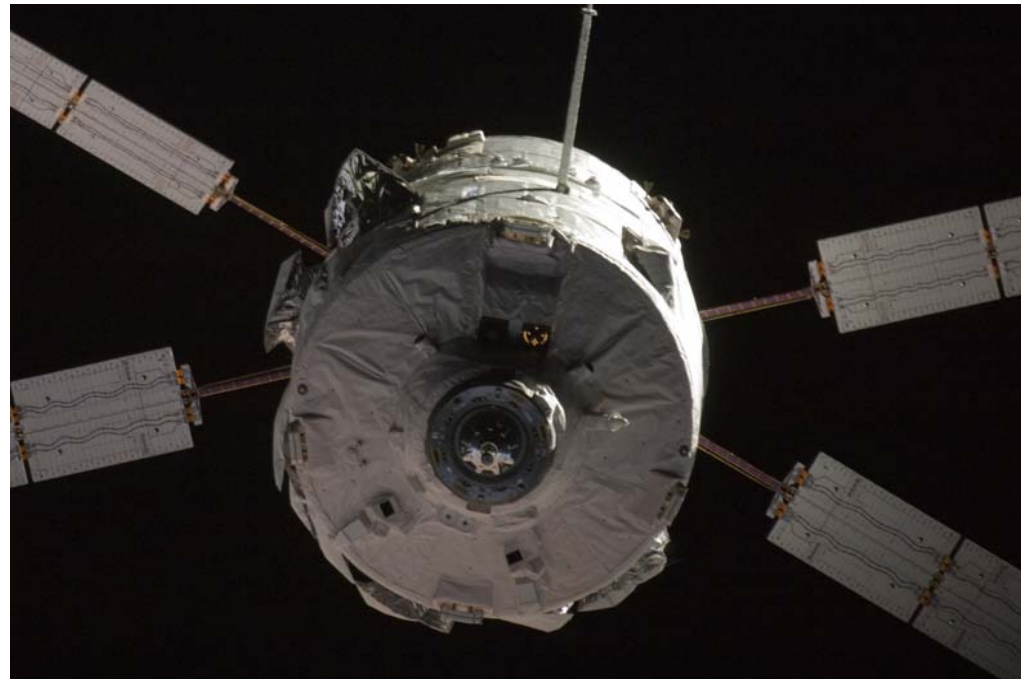




The Russian Docking System and the Automated Transfer Vehicle: a safe integrated concept

M.Cislaghi, C.Santini (ESA / ESTEC / ATV Project)



ISS016E034176



Human Spaceflight
SPACE FOR LIFE

**Vladimir Syromyatnikov (1933-2006) – Rocket & Space Corporation “Energia”
Inventor and Designer of the Russian Docking System**

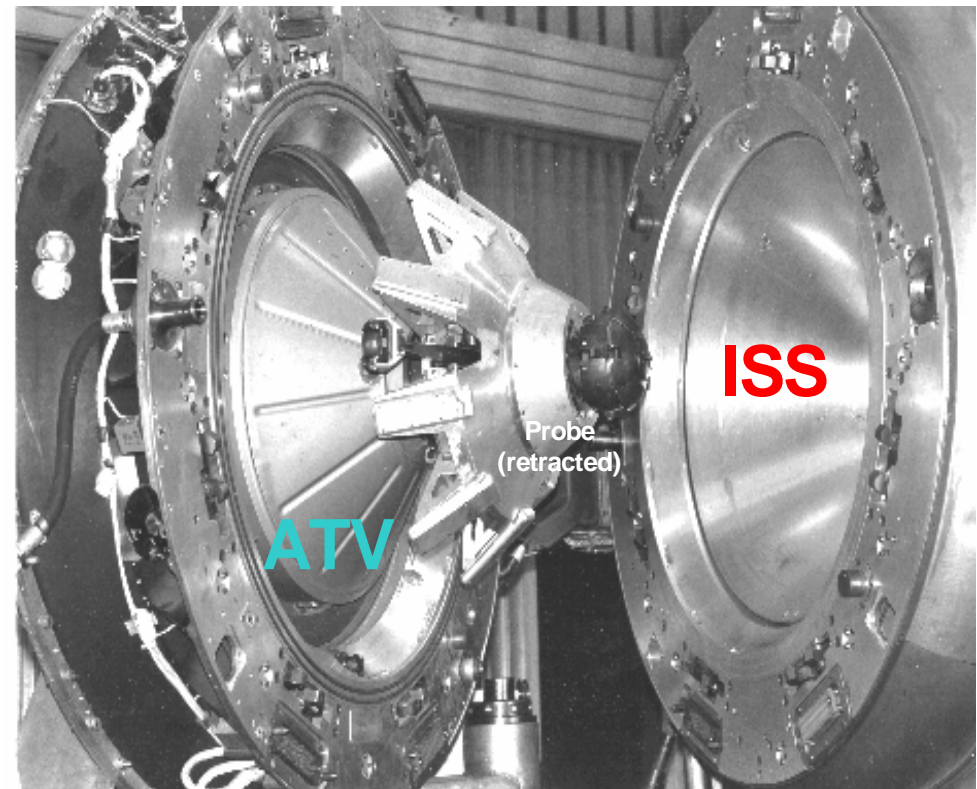
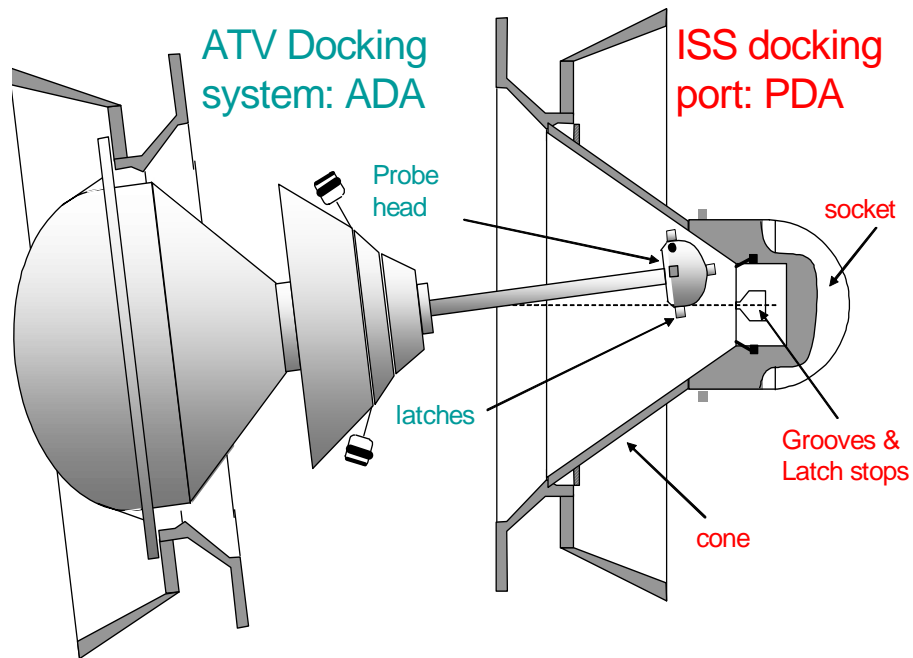




ATV / RDS integration – historical data

- “Probe-and-Drogue” Russian Docking System initially designed by RSC-Energia in the sixties, first successful in-orbit utilisation in 1971 (docking to Salyut-1), several versions developed since then, standard mechanism for all Russian Vehicles / Stations dockings
- ESA decision in 1994 to use the RDS on the ATV, integration work started in 1996, initially led by ESA and gradually taken over by Aerospatiale / EADS-ST (now Astrium-ST) with Alenia Spazio (now TAS-I) on ATV side, and by RSC-Energia on RDS side (with Roscosmos acting as formal Russian interface to ESA)
- Different technical cultures, technical standards and more stringent safety requirements to be integrated as well, not only mechanical / electrical / functional interfaces !
- Joint ESA / Russian decision for RDS avionics modernisation (see later) taken in 1999
- First RDS Flight Model mechanically integrated on ATV1 “Jules Verne” in August 2003
- Qualification of the RDS specific functionalities for ATV completed in summer 2006
- ATV / ISS docking performed on 3rd April 2008, undocking on 5th September

ATV to ISS docking using the Russian Docking System





RDS / ATV integration

Implemented at three levels:

- the Active Docking Assembly (and the Passive Docking Assembly on ISS side) --> re-used quasi "Off-the-Shelf" from Russian vehicles
- the associated control electronics --> deeply modernised or newly developed for ATV
- the ATV on-board software for docking and undocking functions --> entirely new development

Main functionalities in attached phase:

- structural connection between ISS and ATV
- passageway for pressurised cargo transfer in both directions
- transfer of ATV fuel to ISS tanks
- transfer of ISS power to the ATV
- communication between ATV and ISS-RS computers

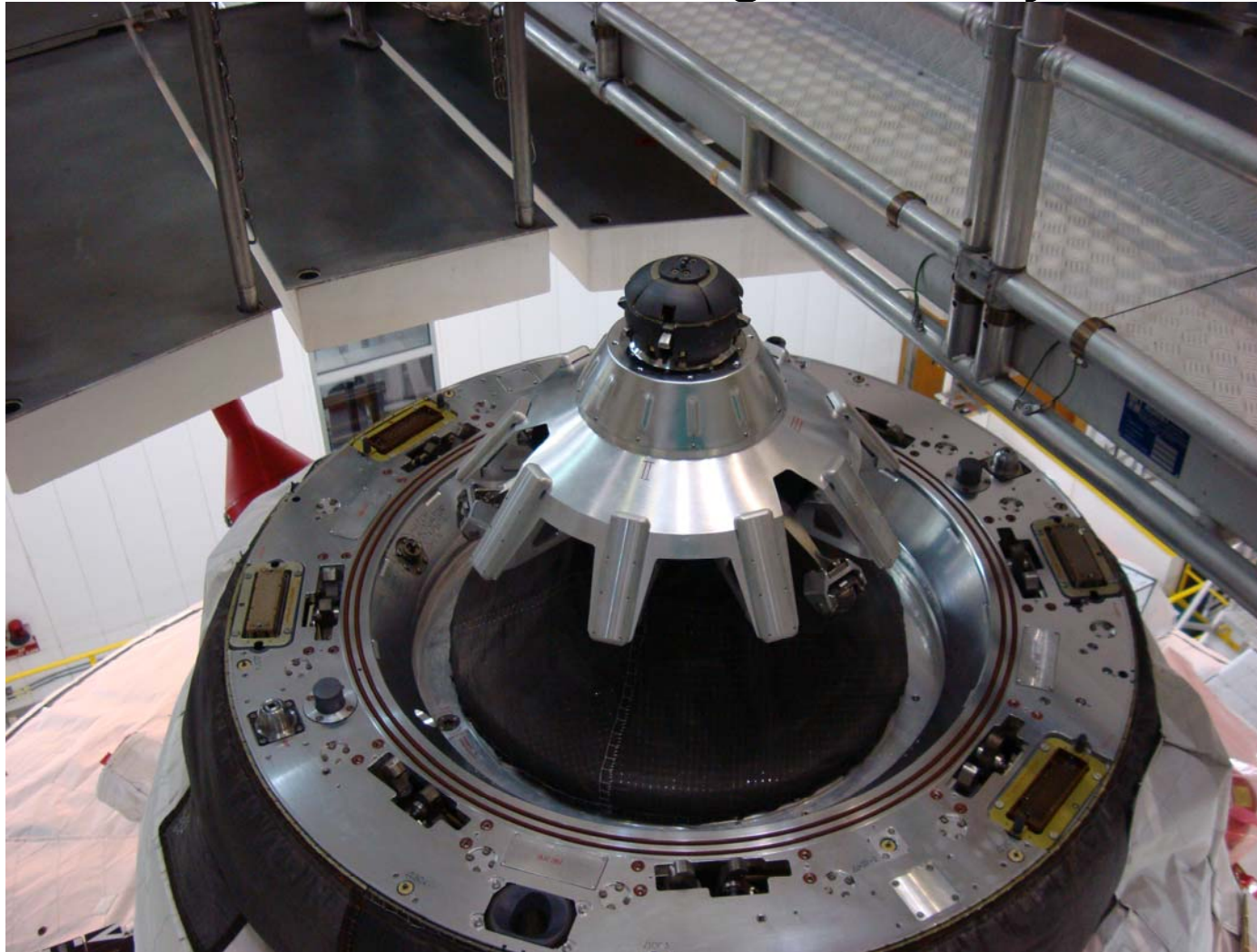
Main functionality during docking / undocking phases:

