

Challenges and Opportunities of International Cooperation for Safety & Mission Assurance (SMA) on the European Service Module (ESM) of the Orion Program

By

Michael L. Ciancone¹, Richard Chase², Horst Tjaden³, Brian VanGenderen⁴ and Mark Hyatt⁵

ABSTRACT

ESA is providing the ESM to NASA for the Orion Program in accordance with the Implementing Arrangement (IA) established between the two Agencies in 2012. This IA is a barter agreement, in which ESA provides Service Module vehicles for the first two flights of Orion in exchange for two servicing missions to the ISS. This arrangement has provided opportunities and challenges to both communities. It represents an important opportunity for ESA to build on its experience in the development and operations of ATV and play an active role in the development and flight of a manned space vehicle. This paper will explore some of the unique aspects of this arrangement as it affects Safety & Mission Assurance (SMA).

The assessment of ESM compliance with applicable safety requirements is the responsibility of the Joint Safety and Engineering Review Panel (JSERP). The JSERP has two features that are relatively unique amongst NASA safety panels. First, NASA Engineering and SMA organizations co-chair this Panel. Previously, Safety has chaired, with Engineering as a member of the Panel. Inclusion of Engineering as a co-chair has offered greater leverage within the technical community. Second, the JSERP includes a second set of co-chairs from ESA Engineering and ESA Product Assurance and Safety (PA/S) organizations. This recognizes the international arrangement as one of partnership.

Another source of both opportunity and challenge is the differing experience base of ESA and NASA. NASA has decades of experience in manned spaceflight, dating back to the Mercury program and following through Gemini, Apollo, Apollo-Soyuz, Skylab, Shuttle and the International Space Station. The risk posture for manned missions is much more rigorous than for unmanned missions. ESA brings a wealth of knowledge as well, with their flights of Ariane and Automated Transfer Vehicle (ATV), development and operation of the Columbus module on ISS, and satellite programs. The result is that both parties have developed paradigms related to risk and failure that contribute to ESM discussions.

Orion represents humanity's first venture beyond Low-Earth Orbit (LEO) in over fifty years. Much of that experience is captured in program documents, but first-hand knowledge is limited to a few spaceflight veterans. Missions to LEO have offered the opportunity of direct, near-instantaneous communications and assistance, and the ability to return to Earth within a matter of hours in case of emergency. Outward-bound missions do not have these features and will require a more autonomous spacecraft with attendant safety-related issues.

This paper will explore these and other challenges as we approach the flight of the first Orion vehicle.

¹ NASA Johnson Space Center, Houston, Texas, USA

² European Space Research and Technology Centre, Noordwijk, The Netherlands

³ Airbus Defence and Space, Bremen, Germany

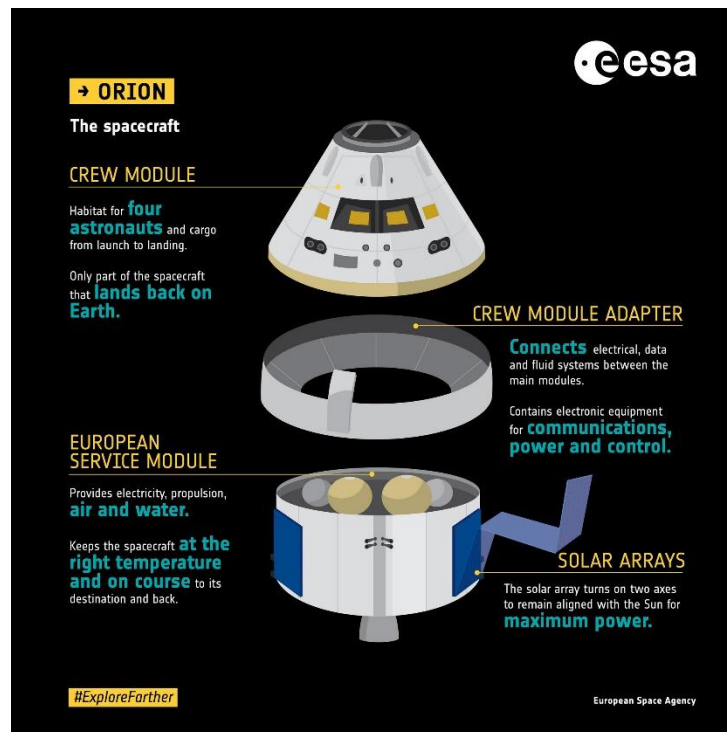
⁴ Lockheed Martin, Denver, Colorado, USA

