Verification and Implementation of Operations Safety Controls for Flight Missions

Cheryl L. Jones
International Space Station (ISS)
Safety & Mission Assurance (S&MA)
Houston, TX
Cheryl.L.Jones@nasa.gov

James R. Smalls
International Space Station (ISS)
Safety & Mission Assurance (S&MA)
Houston, TX
James.R.Smalls@nasa.gov

Alicia S. Carrier
International Space Station (ISS)
Safety & Mission Assurance (S&MA)
Houston, TX
Alicia.S.Carrier@nasa.gov

Abstract - *This paper illustrates the complexities involved with the tasks necessary to ensure safe operations for flight missions based on International Space Station (ISS) operations experience and other researched material. The experience is derived from Safety and Mission Assurance Operations on the safety console in the ISS Mission Evaluation Room. The focus is on roles played by operations engineers in executing strict flight product verification through phases of Implementation Verification, Certification of Flight Readiness, and Visiting Vehicle Operations. The paper highlights the manner in which operations engineers help to ensure safety and mission success through application of systems engineering and project management principles.*

Keywords: International Space Station, operations safety, mission assurance, systems engineering, implementation verification, flight readiness, visiting vehicle operations.

1 Introduction

Approximately eleven years ago, the International Space Station (Figure 1) launched its first module from Russia, the Functional Cargo Block (FGB). Safety and Mission Assurance (S&MA) Operations (Ops) Engineers played an integral part of that endeavor by executing strict flight product verification as well as continued staffing of S&MA's console in the Mission Evaluation Room (MER) for that flight mission. How were these engineers able to conduct such a complicated task? They conducted it based on product verification that consisted of ensuring that safety requirements were adequately contained in all flight products that affected crew safety. S&MA Ops Engineers apply both systems engineering and project management principles in order to gain an appropriate level of technical knowledge necessary to perform thorough reviews which cover the subsystem(s) affected. They also ensured that mission priorities were carried out with great detail and success.

Simply defined by the International Council on Systems Engineering (INCOSE) System Engineering Handbook [1], "a system is an integrated set of elements that accomplish a defined objective." The product verification phase executed by S&MA Ops Engineers creates a system whose function is to use the available resources as inputs to produce an output that meets the objective. One of the resources is the technical knowledge available through formal education, training/simulations, experience, and coordination with specialists (subsystem engineers, subject matter experts. etc). The other resources are the various flight products. The objective is to provide an independent verification of crew safety and mission success in each applicable flight product.

Figure 1. The International Space Station as seen from Space Shuttle Endeavour on July 28, 2009 [2].

Prior to the system performing its function, the system engineering & project management processes begin with the "top-down development" of processes & phases to be applied to each project/flight/mission which are in-line with recommended practices [1, 3]. With approved/ established processes/phases the S&MA Ops Engineers perform "bottoms-up integration and verification" through use of the available resources to the appropriate level of technical depth during the respective timeframe allotted for each project/flight/mission. The system engineering process is used on each level with control gate (review) before proceeding to develop the next lower level of problem and solution descriptions. The output (requirements baseline) at each level is the input to start the next level (iteration). In some instances the S&MA Ops Engineer will perform reviews with customers and stakeholders to confirm the need and obtain concurrence on interim solutions. Reports & assessments continue to move up the management chain at successively bigger picture combinations of solutions (integration) that have been tested (verified).

2 Safety and Flight/Mission Phases

The INCOSE Handbook version 2a [1] defines Systems Engineering as the interdisciplinary approach and means to enable the realization of successful systems. There are several engineering disciplines such as: reliability, supportability, quality, human factors, risk management, safety, etc. Safety is an extremely important engineering specialty within the National Aeronautics and Space Administration (NASA) and a loss of crew is considered a catastrophic event. Safety is not difficult to achieve when properly integrated from the beginning of each space systems project/mission planning. The key is to ensure proper handling of safety verification throughout each flight/mission phase.

