

Experiences with Extra-Vehicular Activities in Response to Critical ISS Contingencies

E. A. Van Cise¹, B. J. Kelly², and J. P. Radigan³, C. W. Cranmer⁴

NASA Lyndon B. Johnson Space Center, Houston, Texas, 77058

The maturation of the International Space Station (ISS) design from the proposed Space Station Freedom to today's current implementation resulted in external hardware redundancy vulnerabilities in the final design. Failure to compensate for or respond to these vulnerabilities could put the ISS in a posture where it could no longer function as a habitable space station. In the first years of ISS assembly, these responses were to largely be addressed by the continued resupply and Extra-Vehicular Activity (EVA) capabilities of the Space Shuttle. Even prior to the decision to retire the Space Shuttle, it was realized that ISS needed to have its own capability to be able to rapidly repair or replace external hardware without needing to wait for the next cargo resupply mission. As documented in a previous publication, in 2006 development was started to baseline Extra-Vehicular Activity (EVA, or spacewalk) procedures to replace hardware components whose failure would expose some of the ISS vulnerabilities should a second failure occur. This development work laid the groundwork for the onboard crews and the ground operations and engineering teams to be ready to replace any of this failed hardware. In 2010, this development work was put to the test when one of these pieces of hardware failed. This paper will provide a brief summary of the planning and processes established in the original Contingency EVA development phase. It will then review how those plans and processes were implemented in 2010, highlighting what went well as well as where there were deficiencies between theory and reality. This paper will show that the original approach and analyses, though sound, were not as thorough as they should have been in the realm of planning for next worse failures, for documenting Programmatic approval of key assumptions, and not pursuing sufficient engineering analysis prior to the failure of the hardware. The paper will further highlight the changes made to the Contingency EVA preparation team structure, approach, goals, and the resources allocated to its work after the 2010 events. Finally, the authors will overview the implementation of these updates in addressing failures onboard the ISS in 2012, 2013, and 2014. The successful use of the updated approaches, and the application of the approaches to other spacewalks, will demonstrate the effectiveness of this additional work and make a case for putting significant time and resources into pre-failure planning and analysis for critical hardware items on human-tended spacecraft.

Nomenclature

<i>Eclipse</i>	= Period of the orbit where ISS is in the shadow of the Earth
<i>EVA</i>	= Extra-Vehicular Activity, commonly referred to as a "spacewalk"
<i>Fault Tolerance</i>	= Refers to the number of failures a system can accommodate and still remain functional. For example, a "single-fault tolerant" system can withstand one failure and continue to function normally.
<i>Insolation</i>	= Period of the orbit where ISS is in direct sunlight.
<i>MDM</i>	= Multiplexer/Demultiplexer. Refers to an ORU that executes software code onboard the US Orbital Segment (USOS) of the ISS. A MDM can be likened to a computer.

¹ Flight Director, Flight Director Office, 2101 NASA Parkway / CA8, Houston, TX, 77058

² Research Integration Manager, ISS Research Integration Office, 2101 NASA Parkway / OZ6, Houston, TX, 77058

³ Flight Director, Flight Director Office, 2101 NASA Parkway / CA8, Houston, TX, 77058

⁴ Mission Evaluation Room Manager, On-Orbit Engineering Office, 2101 NASA Parkway / OB2, Houston, TX, 77058

- Next Worst Failure* = A failure, after a first failure has already occurred, that would have significant detrimental impacts to a spacecraft or systems. Example: Failure of a redundant piece of equipment after the first unit had already failed.
- ORU* = Orbital Replacement Unit. Refers to an assembly of hardware on ISS that is designed to be replaced if it fails instead of being repaired.
- Prepositioned R&R* = Spare ORUs that are stored on-orbit for use in case of a failure.
- Remove & Replace* = Remove & Replace, restoring operation of a component or system by removing the failed equipment and replacing it with a functional spare
- Team 4* = A dedicated team of personnel from all facets that support the ongoing mission (e.g. ISS Program, Flight Operations, Engineering, Safety, Contractor, etc.) brought together to immediately address and resolve a significant anomaly onboard the spacecraft.