⁵ NASA Glenn Research Center, Cleveland, Ohio, USA

1. Overview of Orion European Service Module (ESM)

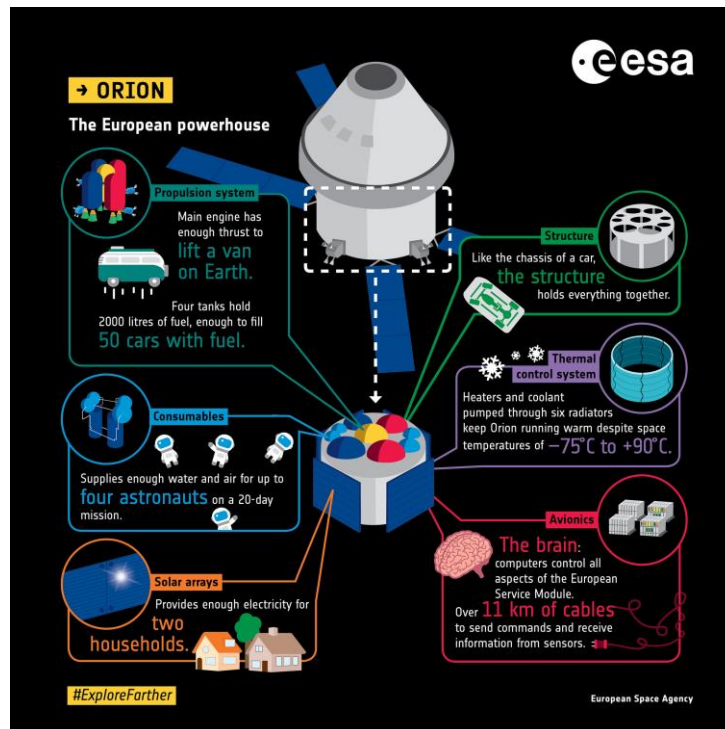
The Orion spacecraft is NASA's next generation vehicle for human space exploration beyond Low Earth Orbit (LEO). It is designed to carry a crew into lunar vicinity and beyond. While the first demonstration test flight (EFT-1) launched in 2014 with a Delta IV Heavy, the first Orion vehicle will launch on NASA's new heavy lift rocket, the Space Launch System (SLS).

The Orion vehicle consists of the Crew Module (CM), the European Service Module (ESM), and a Crew Module Adapter (CMA) connecting both parts of the vehicle. The CM features the habitable pressurized volume to support the four crewmembers and cargo during all phases of the mission. The ESM is an unpressurized module that provides propulsive support for orbital transfer and attitude control, consumables storage (e.g., water, oxygen and nitrogen) for the CM habitable environment, power generation, and active/passive thermal control for rejection of waste heat from avionics systems.



The European Service Module (ESM) is a cylindrical module with a primary structure consisting of longitudinal beams transferring the loads from CMA to the launch interface (co-called "longerons"), an upper and lower platform made of machined aluminum alloy to accommodate the tanks and other equipment, and the internal core structure made of composite panels in a "double-X" configuration. The major part of its unpressurized interior comprises four propellant tanks with a volume of 2100 liters each. Two helium vessels carrying the pressurization gas for the propulsion system are nested in the center of the core structure. Avionics controllers for the various functions are mounted on the composite panels around the tanks. In the nominal configuration, four water tanks carry the water for the crew supply; this number can be expanded up to seven, based on the mission needs. The external body of the ESM consists

of eight radiators of varying size, which dissipate the waste heat into the radiative sink of space and function as protective shields against micrometeorites and orbital debris.



For power generation, four solar array wings are mounted on the lower end of the module. Once deployed, each wing can gimbal via a two-axis mechanism to achieve an optimum angle maximizing the solar power generation. The inner axis is used to “cant” the wings, i.e., tilt the wings forward or backward during major boost maneuvers to reduce the mechanical stress on the wings structure.

