THE CHALLENGES OF THE FDIR DESIGN IN HERA SPACECRAFT: SPACECRAFT AUTONOMY AND INTERACTION WITH THE CUBESATS

Ylenia Di Crescenzio [(1)]

[(1)] *OHB System AG, Universitätsallee 27-29, D-28359 Bremen, ylenia.dicrescenzio@ohb.de*

ABSTRACT:

Hera is ESA's contribution to the Asteroid Impact and Deflection Assessment (AIDA) collaboration. As part of the world's first test of asteroid deflection, Hera will perform a detailed post-impact survey of the target asteroid, Dimorphos – the orbiting moonlet of a binary asteroid system known as Didymos. While doing so, Hera will also demonstrate multiple novel technologies such as autonomous navigation around the asteroid and gather crucial scientific data to help scientists and future mission planners to better understand asteroid compositions and structures.

Additionally, Hera will carry two CubeSats (called "Milani" and "Juventas") which will detach from the probe after arriving at the Didymos system and conduct experiments independently.

OHB System AG has been awarded by ESA as the prime contractor for the design and manufacturing of the Hera spacecraft. Hera has been approved in the ESA ministerial of 2019 and is planned to be launched already in October 2024 in order to arrive at the Didymos system at a time that allows sufficient radio contact with Earth. Therefore, the schedule for the development, integration and testing of this spacecraft is very tight.

The Hera spacecraft design also includes FDIR (Failure, detection, Isolation and Recovery) as key element to ensure the integrity of the spacecraft in case of anomaly. The starting point of the FDIR design is the analysis of the relevant equipment failures. The different subsystem FDIR need to be harmonised with each other. The fundamental objective of FDIR is to isolate the failure and perform the required recovery to guarantee the spacecraft's safety and survival. As common in most spacecraft missions, Hera FDIR is defined in different levels with the goal to attempt recovery on the lowest level possible, close to the root cause of the anomalous behaviour.

The paper will describe how the complexity of the spacecraft and the tight schedule have impacted the design and the validation of the FDIR concept. Additionally, since Hera is the first ESA mission that foresees the usage of two CubeSats in a deep space mission, the interface with the mother spacecraft will be described. The design of the CubeSats is completely independent from the mother spacecraft. However, during the 800 days cruise phase, the CubeSats are hosted inside the mother spacecraft. Therefore, the Hera FDIR is also considering CubeSat failure isolation when they are in stowed position. Furthermore, Hera FDIR covers CubeSat anomaly detection during the CubeSat deployment phase.

Once the CubeSats are deployed, Hera acts as a space-to-ground relay for both Milani and Juventas. In this phase, the Hera spacecraft is transparent for the CubeSats since it merely stores and routes TM and TC to ground.

The operations at the asteroid system last approximately six months during which the mission objectives shall be fulfilled. Different sub-phases have been defined in which the Hera S/C shall fly progressively closer hyperbolic arcs over the Didymos system. During this phase, the S/C makes use of (semi-)autonomous navigation. The different phases pose challenges to the FDIR design which will be described in detail in the paper.

INTRODUCTION ON HERA MISSION

As part of the world's first test of asteroid deflection, Hera spacecraft, named for the Greek goddess of marriage, will perform a detailed post-impact survey of the target asteroid, Dimorphos – the orbiting moonlet of a binary asteroid system known as Didymos.

Now that NASA's DART mission has impacted the moonlet, Hera will analyse the mass of Didymoon, the shape of the crater, as well as physical and dynamical properties of the orbiting moonlet. The spacecraft would perform high-resolution visual, laser and radio science mapping of the moon, which will be the smallest asteroid ever visited, to build detailed maps of its surface and interior structure.

In addition, Hera will demonstrate new technologies: from autonomous navigation around an asteroid to low gravity proximity operations. The spacecraft will operate like an autonomous vehicle, fusing data from different sensors to build up a coherent model of its surroundings. The resulting autonomy should let Hera navigate safely as close at 200 metres from the surface of the smaller asteroid 'Didymoon', enabling the acquisition of high-resolution scientific observations down to 2 cm per pixel – focused on the impact crater left by the DART spacecraft crashing into Didymoon to divert its orbit.

Hera will also deploy Europe's first 'CubeSats' (miniature satellites) into deep space for close-up asteroid surveying, including the very first radar probe of an asteroid's interior.

Spacecraft Overview

The Hera spacecraft is built by an industrial consortium led by OHB System AG. The spacecraft is a small-to-medium-size planetary spacecraft with a cubic shape, 1.6 × 1.6 × 1.7 meters, and a mass of approximately 1280 kg. It is powered by 13 m^2 of solar panels. Power storage is achieved thanks to a Lithium-Ion battery. A Power Conditioning and Distribution unit (PCDU) is in charge of distributing the power to the different units as well as providing a driver interface for the firing of explosive and non-explosive actuator components.

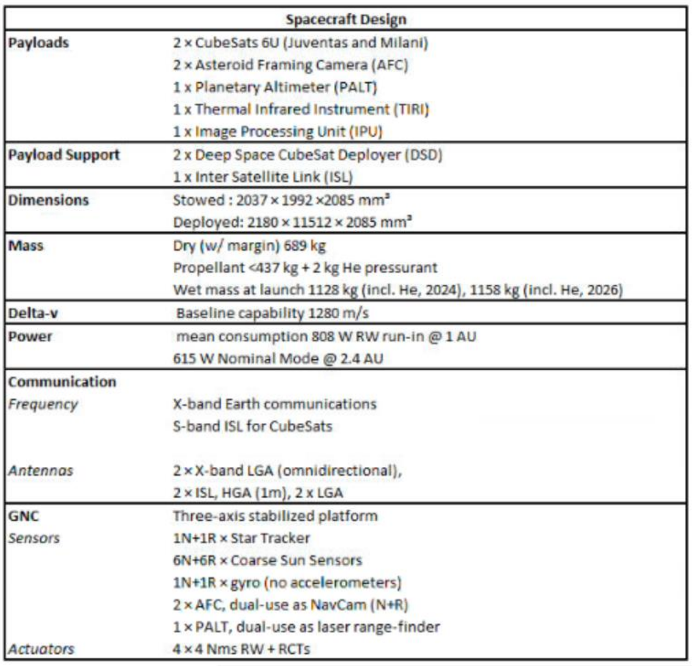
Hera is three-axis stabilized. Attitude is maintained by four reaction wheels, as well as gyros, star trackers, Sun sensors, and the Asteroid Framing Cameras. The Guidance Navigation and Control (GNC) software also includes functionalities for fully autonomous guidance and for the autonomous computation of manoeuvres during very close fly-bys in the so-called Experimental phase. In this phase also a planetary altimeter will be employed for attitude guidance.

