Safety in GNC systems design for In-Orbit Servicing during close proximity operations

Anthea Comellini [(1)], Davide Casu [(1)], Vincent Dubanchet [(1)]
Hervé Renault [(1)], Lorenzo Bitetti [(1)], Pierre Dandré [(1)]

[(1)] Thales Alenia Space – 5 allée des Gabians, 06150 Cannes (France)
name.surname@thalesaleniaspace.com

ABSTRACT

The current paper focuses on the impact of best practices and guidelines for safe Close Proximity Operations in the scope of In-Orbit-Servicing missions on the conception, the design, the Validation and the Verification of the GNC system. After introducing the key safety requirements for safe Close Proximity Operations, their impact on the GNC design during the different phases of the rendezvous will be discussed in details, with a focus on specific analyses and tests that are required to validate and verify the GNC design and requirements. Finally, the whole validation and verification process will be described, detailing the tools required at each stage of the process and in each of the programme phases. The final aim of this paper is to allow for a better understanding of the criticalities of In-Orbit-Servicing missions, with the derivation of GNC requirements complying with safety requirements and addressing safety guidelines. It will be shown how the main critical requirements are verified through the workflow of the GNC system from early conception to validation and verification.

1 INTRODUCTION

Although interest is rising in the execution of rendezvous (RDV), proximity, and capture operations for In-Orbit services, the definition of accepted technical and safety standards for In-Orbit Servicing (IOS) to carry out in a safe and responsible manner these operations is still an on-going process. The need for safety standardization has been identified by major agencies. Stakeholders, industry led organizations (e.g., CONFERS), standardization organization (e.g., ISO) and working groups such as the ESA-led Close Proximity Operations (CPO) are working in this direction, to derive guidelines and standards for safe close proximity operations. The economic context of these projects is challenging, and design rules and verification methods inherited from crewed rendezvous mission are probably over constraining. On the other hand, either from the space debris mitigation point of view or from a commercial and insurance service point a view, an adequate level of safety shall be implemented and demonstrated. Availability of adequate design and verification tool is thus considered essential to support in an exhaustive and cost effective way these verifications. The final aim is to perform IOS missions in a safe and sustainable way based on guidelines applicable to most of the considered services.

The current paper focuses on the impact of best practices and guidelines for safe CPO on the conception, the design, and the validation and verification (V&V) of the GNC system. The GNC system is key for most of the safety requirements in order to reach the required level of autonomy. Indeed, it is a high critical system for such missions by making use of autonomous guidance and navigation capabilities, coordinated control of robotic arm and Servicer's platform, overall FDIR (Fault Detection Identification and Recovery) strategies and autonomous Collision Avoidance Maneuvers (CAMs). The process of ensuring Safety with a low probability of collision is far to be taken for granted for these very complex missions.

The paper is structured as follows: firstly, the major key safety requirements will be detailed in Sec.2, with a focus on those having a direct impact on the GNC design. Mission Analysis (MA) and Concept Of Operations (ConOPS) of the rendezvous approach must take into account these safety requirements from concept design, thus impacting on the GNC strategy. This is discussed thoroughly in Sec.3, where the major design drivers for the GNC system will be detailed, focusing on how the GNC system can be developed to meet the safety requirements. Finally, in Sec.4 the overall GNC workflow, from design and development to validation and verification, to ensure a safe but cost-effective IOS GNC product will be presented. GNC analyses, methodologies and tools proposed to be used along this workflow will be detailed.

2 KEY SAFETY REQUIREMENTS

For uncrewed rendezvous mission such as IOS missions, mission safety mainly translates in avoiding the generation of any debris during the CPO. Debris could be generated due to:

1. Unintentional breakup of the servicer or the client.
2. Intentional generation of micro-debris during the servicing operations (e.g., caused by the use of some capture method such as harpoons, intentional perforation of S/C surfaces such as MLI to enable refueling operations, etc …).
3. Collision of the servicer or the client with third parties.
4. Unintentional degradation of the client (or the servicer) performance during servicing operations, preventing the client (or the servicer) from continuing its nominal mission after the IOS and precluding the possibility of carrying out End-Of-Life disposal.
5. Collision of the stack with third parties.
6. Collision of the servicer with the client.
7. Loss of the mission of the servicer or the client, potentially due to unsuccessful IOS operations, which would leave one or more spacecraft in orbit.

The first two points result in requirements that cover different disciplines such as system engineering and mechanics. The third point, i.e., collision avoidance of the servicer (or the client) with third parties, requires measures that are not CPO specific (except for particular cases that will be detailed in Sec.3.2). On the other hand, the fourth, the fifth and the sixth points translate into CPO specific requirements that affect the design of the mission starting from the ConOPS, with direct impacts the GNC system. This is discussed in details in the current Section.

2.1 Safety requirements during CPO phases

To avoid undesired collisions during CPO, the notion of zones in which the servicer enters only after positive assessment of a set of conditions is introduced. This concept is inherited from crewed missions: the International Rendezvous System Interoperability Standard [3] states that "*Safety regions are critical to contributing to mission safety and success, and have an impact of expected performance of Guidance, Navigation, and Control. The intent is to have common zones/regions for all vehicles performing Rendezvous, Proximity Operations and Docking with a target vehicle.".* Not all the zones needed for the safe execution of crewed rendezvous are also needed in IOS. In Issue 2.0 of ESA's "Guidelines for safe Close Proximity Operations" [1] two zones, centred at the Client's CoM (Center of Mass) are defined: **the Approach Zone (AZ)** and **the Keep Out Zone (KOZ)**.

The first zone encountered by the client during its approach is the AZ, with a size that is mission dependent, usually in the order of magnitude of some kms. The KOZ is smaller around the client, its size is mission dependent too, usually around a hundred of m. These zones can be entered only after the positive assessment of a set of condition that we will detail further. GO/NO-GO can be issued either from TC -requiring therefore Ground Station visibility-, or autonomously –implying a higher

level of autonomy of the servicer. These decisions are taken in correspondence of *decision points,* another concept inherited from crewed missions (see [3]) that can be explained as follows: to execute an IOS mission to and/or from the client vehicle, there will be a series of decisions to safely and incrementally implement the mission timeline. The points in which these decisions are taken are the *decision points.* These points have to be intended as *Operational points* (i.e., they have a predefined position in the mission timeline, and they do not correspond to a predefined location or geometrical envelope in which the decision has to be taken. However, they might have to comply to some geometrical constraint, such as being placed outside of a given Zone). Decision points are mission specific, defined by trajectory design, ConOPS and servicer performance. However, in order to ensure mission success and safety, a minimum set of decision points needs to be defined. These are the points where the servicer (either autonomously or through Ground communication) assess a set of conditions (i.e., GO/NO-GO conditions) before initiating an intentional entry in a zone and/or the initiation of the next rendezvous phase. Decision points represent -in the mission timeline- the boundaries between the different CPO phases, as detailed in the following paragraphs and pictured in Figure 1.