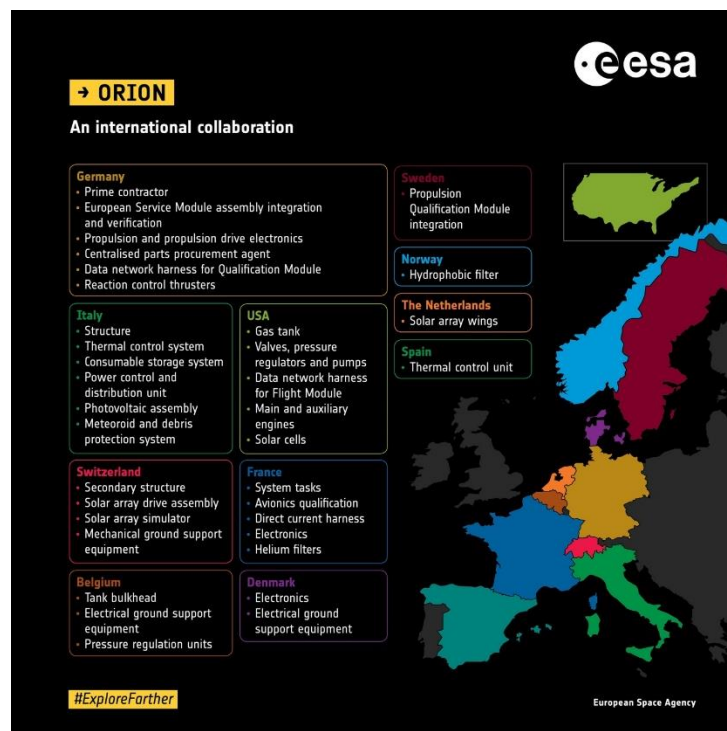
Four composite gas tanks are located on the forward end of the ESM containing oxygen and nitrogen for the crew module. Additional equipment, such as the pump assembly for the thermal fluid system and the pressure regulation for the propulsion system, are located on the upper surface.

The main engine (OMS-E) is located on the aft end of the ESM. The thrust vector control can gimbal the engine for orbital transfer maneuvers. Eight Auxiliary Thrusters positioned around the main engine are used for smaller maneuvers and as back-up for the main engine. Twenty-four (24) smaller thrusters provide attitude control and are grouped into six thruster pods located around the exterior of the ESM. Thick heat shields protect the ESM aft side from the engine heat.



The ESM in preparation for transport to the U.S. Credit: NASA.

The main ESA contractor, Airbus Defence and Space, in Germany, builds the ESM. Many companies from ESA member states, and in some cases US suppliers, develop and manufacture the equipment and subsystems. NASA provides some items, such as the Orbital Maneuvering System Engine and Thrust Vector Controllers (OMS-E/TVC) (a heritage system from the US Space Shuttle) as Government Furnished Equipment (GFE). Airbus performs the final ESM integration in Bremen, Germany, before shipping the ESM to the Kennedy Space Center in Florida for integration with the Orion vehicle. The figure below provides an overview of the European countries participating in the ESM program.



The ESM resembles ESA’s Automated Transfer Vehicle (ATV), from which it evolved, but the ESM has some major differences compared to its ATV heritage design, as noted in Table 1:

	ATV	ESM
Primary structure	Cylindrical shell	6 Longerons
Propulsion system regulation	Mechanical	Electronic
Propulsion system dimensioning	4 x 400 N main thrusters	27.7 kN OMS-E main engine
Solar Array Drive	1 Axis of rotation	2 Axes of rotation
Thermal control	Heat pipes	Active system with cooling fluid loops
Avionics bus	Mil bus	TT Ethernet
Control system	On-board computer	Controlled from crew module
Potable water supply	Spherical tanks, manual transfer to ISS by crew filling “bags” from the tanks	Pressurized cylindrical tanks, transfer to crew module by piping connection

Table 1: Key Differences between ATV and ESM

In addition, the ESM obviously faces a much different mission environment in term of temperatures, radiation, micrometeoroids, solar flares, and launch environment of the new SLS launcher, compared to the ATV, which was launched on Ariane 5 and operated exclusively in LEO.

While most of the ESM development was performed in Europe, the qualification testing was distributed to various sites worldwide. The main test models and activities are as follows:

- **Propulsion Qualification Module (PQM)** for verification of the propulsion subsystem at the White Sands Test Facilities (WSTF) in New Mexico, U.S.A.
- **Structural Test Article (STA)** for structural verification at the NASA Plum Brook Station (PBS) in Sandusky, Ohio, U.S.A.
- **ESM Qualification Facility (ESM-QF)** for functional verification at Airbus facilities at Les Mureaux, France
- **Integrated Test Laboratory (ITL)** for Integrated Vehicle functional verification at Lockheed Martin facilities in Denver, Colorado, U.S.A.