I. Introduction

The International Space Station (ISS) Program began to investigate, develop, and refine the capabilities for its crews to repair hardware external to the space station prior to the launch of the first ISS module. During the assembly sequence of the ISS, the Space Shuttle launched regularly to the orbiting outpost to bring new space station components, logistics, spare parts, and to exchange crewmembers. If any significant external hardware failures occurred during or between assembly missions, the next mission would be repurposed to include replacement of the failed equipment. As ISS grew in size, the standalone capability to repair or replace critical external equipment grew to be known as the “Big 14” as there were 14 external component types that were deemed critical enough to need rapid repair or replacement by contingency spacewalk. In 2006 and 2007, the Big 14 team documented processes, procedures, and assumptions for these contingency spacewalks¹. The list of Critical Contingency EVA (CCE) equipment included replacement of Sequential Shunt Units, Direct Current Switching Units, Main Bus Switching Units, DC-to-DC Converter Units, Remote Power Controller Modules, Pump Flow Control Subassemblies, External Control Zone MDMs, Photovoltaic Control Unit MDMs, Interface Heat Exchangers, Pump Modules, and Flex Hose Rotary Couplers. The list also included tasks of backing out Battery Charge / Discharge Units, manually positioning Solar Array Wings, finding and repairing ammonia coolant line leaks, and finding and repairing pressure hull breaches due to impact by micrometeoroid orbital debris.

The Big 14 development work, completed in 2008, was put to the test in 2010 when the External Thermal Control System’s Loop A Pump Module failed. This failure resulted in the immediate loss of half the cooling capability of the US Orbital Segment (USOS) of the space station. As the two cooling loops of the ISS cannot be cross strapped and with no backup pump on either loop, all the ISS avionics that receive cooling by that external loop needed to be deactivated to avoid overheating them. It also meant that the capability to reject heat from equipment inside the space station, as well as heat created by the crewmembers, was significantly reduced. Further, if the pump on the only other cooling loop were to fail before the Loop A pump was recovered, nearly all heat rejection capability for the US Segment would be lost and the crew could possibly be forced to abandon the space station. The space station was effectively zero fault tolerant for survival.

The plans and processes developed by the Big 14 team for replacement of a Pump Module were quickly brought to the forefront as part of the Team 4 contingency response process initiated by the ISS Program. Using the Big 14’s plans, a path towards performing the three required Extravehicular Activities (EVAs, or spacewalks) to replace the pump was established. In the very early meetings it was realized, however, that not all of the assumptions and theories established by the Big 14 team would meet the needs of the real-life situation the ISS faced. One notable example of this was that in the Big 14 effort minimal to no funding was made available for performing analysis. Use of the station robotic arm is very analysis dependent, especially in the case of a failed cooling loop. Thus the Big 14 team focused on developing ways for the EVAs to be successful without the arm. Once the failure actually occurred, the ISS Program determined that the best path forward was to accept some risk on using the systems that provide power for the arm as well as to quickly perform as much analysis as possible. This shift in assumptions altered a significant amount of work that the Big 14 team had developed. Additionally, significant details remained to be finalized before the onboard crew training could be completed and the EVAs could take place.

Significant lessons were learned during that first ISS Critical Contingency EVA. From those lessons a larger Failure Response Assessment Team (FRAT) was created. The FRAT included a number of sub-teams with representation from the ISS Program, Flight Operations Directorate, engineering, safety, and EVA teams from both NASA and its contractors. The FRAT’s charter, which remains in effect today, is to lead and manage the effort to

balance the risk versus gain of performing as much contingency EVA development work as possible prior to a failure to ensure the replacement of failed critical equipment can occur as expeditiously as possible.

II. Pump Module Failure and Replacement (2010)

On July 31, 2010, the ISS experienced its first “Big 14” failure. The Remote Power Controller Module (a type of electrical power switch) that provides power to the External Thermal Control System (ETCS) Loop A Pump Module (PM) tripped open due to an overcurrent event. This resulted in a loss of cooling from one half of the ISS’s external power equipment and USOS pressurized modules. Analysis of ISS telemetry confirmed a real overcurrent had been caused by the Pump Module and the pump was declared failed. This failure resulted in a loss of cooling to two of the four major power domains onboard ISS and led the on-orbit crew and on-console flight control team to perform an extensive power down. The teams reconfigured space station hardware to best utilize the remaining two power domains. This failure scenario had been encountered in numerous training simulations, allowing the Mission Control team to utilize their training and operational products to save the ISS in an orderly and efficient manner. An Anomaly Resolution Team meeting was held that evening and determined that the only option was to replace the failed pump module.

Additional personnel and resources were brought online to expedite the development, planning, and execution of replacing the Pump Module and returning the ISS to full operational status. The first Team 4 meeting was held on the morning of August 1st, 2010. Discussions focused on getting the team up-to-speed on the current status of the ISS and presenting an overview of the knowns and unknowns associated with recovery. It was immediately decided that an EVA that was already planned for August 5th to perform some standard ISS maintenance and upgrades would be repurposed to support recovery from the current failure. Based on previous Big 14 work, it was known that it would take at least 2 EVAs to fully remove and replace the failed Pump Module. EVA 1 would be geared toward removal of the failed unit and physically installing the spare. EVA 2 would complete installation of the spare Pump Module by connecting its power and fluid umbilicals, as well as stowing the failed Pump Module. Given that both of these EVAs would be scheduled for the full 6.5 hour duration of standard EVAs, it was already known that a third EVA might be required to complete any tasks not completed in the first two EVAs. Other items discussed during this meeting included crew and ground timeline planning, on-orbit crew training and preparation, system reconfigurations required to support the first EVA, and the use of unique hardware and procedures developed specifically for this task. Figures 1 and 2 show the EVA worksite for this pump module.

