ESTUDIO PILOTO DEL SISTEMA DE ATRAQUE Y DESATRAQUE DEL HERMES A LA ESTACION ESPACIAL. EVALUACION CUANTITATIVA

HERMES DOCKING/BERTHING SYSTEM PILOT STUDY QUANTITATIVE ASSESSMENT

J. Muñoz Blasco
(EMPRESARIOS AGRUPADOS)

F. J. Goicoechea Sánchez
(IBERESPACIO)

ABSTRACT

This study falls within the framework of the incorporation of quantitative risk assessment to the activities planned for the ESA-HERMES project (ESA/ CNES). The main objective behind the study was the analysis and evaluation of the potential contribution of so-called probabilistic or quantitative safety analysis to the optimization of the safety development process for the systems carrying out the safety functions required by the new and complex HERMES Space Vehicle.

For this purpose, a pilot study was considered a good start in quantitative safety assessments (QSA), as this approach has been frequently used in the past to establish a solid base in large-scale QSA application programs while avoiding considerable economic risks.

It was finally decided to select the HERMES docking/berthing system with Man Tender Free Flyer as the case-study. This report describes the different steps followed in the study, along with the main insights obtained and the general conclusions drawn from the study results.

SYSTEM ANALYSIS

The HERMES Docking Assembly (HDA) will perform the temporary mating of the Hermes Space Vehicle with the Colombus MTFF (Man Tender Free Flyer) as a primary mission.

The overall purpose of the HDA is to provide a pressurized structural connection between HERMES and MTFF to allow transfer of crew, new equipment and utilities. The HDA is attached to the rear frame of the Hermes Resource Module (HRM) as is depicted in Figure1.

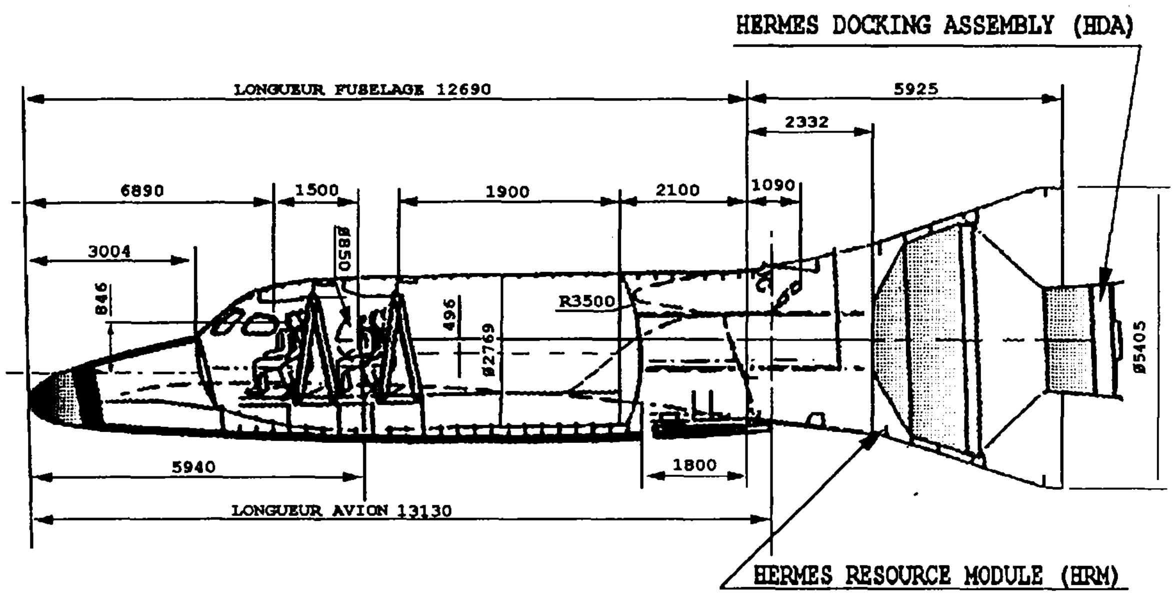


Figura 1. HDA Location

The HDA is divided into the following subassemblies:
- *Structure subassembly.*
- *Guiding/Attenuation subassembly.*
- *Capture latches subassembly.*
- *Structural latches subassembly.*
- *Hatch subassembly.*
- *Sealing subassembly.*

For the docking/berthing activities, a second part is required and provided by the MTFF. It includes: structure subassembly, guiding subassembly, structural latches subassembly and hatch subassembly.