Today, S&MA Ops Engineers continue to conduct flight product reviews across all open flight products. As such, these reviews ensure that each mission is accomplished with safety requirements along with controls heavily embedded in applicable flight products. Most importantly, the S&MA Ops Engineers are required to look for important design and operations controls so that safety is strictly adhered to as well as reflected in the final flight product. This is performed during the S&MA Ops Engineer's safety *implementation verification phase*.

As mentioned above, the United States' first international partnership for aerospace endeavors began with the FGB launch in Russia. The Russian Federal Space Agency is among several other space partners taking part in this adventure that has successfully contributed to the continued growth of the ISS and there is still more equipment to be launched/assembled. More systems now have to be managed due to European Space Agency, Canadian Space Agency and Japan Aerospace Exploration Agency now becoming a part of the ISS (Figure 2). With that said, flight product reviews are now longer and require finer detail to ensure safety is embedded in each finished product as applicable.

Further, every significant open anomaly that occurs in space is also adequately reflected in what is called the *Certification of Flight Readiness Phase*. S&MA Ops plays a large role in this process in that they are responsible for ensuring the safety for each mission to the ISS. In this process S&MA requires that NASA, as well as contractor management, certify each flight mission by signing that all specific safety criteria has been met and that flight readiness is assured. S&MA Ops is a part of this process and they conduct this process by making sure that all issues and discrepancies are identified as proactively as possible. Once a final signature is gained, the flight mission phase can be conducted.

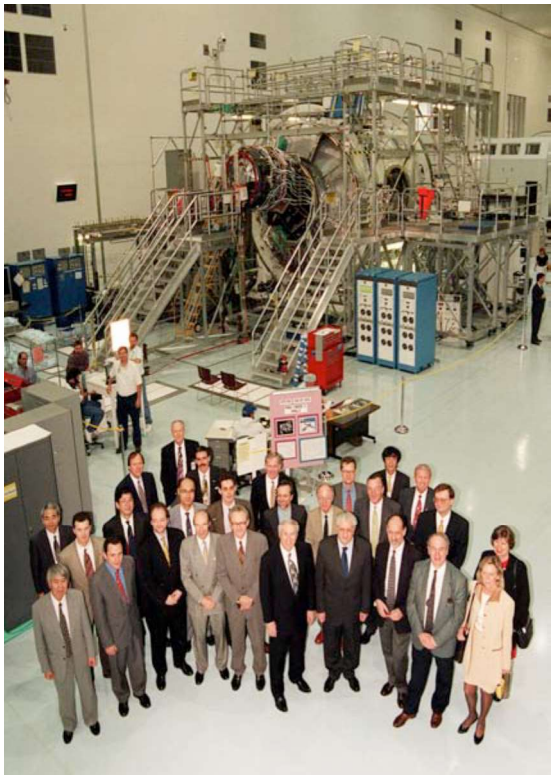

Figure 2. Senior government officials from 15 countries participating in the International Space Station signed agreements in Washington D.C. on Jan. 29, 1988 [2].

Moreover, once a signature is obtained by S&MA, work still has to be conducted to support real-time operations on-board ISS and missions to the ISS by visiting vehicle(s). Conducting *Visiting Vehicle Operations* jointly with the international partner(s) can become extremely complex during the real-time flight missions phase. In fact, in order to be able to provide such a high level detailed review, these S&MA Ops Engineers are put through a robust training program to ensure that they are able to quickly respond as safety specialists to make very critical decisions, with a very short response time during real-time flight operations/missions. All certified console operators contribute by ensuring the safety and success of each mission.

Based on the authors' experience in S&MA Ops on the ISS MER safety console and other researched material, this paper illustrates the complexities involved with the tasks to ensure safe operations/flight missions through the three flight/mission phases mentioned above. Each phase of Implementation Verification, CoFR and Visiting Vehicle Operations is discussed in sections below.