Over the next several days engineering, operations, and safety teams worked around the clock to develop products to train the crew, reconfigure the ISS, remove and replace the failed pump module, and prepare for the next worst failure. Team 4 meetings were scheduled twice daily to bring all of the sub-teams together, ensuring they remained in sync with the multiple ongoing efforts.

EVA 1 took place on August 7th, 2 days later than originally planned but only 1 week after the initial failure. Objectives for this EVA included disconnecting the failed Pump Module electrical and fluid connections, installation of a Pump Module Bypass jumper (providing ammonia volumetric expansion/contraction relief to the rest of the external thermal system when the Pump Module is disconnected), physical removal and stowage of the failed pump module, and physical installation of the spare Pump Module.

While working to disconnect the fluid connections on the failed pump module, one of the connections experienced a small ammonia leak. Given the toxicity of ammonia and that it is a valuable cooling consumable, immediate troubleshooting was required. The first response when this occurred was to cycle the quick disconnect, re-opening and then reclosing the valve that is a part of the connector. Upon re-closure the quick disconnect experienced a substantial ammonia leak and had to be reopened. The remainder of the EVA time was spent trying to troubleshoot the leaky quick disconnect and no additional work was completed toward the Pump Module removal. The crew returned to the airlock after 8 hours and 3 minutes (EVAs are generally planned to be 6.5 hours long). After completion of EVA 1, the Team 4 reconvened to discuss the system configuration after EVA 1, lessons learned applicable to EVA 2, required modifications to the EVA 2 timeline, and EVA/Airlock consumables required to support a third EVA.

Engineering and operations teams met to discuss the leaky quick disconnect observed on EVA 1, potential root causes for the leak, and troubleshooting steps that could be performed in support of EVA 2 to successfully demate the quick disconnect and proceed with the R&R of the failed Pump Module. It was determined that side loading on the quick disconnect during valve open and close operations could prevent the seals from sealing properly. It was also suspected that the initial leak in the QD generated ice crystals or other foreign debris in the valve which then resulted in the even larger second leak that was observed. The fluid lines attached to the quick disconnect were pressurized at approximately 390 psi (26.9 atm). On-orbit crew feedback coupled with testing of quick disconnect

training equipment on the ground indicated that it would be very difficult to minimize side loading at these pressure. (For comparison purposes, fire hoses are typically pressurized between 116-290 psi (8-20 atm).) The ground teams devised a plan that would allow the flight control team to reduce the pressure in the system as low as possible – to the saturation pressure where liquid ammonia can transition to a gaseous state, approximately 130 psi (8.8 atm) before EVA 2. This was done to provide relief to the EVA crew during upcoming quick disconnect manipulations. This pressure was chosen as the target pressure because it provided significant relief to the fluid line stiffness while staying above the saturation pressure of the ammonia in the loop. This minimized risk to the system hardware during subsequent ammonia refill and system repressurization as part of reactivating the coolant loop. Reducing pressure below the ammonia saturation pressure significantly increases the challenges associated with repressurizing and reactivating the thermal loop and is avoided if at all possible. In case the leaky quick disconnect could not be fixed, contingency plans were also developed to depressurize and vent a small portion of the external thermal loop to allow successful demate of the leaking quick disconnect while preserving the majority of the ammonia in the rest of the thermal loop. This was considered a backup plan because the teams wanted to preserve as much of the limited quantity of ammonia as possible.

EVA 2 was performed on August 11th with the goal to troubleshoot, close, and demate the leaky quick disconnect, remove and stow the failed Pump Module, and prepare the new Pump Module for installation but leave it at its stowage location. The reduced pressure on the fluid lines, combined with additional techniques for operating the QD, allowed for the successful disconnection of the formerly leaking connection on the first attempt. The failed pump module was temporarily stowed and the new pump module was prepared for installation. Overall this second EVA lasted 7 hours and 26 minutes.

The crew went outside for the third and final EVA to restore functionality to the external thermal loop on August 16th. The goals for this EVA were to finish preparations of the spare Pump Module, install it into the system including mechanical, electrical, and fluid connections, and clean-up the EVA worksite. Updates to the quick disconnect mating sequence on the new Pump Module were made based on lessons learned from the previous two EVAs. While there were some minor difficulties encountered with the mechanical bolts and quick disconnect mating, the crew was able to successfully complete all of the tasks required to support successful reconfiguration and restart of the external thermal loop.