The integrated flight vehicle is subjected to the following tests:

- Thermal Vacuum/thermal balance and EMI/EMC testing at NASA PBS in Sandusky, Ohio, U.S.A.
- Final acceptance testing and launch operations (ATLO) and Direct Field Acoustic Tests (DFAT) at NASA KSC, Florida, U.S.A.

Generally, test operations teams from industry, with support from engineering experts and test facility personnel, plan, prepare and execute these tests. NASA and ESA are involved as well for support in planning and test oversight during test execution phases. Engineering supports the test evaluation and provide expertise for encountered anomalies or otherwise unexpected behavior of the article under test. Experience has shown that the amount of resources to cover all test activities is quite high at peak times with tests at different sites running in parallel. Differences in time zones, multi-shift activities and travel logistics add further complexity to the management of the overall test program.



ESA's Structural Test Article testing in NASA's acoustic test facility at NASA PBS. Credit: ESA



Propulsion Qualification Module (PQM) hot firing at WSTF. Credit: NASA

2. Experience Heritage

An important source of both opportunity and challenge on the ESM Project of the NASA Orion program is the differing heritage of experience brought to the arrangement by ESA and NASA.

NASA has decades of experience in human spaceflight, dating back to the Mercury program and following through Gemini, Apollo, Apollo-Soyuz Test Program, Skylab, Shuttle and the International Space Station (ISS). The NASA safety culture has evolved over that time as a consequence of the rigorous risk posture for human spaceflight missions. NASA has also learned many technical and organizational lessons over that time that are reflected in the design requirements levied on hardware and in the way in which all opinions are welcomed in safety discussions.

ESA brings a wealth of knowledge as well, with a history of success in the complete range of space projects – launchers, scientific and communications satellites, earth observation, and human spaceflight. The development and operations of five ATVs, including the first fully automated docking of a vehicle to the ISS, provided much of the technology that serve as the design basis for ESM, and many members of the European consortium have worked on either ATV or the development and operation of the Columbus ISS module. The result is that both NASA and ESA have developed paradigms related to risk and failure that contribute to ESM discussions.

Orion will be mankind's first journey beyond LEO in over fifty years, which presents significantly greater safety challenges than missions to the ISS. Much of that experience from the Apollo missions is well-documented, but first-hand knowledge is limited to a few remaining spaceflight veterans. Missions to the ISS have offered the opportunity of direct, near-instantaneous communications and assistance, and the ability to return to Earth within a matter of hours in case of emergency. The Orion missions do not have these capabilities and will require a more autonomous vehicle with robust design features to maximize the crew's ability to return safely to earth in case of anomalies. Given that the ESM provides the means to return the crew, i.e. propulsion, power and life support, there has been intense scrutiny of the ESM design in this context.

These differences between the ISS and lunar missions and between ATV and ESM missions resulted in reassessing certain parts of the ATV heritage design for application to ESM. Two examples illustrate these differences:

- Solar array wing deployment

The deployment system for the ESM wings and the wings themselves were designed based on extensive experience. Airbus DS Netherlands provides the deployment system and wings; they have used a similar design on many satellites and the five ATVs without any deployment failures. However, those wings were not deployed on a crewed vehicle. The deployment of the wings on ATV was done shortly after launch and well before approach and docking to the ISS, hence the deployment was not a topic discussed with the ISS Safety Review Panel as it had no effect on crew safety. In the case of the ESM, wing deployment is performed with the crew on board and is safety critical since it must be successfully completed to ensure sufficient structural integrity for the loads from main engine burns. As a result, the design was analyzed in detail for use on ESM and small but significant design modifications were identified to improve the

robustness of the design, in particular, the means to monitor locking the wing panel hinges in their final positions prior to engine burns.

- Propulsion system robustness

Since the ESM mission will take the crew outbound from earth towards the moon, the engineers have focused a lot of attention on ensuring that the propulsion system can withstand anomalies and continue to maintain the capability for a safe return to earth. Of course, the ATV propulsion system had to meet ISS safety requirements, but it was not required to function to return the crew. For ESM, there was particular attention on failures that could potentially result in loss of engine fuel or oxidizer. Engineers introduced design modifications even at the level of pressure transducers to improve failure tolerance to potential leakage events, and additional robustness means were applied to the production and testing of other components of the system. For future missions of the ESM, additional design modifications are under study to further improve propulsion system safety.