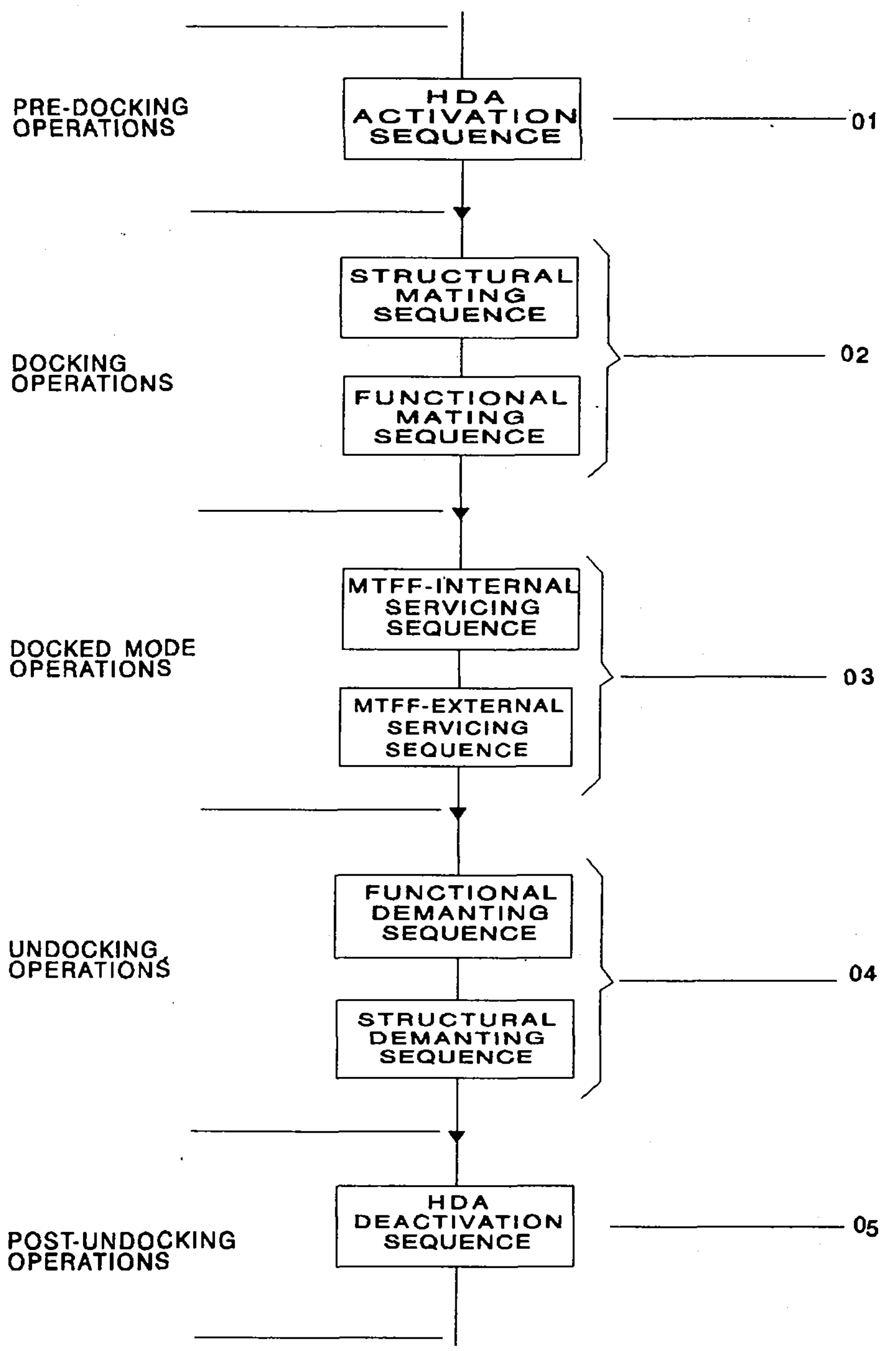
SYSTEM OPERATION

The in-orbit operations included within the scope of the analysis have been grouped and divided into operational sequences as indicated in Figure 2.

HDA FUNCTIONS FOR THE STUDY

According to specific documentation, the various functions which must be assumed by the HDA in the different operating modes are:

HDA OPERATIONAL SEQUENCE
HDA IN-ORBIT OPERATIONAL SEQUENCES



END OF HDA IN-ORBIT OPERATIONS

Figura 2. HDA In-Orbit Operational Sequences

F_1: *STRUCTURAL FUNCTION.*

- F_{1a}: *to provide closure of the HRM pressurized cabin.*
- F_{1b}: *to provide closure of the composite HMS/MTFF pressurized volume (pressure barrier).*
- F_{1c}: *to provide closure of the pressurized passageway, at HMS/MTFF interfaces.*
- F_{1d}: *to provide structural attachment for the composite HMS/MTFF.*
- F_{1e}: *to provide attachment points for the HDA subassemblies.*

F_2: *ENVIRONMENTAL PROTECTION FUNCTION.*

- F_{2c}: *to provide equalization of both vehicles' electric potentials.*

F_3: *HDA CONFIGURATION MANAGEMENT FUNCTION.*

- F_{3a}: *to allow HDA monitoring by the HMS Spacionics.*

F_4: *MECHANICAL DOCKING/BERTHING FUNCTION.*

- F_{4a}: *to provide the capture of MTFF Docking port.*
- F_{4b}: *to provide the centering and closure of both vehicles.*
- F_{4c}: *to provide cancelling of relative velocity between vehicles and absorption of residual energy.*