Hera is also equipped with a bi-propellant pressure regulated chemical propulsion subsystem used for orbit and attitude manoeuvres. It is equipped with three nominal & three redundant 10 N engines, the so-called Orbit Control Thrusters (OCTs) for performing the nominal major impulsive transfer manoeuvres. For specific low thrust manoeuvres, for momentum management, pointing in contingency modes, as well as for attitude control during cruise and during boost manoeuvres, the propulsion subsystem has sixteen 10 N Reaction Control Thrusters (RCTs), including eight nominal and eight redundant thrusters.

Communication with ground is performed in X-band with a fixed high-gain antenna and two low-gain antennas. The high gain antenna is used to communicate with ground for most of the lifetime, while the two low-gain antennas provide omnidirectional coverage during the first weeks of the mission and in the case of failures leading to the impossibility of maintaining a good three-axis attitude pointing accuracy. The communications subsystem will transmit X band telemetry at different rates depending on the distance to Earth.

The environmental conditions during transfer and then in the vicinity of the asteroid have led to the need for a dual passive and active thermal control design. The hot conditions close to the Sun are managed with resources like radiators and coatings. On the other hand, heater power is provided to keep the different units in their optimal operational temperatures.

The Data Handling Subsystem is composed by On-Board Computer (OBC) using dual-core processor, mass-memory for the storage of housekeeping, navigation, and science data and two Remote Terminal Units (RTU), one for the interface to the platform and payloads units and one specifically devoted to interface with the propulsion subsystem. The on-board software runs on one core of the OBC, and its major high-level components are the so-called Central Software (CSW) and the GNC avionics software. On the second core the central software can load and start the Image Processing Software (IPSW), which is needed for the operations at the asteroid.



Spacecraft Design	
Payloads	2 × CubeSats 6U (Juventas and Milani) 2 × Asteroid Framing Camera (AFC) 1 x Planetary Altimeter (PALT) 1 x Thermal Infrared Instrument (TIRI) 1 x Image Processing Unit (IPU)
Payload Support	2 x Deep Space CubeSat Deployer (DSD) 1 x Inter Satellite Link (ISL)
Dimensions	Stowed : 2037 × 1992 ×2085 mm^3 Deployed: 2180 × 11512 × 2085 mm^3
Mass	Dry (w/ margin) 689 kg Propellant <437 kg + 2 kg He pressurant Wet mass at launch 1128 kg (incl. He, 2024), 1158 kg (incl. He, 2026)
Delta-v	Baseline capability 1280 m/s
Power	mean consumption 808 W RW run-in @ 1 AU 615 W Nominal Mode @ 2.4 AU
Communication	
Frequency	X-band Earth communications S-band ISL for CubeSats
Antennas	2 × X-band LGA (omnidirectional), 2 × ISL, HGA (1m), 2 x LGA
GNC	Three-axis stabilized platform
Sensors	1N+1R × Star Tracker 6N+6R × Coarse Sun Sensors 1N+1R × gyro (no accelerometers) 2 × AFC, dual-use as NavCam (N+R) 1 × PALT, dual-use as laser range-finder
Actuators	4 × 4 Nms RW + RCTs

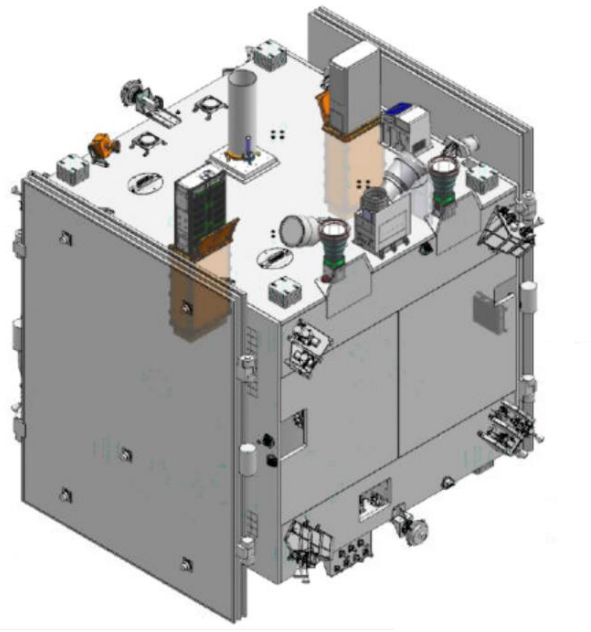


Figure 1. Summary of the Hera Spacecraft

To accomplish its goal and to produce the expected planetary defence and science knowledge, the Hera spacecraft will carry several instruments. The onboard instruments of the Hera mission are [1]:

- Two Asteroid Framing Cameras (AFCs): Their main purpose is navigation and scientific activities requiring observations of the target asteroid system from multiple positions and from various distances during the mission. They will also contribute to the measurement of Dimorphos's mass by providing the necessary data to evaluate the dynamical properties of both asteroids.
- A Spectral Imager (Hyperscout): it provides spectral images of Didymos and Dimorphos in the visible–near-IR wavelength range diagnostic. It will allow searches for evidence of variation in space-weathering effects (subtle spectral slope and silicate feature strength differences) from the DART impact crater, ejecta deposition, and possible resultant surface movement on Dimorphos, as well as spin-induced resurfacing processes on Didymos.
- A microLIDAR (PALT): performs range measurements that will be used to support asteroid 3D topography, fall velocity, wobble of the asteroid (rotation measurements), and target albedo (the instrument measures the power of the received pulse, making it possible to calculate the target reflectivity). The instrument can also be used to support near-asteroid navigation.
- A thermal Infrared Imager (TIRI): is used to investigate thermophysical properties of the surface of an asteroid, especially for the surface particle size distribution and for the surface

thermal inertia of boulders, which is related to microporosity. Using the multiband functions, TIRI will also compare the materials of Didymos and Dimorphos and map the composition difference between the inside and outside of the artificial crater excavated by the DART impact.