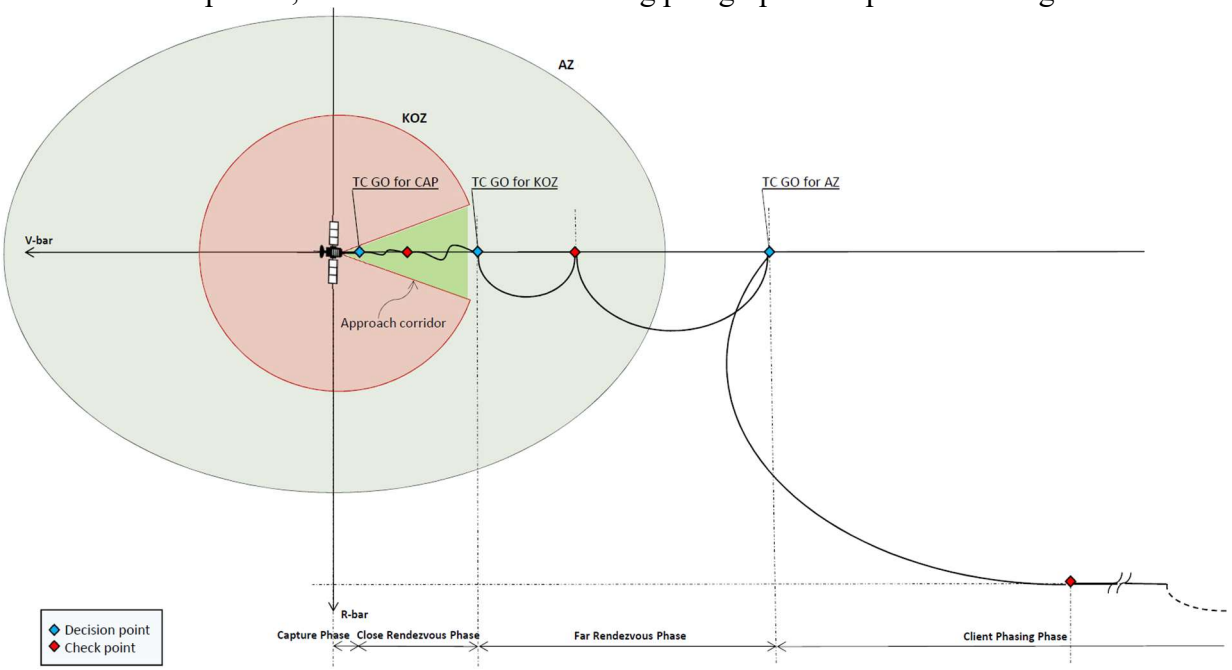

Figure 1: CPO Operational Phases, Zones, and Decision Points

2.1.1 Far Rendezvous Phase

Before arriving at the AZ boundary, the servicer is in the Client Phasing Phase and it is still relying to absolute navigation, thus this mission phase is not considered part of CPO. When the servicer receives the GO allowing to proceed beyond the AZ boundary, the Far Rendezvous Phase (and CPO) begins. One of the condition for the servicer to enter the AZ is to perform relative 3DoF (Degrees-of-Freedom) pose estimation, i.e. the client has to have access to a reliable estimate of the relative client-servicer position. This can be provided by different means (e.g., optical sensor and Image Processing (IP) algorithms, multiple antenna ranging systems, relative GPS) depending on the nature of the client (e.g., relative GPS requires the client to be cooperative, multiple antenna ranging system can be used with a prepared client, while for non-prepared and non-cooperative clients such as space debris optical sensors and associated image processing algorithms are the only solution).

Within the AZ, the servicer can follow any trajectory: it's up to the mission design either to opt for an approach that follows passively safe trajectories (e.g., trajectories that ensure not crossing a certain volume around the client for a given duration), or to rely on active orbit protection. In any case, inside the AZ, the servicer must ensure the capability to Abort or Cancel the approach either autonomously

or from Ground TC. An Abort is an operation to safely terminate the CPO in the event that the **mission safety cannot be ensured**. The Abort command triggers a maneuver (e.g., a CAM) to put the servicer on a safe passive trajectory, and will result in a reconfiguration of the servicer to a state that might not be consistent with resuming the mission objective. On the other hand, a Cancel is triggered when mission safety is not endangered but **mission success can no longer be ensured** with the current state of the servicer, and it does not necessarily result in a CAM. Not possessing the capability of executing these commands autonomously would require having continuous station coverage during the whole Far RDV phase, which could be quite expensive and constraining. It must be noted that, during any CPO phase, for a single point failure within satellite subsystems, the servicer is still able to execute an Abort or a CAM.

2.1.2 Close Rendezvous

When the servicer reaches the KOZ boundaries, it waits for the assessment of another set of condition for the GO/NO-GO to enter the KOZ zone. If the GO command is issued, the Close Rendezvous Phase starts. The KOZ can be entered only through the **Approach Corridor (ApC).** The ApC is a geometrical and dynamical envelope, generally (but not necessarily) understood as a cone originating from the client in which the servicer makes its approach. It encompasses several kinematic and dynamic parameters, such as relative position, range, range rate, relative attitude and relative rotation rate. A violation of the ApC results at least in a Cancel. In order to enter the zone via the ApC, the servicer must ensure 6DoF relative control. Relative 6DoF control is mandatory in order to avoid potential collisions, since the KOZ is the zone in which the servicer performs closing maneuvers that approach the servicer and the client's clearance envelopes until potential tangency. The concept of *clearance envelope* is to be understood as the geometrical area defined in body reference frame around the CoM of the client or the servicer, including all vehicle mechanical parts in all possible configuration (e.g. appendage, movable parts, capture mechanism). In the case of non-cooperative rendezvous with a tumbling S/C, the servicer might have to execute complex synchronization maneuvers in order to align with one of the client's body axis to prepare for capture: a loss of 6DoF control could lead to an imminent risk of collision requiring an immediate CAM.
Within the KOZ, the capability of executing an Abort must be fully autonomous (i.e., without the need of receiving any external command). Another corridor is defined in the KOZ, namely the **Abort Corridor (AbC)**, whose violation result in an Abort. Its definition is similar to the definition of the ApC, with a different range of acceptable parameters.