After completion of EVA 3 the external thermal loop was returned to its operational pressure and the new Pump Module started for the first time. The next day, on August 17th, all of the system hardware reconfigurations that had been put in place due to the original failure were removed and the ISS was returned to a fully functional state.

It was known before EVA 3 started that there would not be enough time to relocate the failed Pump Module from its temporary stowage location at the Mobile Base System (MBS) on the ISS truss to the spot previously held by the now-installed spare Pump Module on External Stowage Platform 2 (ESP-2) on the airlock. Engineering analysis showed that the failed Pump Module could safely remain in its current stowage location until a Space Shuttle mission could retrieve it at a future date (ultimately STS-135 in July 2011).

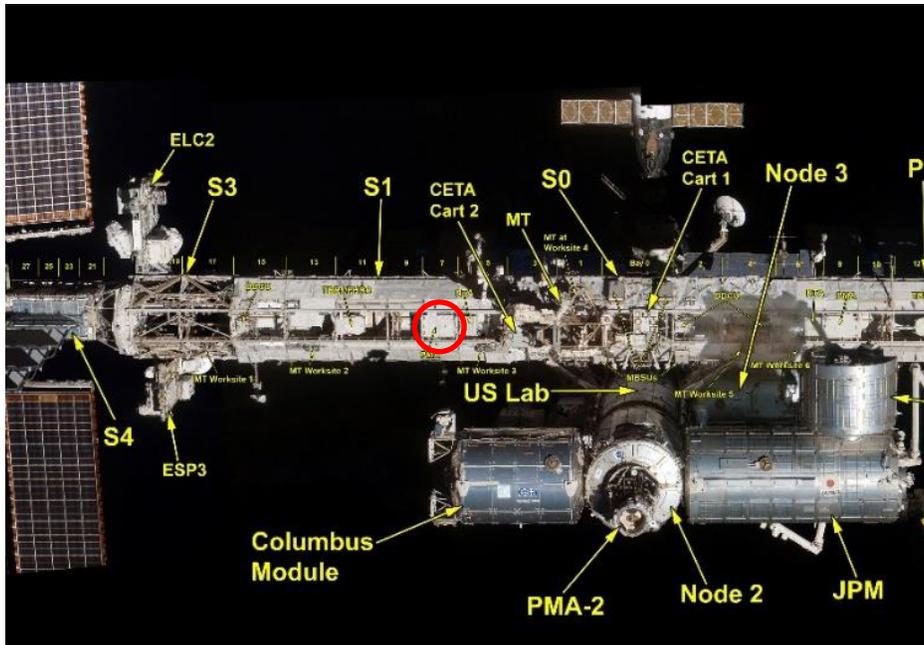


Figure 1. Overview of ISS truss segments S0, S1, and S3. The Loop A Pump Module (circled in red) is located in the S1 truss. Composite photograph from NASA images s130e012949 through s130e012958.



Figure 2. Close up view of the Loop A Pump Module worksite on the front face of the S1 truss segment. NASA image s134e010540.

III. Use of and Deviation from Original “Big 14” Development and Assumptions

The Big 14 development work from 2006-2008 laid the groundwork for the quick response actions the teams were able to take when the Pump Module failed in July 2010. Based on that framework, the Program managers, flight controllers, and engineers were able to more quickly assess the readiness of procedures and training products, determine which analyses would be mandatory to complete before each EVA, and discuss the trade-offs and risks associated with not performing some of the analyses. Without the framework that was built by this effort and the follow-on decisions and risk acceptances it is unlikely the first EVA could have been executed as quickly (one week after failure).

The overall goal of the 2006-2008 Big 14 effort was to develop the operational and engineering products to a level of maturity that would enable the crew to execute the first EVA within 2-4 weeks of the initial failure. When the Pump Module failed on July 30th an opportunity arose to utilize the EVA that had already been scheduled for August 5th, less than a week later. One benefit of the already scheduled EVA was that some work had already been done to prepare both the airlock and the EVA suits the crew would wear. Setting a goal of executing the first EVA so soon both focused and came close to burning out the personnel working the recovery efforts. Many personnel were working 12 or more hour days to support the development of system reconfiguration procedures, EVA timelines, engineering and safety analysis, etc. Ultimately the first EVA would occur on August 7th, just 2 days after the original goal. The thermal loop would be fully recovered within 17 days of the initial failure, much sooner than the time estimated by the Big 14 effort. The Big 14 estimate of 2-4 weeks for the first EVA and one week between subsequent EVAs would have meant full recovery would have taken close to or perhaps even more than a month, instead of just over two weeks.