- An experimental Image Processing Unit (IPU), to facilitate on-board image processing via the implementation of a vision-based algorithm for real time navigation on-board the S/C, and thus enhance the platform's autonomous navigation capabilities. The IPU runs the same algorithms as the image processing software but implemented in FPGA (Field Programmable Gate Array) rather than software.
- A Spacecraft Monitoring Camera (SMC) that will be used to monitor the transferring of the CubeSats Juventas and Milani from stowed to exposed configuration (deployment phase) and the release of the CubeSats into open space (release phase) for public outreach, as well as operational investigation purposes.
- Intersatellite link transreceiver: the main goal is to guarantee the correct communication (sending telecommands and receiving telemetry) between the Hera mothercraft and the CubeSats "Juventas" and "Milani". However, the direct communication between these three objects offers a unique opportunity to carry out, for the first time, a radio science experiment involving precise range-rate measurements between the CubeSats and the mothercraft. Communication is done using S band, with a maximum range of 60 km.

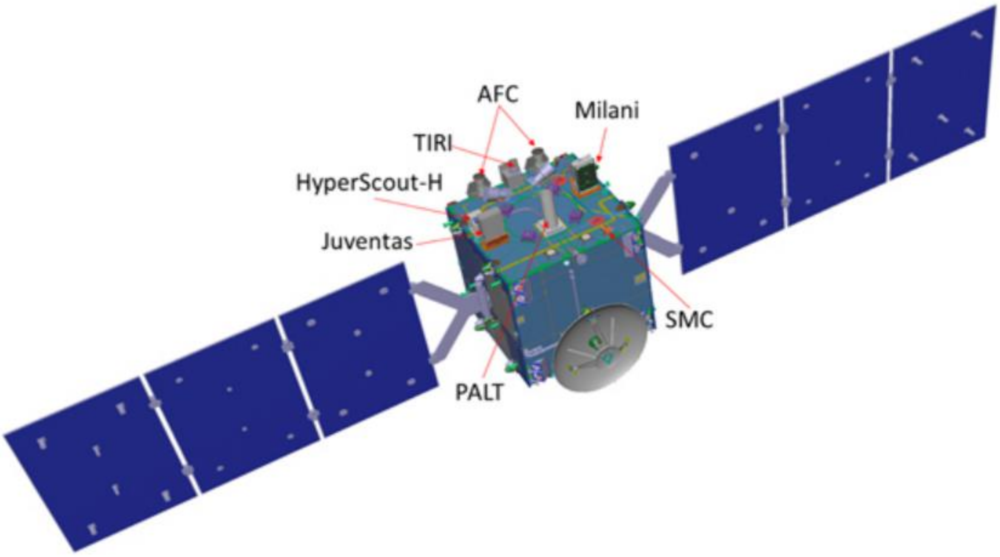


Figure 2. Hera Payload Overview

As already mentioned, Hera will carry two CubeSats that will be deployed at close proximity to Dimorphos and will communicate with the mother craft through the ISL transceiver mentioned above. The two CubeSats are as follows [2]:

- Juventas: It is a 6U CubeSat developed by a consortium led by GomSpace and devoted to the geophysical characterization of Dimorphos.
- Milani: It is a 6U Cubesat developed by Tyvak International with the main goal to perform independent detailed characterization of Didymos and Dimorphos at distances of 5−10 km, supporting Hera observations and enhancing the overall mission science return.

Hera mission Timeline

Hera has been approved in the ESA ministerial of 2019 and is planned to be launched already in October 2024 in order to arrive at the Didymos system at a time that allows sufficient radio contact with Earth.