- establishment (respectively termination) of a stable ATV / ISS attached configuration in safe manner for the ISS and its crew in a highly dynamic, close proximity environment



Human Spaceflight
SPACE FOR LIFE

The Active Docking Assembly

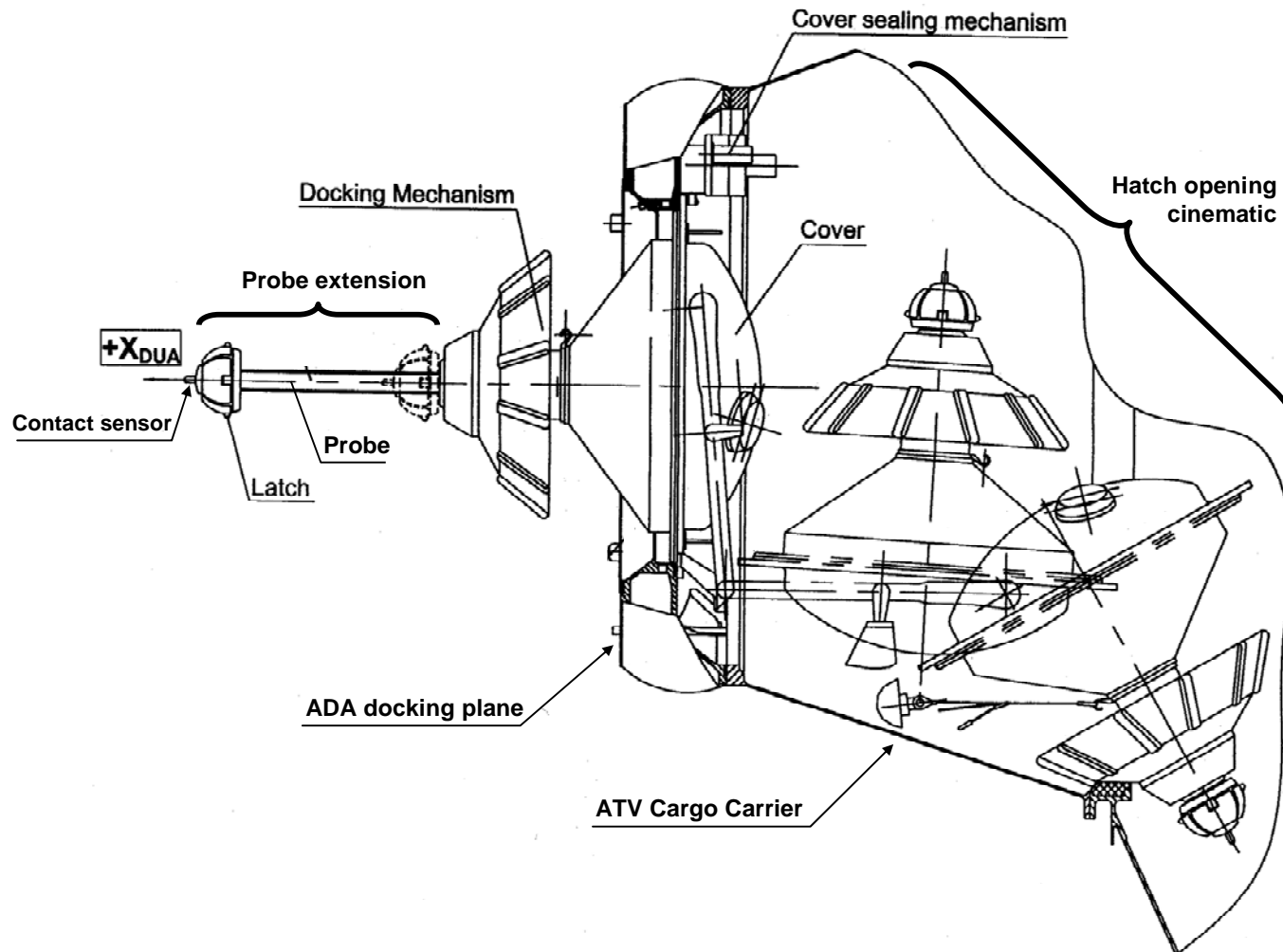




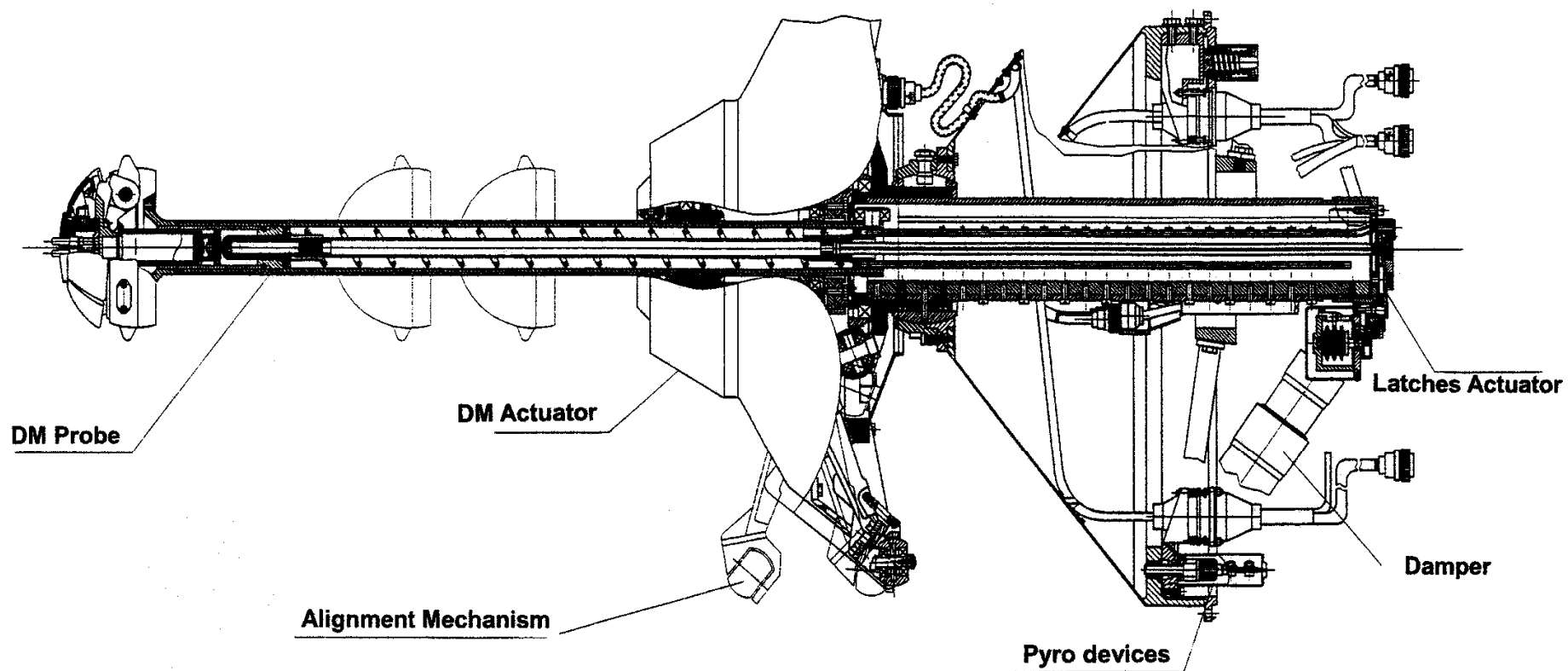
Active Docking Assembly constituents

- a probe with sensitive head to detect contact with ISS, and ensure ATV vehicle capture
- a docking mechanism, providing damping of docking energy and probe retraction with recovery of linear and angular misalignments until final contact of the docking planes
- a sealing mechanism, ensuring rigidity and hermetic sealing at the interface between the two vehicles by means of hooks closing (and vice-versa at undocking)
- a hatch cover with its own opening / sealing mechanism
- one male and one female fluidic connectors for transfer of fuel and oxidiser to the ISS tanks
- four male / female electrical connectors for power and data exchanges between ISS and ATV
- one pressure release valve for evacuation of the air in the ADA / PDA cavity
- one pressure equalisation valve to be used before hatch opening
- various types of analogue and digital sensors
- pyrotechnic devices for emergency separation