During the Big 14 effort, EVA timelines to remove and replace a failed Pump Module were developed to support multiple scenarios. When a Pump Module fails, one of two redundant power distribution boxes (DC-to-DC Converter Units, DDCUs) that provide power to the ISS's robotic arm must be unpowered to prevent overheating and permanent damage to the DDCUs as they are cooled by the failed thermal loop. Concerns had been raised about transporting an EVA crewmember and a refrigerator-sized Pump Module on the robotic arm in a zero fault tolerant configuration. A single failure of the other DDCU could result in the EVA crewmember being stranded on the robotic arm away from ISS structure. It was unknown how long an uncooled DDCU could be powered on before it would overheat. To this end the Big 14 team had developed two separate EVA timelines: one allowing use of the robotic arm and one prohibiting its use. Most of the development focus was put on the procedure that prohibited use of the arm. During the first Team 4 meeting after the Pump Module failure the ISS Program Manager made the decision to pursue an EVA that would use the robotic arm. This allowed the team to focus on a specific recovery effort and execute the first EVA sooner. Engineering analysis was performed at this point that showed that for this particular scenario (tied largely to the solar beta angle) the uncooled DDCU could remain on for the length of the EVA, removing any issues with a potentially stranded crewmember on the robotic arm.

The original Big 14 EVA timelines provided the outline for the sequence of events that would need to occur to successfully remove and replace a failed Pump Module, including unique activities such as mating/demating sequences of the quick disconnects, venting of the failed and spare Pump Modules, and use of the Pump Module Jumper hardware which provided pressure relief for the thermal loop when the Pump Module is isolated. Each of these techniques developed during the original Big 14 effort was carried through into the EVA timeline products that were ultimately executed on-orbit.

While the Big 14 effort worked hard to prepare the ISS teams for recovery of critical failures of onboard systems, no work was performed to determine how to respond to the Next Worst Failure (NWF). While the 2006-2008 Big 14 effort was envisioned in response to a set of failures that would leave the ISS just one failure away from having to be abandoned, it became clear during the July 2010 Pump Module recovery efforts that work needed to be done to determine how to best posture the ISS for survival in the event the Next Worst Failure happened. During the Pump Module recovery efforts, while one team was focused on development and execution of EVAs to replace the failed pump, a separate team was formed to identify, protect against, and prepare for the Next Worst Failure of the remaining pump/coolant loop failing before the already-failed pump was replaced. This team analyzed the impacts of a multitude of different failures and developed the response procedures that should be taken if any of these failures were to occur. Some of these responses included pre-positioning hardware or even taking proactive action in reconfiguring some systems prior to the second failure occurring.

IV. Lessons Learned from 2010 Pump Module Failure

After all major events such as space shuttle missions, ISS expeditions, EVAs, etc. NASA holds a lessons learned meeting with input from the crew, operations, engineering, and safety teams. The intent is to learn and discuss what went well, what went poorly, and what improvements can be made to improve processes, products, training, etc. This meeting is held soon after completion of the activity to keep the lessons learned fresh in everyone's mind. The Pump Module recovery lessons learned meeting occurred approximately 2 weeks after recovery of the thermal loop. It covered lessons learned and recommendations from both technical aspects as well as programmatic and personnel related aspects.

The amount of work required to prepare for and execute the Pump Module replacement EVAs was significantly underestimated. The plans built by the Big 14 effort relied heavily on generic constraints and analyses to infer ISS system configuration requirements, did not fully develop the robotics support procedures necessary to

support the EVAs, focused generic crew training on the ORU removal/install instead of the overall timeline, and did not address systems reconfigurations required to support Next Worst Failure protection. In light of this, recommendations were made to baseline operational products that are as close to execute-ready as possible for post-failure ISS safing, EVA response, and system recovery. Further recommendations were made to make better use of existing historical flight data to expand system operational limits where practical. This would reduce the amount of quick-turnaround, task-specific analysis and ops product development required prior to execution of the first EVA. Another significant realization was that while the official requirement was to conduct the first EVA within “2 to 4 weeks after failure,” the ISS Program will always press on the teams to perform that EVA (and all EVAs if more than one is required) as soon as safely possible.

It was frequently stated that in the lessons learned meeting that “Just because we’re ready for *an* EVA doesn’t mean we’re ready for *this* EVA.” Although the EVA suits and Airlock equipment were prepared for an EVA to occur 6 days after the day the pump module failed, considerable workload was placed on the EVA, robotics, engineering, and safety teams, as well as the crew, to perform the analysis and develop the operational products required to execute the first EVA to meet this August 5 deadline. A recommendation was made to build post-failure timeline templates that indicate the day-for-day activities, analyses, operational product readiness, crew training, etc. that need to occur throughout the entire failure recovery effort (not just up to the first EVA). This template would enable the recovery teams and management to more accurately understand the work required and time it would likely take for completion.