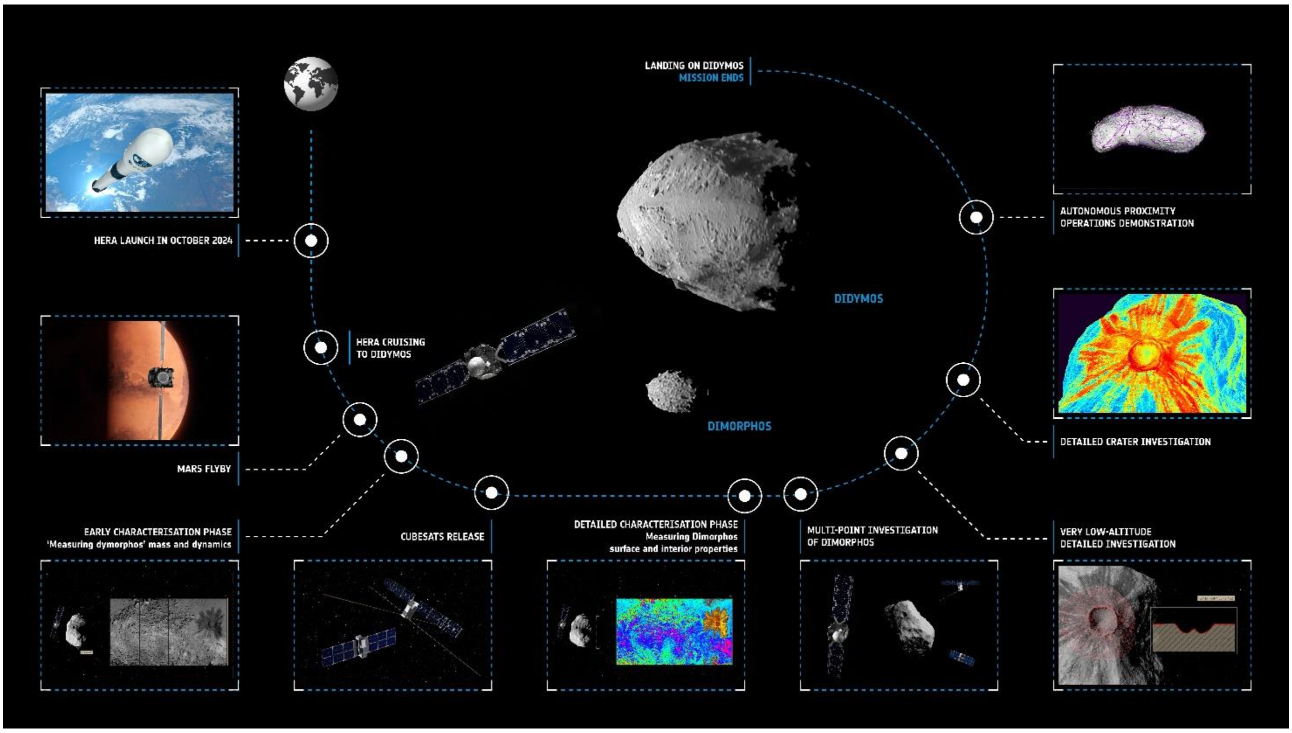

LANDING ON DIDYMOS
MISSION ENDS
HERA LAUNCH IN OCTOBER 2024
AUTONOMOUS PROXIMITY OPERATIONS DEMONSTRATION
DIDYMOS
HERA CRUISING TO DIDYMOS
DIMORPHOS
DETAILED CRATER INVESTIGATION
MARS FLYBY
EARLY CHARACTERISATION PHASE
'Measuring dymorphos' mass and dynamics
CUBESATS RELEASE
DETAILED CHARACTERISATION PHASE
Measuring Dimorphos surface and interior properties
MULTI-POINT INVESTIGATION OF DIMORPHOS
VERY LOW-ALTITUDE DETAILED INVESTIGATION

Figure 3. Hera Mission Time-line overview [3]

After launch and a ~2-days Launch Early Operation Phase (LEOP) in October 2024, the Hera spacecraft is expected to have acquired Sun pointing with its solar arrays deployed. The Commissioning Phase will start immediately after and last for about 2 months, where the functionality of the different spacecraft components will be assessed, including payload health checks. In the first days of commissioning, once the trajectory is determined on ground, a deep space manoeuvre will be performed. The manoeuvre will also be used to correct launcher insertion errors. At this point Hera spacecraft is ready to start its long cruise toward the target asteroids.

The 2-years Interplanetary Transfer Phase to the asteroid system includes another deep space manoeuvre and a Mars swing-by in March 2025.

The operationally safe arrival sequence is going to commence in a distance to the asteroid system of about 300,000 kilometres. In a series of manoeuvres of decreasing delta-v, Hera spacecraft will approach the asteroid system to arrive operationally safe on a hyperbolic arc at 30 kilometres from the Didymos system.

At a distance of 30 kilometres, the Proximity Operations Phase begin. The spacecraft will travel on hyperbolic arcs around the asteroid pair, while collecting data and transmitting it back to Earth.

After an Early Characterization Phase with the closest approach at a distance of 20 kilometres to the asteroid pair, the CubeSats are released from Hera during the Cubesat Deployment Phase. During the Detailed Characterization Phase, Hera and the released CubeSats will continue the asteroid measurements. As the navigation solution has already been refined and tested in the Early Characterization Phase, Hera can safely approach the Didymos system down to 10 km in distance.

This allows for further improvements of the navigation solution, so that during the Close Observation Phase, the pericentre can be lowered down to 4.5 km with respect to Dimorphos.

The Proximity Operations are concluded by the Experimental Phase. In this phase, Hera spacecraft performs very close fly-bys in Autonomous Mode, during which the fully autonomous guidance and navigation will rely on altimeter measurements and feature tracking. The goal is to take the Hera spacecraft at a distance smaller than 1.5 km to Dimorphos, to allow for high-resolution images of the DART impact crater.

Nominally, Proximity Operations are expected to last 6 months, till the end of May 2027. Afterwards, there is room for a potential Extended Operations Phase.

During the End-of-Life Phase, the HERA spacecraft might attempt landing on Didymos, while the CubeSats might do the same on Dimorphos.

FAULT DETECTION ISOLATION AND RECOVERY

The Hera spacecraft design also includes FDIR (Failure, detection, Isolation and Recovery) as key element to ensure the integrity of the spacecraft in case of anomaly. The design of the FDIR includes a trade-off between the maximization of autonomy and mission availability on one side, and satellite design and validation complexity on the other side. FDIR relies on three basic architectural steps to achieve its goals [4]:

- The ability to notice that something bad has happened (fault or failure detection, either by observing the event itself or by observing the change in the system or component state).
- The ability to isolate the fault or failure. This has two aspects: the systems’ ability to uniquely identify the fault or failure from the changes witnessed in the observables, and to prevent it from propagating and causing other failures to occur as a knock-on effect. Of course, it can also be that the same observable is used to diagnose more than one potential failure.
- The third and final step is to recover in time from the fault or failure. This can entail many things, such as simply doing nothing, and waiting for ground to take control and solve the issue. Another approach might be to passivate the faulty component by switching to the redundant unit. A third possibility foresees to start some on-board autonomy function that tries to resolve the failure with a system or subsystem reconfiguration in a different mode.

Overview on the FDIR Architecture:

FDIR complexity should fit the mission requirements. There are two major types of FDIR:

- Simple: in case of single failure the system is put in safe mode and ground intervention is expected afterwards
- Complex: the mission should be continued as much as possible by putting in place more complex recovery procedures on board.

In figure 4 it is possible to some FDIR architecture from the simplest one to the most complex one.