2.1.3 Capture Phase, Stack Configuration Phase, and Separation Phase

During the Close RDV phase, the servicer can approach along the ApC until tangency of the vehicles clearance envelopes. Before proceeding with the *Capture Phase*, another assessment of condition has to be made to initiate the Capture Phase. During this phase the servicer approaches the client, so that the clearance envelopes cross and the servicer proceeds beyond the so called *Point-of-No-Return*, *i.e.*, the moment at which it is safer to continue with capture rather than performing a CAM. Autonomous Abort capability is conserved until this point. The Capture Phase ends with the actual capture (i.e., the action of establishing physical connection between the servicer and the client) and the establishment of a stable stack. After confirmation of capture, the *Stack Configuration Phase* is initiated. The final part of the approach in the KOZ until the capture is confirmed has to be executed under ground coverage. The servicer and the capture operations must be designed to avoid degradation of the servicer and client performance (e.g., especially due to plume contamination and/or impingement, but not in case the client is a space debris). During the Stack Configuration Phase, the servicer (or the client) is able to control the orbit and the attitude of the stack, in compliance with the requirements for subsequent operations to be implemented. Among those functions, collision avoidance capabilities with third parties have to be ensured. Finally, if a *Separation Phase* is foreseen (i.e., the phase in which the *release* takes place, namely the physical separation of the client and the

servicer), the servicer must ensure that the release conditions are compatible with the control capabilities of both the servicer and the client. Moreover, the release mechanism/strategy has to be capable of providing a minimum impulse to either the servicer or the client to create an opening rate, which enables the two objects to move apart along a trajectory where any drift creates no risk of collision between them over a time frame compatible with implementation of an anti-collision maneuver.

2.2 Summary of the safety requirements impacting on the GNC design

In Figure 1, the transition between phases and zones is depicted. Note that both decision points (mandatory) and check point (mission-dependent) are present in the depicted scenario.

We provide in this paragraph a summary of the main safety requirements impacting the GNC system, organized by macro-topics, that will be subsequently expanded in Sec.3, where the impact of these safety requirements on the GNC design and validation will be discussed.

- GO/NO-GO decisions between Phases and/or Zones
    - The design of the servicer integrates the notion of zones, in which the servicer enters only intentionally (either autonomously or through Ground TC).
- Aborts, CAMs and Passively Safe Trajectories
    - An Abort shall be executed any time mission safety is endangered.
    - Within the AZ, the Abort triggering can be either autonomous or from Ground TC.
    - Within the KOZ, the Abort triggering shall be autonomous.
    - Within the KOZ, an Abort is triggered any time the AbC is violated.
    - For a single point failure within satellite subsystems, the servicer is still able to execute an Abort or a CAM.
- Capture Phase, Stack Configuration Phase, and Separation Phases
    - The system should be designed to avoid degradation of client performance (due to multiple causes such as plume impingement, capture strategy, release strategy…).
    - The servicer (or the client) should be able to control the attitude and the orbit of the stack.
    - The servicer must ensure that the release conditions are compatible with the control capabilities of both the servicer and the client.
    - The release mechanism/strategy is capable to provide a minimum impulse to either the servicer or the client to create an opening rate.

Moreover, being relative navigation a key capability to enable safe and successful Close Proximity Operation, a specific requirement is expressed in this scope:

- Relative Navigation
    - The relative navigation solution shall be robust towards degradation of the sensors performance due to external or self-inflicted sources.

3 IMPACT ON GNC DESIGN AND VALIDATION

GNC design consists in specifying all the GNC HW (Hardware) and SW (Software) elements that are necessary to control the servicer vehicle inertially and relatively to the client with as much autonomy as possible, in order to fulfil each phase of the rendezvous and CPO [4]. The ConOPS will specify for each phase of mission which HW and SW elements shall intervene, associated with the Spacecraft and GNC modes. The GNC design shall address the specification of:

- HW and SW matrix;

- GNC requirements for each phase of the mission (e.g., Knowledge and Closed Loop accuracies);
- Sensors and Actuators sizing and accommodation based on observability and controllability analysis;
- The overall OBSW (On-Board-SoftWare) and GNC architecture in terms of GNC modes definition, modes transitions and decision tree;
- Mission and Vehicle Management (MVM) functions to fulfil the required autonomy;
- FDIR strategy (e.g. triggering conditions for CAM), in close collaboration with the RAMS (Reliability, Availability, Maintainability and Safety) and the DHS (Data Handling Subsystem) teams.

The GNC control loop of the Servicer follows a classic automation scheme, with the **Guidance function** providing the reference trajectory and attitude profiles for servicing, checking the safety of the reference profiles and computing the collision avoidance maneuvers during final approach phase in case of contingency; the **Navigation function** providing an accurate and robust estimation of the client motion to the other components by merging the measurements coming from different sensors with a-priori knowledge of the process; and the **Control function,** receiving the Guidance and Navigation outputs and generating the suitable commands to reach the Guidance reference. On top on this traditional GNC loop, the autonomy layer is implemented within the generic "**Mission and Vehicle Management" (MVM)** block which triggers the modes and parameters of the different units of this control loop. The mission phase objectives, autonomy levels and ground interface are managed by the MVM which executes one by one the OBSW applications and collects the status flags of each application, among which the GNC application, to decide upon mode transitions, including in case of anomalies/failure.

In this Section we will discuss the impact of the requirements identified in Sec.2.1 and summarized in Sec.2.2 on the design and validation of the GNC system. Tools and analysis to be carried out in the V&V (Validation and Verification) phases, that will be better thoroughly described in Sec.4, will be also anticipated.

3.1 GO/NO-GO decisions between Phases

The mission timeline and the ConOPS will specify which GO/NO-GO decisions have to be taken before moving to the next phase of the RDV and entering a given operational zone. The location of the decision points should be chosen to ensure safety and stability for a given amount of time. Among the major parameters influencing the definition of the approach strategy, one should consider orbital dynamics and disturbances (e.g., naturally stable orbits and/or station keeping strategy), autonomy or ground visibility/control, propellant performance and consumption, accuracy and operational range of GNC sensors, on-ground and on-board autonomy sharing, and the geometry of the approach. The functional chains and equipment that need to be monitored may vary from a mission to another. Among others, one can mention GNC internal checks of convergence of algorithms/filters and hardware, including cross-checking of performance in case of transition and/or change of the sensors used in the GNC loop, or the status and behaviour or the whole propulsion system, including THR (thrusters) performance and the estimation of remaining propellant. Critical items, parameters and thresholds have to be identified thanks to multidisciplinary analyses, including RAMS analyses to identify the failures having an impact on the safety and mission success. This leads to the definition of the checks and the reconfigurations to be done through the FDIR design and monitoring of the satellite units needed for the next operations. Depending on the mission, the check of the health status can be done autonomously and/or with the ground support. On top on this traditional control loop, the autonomy layer needs to be implemented within the generic MVM block which triggers the modes and parameters of the different units of this control loop. The mission phase objectives, autonomy levels and ground interface are managed by the MVM which executes one by one the GNC applications and collects the status flags of each application to decide upon mode transitions,

including in case of anomalies/failure. Considering the validation phase of such safety mechanisms in the MVM, a key requirement is to check the final Ground interface for TC emulation and the transitions of the functional logics by injecting failures and raising GNC status flags during MIL (Model-In-the-Loop) and SIL (Software-In-the-Loop) tests.