- F_{4d}: *to provide the locking of the HMS/MTFF structural interface.*
- F_{4e}: *to provide the latching of the HMS/MTFF structural interface.*
- F_{4f}: *to provide the unlatching of the HMS/MTFF structural interface.*
- F_{4g}: *to provide the release of the MTFF.*

F_5: *FUNCTIONAL CONNECTION/DISCONNECTION.*

- F_{5a}: *to allow pressurization of passageway by HMS ECLSS.*
- F_{5b}: *to provide linkage/separation of HRM and passageway pressurized volumes.*
- F_{5c}: *to support functional connection of both vehicles.*
- F_{5d}: *to support functional disconnection of both vehicles.*
- F_{5e}: *to allow depressurization of passageway by HMS ECLSS.*

F_6: *MTFF SERVICING SUPPORT FUNCTION.*

- F_{6a}: *to support crew transfer to/from MTFF.*
- F_{6b}: *to support equipment transfer to/from MTFF.*
- F_{6c}: *to support EVA exit in docked mode.*

Later on, the functions that should be adequately safeguarded in each one of the operational modes were identified as shown in Table 1.

	OPERATIONAL MODES				
FUNCTION	*01*	*02*	*03*	*04*	*05*
F1a	X	X		X	X
F1b		X	X	X	
F1c			X		
F1d		X	X	X	
F1e	X	X	X	X	X
F2c		X			
F3a	X	X	X	X	X
F4a	X	X			
F4b		X			
F4c		X			
F4d		X			
F4e		X			
F4f				X	
F4g				X	
F5a		X			
F5b		X	X	X	
F5c		X	X		
F5d				X	
F5e				X	
F6a		X	X	X	
F6b			X		
F6c			X		

Tabla 1. Function Vs. Operational Modes

And the same was done for the subassemblies required to safeguard each one of the functions in every one of the operational modes.