The use of the ISS robotic arm was critical to completion of the Pump Module removal and replacement within 3 EVAs. If it had not been used it is likely that at least one additional EVA would have been required. The team recommended that all future CCE tasks that could make use of the robotic arm should baseline its use to support recovery efforts from critical system failures. Additionally, it was recommended that all of the generic systems constraints that the teams operate under during standard operations be reviewed for flexibilities that can be taken advantage of during off-nominal situations. These include items such as expanding hardware thermal limits, thermal loop pressure management, and equipment power safing requirements.

The teams also identified a suite of new hardware and equipment that would facilitate post-failure system reconfiguration, better posture the ISS for survival in the event of the Next Worst Failure, and make it easier for the EVA crew to manipulate fluid quick disconnects on the external thermal loops².

V. Failure Response Assessment Team Development

In order to address the lessons learned while replacing the Pump Module in 2010, the ISS Program chartered the Failure Response Assessment Team (FRAT). This team identified key focus areas that needed further development for all of the replaceable equipment on the Critical Contingency EVA (CCE) list (the new name for the “Big 14 list”). These focus areas included delving deeper into the engineering constraints pertaining to the replacement of each piece of hardware, documentation of the assumptions used in all of the pre-failure development work, continued development of the operational products needed to perform the repair EVA(s), and protection against a Next Worst Failure,

In order to accomplish as much work in as little time as possible, sub-teams were created for each major area. These sub-teams scrutinized all the ORUs on the CCE list. The Constraints Assessment Team, co-chaired by members of the ISS Program’s Vehicle and Safety offices, focused on the engineering constraints and hardware limitations with the failure of each ORU. The Ops Products and Analysis Team, co-chaired by the Flight Operations Directorate and the ISS Program’s Vehicle Office assessed the readiness of operational products (procedures, crew training, etc.) and ISS hardware analyses. The System Configuration Requirements team, also co-chaired by the Flight Operations Directorate and the ISS Program’s Vehicle Office, developed methods for the ISS crew and flight controllers to best posture the ISS after the first failure so it could tolerate, as best it could, a subsequent serious failure (the ‘Next Worst Failure’). These sub-teams reported their findings to each other as well as to the FRAT Leadership Team, whose members included representatives from the ISS Vehicle Office, Flight Operations Directorate, EVA Office, Johnson Space Center Engineering Directorate, NASA Safety Office, and Boeing Safety Office. Reference Figure 3.

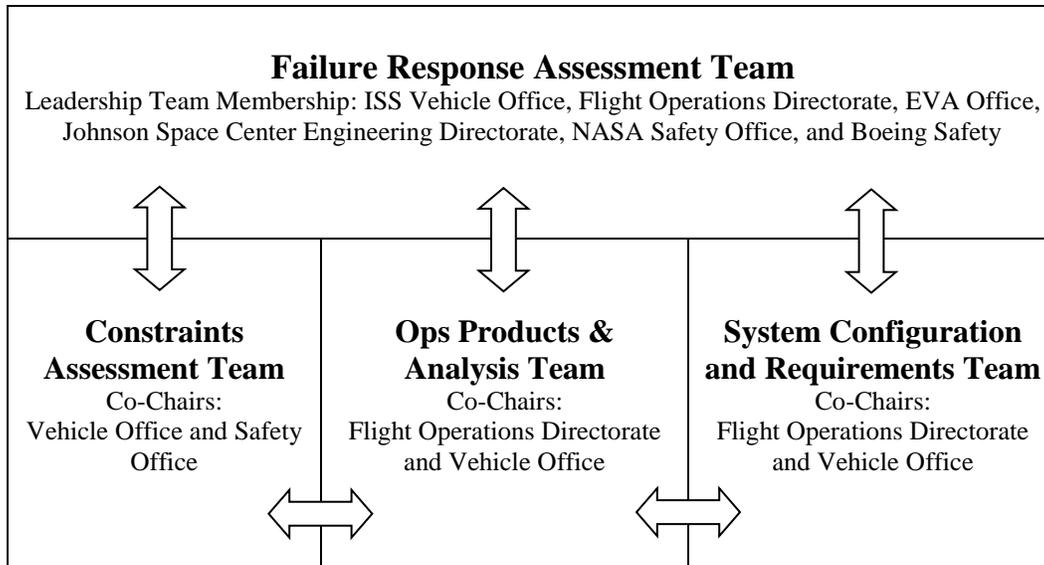


Figure 3. FRAT structure in September 2010 (weeks after completion of Pump Module replacement).