3.2 Aborts, CAMs and Passively Safe Trajectories

Safety requirements in [1] define an acceptable probability of collision risk. However, during the CPO, there is no need to have the servicer computing the current collision risk at any instant of the approach. To ensure the compliance with this requirement, the Abort Corridor is defined inside the KOZ. The Abort Corridor can be seen as an envelope of parameters (namely relative position, range-rate, relative attitude and relative rotation rate) whose violation autonomously trigger an Abort and a CAM. It is therefore in the phase of mission design that the analyses enable to iteratively define the corridor parameters so that -if the servicer stays within its boundaries- mission safety is not compromised and no imminent risk of collision exists. To help the definition of these parameters, some consideration should be done, based on information such as the FoV (Field-of-View) of the relative navigation sensors, the clearance envelopes of the servicer and the client, and the actuations capabilities. GNC analyses and simulation of the design and transition to/from the CAM 'mode' have to be performed in order to demonstrate the capability of successfully triggering and performing a CAM despite the potential failures. Given the importance of the CAM capability, CAM triggering conditions, logic and execution have to be extensively validated and tested as soon as the MIL validation is performed at design stage. It is up to mission design whether to trigger an Abort also in case of a violation of the Approach Corridor. However, the parameters of the ApC should be derived so that their violation does not endanger mission safety, but only mission success. Outside the KOZ, no corridors are defined. The risk of collision should therefore be computed according to some check points in the mission timeline, such as after the execution of any manoeuvre.

It should be noted that there are other conditions (e.g. in case of failures) that may require an automatic Abort and/or CAM execution even if the pre-defined corridor is not violated. For instance, a switch to Safe mode shall not be done before having effectuated a CAM towards a passively safe orbit that does not re-enter the AZ for a predefined duration. It should be noted that, during the final approach with cooperative clients, it could be useful to specify -also for the client- some requirements on the transition to Safe mode, in order to prevent them from having an unexpected attitude change that may lead to a collision.

RAMS and FDIR analyses have to be performed in order to clearly identify in which failure scenario a CAM have to be performed. Generally speaking, the decision to enter CAM mode shall be based on certain "observable" (e.g. GNC status flags, emergency flags, etc.) managed at MVM/FDIR level based on inputs either derived by the GNC applications or outputted by HW elements. Below, a non-exhaustive list of these GNC observables is presented.

- Navigation emergency:
  - Client tracking lost for a predefined duration,
  - Degradation of the filter state covariance, indicating a loss of its convergence,
  - Unresolved conflict between different sources of measurement,
  - Sensor FDIR: any hardware or software issue at the subsystem level.
- Control emergency:
  - Actuator saturation at any time (the risk of a thruster or wheel saturation is highly critical during the last hundreds of meters),
  - Controller inputs outside its design boundaries on the acceptable error levels due to disturbances or hardware malfunction,
  - Actuator FDIR: any hardware or software issue at the subsystem level.
- Guidance emergency:
  - Any trajectory that crosses a zone before having the clearance to proceed into that zone,

- Violation of the Abort Corridor,
- Drifting from safe hold points beyond the accuracies required.

In theory, a suitable combination or decision tree of the high level emergency flags to trigger either a CAM or a Cancel shall be derived. This decision tree shall be checked in priority at each MVM cycle. In the absence of an imminent risk of collision, a safe strategy could be to retreat to previous safe hold point (i.e., execute a Cancel) where the system could take a more complex decision which could imply a reconfiguration at HW and/or SW level, or the execution of an Abort. It should be reminded that the capability to Abort should be conserved even after a single point failure in any of the servicer subsystems, with a direct impact on the FDIR and the choice of the GNC HW redundancies.

By requirement, after the execution of an Abort or a CAM, the servicer must be on passively safe trajectory. Mission analyses and simulations have to be performed in order to derive the trajectories that lead to a passively safe state. The time over which the trajectory remains safe depends on several factors: mainly the chosen trajectory, the predominant disturbing forces at the given orbital regime (e.g. drag force in LEO and solar radiation pressure/SRP in GEO [2]) and the rendezvous context (e.g. single client versus constellation or collocated satellites, for which collision avoidance with third party spacecraft has to be addressed from design). The definition of the passively safe trajectories has thus a large impact on the mission planning and manoeuvers strategy but also on the ground workload or on-board recoveries that have to be put in place in order to guarantee the safety of the whole rendezvous approach. Once the passively safe trajectories have been defined, one has to demonstrate, via analysis and simulations, that the GNC and propulsion design allow to perform the required manoeuvres required by the mission analysis. More details on the tools to be used in the V&V process are provided in Sec.4.

3.3 Capture Phase, Stack Configuration Phase, and Separation Phases

As per a classical space mission, the internal and external sources of disturbing forces and torques have to be taken into account in the GNC design (sizing of actuators, definition of attitude and orbit control modes, etc.). In addition to a classical mission, the needs and constraints of the capture mechanisms design and capture/release sequences have to be considered (e.g. approach velocity, kinetic energy at capture, required performance for the GNC, force and torque at release, etc.). These topics are better discussed in the current section.

3.3.1 Capture Phase

By requirement, the system should be designed to avoid degradation of client performance in all CPO phases (except in case the client is a space debris). During the final meters of the approach and the Capture Phase, plume impingement of the client becomes a major risk. In order to prevent or limit the plume impingement, one can mention measures such as the accommodation and orientation of thrusters (THRs), and some constraint in the specific use of THRs (e.g., the final braking burn toward the client have to take place at a distance which is far enough such that the gas temperature has sufficiently cooled to avoid damage of the structure, and such that the density of contaminating particles is sufficiently reduced to avoid significant condensation when arriving at the client surface). In case of a RDV with a cooperative client, it should be required that the client satellite remains passive during the last phases of the rendezvous when the servicer is in close vicinity, implying that its actuators (i.e., thrusters, reaction wheel, magneto-torquers, etc.) must be used in such a way to avoid any adverse motion or any plume toward the servicer. This constraint aims at avoiding the application of disturbance force or torque on the approaching vehicle and the blinding and/or pollution of its relative sensors. This imply that the client shall test the new AOCS mode and shall ensure with a certain accuracy that the residual velocities are below agreed acceptable values and that its attitude won't derive from the nominal conditions.