3. The Joint Safety and Engineering Review Panel (JSERP)

The JSERP was created to review and approve Flight Hazard Reports (FHRs) associated with the ESM. A couple of features distinguish the JSERP from other NASA safety panels (e.g., PSRP, SRP). First, Safety and Engineering jointly chair the panel, whereas Safety is the sole chair for other NASA Safety panels. This has the benefit of fostering engagement from Engineering support personnel who are also involved in the normal design activities of the various subsystems and can provide insight into the design details. Secondly, this is a joint panel with Engineering and Safety chairs from ESA as well. This joint approach differs from other NASA Safety panels and was implemented due to the specific nature of the agreement between the agencies for the delivery of the ESM to NASA. This Panel therefore has four (4) Chairs. At both agencies, the chairs are independent of the project.



L to R: Robert Hudson (NASA Safety), Rose Flores Jones (NASA Engineering), Rafael Bureo (ESA Engineering) and Rosario Nasca (ESA Safety). Credit: Ciancone

The safety review process began with a Phase 1 review to identify hazards and associated causes. At Phase 2, the safety and engineering community performed a detailed review of the proposed hazard control strategy for ESM, resulting in some design modifications or requests for additional design justifications. Both phases are standard elements of a safety review process. **Phase 3 will be a bit different** as the Panel is relying on a special team of technical personnel, with members designated by Panel representatives, to review verification evidence and recommend closure (or not). The team will present a status of verification activity during Part 1 of the Phase 3 safety review; Part 2 of Phase 3 safety review will provide a more extensive review of open HCVs to establish which ones are appropriate for transfer to a Verification Tracking Log (VTL) and which ones Airbus must complete before Phase 3 approval. This will allow the Panel to focus their attention on changes to the hazard control strategy that occurred since they approved the Phase 2 FHRs.

In addition, the Program approved a number of design changes for the second flight module (ESM-2), while accepting the current design for ESM-1, which will be unmanned.

4. Unique aspects of the ESM Program

The Program has accepted certain risks in order to meet the schedule for delivering the ESM for supporting the NASA Orion missions. Although these risks could have safety implications, they are not managed within the traditional safety activities. The main risks are as follows:

- **ESM-1 delivered before qualification completed**

In order to meet the desired development schedule of the Orion vehicle, and particularly the ESM, the Program adopted an inverted approach to design, development, test, and engineering (DDT&E). The ESM Critical Design Review (CDR) was based on the standard approach of engineering model development and test of the various subsystem components and equipment. From that point, the program proceeded with parallel build and qualification of flight model hardware. The Program accepted this risk in part due to the heritage basis of the vehicle design. The result is that the Program completes the vehicle level assembly, integration and test (AIT) before the associated component and subsystem qualifications are complete. This has resulted in several challenges because of failures during qualification testing, which resulted in dispositions that the Program must therefore address at the vehicle level while it is in the ATLO flow.

- **Refurbishment of heritage hardware – OMS-E/TVC**

Another significant aspect of the ESM development approach was the decision to utilize heritage hardware in order to reduce the overall DDT&E effort required to meet the program schedule. The OMS-E/TVC is a Space Shuttle heritage system. While the overall intent was satisfied, there have been significant challenges associated with this approach. Reconstitution of capabilities for refurbishment, test, and certification for flight have been numerous. Significant effort is also required in the analysis of the heritage design to assure its capability to meet significantly different performance requirements and flight environments than originally intended.

- **ESM-2 integration underway while preparing for Launch of EM-1**

A third programmatic challenge is the support of parallel ATLO activities for ESM-1, while commencing the AIT of the ESM-2 vehicle for the crewed EM-2 mission. This requires the rotation of engineering and SMA personnel between Europe and the Kennedy Space Center (KSC) to support EM-1 ATLO activity, while proceeding with ESM-2 AIT in Europe. ESM-2 AIT is similar to ESM-1 AIT, but ESM-2 must also address previously noted design changes, which include systems for crew presence in the vehicle. In addition, the experience gained from the first Orion mission will come too late for feedback into the vehicle design for the second mission.

5. Integration of ESM FHRs into MPCV Integrated FHRs

As the Orion Prime Contractor, the System Safety Team at Lockheed Martin performs an Integrated Hazard Analysis (IHA) in accordance with the MPCV 70038, Orion Multi-Purpose Crew Vehicle (MPCV) Program Hazard Analysis Requirements. The Integrated Hazard Analysis (IHA) is a top down assessment of all Program hardware, software and operational interactions that identifies both the undesired events (hazards) that can result from those interactions as well as how those events are controlled. The IHA encompasses the Crew Module (CM), Crew Module Adapter (CMA), Launch Abort System (LAS), and the European Service Module (ESM) including all interfaces between these modules. Airbus, as the design authority for the ESM, performs a system-level hazard analysis for the ESM, which Lockheed Martin System Safety then integrates with the IHA. Because the Lockheed IHA is performed more-or-less in parallel with the Airbus system-level hazard analysis and with some differences in approach/execution, it creates some unique integration challenges.