SPECIFIC MODELS

According to the requirements defined in the previous section, a basic model was produced, leading to the non-compliance of the functions which have to be safeguarded for each of the defined operational modes. For this purpose, a logic structure based on the fault tree methodology was used.

A second basic model was also generated to take into account the failures in the first model which could lead to catastrophic or critical failures.

Finally, a third model was created to take into consideration the probability of recovery actions by the crew, both internal and external.

One sheet of the first basic model can be seen in Figure 3.

QUANTIFICATION AND INTERPRETATION OF RESULTS

Once the basic models were created in the first stage of the study, and after obtaining the basic events required to take into account the different failure modes of the various functions included in the scope of the analysis, different failure rates or probability were assigned to all basic events modelled. Generally the sources were: AVCO database, WASH-1400, NUREG/CR-1278 and specific information from the ESA/CNES team.

Four new models were generated from the basic ones, and include the following concepts:

1. *Loss of mission failures of the system.*
   All failures associated with HDA or MTFF components will be included in this category, if they imply but do not ensure the proper function performance by the system without risk to human lives or space vehicles.
2. *Critical failures of the system.*
   Failures of HDA or MTFF components that could represent a risk to space vehicles.
3. *Direct catastrophic failures of the system.*
   Failures of HDA or MTFF components bearing direct catastrophic consequences (risk to human lives).
4. *Catastrophic failures of the system induced by critical failures.*
   Critical failures of HDA or MTFF components for which recovery actions taken by the crew have not been successful.