Numerous solutions exist for the capture and servicing of the client (e.g. rigid capture, flexible capture or contactless method) and the requirements for the GNC (e.g. approach velocity, kinetic energy at

capture, accurate and stable orientation, maximum misalignment, etc.) may therefore significantly vary from a solution to another. Structural and Multi-body analysis have to be performed in order to determine GNC requirements at capture and separation. GNC analyses and simulation (MIL, SIL, PIL/Processor-In-the-Loop) have to be performed in order to verify that the design complies with the performance required for the mission and that it is robust to conditions encountered in orbit, and more specifically those of the capture phase.

3.3.2 Stack Configuration Phase

By requirement, during the Stack Configuration Phase, the servicer (or the client) should be able to control the attitude and the orbit of the stack, in compliance with the requirements for subsequent operations to be implemented. Controllability analysis of the stack configuration shall be done already during GNC design and HW matrix definition. In fact, the GNC units have to be sized, accommodated and orientated so that perturbing forces and torques acting on the stacked spacecraft can be controlled and the desired attitude achieved. Validation and testing since MIL shall then be performed. To this purpose, uncertainties over the client MCI properties must be carefully evaluated and a safety margin must be taken over these uncertainty amplitudes to be used during the control synthesis, depending on its mechanical configuration and uncertain parameters. The controller must be designed and synthesized using robust control methods ensuring analytically the robustness to these MCI uncertainties (e.g., H-infinity robust control validated by mu-analyses over the MCI ranges). These validations are valid in the scope of linear system theory, therefore a second stage of validation is required with nonlinear dynamic model based on Monte-Carlo analyses refined around the worst-cases configurations identified by the previous mu-analyses (more details are provided in Sec.4). For non-cooperative clients, particular attention shall be paid to the dispersion of sensitive parameters during robustness campaigns as for example for client angular rate, MCI properties and 3D model. These figures could be quite different in orbit from the ones expected to be found. Ground tests to de-risk the different scenario shall be carried out with particular attention in representing the real behaviour of the spacecraft before, during and after contact phase. Additionally, some specific analyses and operations (e.g. inspection before capture, execution of attitude maneuvers while stacked, etc.) may be required in orbit in order to update or better estimate the client parameters needed by the GNC system with a reduced uncertainty about the client and the stack. For what concerns more specifically the orbit control, one has to design the GNC and propulsion system of the servicer (THRs size, orientation, accommodation, etc.) so that the required orbit manoeuvres could be performed by the stack, including the collision avoidance manoeuver and disposal ones, if applicable. It should be noted that in the case of a cooperative client, it might be possible that the client is still the responsible of AOCS and CAM during the Stack Configuration Phase.

3.3.3 Separation Phase

Per design, the release mechanism and the separation sequence have to be designed so that the attitude and the angular rates are within the maximum acceptable values required by the client and/or by the specific mission application (e.g. given attitude to resume the mission and/or to guarantee the client AOCS take over, spin movement, specific condition for the re-entry, etc.). For this purpose, force and torques at separation have to be evaluated and taken into account in the client AOCS simulator in order to demonstrate the feasibility and performance of the attitude control. Multi-body dynamic analysis, including stochastic analysis taking into account dispersions (force at separation, velocity and kinetic energy at separation, bodies geometrical scattering, etc.), have to be performed in order to validate the aforementioned design. Moreover, the release mechanism/strategy has to be capable to provide a minimum impulse (e.g., through the use of springs) to both the servicer and the client to create an opening rate, which enables the two objects to move apart along a trajectory where any drift creates no risk of collision between them over a time frame compatible with implementation of any

subsequent CAM. After this separation step, the releasing operations should allow the use of the servicer THRs without risk of plume impingement on the client by reaching a sufficient inter-distance.

3.4 Relative Navigation

Relative Navigation is a key capability to enable safe CPO. The servicer must be designed to provide the required relative navigation solutions to meet the mission pointing and accuracy performance requirements taking into account the degradation of the sensors performance due to external or self-inflicted sources (e.g., presence of Earth or other bodies in the background of the optical sensor FoV, plume effect, …), and different rendezvous operational conditions (e.g., illumination conditions, thermal conditions, …). Illumination significantly varies from an orbital region to another, and along the orbit itself. This can lead to changes in the behaviour of some optical sensor, which become inoperable when saturated. By design, the navigation sensors suite and parameters shall be chosen based on mission and illumination constraints derived by mission analysis for both nominal mission timeline and non-nominal strategies, including trajectories to be followed in case of CAM, abort, retreat, provided that similar sensors are used in these phases. At the same time, the mission timeline can be adapted to the specific needs and illumination constraints of the selected hardware. Active sources of illumination may be used: in this case, the intensity and spectrum of the illumination device have to be characterized and taken into account in the design and verification of the image processing tools and algorithms. In addition, its power consumption has to be taken into account in the power budget. The selected solutions shall be then validated through simulations (e.g. generating synthetic images for Image Processing) but also during HIL (Hardware-In-the-Loop) in robotic facilities with representative HW both in terms of Real Time processors and space-camera-like equipment. The validation of the Navigation solution shall comprise extensive robustness campaign considering different illumination/observability conditions as per test plan. In case a thermal infrared camera is used, thermal aspects should be considered as well. Thus, different uncertainties, disturbances and environmental conditions affecting the relative navigation chain should be considered. At sensor level one may cite, among others:

- Illumination conditions for visible visual sensors,
- Thermal conditions of the client for thermal visual sensors,
- Uncertainties on the sensor properties (optics, electronics…),
- Uncertainties on the client shape and model knowledge,
- Uncertainties on the client material and visual/thermal aspect (reflectivity, aspect/colour,…).

And at the filtering level:

- Uncertainties on the mounting of the sensors (accommodation, thermal bending, …),
- Uncertainties on the MCI properties and GNC parameters for the filter dynamic models,
- Uncertainties of orbital disturbances (relative drag, relative solar pressure…) over the dynamic filter relying on a nominal relative dynamics model.