For the Lockheed Martin IHA, the goal is to provide a comprehensive assessment of hazards and their controls that includes all Orion flight hardware and flight operations as an integrated system within the context of the flight environment. The individual hazard reports that comprise the IHA are hazard-based as opposed to subsystem-based. For example, rather than creating a hazard report in which the hazards of a particular subsystem are assessed in isolation, such as “Failure of the Electrical Power System (EPS),” the IHA hazard report would assess “Loss of Power Generation.” This approach broadens the scope to include failure modes outside of the EPS hardware such as a failure within the Guidance, Navigation and Control (GN&C) subsystem that results in an erroneous sun-pointing attitude for the Solar Array Wings. While the hazard-based approach is more comprehensive and effective, it makes merging ESM-only hazard reports from Airbus much more complex since subsystem failure modes and controls are dispersed and intermingled with other subsystems in the Lockheed IHA hazard reports. The complexity of the hazard report integration drives increased time and resources.

One factor that further logistically complicates the integration is the parallel nature of the Lockheed and Airbus hazard report creation, review, and approval (MSERP/JSERP) process. While Orion has established schedules that place Airbus hazard report review/approval ahead of the Lockheed IHA review/approval, the reality has been that these activities have been more-or-less in parallel, greatly decreasing the time available for integration at the IHA level.

Differences in hazard analysis approach and execution such as ground rule assumptions, handling of operational controls, hazard transfer protocol, citing of quality assurance processes, and even hazard cause, control, and verification organization and formatting presented some unique integration challenges.

The Lockheed System Safety team had the benefit of co-developing ground rules for performing the IHA with NASA, going through multiple Safety Panel reviews, and incorporating lessons learned since 2007 for Orion (then part of the Constellation Program). When NASA reached agreement with ESA in 2012 to provide the ESM and associated hazard analysis, NASA provided ESA with a copy of a Constellation-era IHA to use as an example of what the Safety panel is expecting. However, there had been many changes to the approach for hazard analysis development during the transition from Constellation to MPCV of

which ESA/Airbus was not aware. This resulted in misalignment of the first iterations of Airbus hazard reports with current expectations.

The use of compliance to European/ESA/Airbus standards as hazard controls introduced the challenge of determining equivalency to U.S. aerospace industry and NASA standards. Long-standing aerospace industry and NASA standards, with years of heritage and lessons learned, form the bedrock of much of Orion's hazard control strategy. When assessing the overall likelihood of occurrence for a particular hazard - based upon the controls in place - design compliance to NASA standards is a major factor. While ESA levied many NASA standards on Airbus for compliance, in many cases the standards were tailored which required assessment by the IHA hazard report author to determine level of equivalency to aid in assigning an integrated likelihood of occurrence. NASA has coordinated reviews of selected European Cooperation for Space Standardization (ECSSs) to consider whether they "meet-or-exceed" the comparable NASA standard. This comparison allows ESA to levy ECSSs on European industry rather than incur the risks associated with imposing unfamiliar standards on them.

6. Cultural interfaces

Anyone who has worked on a project knows that one of the most important aspects is interfaces. Interfaces can be the source of much grief when, for example, bolt holes do not line up or software modules cannot communicate due to protocol issues. In the ESM project, one of the most important interfaces is between the teams. As previously noted, there are many participants spread across Europe and the US, spanning nine time zones and including multiple nationalities and languages. Although English is the designated language of the ESM Project, participants must give careful attention to written and spoken communications to ensure smoothly operating interfaces are maintained. The native English speakers need to keep in mind that most of the European partners are not using their mother tongue so participants must listen to understand what is intended, even if the words are not precise. This is obviously not only an issue for safety but it has come up in the production of the Flight Hazard Reports where we need to be clear about identification and control of hazards in the system.

7. Conclusions

We have highlighted some of the interesting aspects affecting safety of the ESM in this paper. The development has been challenging due to the demanding schedule and the related programmatic constraints. We have had to make some hard compromises in order to deliver ESM-1 but it has provided an opportunity for the European and U.S. partners to develop new means of working together that will assist us going forward with the production of further Orion vehicles for the return to the moon.