The initial work for the FRAT and its sub-teams was to establish the extent of the open work to further refine the Big 14 team’s work to meet the level of detail required based on the experiences from the 2010 Pump Module failure.

The Next Worst Failure (System Configuration and Requirements) team started from scratch as this was a facet of the preparation process the Big 14 team did not investigate. This team identified several scenarios that would need to be investigated and brought to the ISS Program for direction on how far the preparation for these multiple-failure cases should proceed. Identified Next Worst Failure cases included failure of both External Systems MDMs, loss of the function of both External Thermal Control System cooling loops, permanent loss of one of the ETCS cooling loops, and various second failures after the failure of a Main Bus Switching Unit.

The Ops Products and Analysis team identified that while most of the Big 14 procedures and products were useful, they needed to be significantly updated due to changes in baseline assumptions. This meant first documenting the generic and ORU-specific assumptions, determining the required engineering analysis based on those assumptions, and incorporating the analysis results into the actual spacewalk procedures. The Constraints Assessment team worked with the Ops Products team to identify the numerous assumptions as well as the vehicle, program, and safety risks associated with those assumptions. All of this work was reported regularly to the FRAT Leadership Team and from that team to the ISS Program.

Once the initial review by the sub-teams was completed, the FRAT reported to the ISS Program in March 2011. This report included not only the summary of the teams’ work but also proposals for additional hardware, such as fluid and power jumpers, that could be flown to the space station to help improve the ability to withstand a Next Worst Failure. At the ISS Program meeting in March 2011, it was agreed that there still remained significant work ahead to best posture ISS to be ready for another critical failure. A longer term ‘sustaining’ approach was agreed to for the FRAT. The Constraints Assessment team was merged with the Ops Products and Analysis team. That Ops Products team would work to identify a listing of analysis that needed to be completed in advance of a failure to best enable accurate EVA products and procedures. Once identified, a subset of these analyses would be funded to be performed prior to equipment failure. By having these analyses and products in place prior to failure, the time between failure and the first repair EVA could be made as short as possible. Also at the March 2011 meeting the number of ORUs on the CCE list was refined. Some ORUs and tasks were removed (replacement of Sequential Shunt Units, Direct Current Switching Units, Pump Flow Control Subassemblies, and Photovoltaic Control Unit MDMs, along with backing out Battery Charge / Discharge Units and manually positioning solar arrays) and others were added (replacement of Nitrogen Tank Assemblies, Ammonia Tank Assemblies, solar array Bearing, Motor, and Roll Ring Modules, and solar array Electronics Control Units), resulting in an updated list of 13 ORUs (the “Big 13”).

With work being performed by multiple sub-teams and even smaller groups within each sub-team, a single repository was required for all data in order to keep all the teams in sync. More importantly, in the event of a failure necessitating a contingency EVA, the necessary documentation needed to all be in a single location. For these reasons, a single FRAT website was established. This website, similar to the Big 14 team website, had sub-pages for each of the eleven ORUs, as well as for ammonia leak location and pressure hull breach location and repair. All assumptions, crew and ground timelines for work to be performed after a failure, engineering analysis plans, next worse failure plans, and EVA products could be placed on this website. Some final products, such as actual engineering analysis results, were not stored on this website. Links to the engineering repositories were provided instead. Final operations products, from crew procedures to training materials to reference information, were added to the crew's procedure viewer tool so that the information would be readily accessible to both the ISS crews and the flight control teams if needed. Also on the FRAT website was a standalone presentation to be used at the first Team 4 meeting after a hardware failure. Reviewed and updated regularly, this document is an overview instruction on how the FRAT products and processes have been setup to assist the contingency response teams in preparing to replace the failed hardware. This document helps bridge the gap between pre-failure analysis and assumptions to the actual post-failure situation and open work.

A key component of the FRAT assessment is engineering analysis. There are numerous analyses required to be performed in order to safely and successfully perform an EVA. These range from thermal clocks and limits on hardware, structural loads constraints, torque settings for installing and removing fasteners, to plasma environment forecasts and numerous more. Many of these analyses can be performed generically, prior to the actual failure. Other analyses can be performed prior to failure but because the results may vary based on the environment (time of year, angle between ISS and the sun, etc.), numerous iterations may be required. In other cases, the analyses can only be performed after the failure occurs when the exact situation is known. The ISS Program had the contractor team develop an Integrated Operations Product Template (IOPT) that, for each ORU, listed every possible analysis that may be required in order to replace each ORU. The IOPT also identified the dependencies for each analysis item (e.g. output from other analyses or crew procedures). From that list, the Ops Products and Analysis Team determined which analyses should be performed prior to failure, which after the failure, and which may not be needed at all. Two key factors were assessed in recommending each analysis item for pre-failure funding. One was whether performing the analysis in advance would significantly reduce the time between the failure and the first EVA. Another factor was whether the analysis result could significantly affect the EVA procedures (and could thus delay the EVA if the procedures had to be changed after the failure occurred). Figure 4 illustrate the decision tree. The culmination of the IOPT assessments enabled the ISS Program to define, prioritize, and fund a vast amount of pre-failure analysis while also identifying the scope of analysis work that would remain after the failure for each ORU.