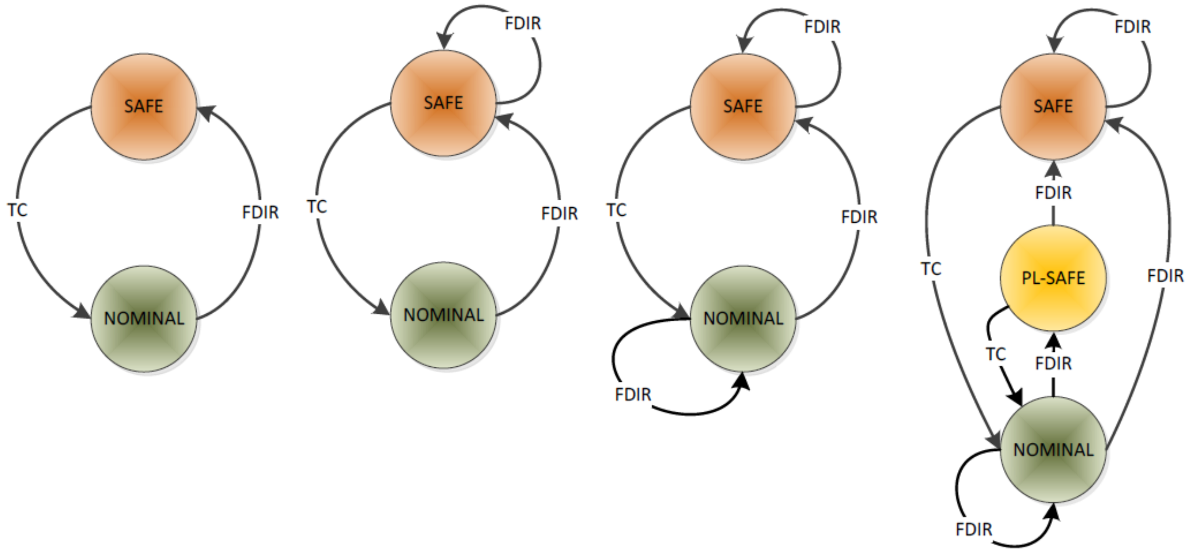


Figure 4. Overview of possible FDIR architecture and their complexity

FDIR levels play an important role in the characterization of the structure of an FDIR architecture. The following hierarchical model is often considered to be the baseline for the FDIR design of different spacecraft mission:

- Level 0: Internal failure without any impact on the rest of the system and its global behaviour (e.g. internal unit EDAC) which is usually recovered by the unit itself without any need of reconfiguration.
- Level 1: Component failure degrading or interrupting the service provided by this component, that can be easily recovered by a switch-over to the redundant unit or resetting the unit.
- Level 2: Failure related to a subsystem (i.e. which cannot be related to a particular component of that subsystem, such as anomalous attitude pointing accuracy), that can be resolved by a reconfiguration at sub-system level (e.g. reconfiguration into sun-pointing mode to optimize the sun incidence over the solar array and, if needed, switching off payload unit)
- Level 3: Central computer irrecoverable failure that degrades or interrupts the mission and that requires a reset of the on-board computer or a switch-over to the redundant on-board computer lane.
- Level 4: Major on-board failure that causes global system abnormal operation, leading to definitive loss of part or all the spacecraft that are recovered by a transition to Safe Mode in which only the essential unit are kept ON.

Overview on Hera FDIR:

In Hera spacecraft, FDIR recovers the unit level failures without Ground intervention by switching over to the redundant unit when available or by switching off the faulty unit. In case more than one failure or complex failures happens, FDIR aims to keep the S/C safe via switching off the payload and reconfiguring the spacecraft into less complex spacecraft modes that it is using all the available redundancies on-board.

Hereafter the main responsibility of Hera FDIR:

- FDIR is responsible to ensure that the different units are kept in their design thermal range, by spotting possible failures on the heater line or in the thermistors reading and reconfigure to the redundant unit to avoid that the unit itself, payload or platform, is damaged by being exposed to a temperature outside the acceptable range. Additionally, it takes care of switching off the unit in case an overtemperature is detected on the internal unit thermistors to isolate a potential unit failure.

- FDIR ensures that the battery voltage does not fall below a predefined value by implementing a cascade of thresholds and reconfigurations up to the hardware level FDIR implemented on the PCDU, which mechanically shout down all the non-essential units.
- FDIR ensures that the current of the unit does not go outside the expected range with a two levels FDIR, the software level that foreseen a unit reconfiguration in case anomalous power consumption is detected and the hardware level implemented directly on the LCL (Latching Current Limiter) for which the unit is mechanically switched-off by opening the LCL that connects the unit with the PCDU.
- FDIR ensures that the GNC software can keep the attitude of the spacecraft in the different spacecraft mode by implementing different cascade of failure detection and reconfiguration. The first level covers the check on the validity of the data provided by the different units (gyro, star tracker) and the checks on the health of the unit itself (temperature, currents) and these failures are isolated with a unit reconfiguration. Additionally, checks on the attitude errors are performed and isolated with a spacecraft mode reconfiguration whenever it is not possible to understand the root cause of the anomaly.
- FDIR is responsible to monitor the time since no telecommand is received by the spacecraft to ensure that there is no issue with the communication with ground. Three different cascade of recovery set to different thresholds have been implemented; from the simple reconfiguration of the transponder from nominal to the redundant one to isolate a potential failure of the transponder to the full spacecraft reconfiguration into Safe Mode with a consequence on-board computer switchover to cover the scenario that the on-board computer is not properly decoding telecommands. Additionally, as last attempt to recover the communication also a switch-over from the high gain antenna to the low gain antenna is executed.
- FDIR ensures that there is no Sun-intrusion on the payload unit’s boresight that may lead to permanent degradation in performance or damage of the units itself. This is done by monitoring the sun illumination angle with respect to the spacecraft body axis and to perform a unit reconfiguration and unit switch-off if the threshold is violated.
- FDIR is responsible to identify possible failure of the thruster during the execution of a manoeuvre and to react to this failure by aborting the propulsion activity and by reconfiguring the spacecraft into safe mode to ensure that there is no issue in controlling the attitude after the reconfiguration.
- FDIR is responsible of monitoring the communication between the central software and the different platform and payload unit and react if an anomaly is identified either by switching off the unit, or by reconfiguring the communication channel to the redundant one. Additionally, as last attempt, a complete OBC processor module reset is executed by FDIR whenever the communication with several units is in fault.
- FDIR is also responsible to monitor that no major failure occurs on the on-board computer itself. This is achieved either by monitoring its health telemetry as current or temperature, and by monitoring OBC internal error logs and task handling performance. If any anomalous behaviour is identified FDIR perform a full OBC reset or switchover with a consequent transition to Safe Mode to avoid that the OBC malfunction would endanger the safety of the mission.

HERA FDIR DESIGN AND MISSION TIMELINE

The basis for the FDIR configuration is the system and subsystem Mode. S/C modes are fully managed by the CSW. Upon commanded transition from one mode to another the CSW commands all subsystems to the needed configuration based on equipment lists and other maintained tables. The GNC-ASW is also commanded to the internal sub-modes according to the mode transition.