Data Fusion of inertial and relative measurements is another CPO-specific thematic, especially in the final phase before capture, when additional sensors (e.g., robotic arm camera) come into play. Conflicting control inputs/outputs may arise, for instance, in case of redundant systems or different technologies (e.g. two sensors providing different measurements and/or leading to different estimation of the state), but also in case of decentralized control and FDIR (e.g. spacecraft AOCS and robotic arm control). These aspects have to be taken into account in the GNC design and while defining the MVM and fault management strategies in order to be able to identify and discard wrong outlier measurements and especially drifting ones over time.

4 GNC V&V PROCESS AND TOOLS

In each programme, a flow-down from Mission and System requirements is made to derive high level GNC requirements. In the specific case of an IOS mission, Mission and System requirements include also the requirements mentioned above and which are needed to ensure the safety and success of the operations. In Figure 2, the overall GNC workflow is depicted with respect to the Programme phases. The first step to derive GNC requirement from Mission and Safety requirements is one of the key challenges as it drives all the subsequent tasks. In Figure 3, the activities of this generic workflow are detailed with the GNC design, validation and verification processes, describing the workflow from GNC requirements to GNC qualification. These steps are detailed in the following paragraphs.

4.1 GNC Design

GNC requirements shall encompass also the GNC performance budget, which is interconnected with the overall System performance budget. Note that, for more "standard" AOCS development, these budgets are named *System and AOCS pointing budgets*. The sizing of GNC system and subsystem is usually performed as early as Phase A. It is of paramount importance for any model-based approach to carefully assess the models uncertainties, disturbances and disturbances (Figure 3). A good representativeness of models is crucial for model-based approach, to prevent from non-conformities that could rise in later steps of the V&V process, with major impact on the programme. It is important to take into account orbital disturbances such as drag, SRP, Earth gravity potential harmonics, and gravity gradient. Differential effects of SRP and drag play a crucial role in RDV relative Dynamics, especially when the client and servicer ballistic coefficients are very dissimilar, leading to a differential motion. From the trajectory design point of view, a key role is played by the actuation chain and thrust errors. The design of the RDV strategy and trajectories shall make use of passively safety concept when possible, and take suitable margins coming from all different sources of errors (both endogenous and exogenous). The navigation filters shall be designed and tuned considering to be robust toward the behaviour of the measurement models (e.g. delayed and infrequent measurements coming from IP algorithms). Robust Control synthesis shall take into account the flexible dynamics and sloshing models and evaluate all associated uncertainties. Usually a performance assessment at models and closed-loop levels is required to corroborate the design and be confident of the quantitative figures of the GNC requirements by PDR (Preliminary Design Review), as pictured in Figure 2.

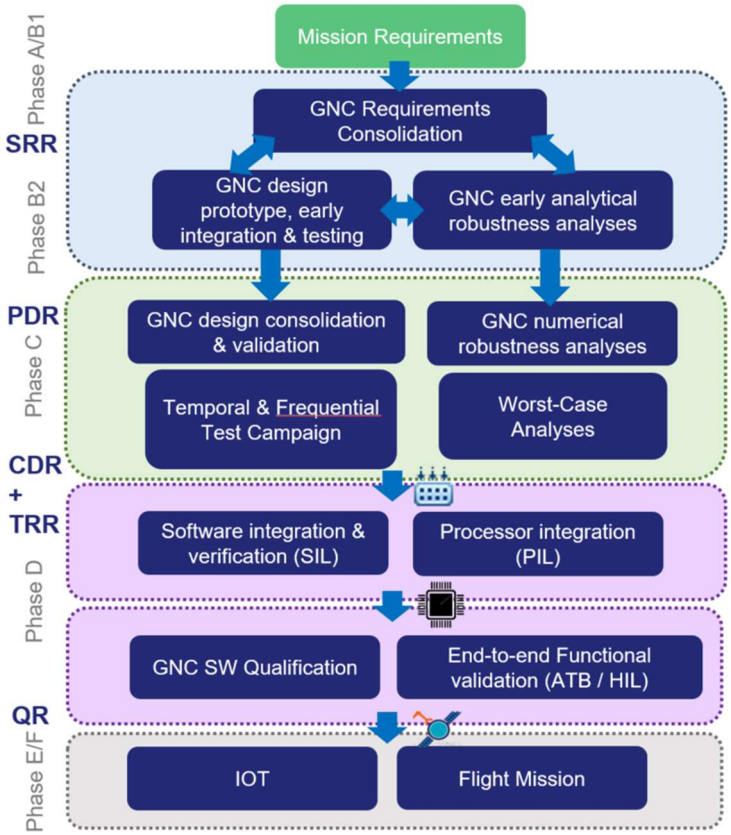

Figure 2: V&V process along the Phases of the Programme

4.1 GNC Validation

GNC Validation is performed at different steps of the programme. Several types of analyses from Linear Covariance Analyses (LCA) to Monte Carlo (MC) analyses applied to increasingly accurate models (of the environment and the spacecraft) can be used in different phases of the design, development and validation of the GNC system. LCA is a tool for preliminary analysis in early phases, while MC analysis can have different level of complexity and make use of the Functional Engineering Simulator (FES). These tools are useful to verify that the derived ConOPS and mission analysis strategy for the rendezvous approach are consistent and that the trajectory dispersion are acceptable. The LCA method [6] is based on propagation of covariance state errors very similar to an augmented Kalman filter technique. This technique has been used successfully in the frame of the ATV preliminary trajectory design in order to tune the flight monitoring system thresholds and verify short to midterm trajectory behaviour for nominal manoeuvres and CAMs. The method provides very fast results with respect to MC analyses, and it is conservative under certain hypotheses (such as the linearity of the problem), thus it is suitable for preliminary design and validation of the RDV strategy and guidance, but does not replaces the MC analysis. Full MC non-linear analyses shall be done to validate the trajectories for the nominal, the worst case, and the contingency scenarios (e.g. recovery after navigation chain loss, thruster failure, collision avoidance maneuvers starting from anomalous initial conditions, …). Contingency analyses shall cover for different situations contemplating FDIR detection & recovery, addressing all phases of the mission from phasing and long range navigation to capture, servicing operations, and release, but also recovery from emergency CAMs.