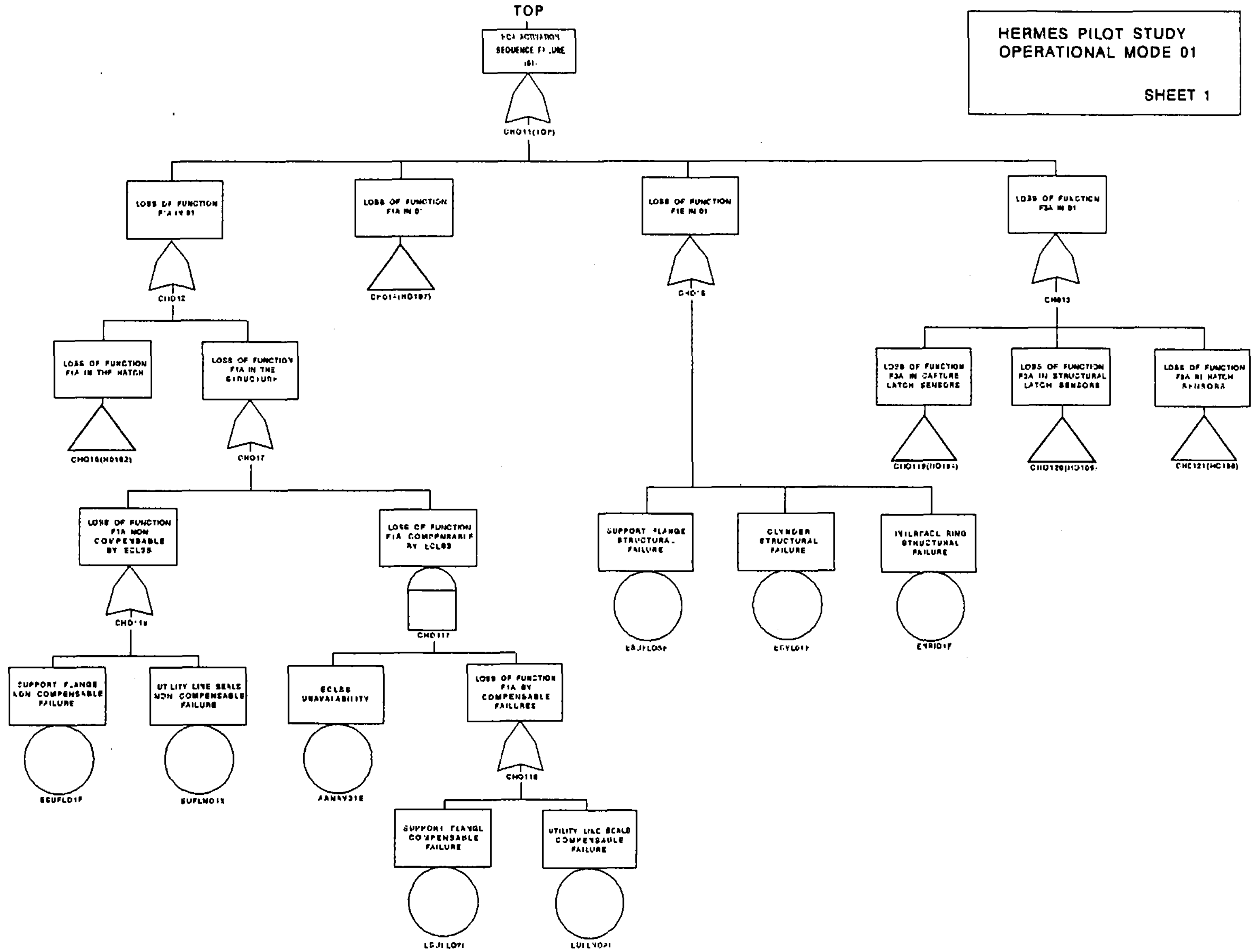


Figura 3. Hermes Pilot Study 01 Sheet 01

Furthermore, the results obtained were divided according to the three different operational phases: Docking Phase ($0_1 + 0_2$), Servicing Phase (0_3) and Berthing Phase ($0_4 + 0_5$).

Finally, a series of sensitivity analyses were carried out for the final part of this section, to evaluate the influence of some probabilities and assumptions on the final results.

GENERAL CONCLUSIONS

The first conclusion (and perhaps the most significant one) is the suitability of this type of quantitative studies for the obtainment of relevant priorities for the different aspects of risks and safety associated to the different consequences intended to be minimized. Throughout the development of the project, the usefulness of a quantitative model was clearly demonstrated, when considering the strictly mechanical aspect of the system design and required support systems, as well as the impact of human action on them. These quantitative models allow for the evaluation "a priori" of design improvement effectiveness and need for redundancies, while they leave evidence of possible failures derived from events initially considered as minor, but which become significant in joint events which are difficult to evaluate with a qualitative method.

Application of these techniques to the first stages of a project design allows to evaluate possible solutions to specific problems while they still do not have a significant impact, thus obtaining a more rational use of the existing resources.

It is also interesting to point out that during the project, great uncertainties came up regarding the data to be used for the models, from the specific aircraft industry database point of view as well as from human reliability estimates.

Finally, the use of a specific system to bring out evidence of dependencies due to common cause failures (through factor) has permitted to leave evidence of single-way failures on subsystems and redundant components, which otherwise would have come up as independent failures.

REFERENCES

1. *HERMES Docking Interface, Phase B3 Final Report, January 1989.*
2. *HERMES Docking Assembly Operational Flow Analysis, HMS-HDA-TN-SN-001, 10/07/90.*

3. *Requirements Specification for HERMES Docking Assembly, H-CF-1QD-01-AS, 19/07/90.*
4. *HERMES Docking Assembly Operational Flow Analysis, HMS-HDA-TN-SN-001, 16/11/90.*
5. *HERMES Pilot Study. Contract number 9093/90/F/PT.*
6. *System Safety Requirements for ESA Space Systems and Associated Equipment, ESA PSS-01-40 Issue 2, September 1988.*
7. *Reliability Engineering Data Series (Failure Rates), AVCO Corporation, April 1962.*
8. *NUREG/CR-1278. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, Final Report, 1983.*
9. *NUREG-75/014, WASH-1400, Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants, NRC, October 1975. Appendix III, Failure Data.*
10. *US NRC, Procedures for Treating Common Cause Failures in Safety and Reliability Studies: NUREG/CR-4780, January 1989.*