Hereafter the list of the mode implemented in Hera:

- Launch Mode (LAU): the main goal is to reach a clearly defined, minimal configuration after power ON and to maintain thermal control during launch.
- Spacecraft Initialization Mode (SIM): the main goal is to execute a set of autonomous activities after separation from the launcher upper-stage to reach a stable spacecraft configuration in terms of attitude control, power generation and thermal control.
- Nominal Mode (NOM): the main goal is to provide all spacecraft functions necessary during nominal operations in the transfer and proximity operations, including communications and pointing performances to operate the platform and the instruments. This includes autonomous GNC functions required for the core mission phases of the proximity operations.
- Autonomous Mode (AUT): experimental mode providing autonomous GNC functions, including feature-tracking navigation and on-board translational-manoeuvre guidance.
- Safe Mode (SFM): this is the first and main barrier to guarantee spacecraft safety in a three-axis stabilized attitude control mode, maximizing communications capability with high-data-rate communications and accelerate ground recovery operations.
- Survival Mode (SUV): second and ultimate barrier to guarantee spacecraft safety in case attitude guidance is lost, or ultimate escalation occurs.

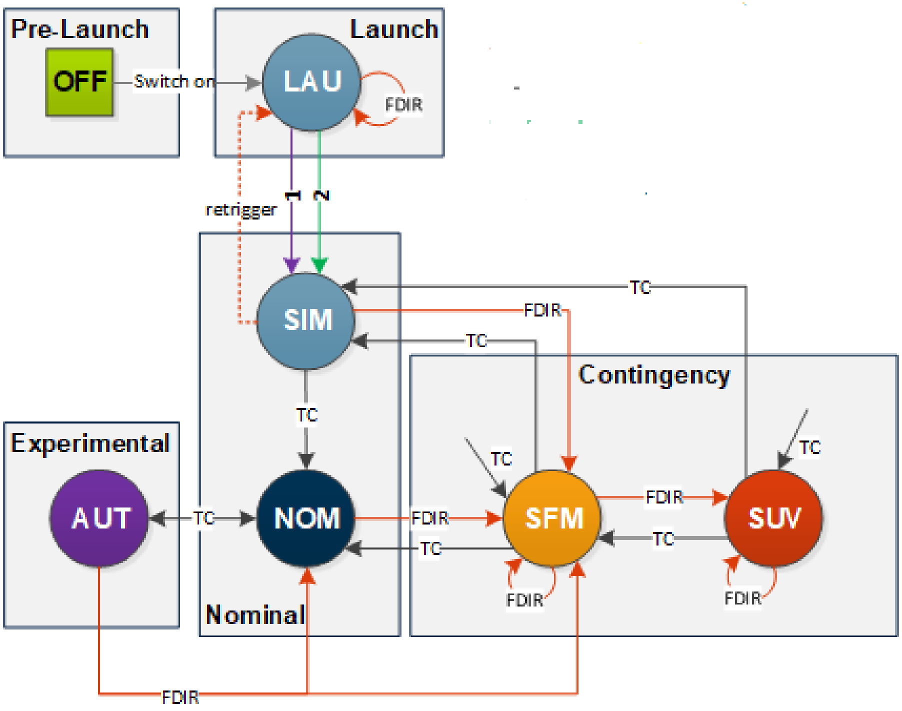


Figure 5. Hera S/C Mode Overview

Hera FDIR during LEOP and Cruise

The LEOP is one of the most critical phases of a mission. Once the spacecraft separates from the dispenser it changes his mode from Launch to SIM. In this phase it performs the following critical activity:

- the Venting of the Propulsion subsystem that it is needed to evacuate all gas present in the tubing upstream of the thrusters and downstream of the pyros-valve

- the Priming of the thruster by firing all nominally closed pyro valves downstream of the propellant tanks, allowing propellant to flow towards the thrusters
- the first Sun Acquisition GNC mode transition using the thruster as actuator.
- deploy the Solar Array Wings.

In Hera all these critical activities are performed by an auto-sequence. To ensure that the design is failure tolerant in this critical failure the following principles have been implemented:

- Nominal and Redundant sides of all units and all interfaces are always executed during the Priming and for the Solar Array deployment, leaving no possibility of untried interface. This removes the possibility of one single failure affecting the sequence.
- In case of unit failure, the spacecraft will switch over to the redundant unit. When needed Nominal and Redundant units are operational so that there is no risk that a switchover is impacting the auto-sequence. This is achieved by setting both RTU ON during venting and priming and both PCDU ON during Priming and during the solar array wings deployment.
- In case of OBC reboot, the auto-sequence will restart on the redundant processor module, skipping all previously executed steps of which the successful execution is tracked via flags set in Safeguard Memory (SGM)

Once the auto-sequence is completed then it is up to ground to command the spacecraft by activated the necessary unit and the perform the required spacecraft mode transition via TC.

The LEOP and the Commissioning phase are also critical because it will be the first time that the different units are switched on in space. Due to this it is important that the FDIR are correctly tuned to avoid false alarm and, at the same time, to react in case of failure to avoid any propagation that could endanger the mission itself.

Once these phases are over Hera will start its long cruise toward the asteroids. In this phase the contact with ground will be reduced to be roughly once a week. It is important that FDIR ensure the autonomy of the spacecraft. To achieve this result, the FDIR will take care of reconfiguring a unit to its redundant one in case the failure can be isolate to the unit level by setting the nominal one to unhealthy. Safety measure at also implemented to avoid that one monitoring can trigger more than once. In fact:

- the SW does not allow to switch-on a unit that it is already set to unhealthy.
- once a monitoring is triggered it remain into fail status till ground interventions

It is worth to mention that a real double equipment failure it is unlikely to happen, especially in a short time-frame as can be one week, therefore the fact that a specific monitoring cannot trigger more than once it is also ensuring that in case a false (not well tuned) alarm is triggered than the redundant unit is kept on and if there is no real failure on-going it can still be used by the spacecraft.

At the same time, if the unit reconfiguration did not fix the issue higher level FDIR will trigger by leading to a S/C transition to Safe Mode. The transition to Safe Mode also ensures that the mission timeline is cleared up and there is not risk that TC loaded on-board of the scheduler are executed. Once the transition is completed the software is also resetting the status of all the FDIR back to running.

Hera FDIR and the CubeSat

As mentioned, Hera will carry two Cubesats which will detach from the probe after arriving at the Didymos system. They will spend the full cruise (~2.2 years) in stowed position inside the Deep Space Deployers (DSD). Deployers are not usually designed to host active Cubesats inside, given that Cubesats are off, during launch ascent, and deployment. On Hera, the Cubesats will be switched on several times during the interplanetary Cruise phase, for the duration of the stowed health check test, which spans from 29 minutes to 45 [2].