3 Implementation Verification

In order for any activity to materialize on orbit, it goes through a rigorous review process. S&MA's initial involvement in this process is the implementation verification phase. Since hazards are common threats to the crewmembers on orbit, it is very important that flight products are adequately reviewed. Flight products consist of procedures and flight rules. Procedures are steps that instruct the crew on how to perform a specific task. Flight rules are directions to the Flight Control Team in Mission Control Center on how to get the vehicle (ISS, shuttle, etc.) in a safe posture. During this phase, S&MA verifies that any hazard controls associated with activities via flight products are properly implemented. In order to condense the quantity of risks exposed by the crewmembers, controls are put in place. Controls are defined as mitigation steps put in place to reduce risk. The Ops team ensures that hazard controls are implemented within all flight products with a direct impact on safety. With each product review, the Ops Engineers are able to provide an independent assessment on the validity of hazard control implementation. So how does S&MA perform these complex verifications successfully? Each Ops Engineer has to go through the following stages to perform these assessments properly:

1. Training
2. Tools
3. Feedback

Before an engineer can perform this verification, they are trained on the expectations of being a safety representative. Within the training, the team gains knowledge of vital safety documentation that aids in the review of flight products. The key safety documentation used during this review are: Hazard Reports (HRs), Failure Modes and Effects (FMEAs), Operation Control Agreement Database (OCADs) and Space Station Program (SSP) documents. HRs are the outlines of hazard analysis that has been performed based on a condition, a piece of hardware or situation. Within these reports, the description of the hazardous condition, cause and controls are documented. FMEAs are descriptions of various failure modes and workarounds of a piece of hardware. OCADs illustrate the operational workarounds that are put in place to control the hazard through flight rules, procedures or training. SSP documents explain the numerous requirements levied by the SSP.

In addition to understanding the required documentation, the engineers are also trained to work with the technical expert for that subsystem to gain additional insight. Through the knowledge obtained through this vigorous training program, the Ops team is able to review the flight products and verify that they are in line with the correct safety documentation.

Along with training, to ensure that the team is reviewing from the same set of standards, there needs to be adequate tools in place. In particular, a tool used by the Ops team is an access database. This database houses all reviews performed by the team and is used as a historical tracking mechanism. Within the database is a checklist which facilitates an itemized list of requirements that each engineer should confirm to ensure a standardized review of each product.

The final phase to ensure that flight products are implemented properly occurs during the feedback stage. When the review is complete and there is a discrepancy with one of the flight products and the applicable safety documentation, feedback is given to that respective hardware owner. This final phase ensures that there is a closed loop accounting system in place to prevent any gaps. Moreover, and as mentioned above, Certification of Flight Readiness is a subsequent phase that occurs just before a flight launches.

4 Certification of Flight Readiness

Certification of Flight Readiness (CoFR) is an assessment process that ensures adequate certification for flight activities performed by the NASA program. This certification is based on the evaluation and disposition of various organizations' endorsement codes. Endorsement codes are utilized within the CoFR process to show that open work has been examined, the endorsement guarantees that all obligated work has been performed, and a signature from the appropriate organization is then gained by the ISS Program Office. However, before an endorsement signature is obtained, an assessment is conducted to ensure that a successful mission is completed without much complication. As such, this assessment ensures operational readiness and the safety of the ISS on-orbit flight assembly operations. The assessment provides operations as well as other organizations with a look at open work that may impact the flight mission. Moreover, several organizations take part in this assessment to certify that tasks, activities, and products related to endorsement statements have been accomplished [4]. The following are important factors involved in Operations Safety Assessments:

1. Hazard
2. Controls
3. Weighing Risk
4. Mitigating Risk
6. Implementation

Hazards are identified at the beginning of the Operations CoFR cycle, very early within the process. The identification of hazards is a very critical process within the CoFR assessment in that verification has to be made by the Operations engineer to address safety requirements that may be violated. Once a violation has been identified, operations further looks at the application of various

control philosophies and methods. Moreover, hazard controls are then examined to determine whether additional engineering controls are needed or whether the hazards can be managed. For example, applying engineering controls could possibly consist of adding a monitoring device into a flow system to ensure that a relief valve is functioning at the correct pressure level. An example of a management control would be adding a safety review of a change to a system or update of a system to ensure that adequate safety implementation is in place for the new change or system update [5].