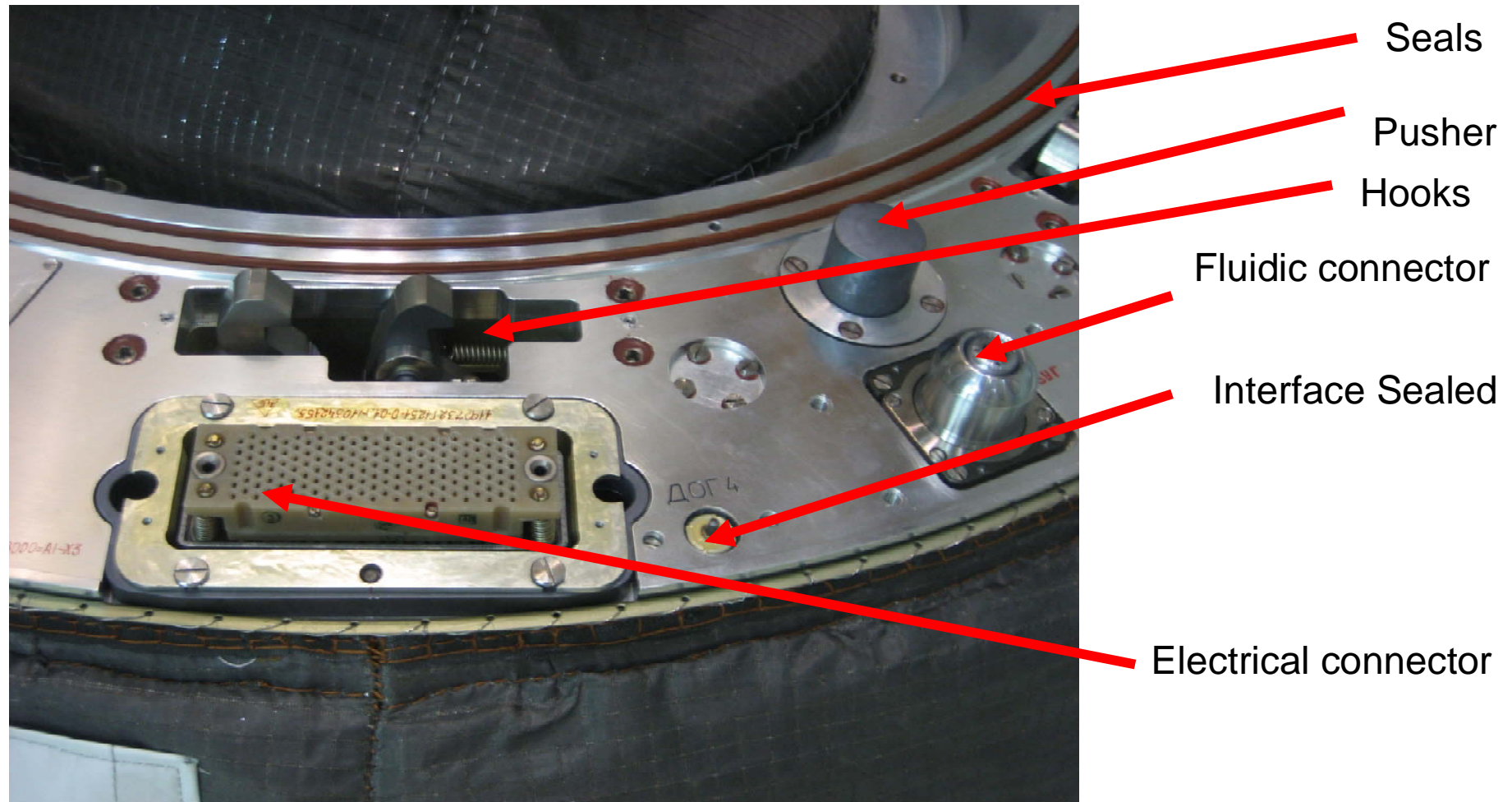
Active Docking Assembly lay-out



Detail of the ADA Docking Mechanism



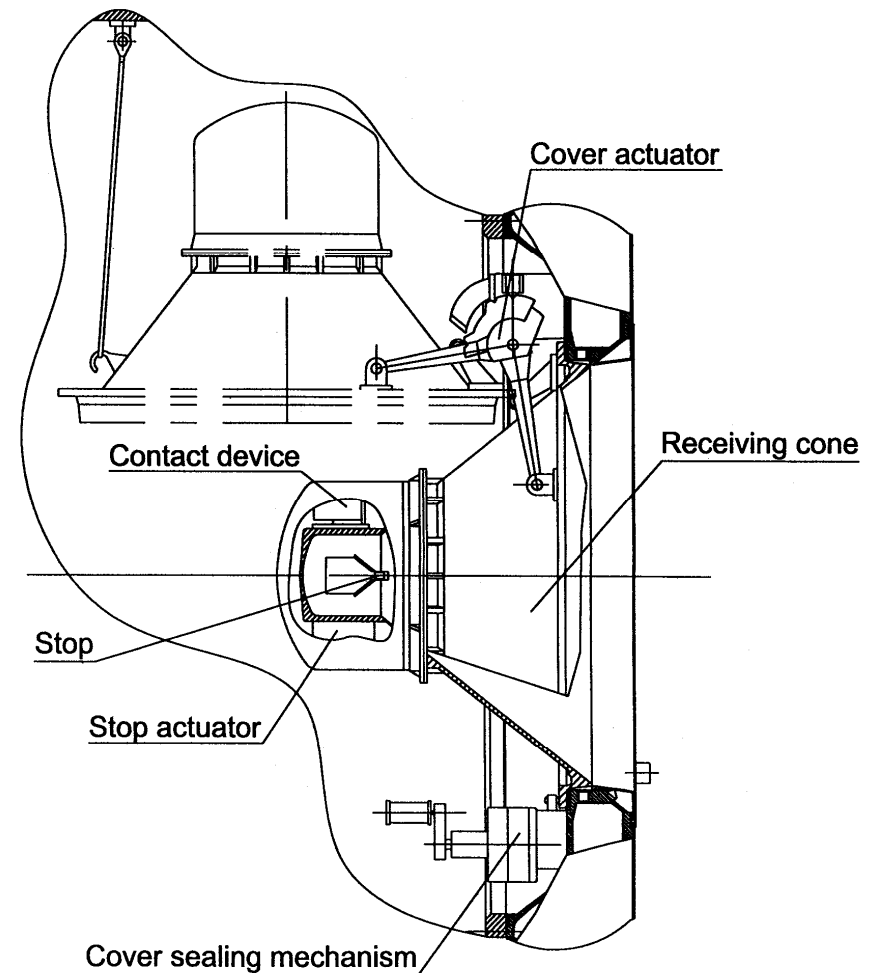
Details of the ADA / PDA interface



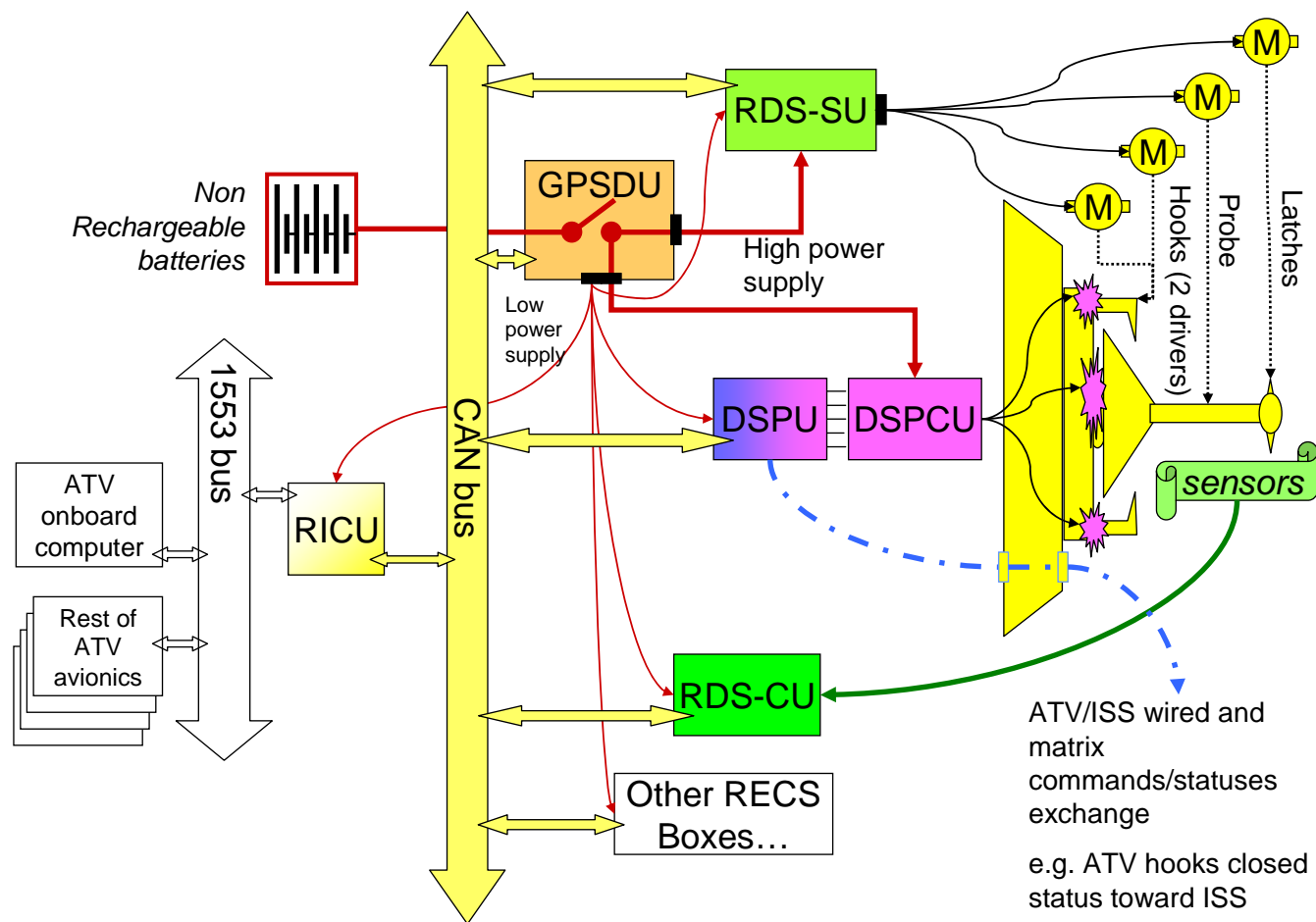
The Passive Docking Assembly

Includes the following main elements:

- a receiving cone, which guides the ADA probe head into the PDA Socket where the ATV mechanical capture will be achieved
- a socket, containing sensors to detect the probe head, and grooves for ATV capture and roll alignment
- a structural ring carrying the ISS hooks, the electrical and fluidic connectors, the post-release distancing pushers and various sensors
- a hatch cover with levers for manual opening / closing
- etc.



Avionics architecture for RDS





RDS Avionics

- Integrated within the so-called Russian Equipment Control System (RECS)
- Physically installed inside the ATV pressurized module
- Developed for the ATV, or modernised from Russian Vehicles (e.g. adding the capability to operate in vacuum)
- Based on Controller Area Network (CAN) data bus communication architecture, and including the following units relevant to the RDS functionalities:
 - the RICU, connecting the whole RECS to the rest of the ATV avionics
 - the GPSDU, supplying low power and high power to the whole RECS
 - the RDS Switching Unit, switching the ADA electrical drivers and other mechanisms such as the pressure release valve and the electromagnetic brake
 - the RDS Control Unit, performing the logical processing of the signals from the ADA sensors and actuators contact devices, ensuring the signal exchange at the RDS / ATV interface and controlling the RDSSU via the CAN bus
 - the DSPCU, firing the pyrotechnic devices on the ADA
 - the DSPU, controlling the DSPCU and exchanging statuses and commands with the ISS via wired and matrix links once the PDA / ADA electrical connectors are mated

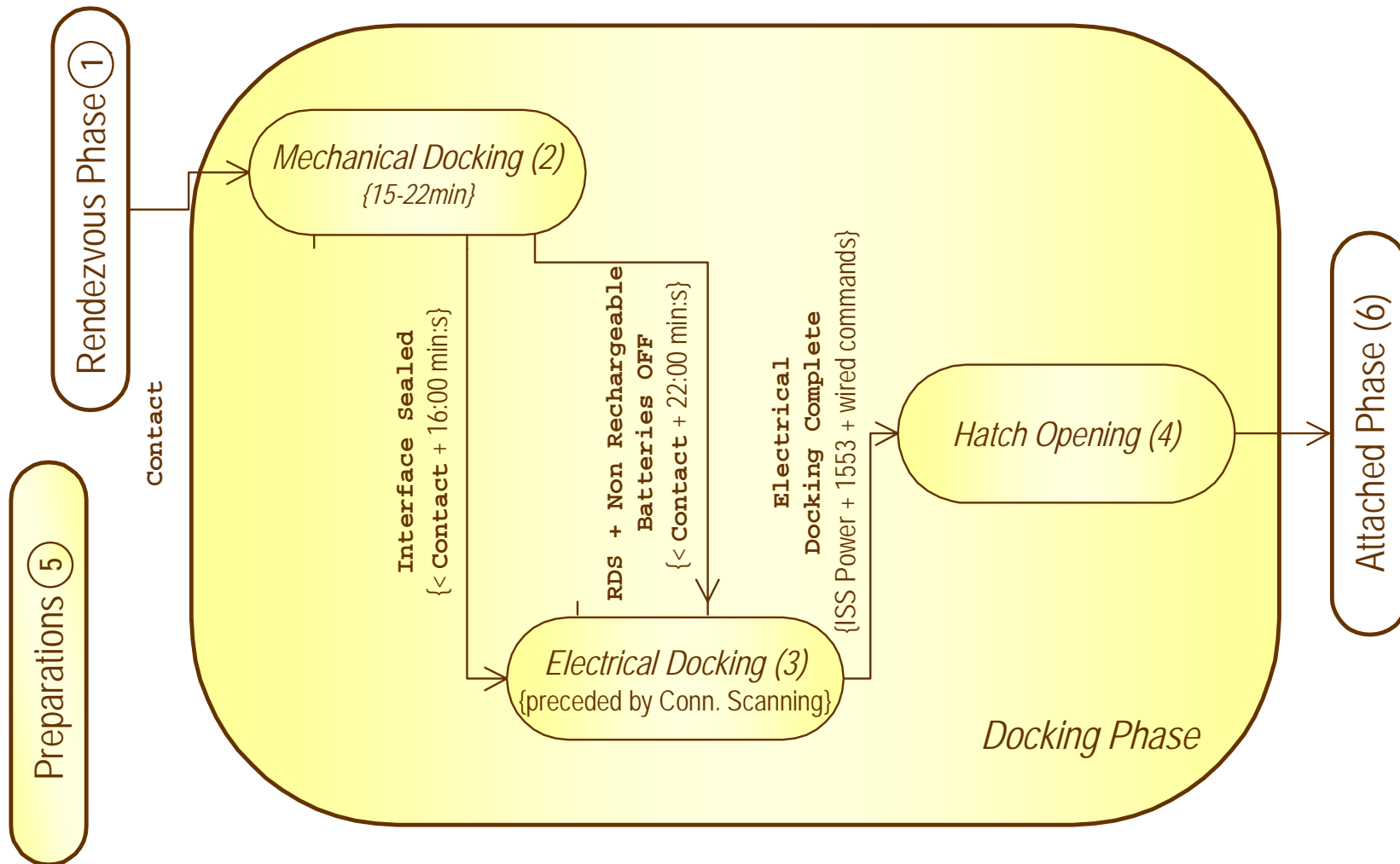


RDS / ATV interfaces

The ATV Flight Application Software controls the docking / undocking process by means of ADA signals provided to the ATV Fault Tolerant Computer (FTC). This includes tasks such as:

- monitoring the RDS (and RECS) parameters
- performing on-board FDIR interventions as required
- at docking, disabling the automatic vehicle control since the first ATV / ISS contact, and
- performing a “post-contact” thrusters firing required to achieve the correct ATV capture, or
- enabling a fly-away manoeuvres in case of failure of the docking operation
- at undocking, providing detection of the separation in order to enable the ATV control for departure
- etc.