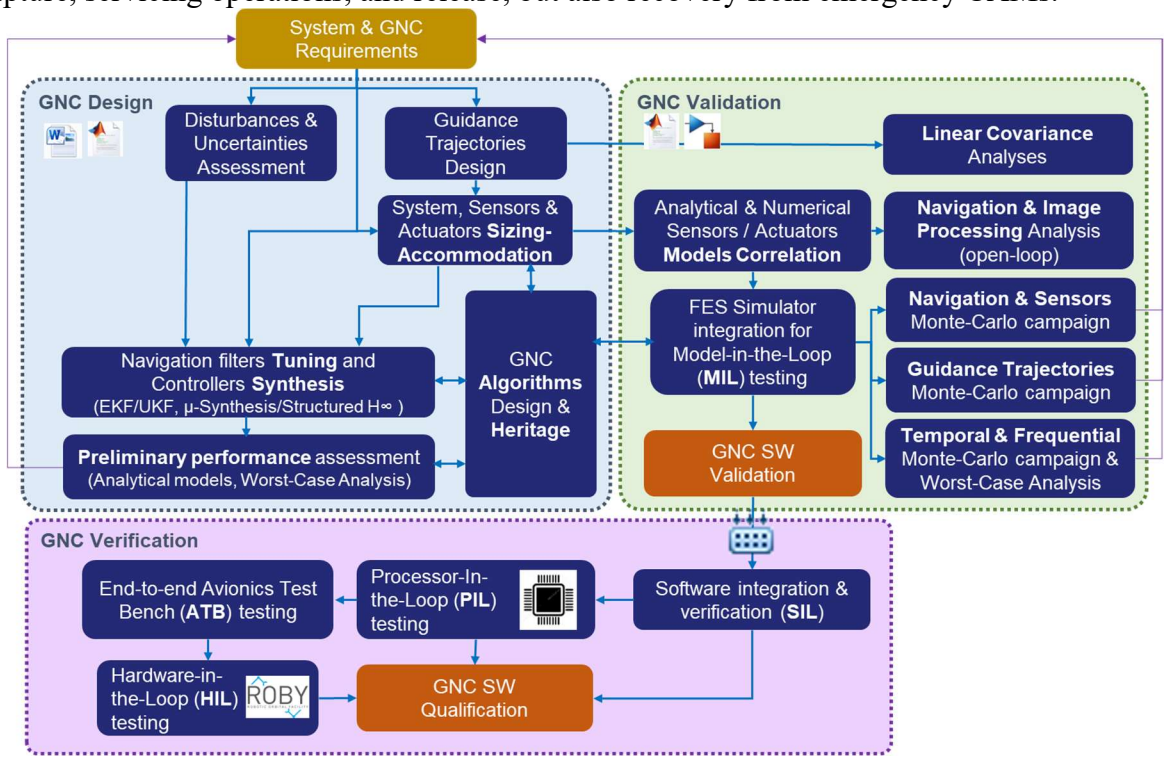

Figure 3: GNC Design, Validation, and Verification process

At this stage, open-loop navigation chain simulations must be carried out. A dedicated robustness campaign shall be made with a synthetic image generator and IP algorithms in-the-loop. In this sense, several commercial or internal tools (ex. Thales Alenia Space image generator SPICAM, ESA PANGU, etc.) allow to simulate different illumination conditions on the spacecraft surfaces and thus on the performance and robustness of GNC. Extensive tests in ground test facilities shall be performed to de-risk and calibrate certain parameters which are not perfectly modelled in MIL testing. For example, the IP algorithms perform differently with images from real cameras, and most of time a re-calibration of them is needed. Not all facilities are suitable to test the entire scenario: some are mainly

used for the approach phase of the RDV, the mission and the spacecraft mock-up must be properly scaled and particular attention must be paid on reproducing (and varying) the illumination conditions. This class of facilities (e.g. Thales Alenia Space ROBY in Cannes, GMV Platform-Art© in Madrid - [8],[9]) are suited for SIL, PIL and HIL to test the overall GNC closed loop for the RDV phases (see Sec.4.2).
Advanced phases of the IOS project make extensive use of several GNC tools from Robust control synthesis, frequency analyses, scattering and worst case analyses (WCA), up to extensive performance and Robustness & Sensitivity (R&S) campaign in MIL environment making use of the FES simulator. A reference run allow to adjust the tuning of the different algorithms and to analyses the main performances in closed-loop, and Monte Carlo R&S analyses shall be used to derive suitable confidence levels with temporal or frequential interpretation validating GNC performance requirements. The R&S campaign allow testing the robustness of the GNC architecture and tuning to scattered parameters representative of model uncertainties. In fact, the reference run simulates the behaviour of the servicer in a condition where its main features are known. This condition is optimistic, but not strictly unrealistic, as dedicated in-orbit calibration procedures could allow the refinement of some parameters before engaging into the final approach phase. However, some residual uncertainty will still remain. Thus, it should be proven that the GNC application allows to cover these cases, in order to show the robustness of the solution and quantify the performance degradation on realistic or slightly degraded scenarios. The test campaign is done using the same flight plan defined for the reference run. In order to perform the overall R&S GNC campaign, a representative model of the IP and computer vision chain can be used, if nominal and worse cases analyses have been separately performed to validate the navigation chain.
Other derisking activities at this stage might include tests in air-bearing facilities, or in facilities able to represent microgravity, in order to simulate the free floating behaviour of the platform and the dynamic response at contact, and to test critical mating operations and strategies (e.g. robotic arm berthing & grasping, docking and un-docking).
The Validation phase ends with the CDR (Critical Design Review), as pictured in Figure 2.

4.2 GNC Verification

GNC Verification makes use of the Avionic Test Bench (ATB) and robotic test bench facilities to verify the compliance with the requirements (Figure 3). In the last few years, the emergence of model-based system engineering techniques, combined with the consolidation of the modelling, simulation and code generation tools, have offered an opportunity to deploy a consistent framework for rapid algorithm prototyping which spans from preliminary design up to functional validation on representative avionics. Figure 4 shows the V-cycle for the AOCS/GNC development process with automatic code generation. This framework, developed in Thales Alenia Space, is particularly well suited for R&D GNC studies, as it allows to evolve very quickly from design and early characterization of system performances based on simulations, to the demonstration facility (e.g., avionic test bench, “flat sat”, or robotic bench). The framework is based on common building blocks and processes used by Thales Alenia Space teams for all their AOCS/GNC flight software development and it is currently used for the EROSS-IOD advanced phases ([5],[10]). Flight SW is thus automatically generated making use of this pre-validated autocoding framework and tools. SIL non-regression tests verify conformity with respect to MIL tests. PIL testing verify SW CPU and memory allocations, which should have already been properly sized during early processor integration derisking activities. Note that PIL tests are a form of SIL tests where the OBSW algorithms are tested into the RAM of a flight representative motherboard. PIL allows testing the GNC SW in flight realistic conditions with respect to the avionics (representative processor of the flight models). The ATB validates the overall interconnected functional chains at functional level allowing PIL and HIL testing. This real-time facility incorporates an on-board computer running the autocoded GNC functional algorithms in real-time, connected to a number of sensors and actuators

in the loop. An external simulation computer generates a simulated response, which is used to stimulate the sensors (for example, using robotic facilities). These sensors generate measurements that are processed in real-time by the on-board computer, which generates commands for the actuators that are also fed back to the external simulation computer. Overall HIL integration and testing is to be accompanied by tests in robotic test bench facilities to verify functional, performance, and robustness requirements with real laboratory images. Please note that image generators are to be previously validated and correlated with real vision systems HW, laboratory and flight images in earlier phases (see Sec.4.1). After this performance testing, the GNC SW application usually undergoes the usual SW qualification in the end before releasing the flight version.