Weighing the risk associated with all open tasks is extremely important in that a decision has to be made to determine what to do about the problem. Risk mitigation is "a risk response planning technique associated with threats that seek to reduce the probability of occurrence or impact of a risk to below an acceptable threshold" [3]. Of course operations safety will do everything practical to ensure that the activity is performed with safety as the first priority. However, best practices have to be employed whenever the activity is examined. Therefore, operations will look at previous similar activities that have already been performed to consider the amount of risk to accept or not. Also, Ops has to determine whether safety requirements and/or standards are still being met by accepting the risk associated with the activity. Furthermore, operations always works very hard to get rid of all hazards; since that is not always possible, lots of works goes into looking at ways to reduce risk [5].

Since risk cannot always be controlled, certain principles can be applied to reduce hazards:

1. The option of performing a different method to accomplish the task
2. Monitoring the hazard
3. Design barriers
4. Personal Protective Equipment
5. Time to Effect
6. Redundancy Design

Implementation is a last factor discussed; this phase is actually where the plan, model, design or specialization comes to life. The activity is executed after this process is conducted. Moreover, since the activity is conducted after this step, Ops is very concerned with the implementation process. Their concern is based on the fact that this process requires extensive coordination with various stakeholders because this process is not easy. For example, though several different options are weighed and various experts weigh the risk, there is a lot of work that goes into deciding how to implement the activity. For instance, a chosen strategy has to be selected based on the highest results that can be received from safety; this option has to be the best choice.

Additionally, because a large amount of work is carried over from one flight mission to the next, Ops works their CoFR cycle several months before a flight mission is approved for launch. In addition to the important factors that Ops Safety utilizes to perform the safety assessment, Ops CoFR also consists of the disposition of several endorsement code activities. The endorsement code activities consist of evaluating limited-life hardware and several other hardware dispositions. In addition to dispositioning hardware, Os also ensures that risks that may affect logistic and maintenance planning is adequately addressed/removed to support the flight on-orbit operations. Ops also evaluate all reported hardware/software issues to ensure that all non-conformances have been resolved before flight and that all risk management activities associated with the launch package, flight and on-orbit operations have been completed and documented as acceptable. For example, anomalous hardware seen on previous flights may have not been appropriately resolved, and that anomalous behavior may hinder flight operations for the upcoming flight being assessed. Moreover, Ops also evaluate any associated open work that may affect support facilities. Os also ensure that personnel are certified and that procedures are in place so that certified personnel are equipped to support launch. Also through this process, Os ensures that adequate safety requirements are heavily embedded within all flight products.

In the event that any discrepancies are found with the CoFR assessment, Ops will weigh the outcome of the results with NASA management to determine whether a CoFR "Exception" and/or "Constraint" to that flight exists. Once all CoFR products are adequately evaluated and dispositioned, a final CoFR endorsement signature is provided by the S&MA Program Office to conduct the flight mission.

5 Visiting Vehicle Operations

Implementation Verification and CoFR are also performed for visiting vehicles with an additional step of observing export control laws. Russia, Canada, Europe and Japan are established international partners due to the presence of their module(s), equipment and/or personnel that has been on the ISS. The United States and our international partners have visiting vehicles that are used to transport/equip the ISS's crew and to assemble/maintain the ISS. The United States and Russia have human space flight vehicles – Space Shuttle Orbiter and Soyuz (respectively). Russia, Europe and Japan have successfully launched and docked/berthed automated cargo transfer vehicles to the ISS (Figure 3). The United States is currently developing an automated transfer vehicle.

Figure 3. European Space Agency's "Jules Verne" Automated Transfer Vehicle (ATV), September 5, 2008 [2].

S&MA Ops Engineers played a significant role on the road to NASA and its international partners' achievement of this amount of space traffic. S&MA Ops engineers begin with understanding export control laws/scenarios and impacts of cultural differences prior to beginning support of multi-lateral meetings/ panels and product reviews. Understanding export control laws/scenarios begins with Section 38 of the Arms Export Control Act (22 U.S.C 2778) [6], which authorizes the President and Secretary of State to control the export and import of defense articles and defense services. The U.S. Munitions List (USML) (22 CFR Part 121) includes defense related items (hardware, software, information, know-how, and services) that are subject to export controls defined in the International Traffic and Arms Regulations (ITAR) and administered by the U.S. Department of State.