When the Cuebsat are in Stowed configuration the connection between Hera and the Cubesat is done via an umbilical electrical and mechanical connection called Life Support Interface Board (LSIB) [2]. Milani and Juventas have their own FDIR configuration. In case of anomalous behaviour, the Cubesat will raise a flag called abort line and Hera will react to it by switching off the units. The abort line is the substitution of a safe mode transition during the cruise phase, and it is used as reaction to critical failure detected by the Cubesat as for example the overtemperature of the battery.

At the same time Hera is also monitoring two temperatures in the interconnection between the motherhood and the spacecraft to avoid that possible overheating of the CubeSat propagates on the main spacecraft.

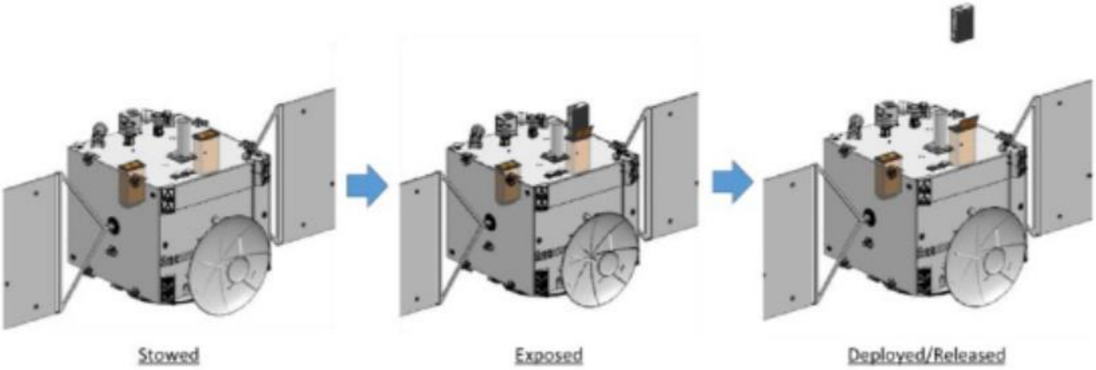


Figure 6. CubeSat and Hera spacecraft

A special care it is also taken by Hera FDIR when the CubeSat are in exposed configuration. In this configuration, the CubeSats are mechanically attached to the Hera S/C, but already exposed to the space environment. The umbilical connection routed through the Deep Space Deployers still provides data and power between Hera and CubeSats.

In case Hera experience a transition to Safe Mode when the CubeSat is exposed the unit is kept ON after the reconfiguration and the switch-off of the non-essential loads and this is achieved by saving the status of the CubeSat in the SGM.

Once the CubeSats are deployed, Hera acts as a space-to-ground relay for both Milani and Juventas thanks to the ISL. In this phase, the Hera spacecraft is transparent for the CubeSats since it merely stores and routes TM and TC to ground. At the same time, the CubeSats will have their own FDIR system that it is completely independent from Hera with Safe mode transition as reaction to mayor failure.

Hera FDIR in Autonomous Mode

The Spacecraft Mode in this phase is expected to be autonomous as this mode allows an autonomous attitude profile that will maintain Didymain or Didymoon in the field of view of the camera. Different image processing technique have been implemented in the GNC SW in the different phases of the proximity operations.

During the Early Characterization Phase and the Detailed characterization Phase the objective of the image processing algorithm is to autonomously determine the Line of Sight to the centre of Didymain (primary in the Didymos binary system), for further use in optical navigation. Indeed, the Line-of-Sight measurement will be used by a navigation filter that will be able to estimate the relative position with respect to the asteroid system. During the Close Operation Phase, the navigation information is obtained by applying the centre of brightness algorithm to Didymoon. In case of anomalous behaviour of the image validity and image processing algorithm FDIR will take care of reconfiguring the spacecraft from the Autonomous Mode to the Nominal Mode with reaction wheels as actuators.

The Crater Observation Flyby will be the most challenging phase for the GNC as it will involve the combination of different technologies that implies autonomous translational navigation and guidance. In fact, during very close fly-by the autonomous navigation solution implemented in Hera is vision based relative navigation system which captures images from one on-board asteroid frame camera. Hera's data-fusion-based guidance and navigation FDIR is designed to identify errors in real time through ongoing sensor cross-checks, to isolate them as needed by triggering sensor or actuator reconfigurations similarly to what it is done for the nominal scenario. In case of extreme emergency, Hera FDIR is designed to trigger an autonomous collision avoidance manoeuvre instead of a Safe Mode transition when the spacecraft is close to the asteroids, and this is also achieved thanks to some flags saved in the SGM. The objective of the Collision-Avoidance Manoeuvre is to ensure that - when activated in the presence of a severe failure - the spacecraft exits the sphere of influence of the system, minimizing the collision risk with any of the asteroids.

CHALLENGES OF HERA FDIR DESIGN

As reported in the ESA website in the design and development of Hera Spacecraft industries from 17 different European country have been involved [3]. One of the first challenges in the design of the Hera FDIR has been the need to merge the inputs coming from the different subsystem and units.

In particular, some fault detection mechanisms are implemented on subsystem level (e.g. the GNC SW have its own logic of detecting failure) or on unit level (e.g. ISL and Hyperscout are generating their own on-board events to notify the user about anomaly detected by the unit itself). At the same time, it was necessary to limit only to the central software the capacity to execute the recovery. This is needed to have a clean configuration after the recovery since it is also very important to consider the interfaces with all the other units and subsystems. On the others hand it is also important to avoid having multiple recovery happening at the same time.

The second challenge on the Hera FDIR design has been the schedule. Since the mission was approved only at the ministerial of 2019 to be launched in 2024 the Hera design could not follow the traditional V model.

To understand how fast the development of Hera mission has been, it is interesting to make a quick comparison to similar ESA mission. In fact, ESA classified as fast mission, series F, mission that follow a fast implementation plan in which the time from selection to launch readiness is less than 10 years. Among this F-class mission it is possible to find Comet Interceptor and Arrakihs. Comet Interceptor has been approved in the same ministerial as Hera and it is planned to be launched in 2029 (~10 years from approval to launch). Arrakihs has been approved in 2022 and it is expected to be launched in 2030 (~8 years from approval to launch).

Mission classified as Small (S-class) as Cheops that has dimensions similar to Hera (1.5*1.5*1.5 m) also requires more than 7 years from development to launch (approved in 2012 and launched at the end of 2019).