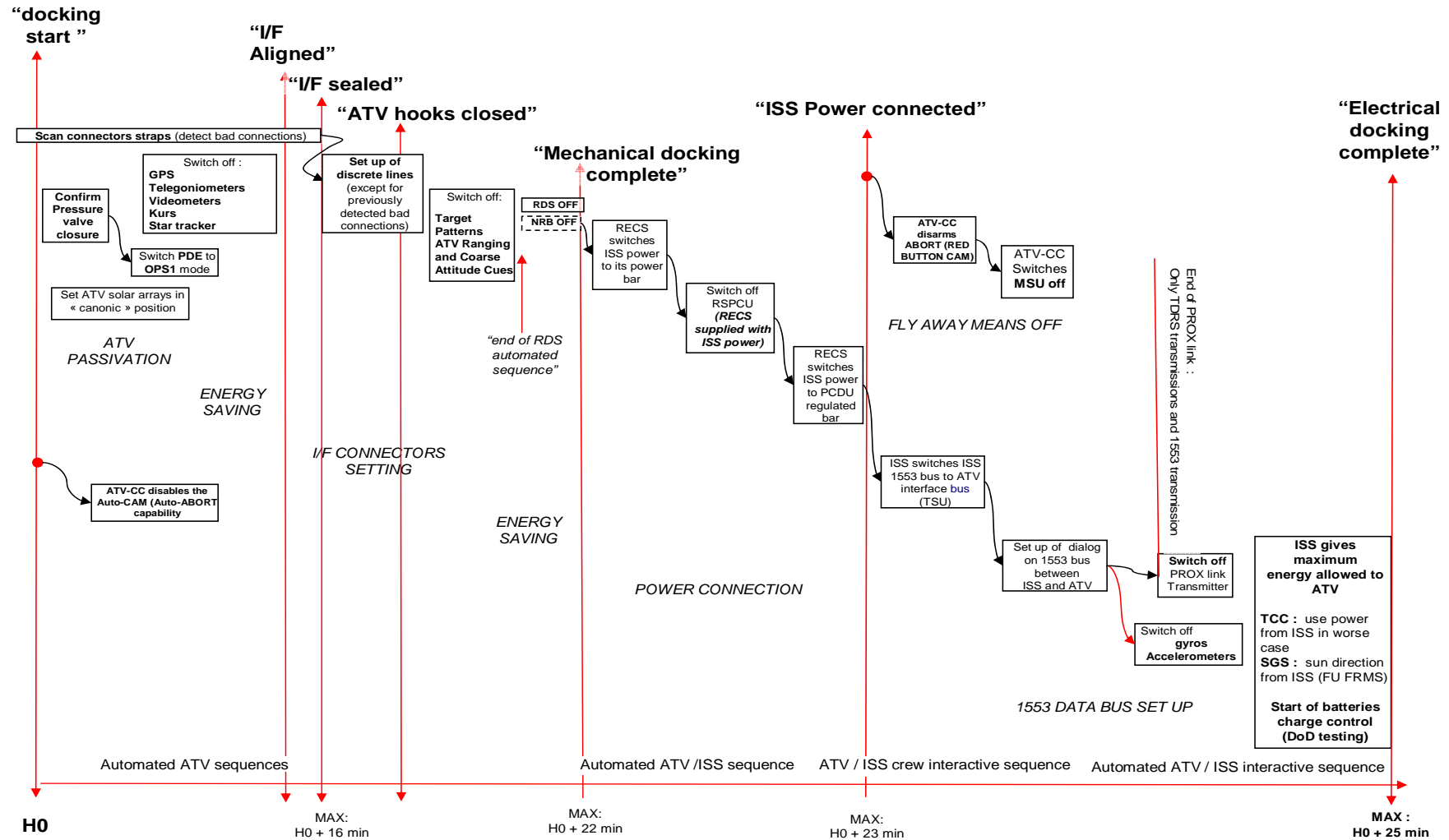
Docking sequence





Human Spaceflight
SPACE FOR LIFE

Docking detailed sequence



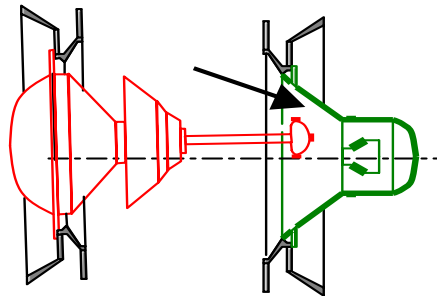


Nominal docking process

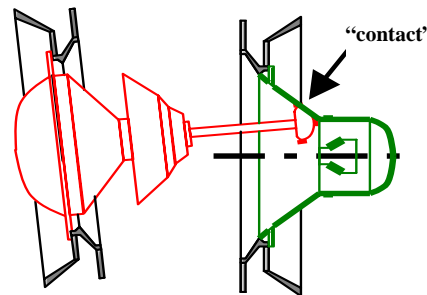
- First ATV contact with the ISS happens within the following dynamic envelope:

Relative longitudinal velocity	0.05-0.10 m/s	Relative total lateral velocity	< 0.02 m/s
Relative angular rate (pitch/yaw)	< 0.15 °/s	Relative angular rate (roll)	< 0.4 °/s
Lateral misalignment/eccentricity	< 0.10 m	Misalignment of long. axes (roll)	< 5.0 deg.
Misalignment of long. axes (pitch/yaw)	< 5.0 deg.		
- At ADA probe contact with ISS, a post-contact force is initiated by the ATV computer for a maximum of 10s, to force the probe into the socket
- Upon capture event the ISS goes into free drift
- Mechanical docking automatically carried out by the RDS without any external command
- Upon “Mode Executed” event generated by the RDS at the end of the automated mechanical docking sequence the FTC switches off the RDS and the Non-Rechargeable Batteries
- Electrical Docking interactively executed between ATV and ISS, completed when ATV and ISS power, wired commands / signals and data handling (Mil-1553) are connected
- Hatch opening is an essentially crew actuated operation, after which the ATV attached phase operations start

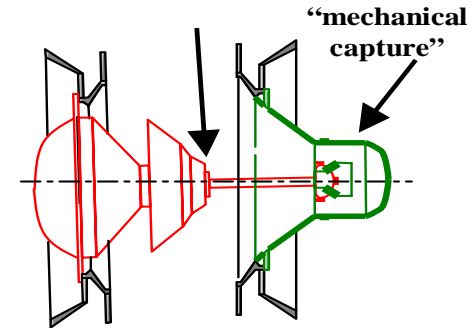
Mechanical docking sequence



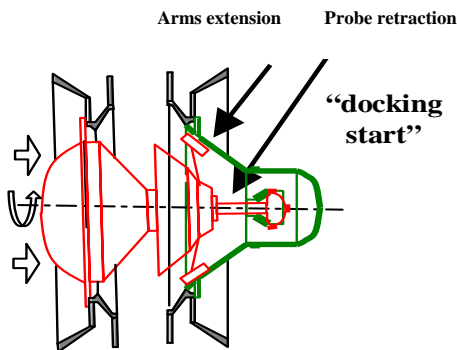
ATV probe is at less than 74cm from ISS PDA docking cone.
ATV can not avoid touching the cone



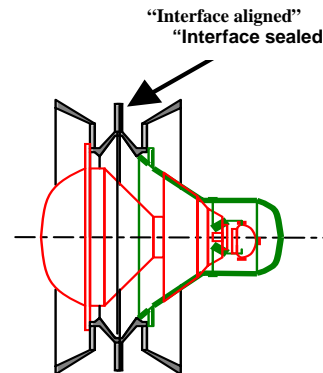
1st Contact : probe head touches ISS PDA cone.
“post contact thrust” done by propulsion



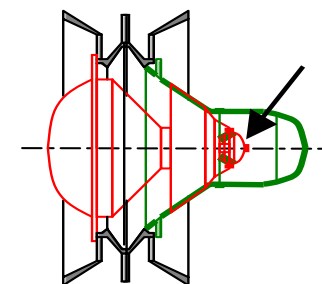
Probe head into PDA socket.
ATV movement damping (EMT brakes on)



Probe retraction:
levers extension for
ATV aligning.

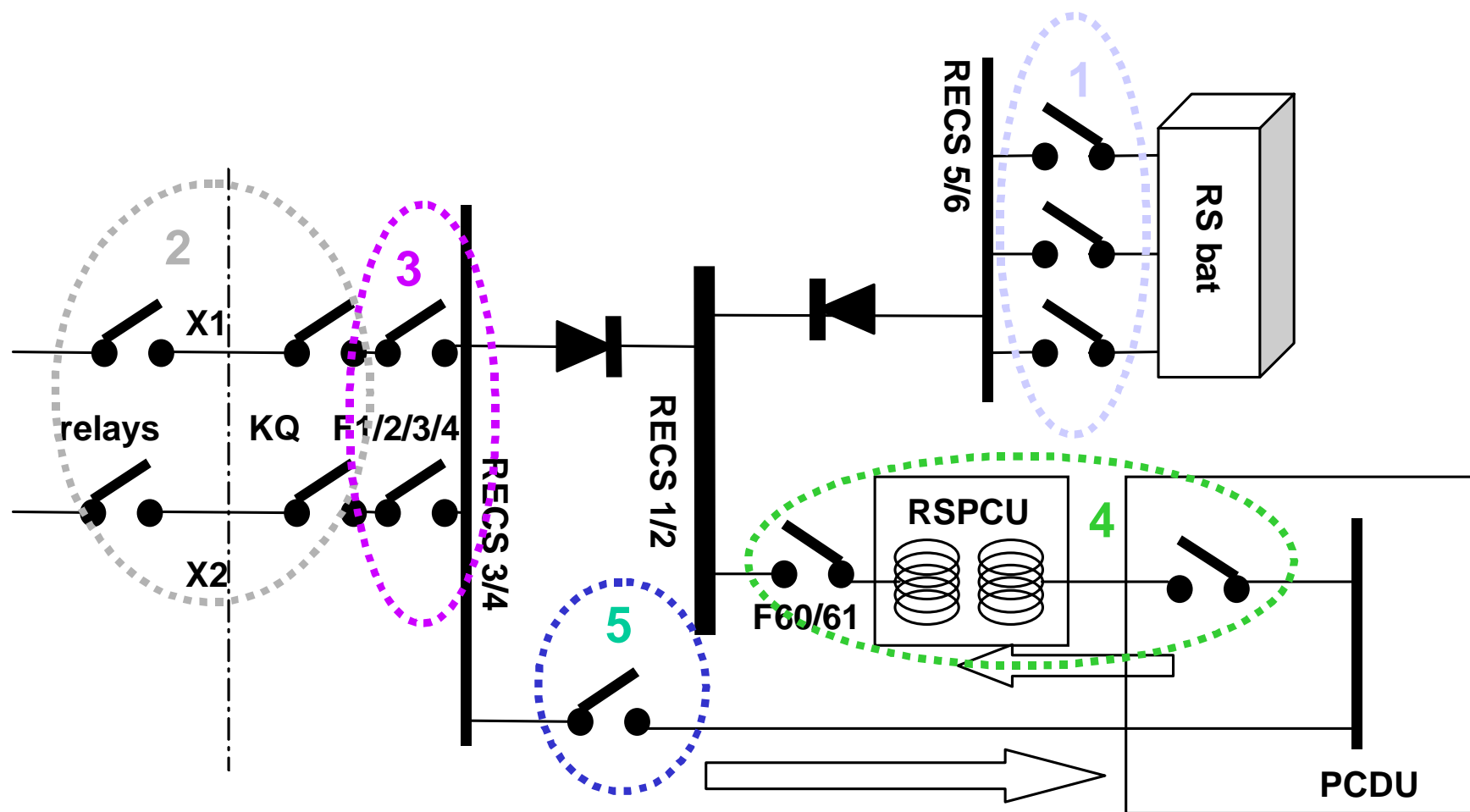


Interface aligned : ISS and ATV interface rings touch
Interface sealed : ATV hooks are closed
ISS hooks closed upon ATV wired status