Once it is determined an item is not controlled by ITAR, then the Export Administration Regulations (EAR) defines export controls and commodities (hardware, software, and technology) that are subject to the export control authority of Parts 730 through 774 of the Code of Federal Regulations (15 CFR 730-774) that are administered by the U.S. Department of Commerce. EAR-controlled items are referred to collectively as the Commerce Control List (CCL). The CCL (15 CFR 774) is part of the EAR. The CCL describes "dual-use" commodities (that is, hardware, software, or technology which can be used for either military or civil purposes) that are subject to EAR export controls, according to the EAR categorizing system of Export Control Classification Numbers.

After completing at least the required level of export control training the S&MA Ops Engineer will proceed to begin interactions with the international partner which may involve technical e-mails/discussions and/or obtaining ITAR/EAR controlled technical documents necessary for achieving the foundational understanding of the respective visiting vehicle in order to perform flight product reviews.

The interactions with international partners in regards to reviewing documents/flight products for their respective visiting vehicles is similar to doing product reviews related to their respective modules on ISS with the addition of more simulations and the introduction of demonstration flights/criteria. Due to cultural differences it may become necessary for S&MA Ops Engineers to occasionally or nominally support multilateral teleconferences, panels and/or face-to-face meetings at off-nominal times due to different time zones/holidays and for extended durations to allow for translation. S&MA Ops Engineers support these forums in order to participate in discussions on flight product reviews and ensure proper implementation(s) of safety controls. In most cases the implementation of safety controls will be described in multi-lateral flight rules that are easily accessible to all international partners involved. However, there will be some implementations that will be described in internal documents of one of the international partners to which the S&MA Ops Engineer will have to request access.

S&MA Ops engineers will also participate in the defining and approval of first flight demonstration criteria to verify that no safety controls are violated or missing. The S&MA Ops Engineer will then evaluate the visiting vehicles' ability to successfully pass their criteria while performing demonstration maneuvers and commanding during simulations and actual flight. The S&MA Ops Engineer will also review the international partner's independent safety verification report for accuracy and completeness.

6 Summary

Unique flight tasks that are required before a flight/mission occurs serve to illustrate the vast complexity of the Implementation Verification, CoFR and Visiting Vehicle Operations phases. Moreover, because extensive reviews take place early on, along with in depth assessments being heavily embedded into flight products, several flight/missions appear to be performed without much complication. So in the public eye these tasks seem easy. However, though these tasks may seem to be conducted without complexity, several man-hours are poured into each flight product to ensure that tasks are performed correctly. For example, safety is a very important key aspect of these flight products and it greatly contributes to the reason that a flight/mission is carried out with great success. For instance, several phases and reviews are accomplished by several organizations that have a vested interest in the success of every flight/mission. These organizations have several experts that are able to provide technical input and they also heavily weigh into the flight products at the beginning of the flight/mission planning stages. These organizations are also key players at ensuring that flight/missions are accomplished without failure. Therefore, successful flight/missions are carried out by the assistance of several expert organizations along with various safety organizations and they are the key reason that complex tasks are performed with great success.

References

[1] INCOSE, *Systems Engineering Handbook*, version 2a, Seattle, WA 2004.

[2] Use of image and caption complies with "Guidelines Regarding the Use or Reproduction of NASA Material Obtained From a JSC Web Pages," http://www.jsc.nasa .gov/policies.html#Guidelines, Feb. 2008.

[3] Project Management Institute, *A Guide to the Project Management Body of Knowledge: PMBOK Guide - third edition*, ANSI/PMI 99-001-2004, Newtown Square, PA, USA, 2004.

[4] D. McMullen, "Space Station Safety & Mission Assurance Certification Guide," NASA Lyndon B. Johnson Space Center, Houston, Texas, USA, 2002.

[5] N.J. Bahr, *System Safety Engineering and Risk Assessment: A Practical Approach,* Taylor and Francis Publishing Company, New York, NY, USA, 1997.

[6] U.S. State Department, Policy–Directorate of Defense Trade Controls, "The Arms Export Control Act," http://www.pmddtc.state.gov/regulations_laws/aeca.html, Updated Jan. 21, 2009.