By this comparison with similar ESA mission, it is quite clear that Hera implementation plan has been fast and therefore it was necessary to perform some changes on the classical design approach. In Hera the verification and validation of the different functionalities has been, partially, run in parallel with the development of the CSW. To make this possible it was necessary to plan the different test also considering the readiness of the software. Of course, this was increasing the complexity of the test schedule, the complexity of the investigation of the anomaly since it was not always possible to distinguish immediately issue from the hardware respect to software limitation and sometimes it has also led to the need to run delta-test in order to fully close the requirements.

FDIR Implementation

The FDIR of Hera are implemented as part of the Satellite Reference Database (SRDB) using the default Packet Utilization Standard (PUS). In particular, the following services have been used:

- Service 5: Event Reporting.

It is used to notify ground about the anomaly that it is affecting the spacecraft and it has four different severities: info, warning, error, and alarm. The event also contains the information on the generation time.

- Service 12: Monitoring service

It is responsible of the detection of the failure by the implementation of two possible type of monitoring:

  - Limit check: The selected parameter is monitored versus a low or high limit.
  - Expected value check: The selected parameter is monitored versus an expected value.

The service 12 ensure that when the monitoring of a specific telemetry fails, an event report is generated. The Service 12 is extended also to "Functional Monitoring". This new feature implies that the event generation is activated only when more than one failure takes place.

- Service 19: Event and action service

This service is responsible of the recovery from the failure by providing for each event a corresponding action. The action can be a single telecommand or can be the activation of a dedicated sequence for complex FDIR recoveries that require more than one telecommand.

- Service 21: Request Sequence

It is called by the service 19 when the recovery cannot be executed by a single telecommand.

Once all the different services were implemented in the SRDB they were translated into xml files to be integrated in the CSW. It was not possible to implement all the monitoring definitions at once, in fact, the payload unit data management was the last one that was integrated in the CSW. For these reasons, sometimes, even if the telemetries monitored by the FDIR was already available in the SRDB it was still not know by the software and therefore the integration of some specific FDIR had to be postponed to a later stage.

At the same time not all the telemetries can be used for the FDIR, in particular the software did not allow to insert monitoring on some specific datatype as byte array. In this case, it was necessary to modify the telemetries definition to allow the FDIR to be implemented.

It was also important to ensure that the telemetries were calibrated in the proper way and sometimes it was necessary to wait for the calibration to be in place, either at software or at SRDB level, before that the FDIR implementation could be properly done.

Consistency check have been executed prior to the integration of the xml file in the central software. Therefore, each xml files delivery to the central software implies some debugging activities to be executed on the xml file to ensure a smooth integration.

FDIR Validation:

The first step of the validation of the FDIR is the review of the FDIR design respect to all the possible failure tracked in the different failure analysis of the different units to be sure that nothing was missed. The second step is to verify that all these services work as expected and that there have been no mistakes in the implementation. In case a mistake in the implementation is identified it shall be fixed in the SRDB. The updated configuration can be available only after a software patch with the updated xml file. Of course, it is also possible to modify the FDIR definition via telecommand. Event action can be redefined and limits checks on the monitoring can be adjusted but only the fix on the SRDB ensures that the changes is kept also in future software versions.

Once the implementation check is over it is possible to start with proper execution of the FDIR tests. The tests are executed by using all the available platform e.g., the Software Validation Facilities (SVF), the engineering model and the Flight model. In particular, the high number of tests, the time effort to create and execute them, and the difficulties in fault injection on hardware lead to the need to build an efficient modular test approach.

The tests are executed on simulation-based software validation facilities only, whenever pure software functionalities are verified without influence by the hardware. In this environment, it is relatively easy to insert the failure that sometimes are impractical to reach on flight model hardware. Anyway, whenever the hardware is commanded, or it's reconfigured in the scope of FDIR recovery the tests shall be executed (also) on hardware facility (Engineering Model or Flight Model). During this test it is possible to verify the correctness of the time delay in between telecommand executed by the recovery sequence and, also, the interconnection between the unit and the software including spotting possible issue with the telemetries monitor by the FDIR. Sometimes the finding during the different test leads to the need to modify the FDIR definition and to plan the execution of a delta test.

On top of this, complex test scenario that also consider the mission timeline are foreseen to be executed prior to the start of the launch campaign. During these tests, not only the single FDIR is under test but the full behaviour of the spacecraft as system. This is done, for example, by simulating failure during the initial phase when the auto-sequence is running to verify the behaviour of the different spacecraft subsystem and to confirm that no criticality has been identified. At the same time a system level test is also executed by injecting failure on the spacecraft when it is fully operational, with the payload units operational and the CubeSat exposed to confirm that after a critical failure that leads to the reconfiguration into Safe Mode all the subsystems are correctly handled by the CSW.

CONCLUSION

Hera will prepare the way for future interplanetary missions by testing deep-space navigation and guidance, inter-satellite communication between the main Hera spacecraft and its CubeSats as well as proximity operations in the asteroid's extremely low-gravity environment.

The seamless real-time data fusion in an algorithm-based technique is seen as essential to the coming class of autonomous 'space servicing vehicles', tasked with refuelling or repairing satellites or removing large items of space debris.

For these reasons the various lesson learned that will be taken from this mission in the design of the FDIR can became the basis for the FDIR design of future mission not limited to similar interplanetary mission to the asteroid but can be reused in different type of spacecraft project as the coming class of autonomous "space servicing vehicles".

REFERENCES

[1] Patrick Michel, Michael Küppers, Adriano Campo Bagatin, Benoit Carry, Sébastien Charnoz, Julia de Leon, Alan Fitzsimmons, Paulo Gordo, Simon F. Green, Alain Hérique, *"The ESA Hera Mission: Detailed Characterization of the DART Impact Outcome and of the Binary Asteroid (65803) Didymos"* The Planetary Science Journal, 2022.

[2] F. Perez Lissi, P. Martino, D. Escorial, I. Carnelli, "*Main challenges of Cubesat piggyback on an Interplanetary Mission: The HERA Cubesats, a technology demonstration case"* in 4S Symposium, Vilamoura, Portugal, 2022.

[3] ESA, Hera mission - https://www.Heramission.space

[4] "*SAVOIR FDIR Handbook - SAVOIR-HB-003*" 2019.