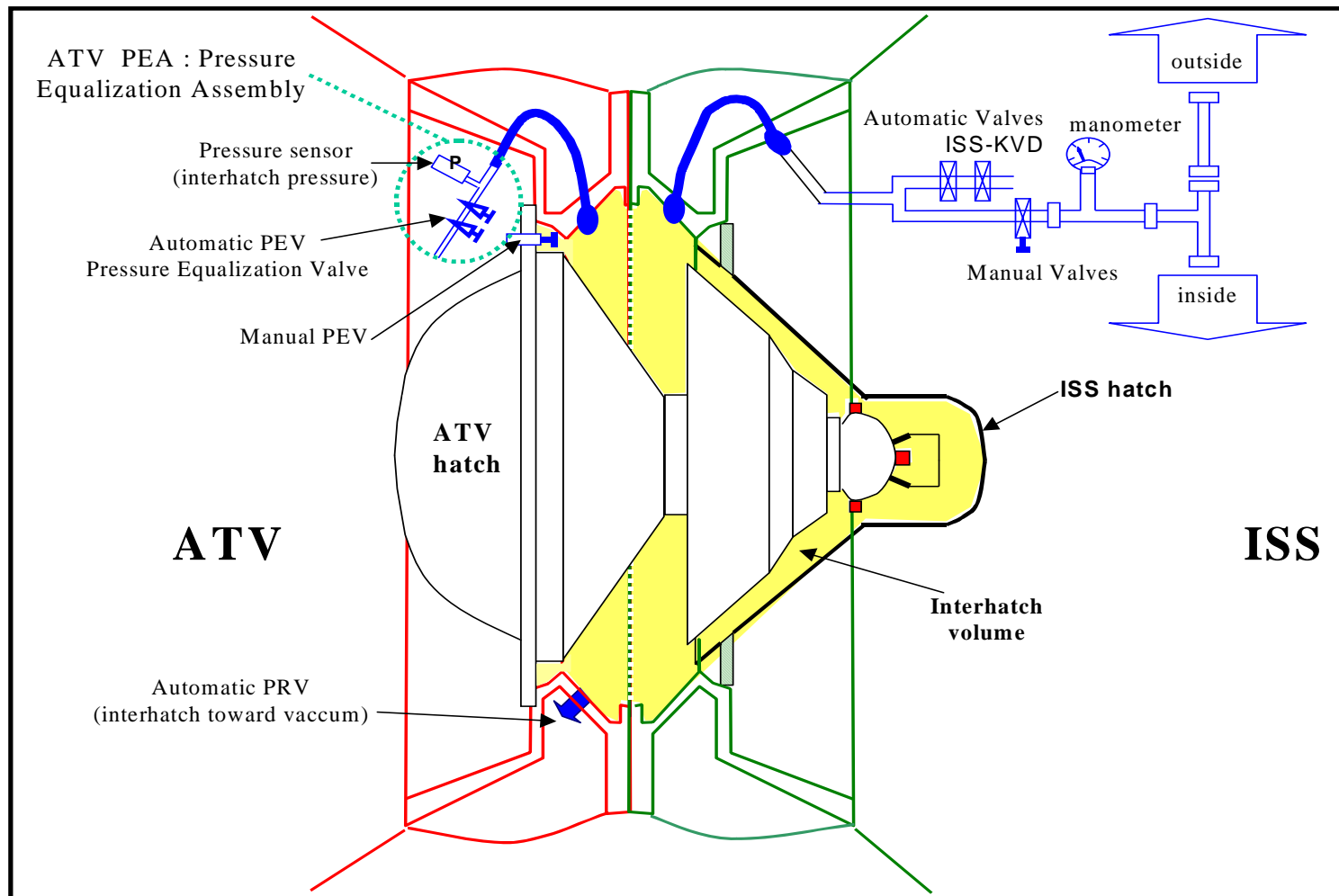


latches retraction and probe
final retraction :
ADA in “stow” configuration

Electrical docking sequence



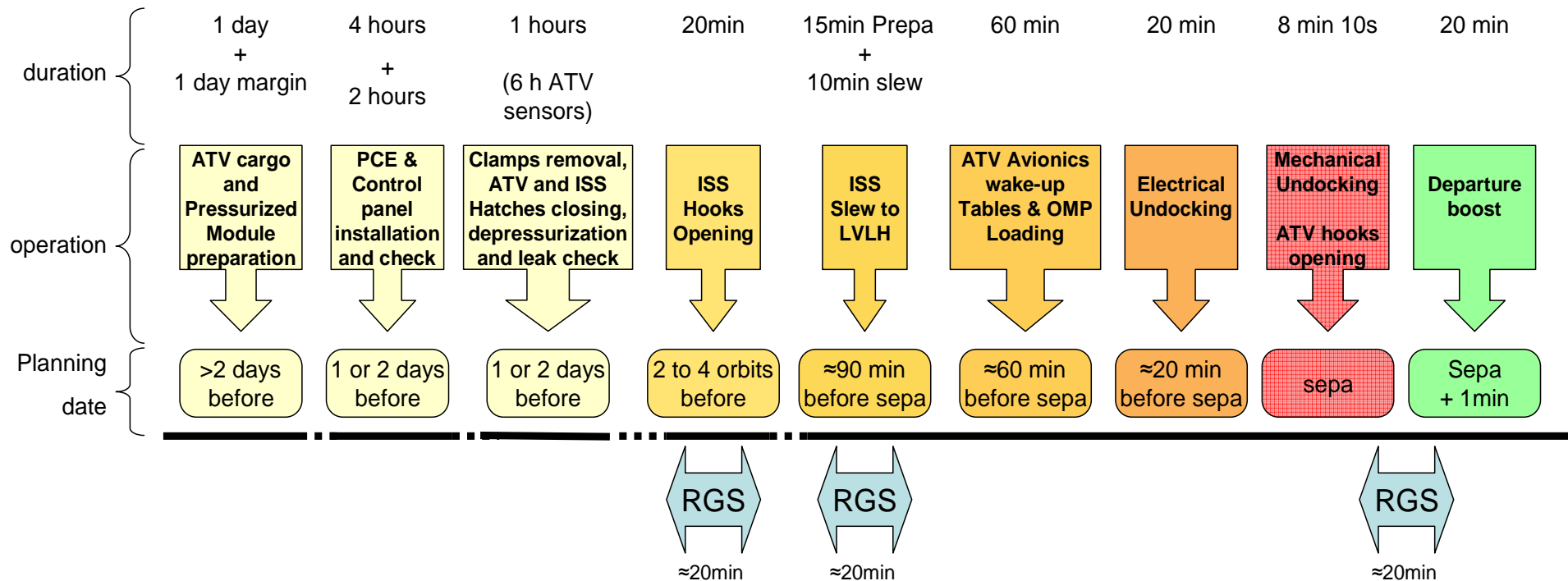
Inter-hatches pressure management devices





Human Spaceflight
SPACE FOR LIFE

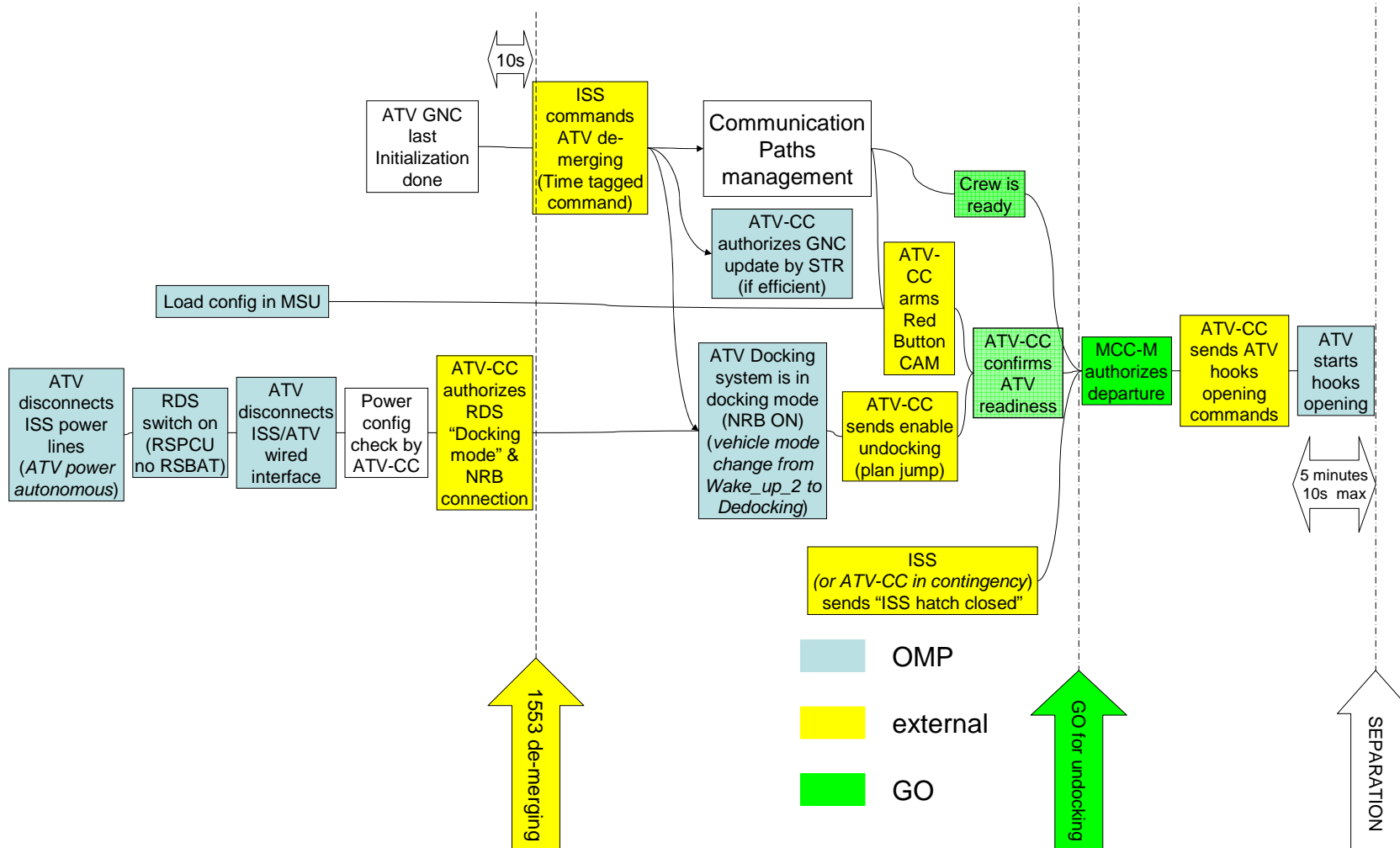
Nominal undocking sequence



Additionally, not noted in the above chart:

- manual disabling of the safety barrier for RDS pyros before closing the ATV hatch
- disconnection of the ISS/ATV communication bus about 10 min before mechanical separation
- first distancing impulse provided by spring pushers on ADA and PDA rings
- detection of separation performed by ADA and PDA sensors

Undocking integrated logic





RDS safety overview

The RDS is one-Failure-Tolerant for nominal operations of the system and two-Failures-Tolerant for contingency operations preventing catastrophic consequences.

Before contact with the ISS, the ATV is autonomously capable of retreating to a safe position, triggered by its own on-board failure detection algorithms.

As a rule, no external interventions by either control centres or ISS Crew are needed during the docking process to satisfy the required levels of failure tolerance.

However some exceptions have been identified by a thoroughly performed RDS FMECA as potentially inducing risks on the ISS for the docking phase:

- during final approach 3 double failures generate “feared events” not controlled at RDS level:
 - a) the absence of detection of physical contact with ISS,
 - b) the untimely detection of physical contact with ISS when ATV is still away from ISS
 - c) the ADA in wrong configuration for docking
- when the RDS is performing the junction of ATV and ISS, the residual system-level dangers are the impossibility to finish mechanical and electrical docking within the allowed time

For these exceptions a “system-level operational recovery” has been developed.



ADA safety principles

- ADA safety based on a redundant design, as nearly all drivers' sensors and actuators are doubled, giving a complete "one failure tolerance" for the continuation of the operations, except for:
 - the probe actuator, whose reliability however has been proven by decades of flawless in-flight use
 - the latches extension / retraction driver, however in this case an equivalent action can be performed from ISS side to release the ATV probe head in case of failure
 - the pressure release valve, however also in this case ISS backup means are available to release the air trapped in the inter-hatch volume before ATV departure
- Second failure tolerance provided by the RDS pyrotechnic devices, thus emergency separation is always possible in off-nominal situations
- In turn the pyrotechnic system is 1-FT for its actual operations and 2-FT against untimely activation