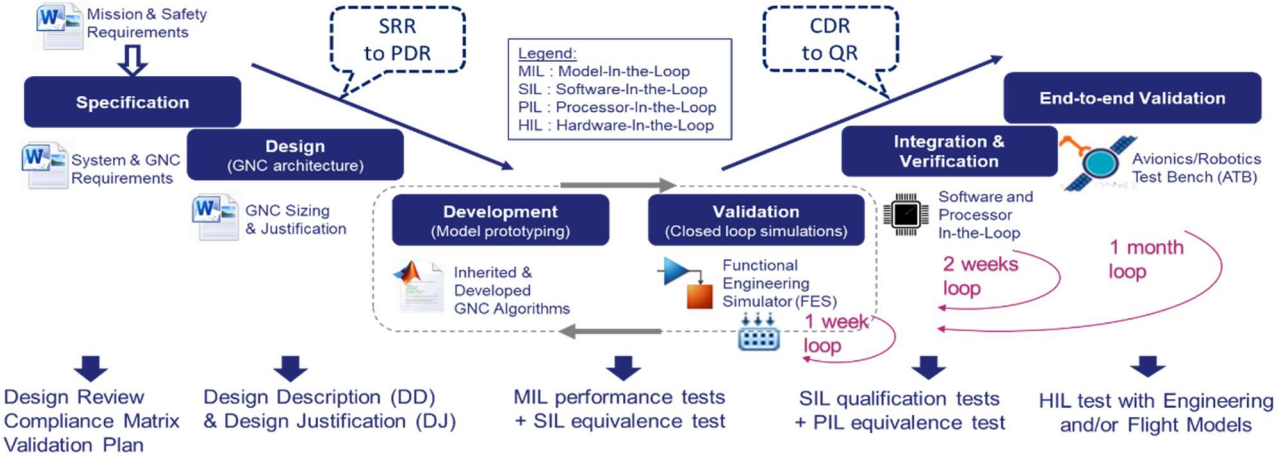

Figure 4: V-cycle for the AOCS/GNC development process with automatic code generation

4.3 In Orbit Testing and In Orbit Demonstration

Experience had shown that it might be difficult for ground test facilities to duplicate all the aspects of the space environment that have an impact on the relative sensor performance. In Orbit Testing (IOT) may be required in addition to ground testing, to subject new hardware and software to a wider range of flight conditions (particularly in-orbit illumination). Moreover, In-Orbit fine calibration and re-tuning of IP algorithms, GNC, and Robotic algorithms shall be performed prior to the nominal mission and after the commissioning of the servicer. Moreover, manoeuvre such as CAM shall be tested outside the AZ before initiating the CPO. It should be noted that in [1] it is required for all the capabilities and functionalities needed for mission safety to be commissioned in-orbit before nominal operations.

In some peculiar case, whole end-to-end In Orbit Demonstration (IOD) could be required [6], in compliance with the ISO 24113 standard on Space Debris Mitigation: any new technology or approach for a servicing mission inside a protected region should be qualified during an IOD mission. Demonstration in Low Earth Orbit (protected region A) should occur at sufficiently low altitudes to comply with the ISO24113 rule while also being considerate of human spaceflight activities. Demonstration in the Geostationary orbit (protected region B) should be carried out outside the region.

5 CONCLUSION

In this paper we have focused on the impact of safety guidelines and requirements on the design and validation of the GNC system for In-Orbit-Servicing. To support it, a special attention has been given to the transition between zones and phases, Abort and CAMs capabilities, passively safe trajectories, control of the stack, and capture/release operations. The GNC design process has been detailed,

describing the workflow from GNC requirements to GNC qualification, through the steps of GNC design, GNC validation and GNC verification and during the different phases of a programme. Tools and analysis to be carried out in the V&V phases have been discussed.
This V&V pipeline is currently implemented in the EROSS IOD programme [4][5], expected to be launched in 2026.

6 REFERENCES

[1] https://blogs.esa.int/cleanspace/2021/11/15/esa-publishes-guidelines-for-safe-close-proximity-operations/ ESA's Guidelines on Safe Proximity Operation, Issue 2.0.

[2] Fehse, Wigbert. Automated rendezvous and docking of spacecraft. Vol. 16. Cambridge university press, 2003.

[3] International Rendezvous System Interoperability Standards, 2019.

[4] D. Casu, V. Dubanchet, H. Renault, A. Comellini, P. Dandré, EROSS+ Phase A/B1 Guidance, Navigation and Control design for In-Orbit Servicing, ESA GNC-ICATT 2023.

[5] V. Dubanchet, D. Casu, A. Comellini, A. Giglio, J.A. Bejar Romero, S. Torralbo Dezainde, M. Alonso, EROSS+ ground demonstrations from Model to Hardware in the Loop validation, ESA GNC-ICATT 2023.

[6] D. Geller, "Linear Covariance Techniques for Orbital Rendezvous Analysis and Autonomous Onboard Mission Planning", JGCD, doi: 10.2514/1.19447.

[7] French Space Operations Act, Projet d'amendement, December 2022.

[8] V. Dubanchet, S. Andiappane, D. Mora Portela, A. Rodríguez Reina, M. Suatoni, "Experimental assessment of I3DS performances: a suite of sensors for on-orbit rendezvous", in *Proceedings of the 70th International Astronautical Congress (IAC)*, Washington D.C., United States, 21-25 October 2019, IAC-19.D3.2B.2x49494.

[9] V. Dubanchet, et. al., "EROSS project – Ground validation of an autonomous GNC architecture towards future European servicing missions", in *Proceedings of the 70th International Astronautical Congress (IAC)*, Dubai, United Arab Emirates, 25-29 October 2021, IAC-21,D3,2B,10,x64910.

[10] P. Dandré, et. al., "AIMONS, Validation & Verification process update of GNC OBSW application", in P*roceedings of the 12th ESA Conference on Guidance, Navigation & Control Systems*, Sopot, Poland, 2023.