RDS avionics safety principles

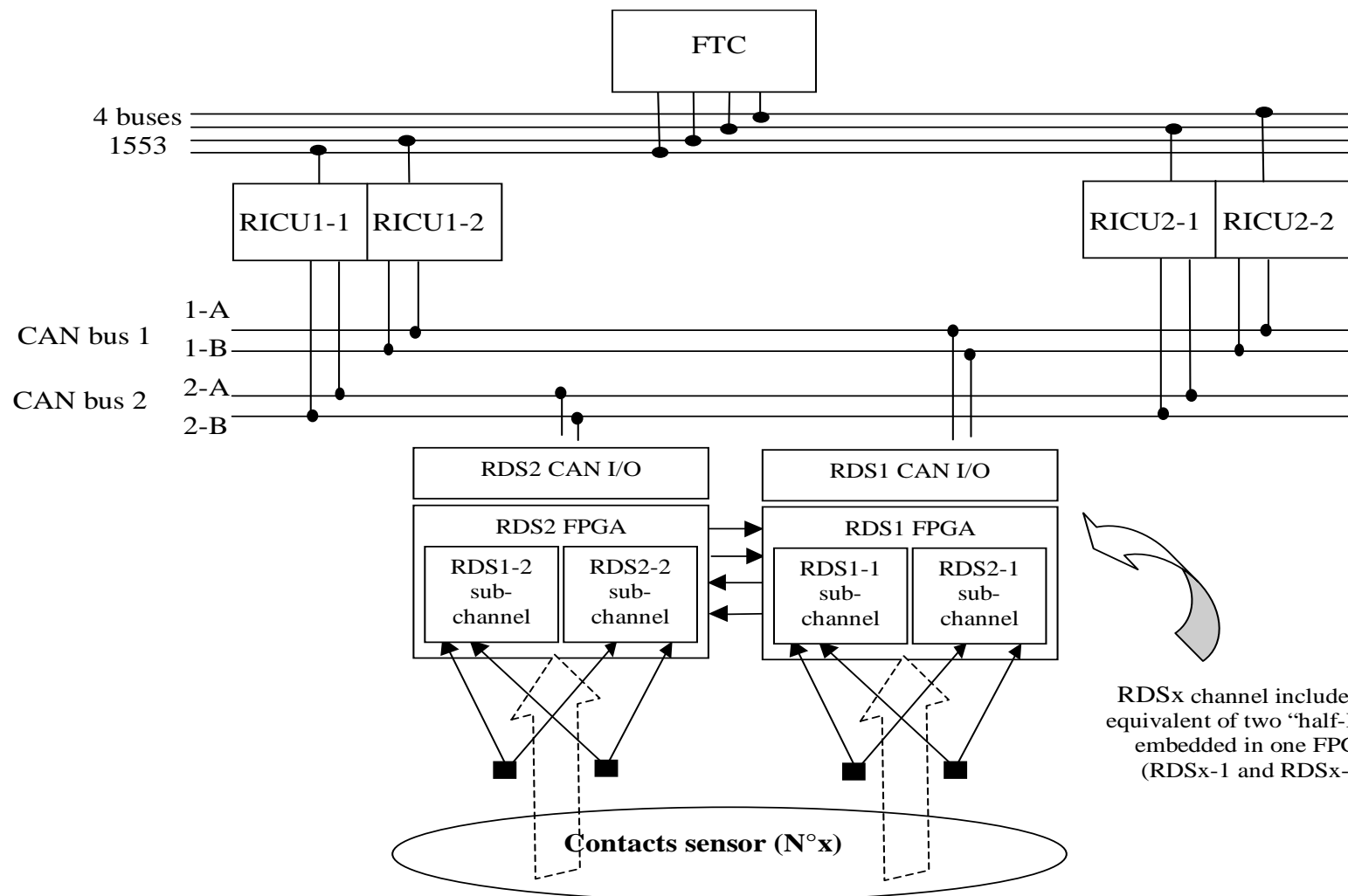
The RECS design is 2-FT for the control of the RDS:

- for nominal docking/undocking operations, there are two channels working in hot redundancy, each one using its own CAN data bus, connecting 2FT designed avionics
- for the pyrotechnic devices operation, requested only after two previous failures, 2 DSPUs and 1 DSPCU are used

The power supply design is provided with high energy margins, and its design is also 2FT:

- two lines provide the “low power” supply to the docking system, using ATV solar arrays’ generated power via two dedicated interface boxes
- at same time two Non-Rechargeable Batteries (of 3 strings each) nominally provide the “high power” to the RDS actuators, but they can also provide the complete power to the RDS in case of need

RDS avionics redundancy



RDSx channel includes the equivalent of two “half-RDS” embedded in one FPGA (RDSx-1 and RDSx-2)



RDS avionics redundancy

RICU - 2 units with 2 channels each - RECS interface with 4 ATV Mil-1553 buses and with the rest of the RDS avionics via the CAN bus – each RICU power module consisting of 2 independent lines, whose switching is controlled by an external command.

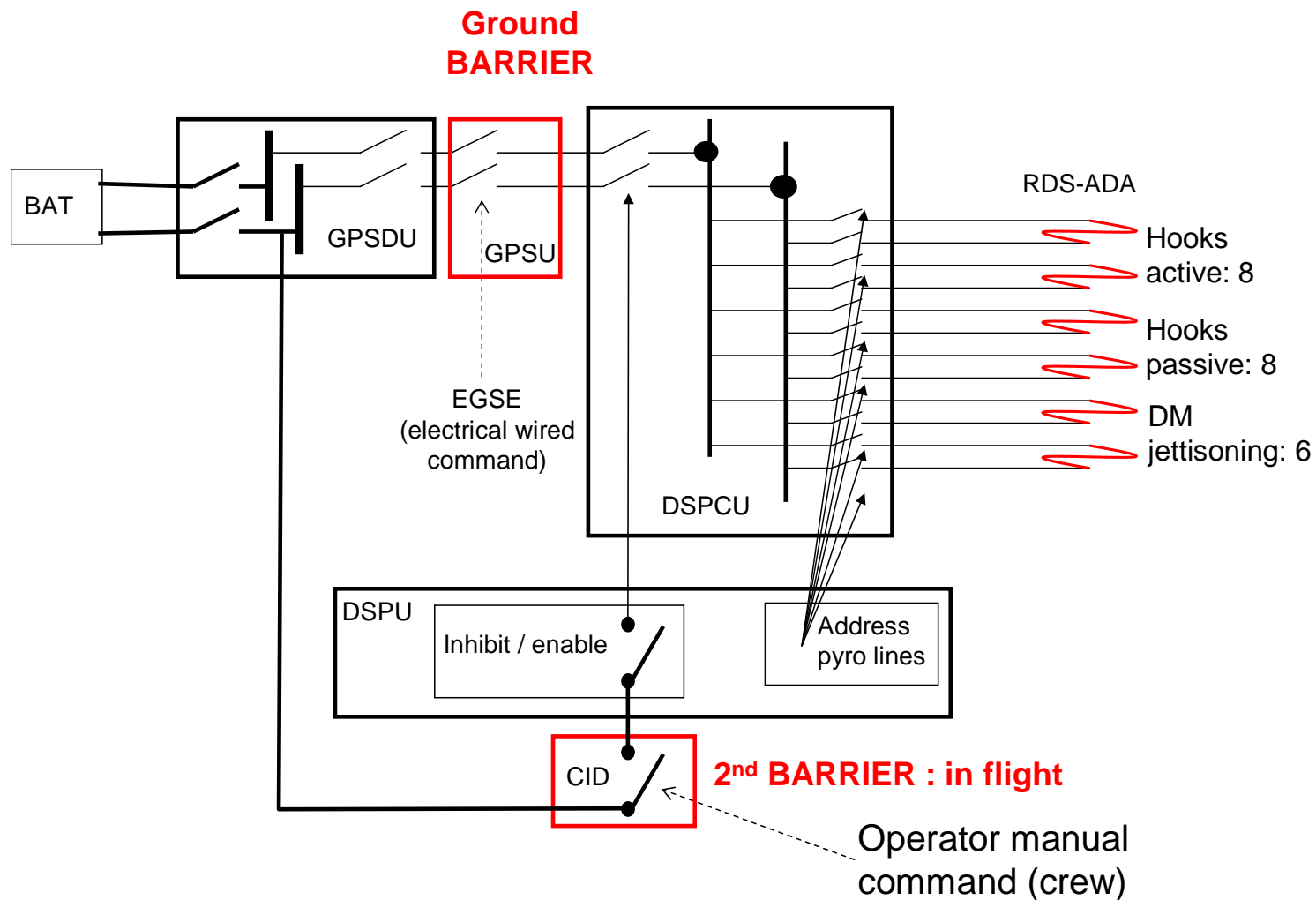
GPSDU - 1 unit with 2 redundant channels - CAN bus interface in hot redundancy and the logic module in cold redundancy – 2 low-power and 2 high-power buses - not based on PCBs but on solid copper rods supported by glass-fibre brackets with outputs to the various power users made by cables wrapped around the bus rod (Russian vehicles inheritance).

DSPCU – 1 unit reused from Russian vehicles - relay-based, two stages of commands, 1st one for low-level relays, 2nd one for power relays, commanded by the relay of the 1st stage - each stage working according to a majority law, arming commands executed only for acceptable combinations - additionally, the Crew Interlock Unit (CID) manually inhibits the DSPCU against unwanted pyrotechnic activation commands.

DSPU – 2 units, each with 2 cold redundant channels, with only one channel active at a time - can be used both in hot or in cold redundancy – each DSPU power module consisting of 3 independent lines, whose switching is commanded by an external command.

RDSSU and RDSCU – 2 different units - completely redundant design, each channel being built on 2 sub-channels that ensure its complete one failure tolerance.

Pyros control schematics





Feared event “blindness of docking sensors”

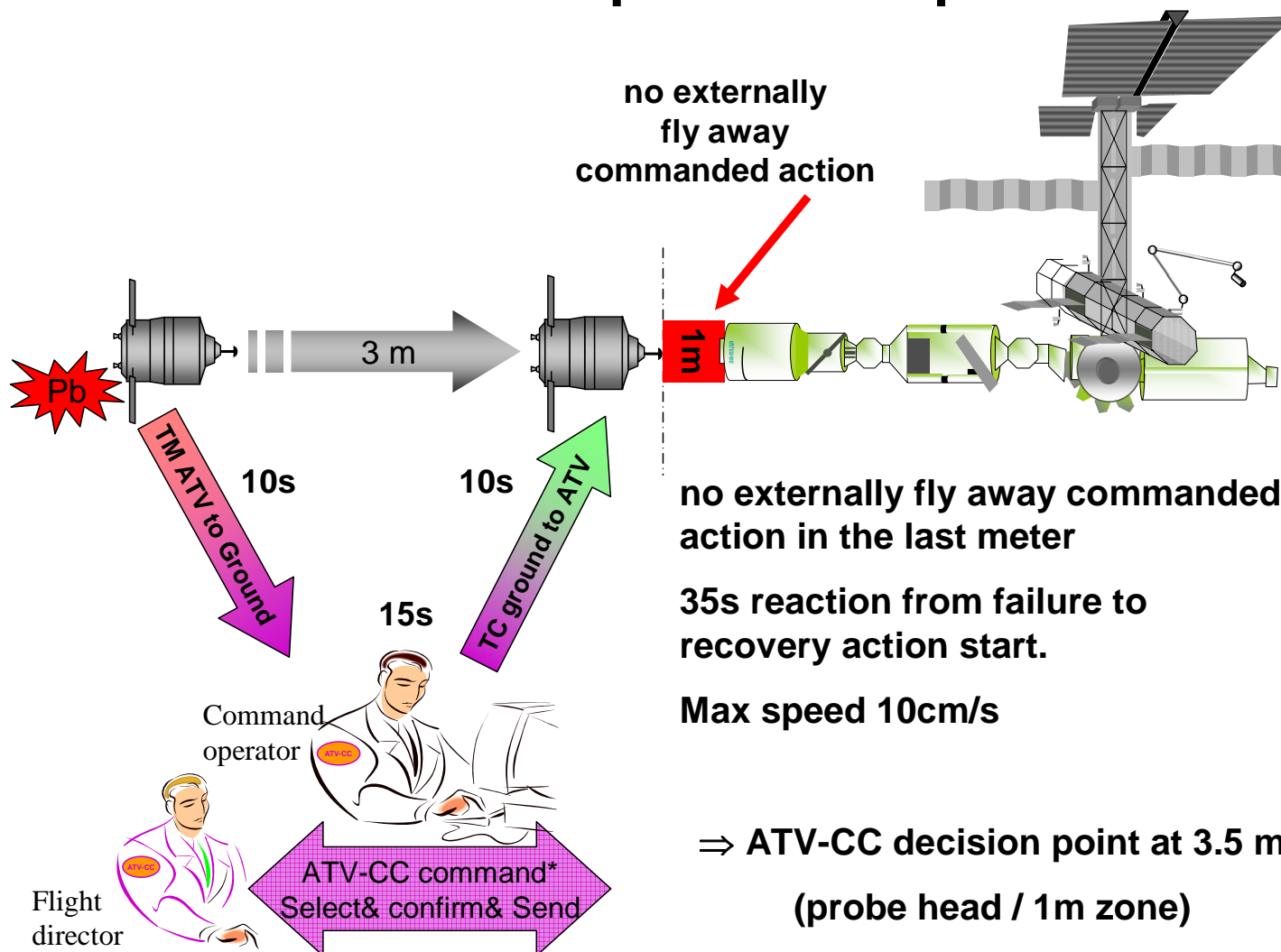
In case of inability of the docking sensors to detect the different docking events and to inform the FTC accordingly:

- the ATV computer would interpret the vehicle immobilisation as a major propulsion problem, thus switching to “survival mode” and initiating a “fly-away” (CAM) manoeuvre, and
- in survival mode the RDS would be unable to detect its failure state, and thus unable to perform any docking (and undocking).

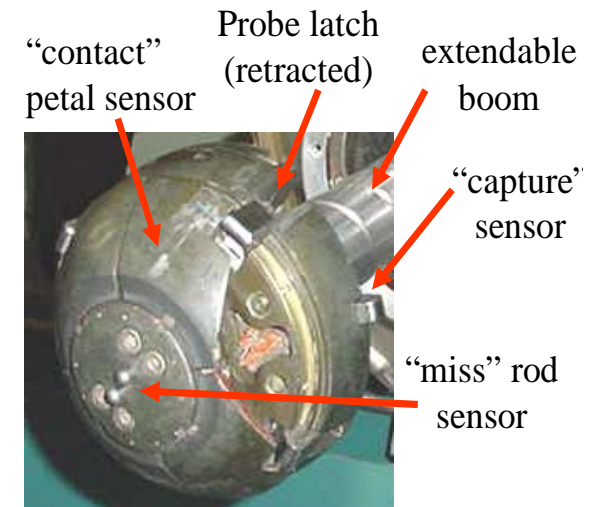
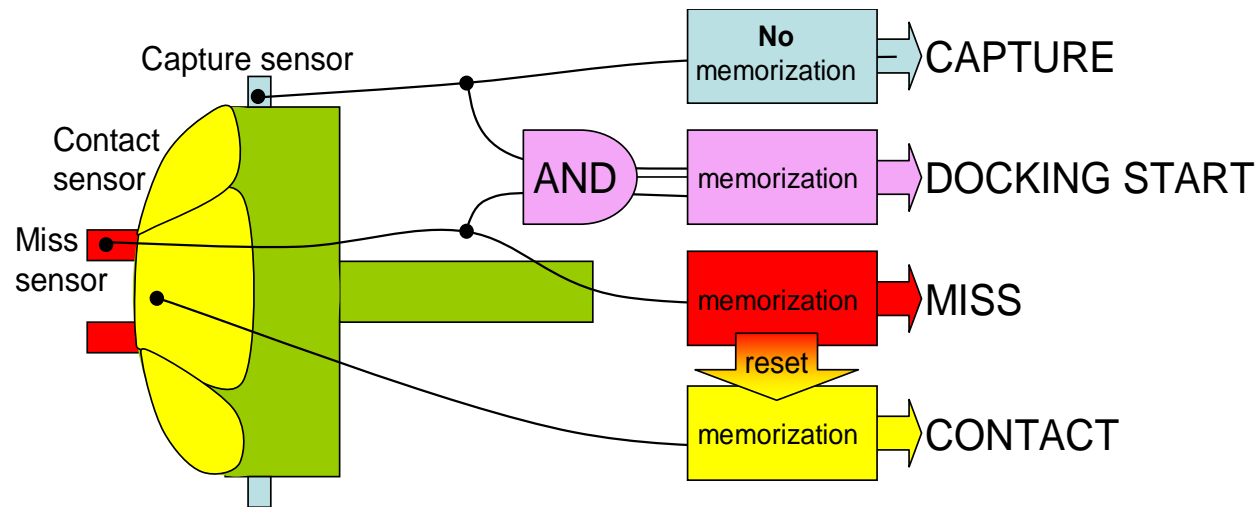
The system-level counter-measures against this case are as follows:

- at S4 hold point (20 m from ISS) ground controllers give a “No-Go for docking” in case the activation of the two RDS avionics channels is incorrect, i.e. in case of no acknowledgement of the “automatic docking” mode,
- from S4 to about 3 m from the ISS (ground control “hands-off” point) several RDS parameters not covered by on-board failure detection are constantly monitored from the ground, and if an anomaly is detected the ground controller may directly request ATV to fly away,
- if an anomaly is detected between 3 m and 1 m from the ISS, the ISS crew will be requested to command the ATV fly away manoeuvre,
- closer than 1 m from contact (crew “hands-off” point) no counter-measures are possible, because due to its inertia the ATV would be captured anyway by the ISS, however the probability of this occurrence has been assessed and accepted as negligible --> risk zero does not exist ...

Hands-off point concept



Logic on probe sensors





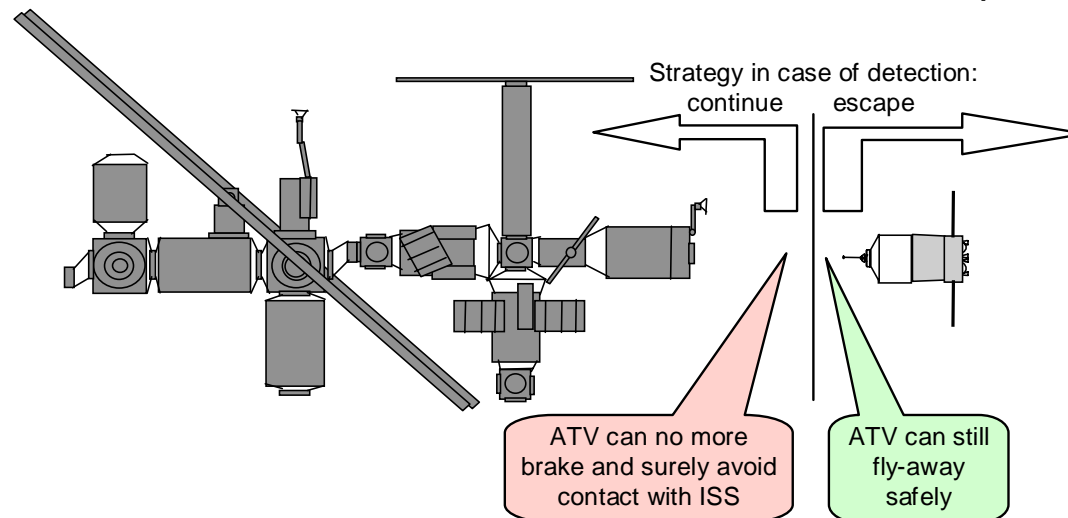
Human Spaceflight
SPACE FOR LIFE

Feared event “untimely detection of capture”

In case of capture untimely detected while the ATV is still away from the ISS, the effect would exactly contrary to the previous case, as the ATV computer would immediately disengage its flight control system, and the ATV would be in “free drift” close to the ISS.

Dynamic simulations have shown that if the loss of flight control occurs at distances of less than 1 m from the ISS, in any case the ATV still will be correctly captured (then docking will continue according to the “any attitude departure” logic – see later)

if the loss of flight control occurs outside 1 m, it can be compensated by means of an external (ISS crew or ground) intervention to command a fly-away manoeuvre, however not before a pre-defined interval of time needed to confirm that the ATV will never be captured anymore.





Feared event “untimely activation of ADA actuators”

They can either provoke the untimely release of the ATV during the docking, e.g. in case of latches retraction after capture but before hooks closing, or bring the ATV in the wrong configuration for capture, e.g. in case of probe and / or latches retraction before capture.

At first level these risks are mitigated by avionics integrity checks performed shortly before launch, to lower this kind of risk to an acceptable value.

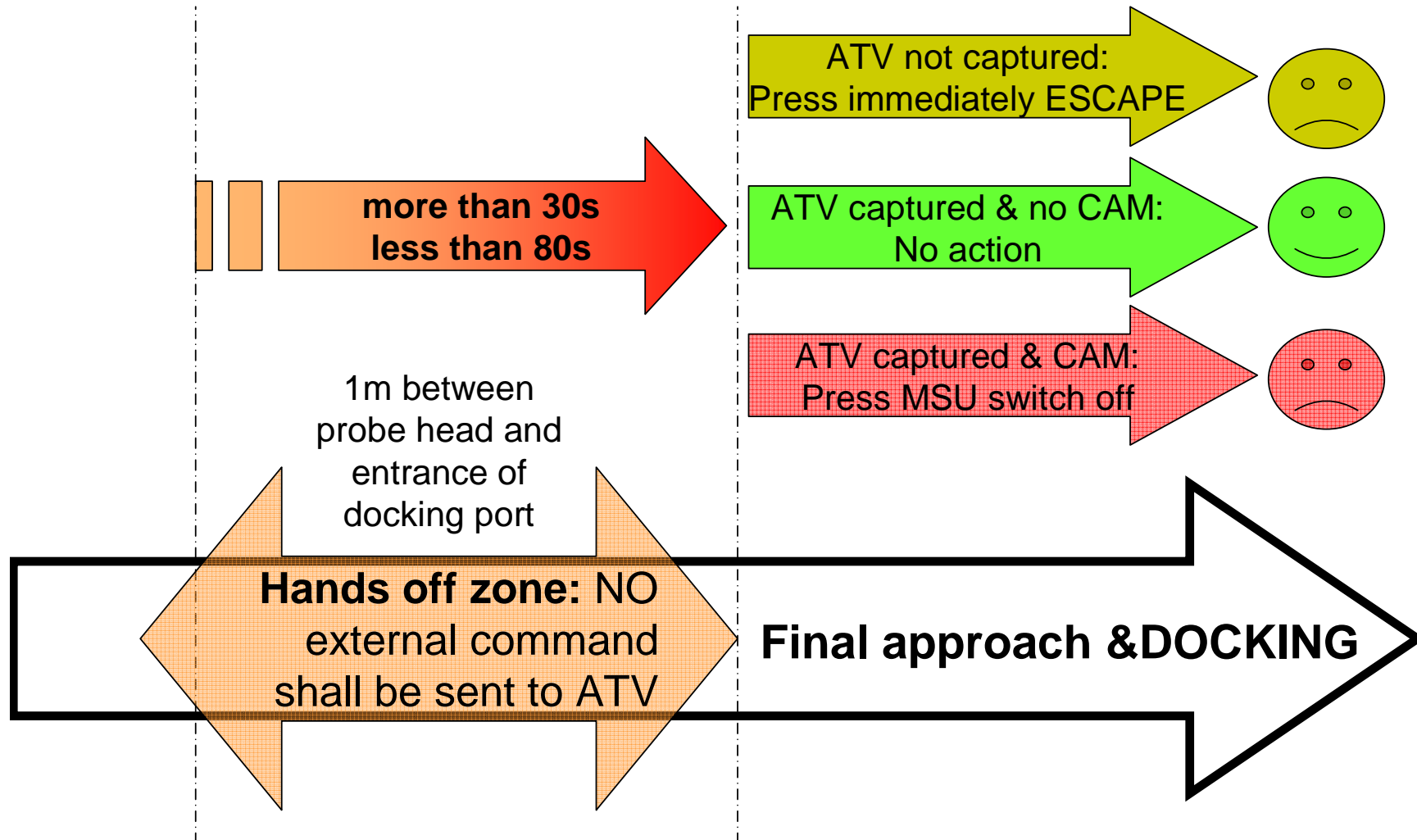
Then during flight the available counter-measures are similar to those described for the case of RDS blindness:

- several ground controls are performed to detect hidden failures of the docking system,
- at S4 hold point, ground controllers give a “No-Go for docking” in case the “Ready to dock” signal is not received from the two RDSCUs,
- from S4 to ground control “hands-off” point, there is a constant monitoring of the signal “Ready to Dock”,
- from the “hands-off” point onwards, this feared event has been accepted based on the very low credibility of the untimely actuator activation in this extremely short interval of time (some operational countermeasures are anyway still available even during this stage)



Human Spaceflight
SPACE FOR LIFE

Summary of crew actions at docking





Any attitude departure – the problem

After capture the ISS and ATV attitude are no more controlled (free drift) in order to reduce the interface loads during the initial part of the mechanical docking process.

The maximum acceptable duration of this instable situation is limited to 110 min due to:

- the need of recovering the ISS attitude, otherwise its ground communication capabilities would be compromised by the bad antennas orientation,
- the need of feeding the ATV with ISS energy, otherwise the vehicle capabilities would be gradually jeopardised.

Therefore it is necessary that either the ATV / ISS interface is stiffened with the electrical inter-connection established, or the ATV leaves the ISS within this delay.

This contingency shall be manageable by the on-board crew, at least until when the ISS+ATV attitude control resumes, due to the likely loss of ATV contact with the ground control centre.

Depending on the step of the docking sequence when the contingency occurs, on the achieved mechanical stiffness and on the ATV fly-away capability, a specific safety scenario has been developed.



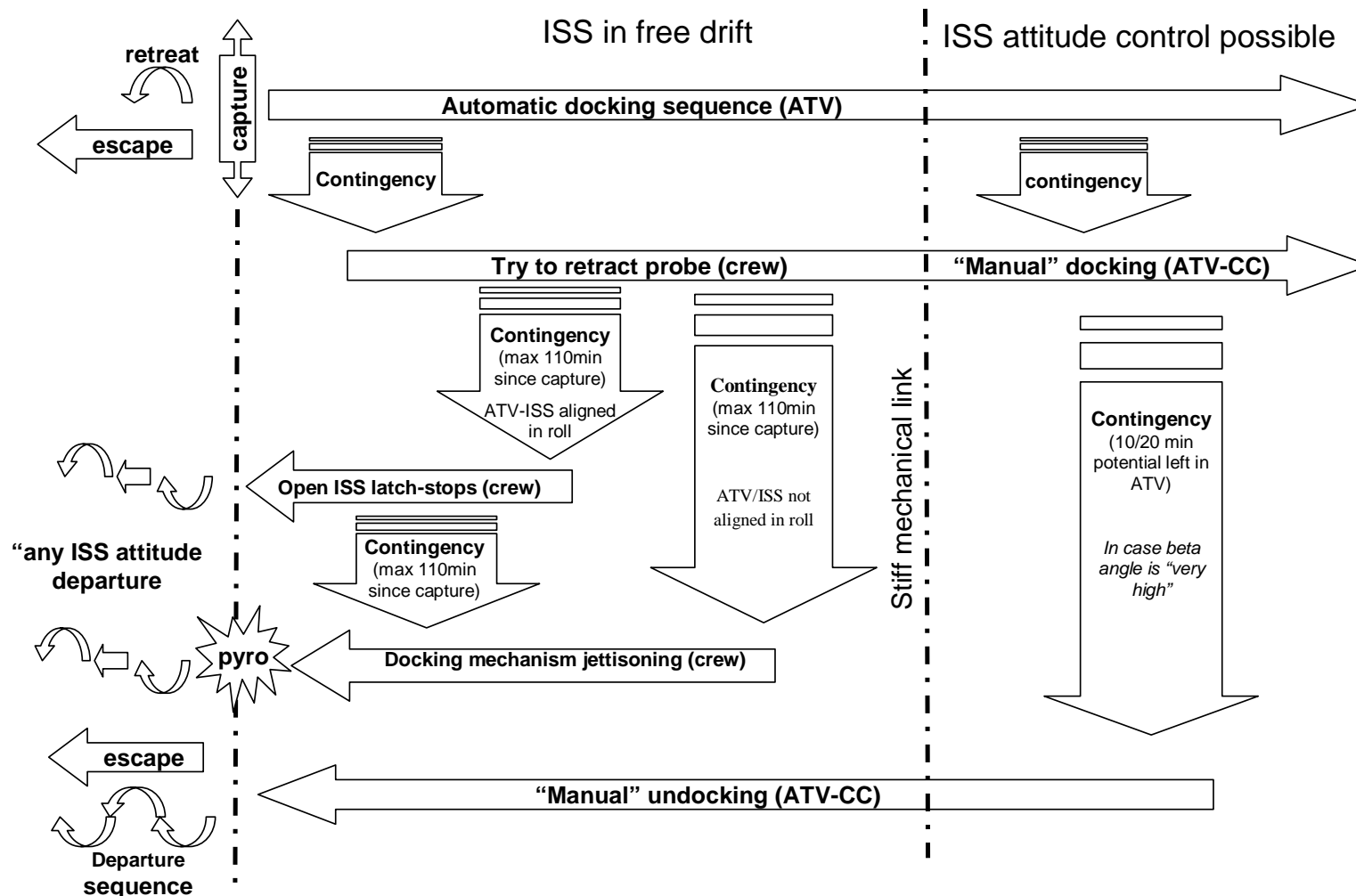
Any attitude departure – the solution

- If the probe is retracted enough (not more than 30 mm between PDA and ADA flanges) the crew may command the ISS to return to controlled attitude --> the ATV ground control centre may complete the mechanical and electrical docking through individual commands whose detailed sequence depends on the encountered failure.
- If the probe is not sufficiently retracted when the double failure occurs, the crew try to resume the probe retraction triggering an ATV on-board contingency plan --> if this attempt is successful, the previous case applies.
- If the probe retraction at least allows the ATV / ISS alignment in roll (not more than 192 mm between PDA and ADA flanges), the crew can release the ATV from the ISS side, and then trigger a specific 0 FT fly-away procedure compatible with any ISS possible attitude.
- If the probe cannot be retracted enough even to align the ATV in roll with the ISS, as last resort the crew must fire the pyros jettisoning the docking mechanism from the rest of the ADA, and then trigger another specific fly-away procedure --> in this extreme case the docking mechanism shall be removed by EVA from the SM aft port, while the ATV mission is definitely lost.



Human Spaceflight
SPACE FOR LIFE

Any attitude departure – logic diagram





Electrical contingencies

If failures occur during the electrical docking, the ATV must be able to leave while the on-board energy is still sufficient, as the solar panels orientation is non-optimal during that phase

Therefore the Depth of Discharge (DoD) of the ATV batteries must always keep a reserve sufficient for executing a safe qualified escape manoeuvre, should this become necessary

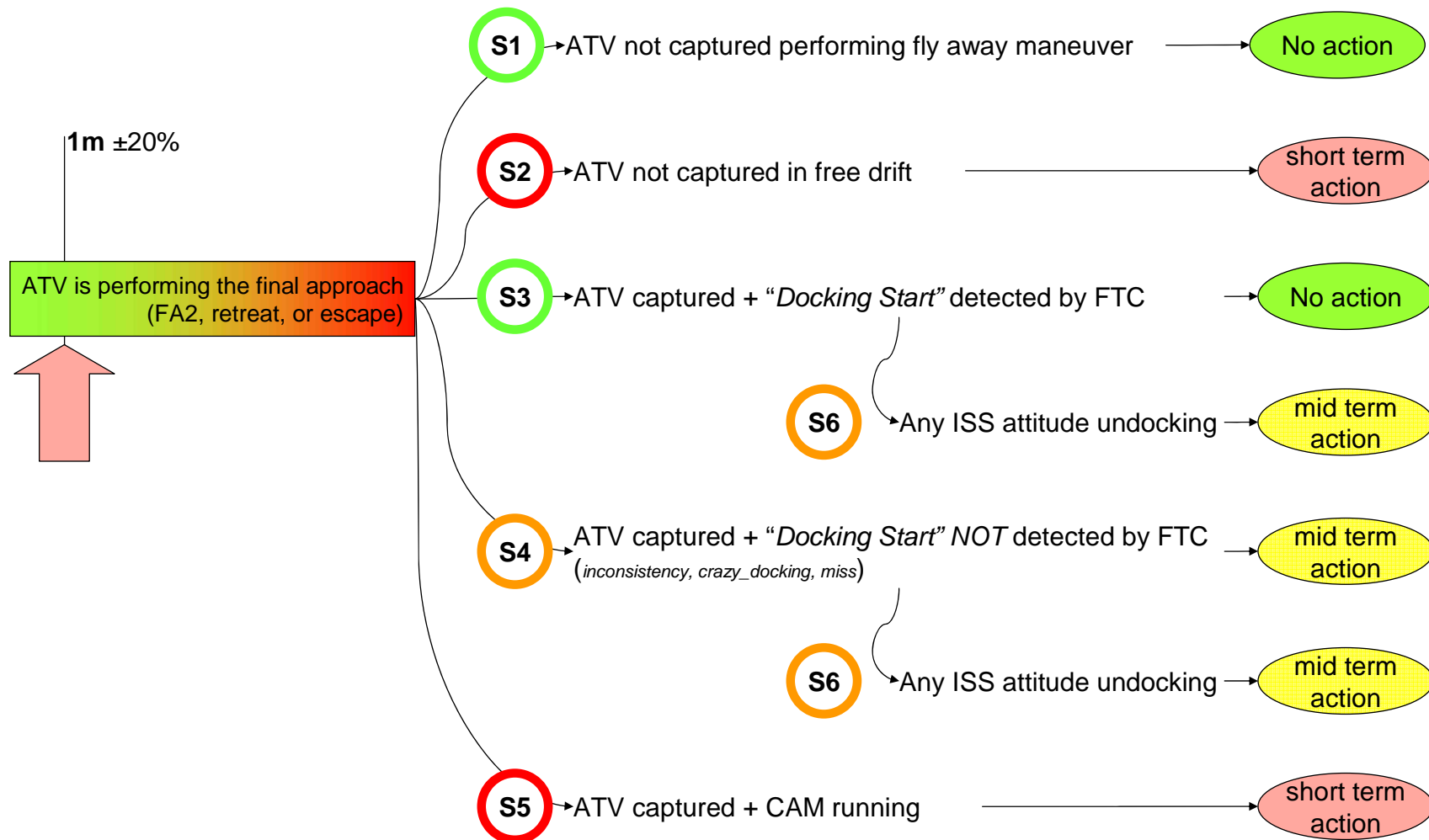
Additionally, the Non-Rechargeable Batteries must always maintain a sufficient reserve for an undocking manoeuvre.

If an electrical problem occurs after merging of the ATV and ISS Mil-1553 data buses, the ATV may leave using the nominal undocking sequence, with available time depending on the DoD of the ATV batteries

If the opening of the ADA hooks is impossible, as last resort the undocking will triggered by the ATV ground control centre, by firing the pyros hooks --> loss of ATV mission as no re-docking would be possible

For other electrical docking contingencies, such as absence of power connection between ISS and ATV, no recharge of ATV batteries, etc., specific operations will be decided and implemented by the ground depending on the actual failure and on the ATV configuration

Summary of actions for ATV docking contingencies





Safety principles during undocking

The RDS system avionics FMECA has confirmed the general compliance of the RDS design to the failure tolerance requirements, according to the following main lines:

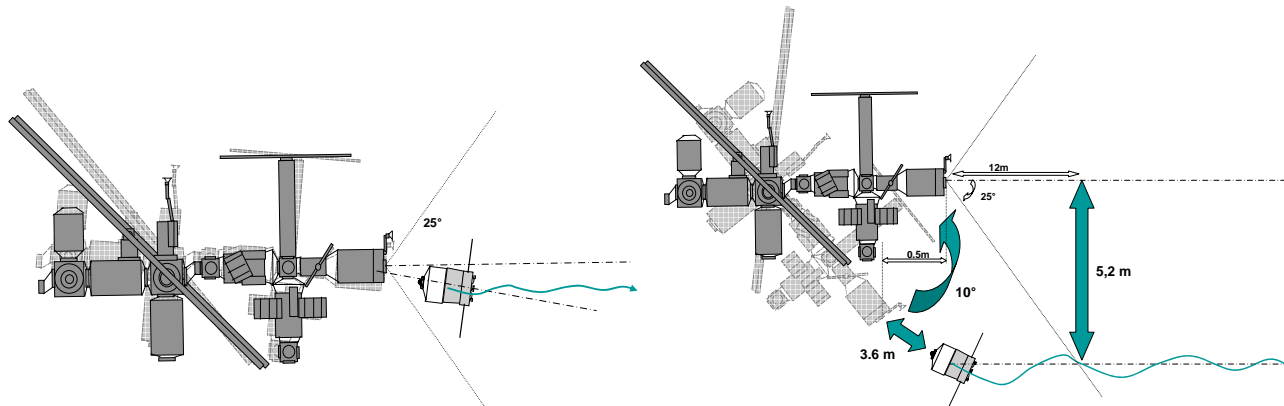
- the nominal undocking procedure is 1-FT
- since there are no failures at RDS level in common with the pyrotechnics undocking procedure, the RDS pyrotechnics system can always be used to release the ATV in extreme cases
- the RDS design is 2-FT for inadvertent undocking commands, for both nominal (hooks opening) and pyro undocking, preventing the risk of ISS depressurisation and uncontrolled ATV departure
- the risks not to be able to open the ADA pressure release valve and depressurise the inter-hatch volume is covered by ISS means to be possibly installed by the crew



Undocking safety – time constraints

Undocking contingencies never request quick reaction, even during the irreversible phase of ATV hooks opening, because:

- before hooks opening, the ATV is still tightly attached to the ISS, and recovery procedures can be performed without time criticality by the ground control centres
- during hooks opening, if the ATV is not yet released, the ISS PDA hooks can be closed again, after which recovery procedures can be performed without time criticality by the ground
- after ATV release, the vehicle trajectory is safe for a few hundreds of seconds, allowing the ground control centres to send on time the fly-away command to ATV even if the ATV on-board automated systems did not detect its released status



Relative attitude ISS/LVLH/ATV at departure (*exaggerated for presentation purpose*)



ATV and ISS time constraints for departure