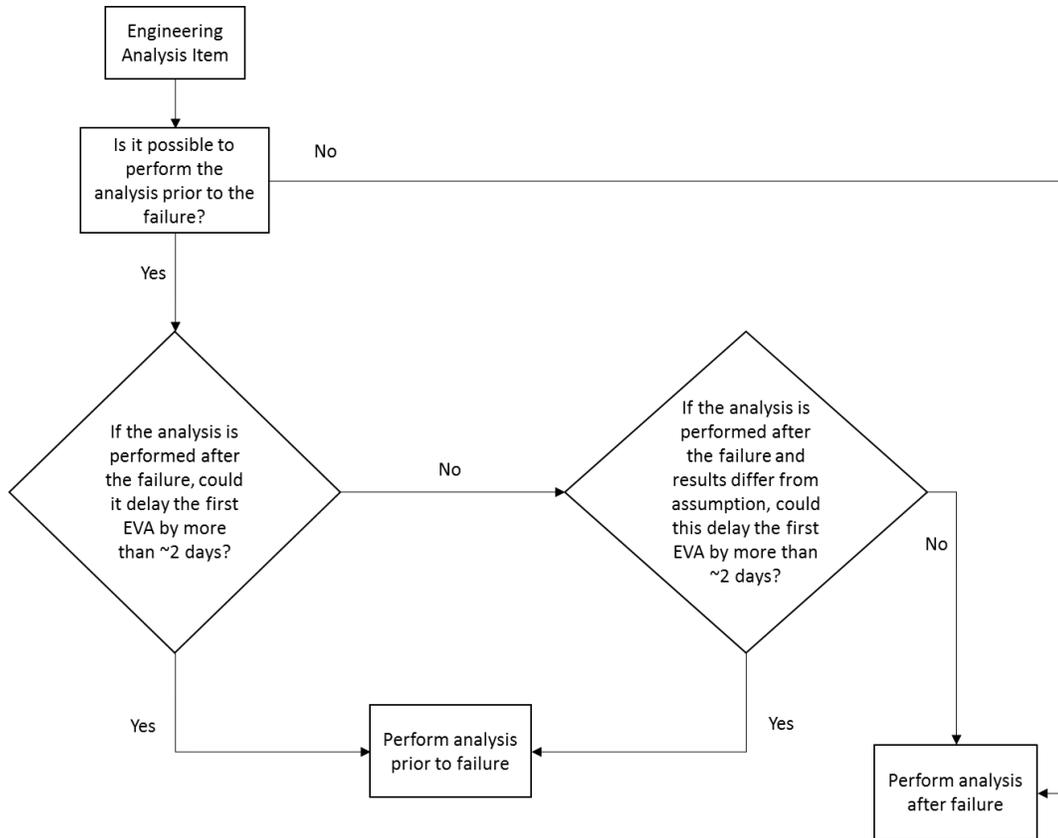


Figure 4. Decision process for recommending whether the ISS Program should perform IOPT analysis prior to the failure of the hardware or wait until after the hardware has failed and an EVA to replace the hardware is required.

VI. FRAT Work Tested

In the Fall of 2011, a Main Bus Switching Unit (MBSU) lost communication with the MDM that controlled it. The MBSU is a major component in the ISS electrical power system. It contains numerous relays that route power from the solar arrays to various pieces of equipment across the station. After this failure, the MBSU was still routing power but could not be reconfigured. Though not performed regularly, reconfigurations are often necessary in response to various power-related failures. The MBSU is a piece of hardware on the CCE list and work was started to develop an EVA to replace it. After some review, however, the engineering teams recommended and the ISS Program agreed that it would be acceptable to wait a few months – until an EVA already planned for August 2012 – to replace the hardware. This delay enabled the EVA development team to utilize FRAT processes and initial products developed by the Big 14 team to create a MBSU replacement plan that would also leave room in the EVA timeline to complete other maintenance tasks.

The MBSU replacement EVA did not go as expected, however. There was difficulty installing the spare MBSU into its proper location on the space station’s truss due to damage to one of the bolt receptacles. A follow-on contingency EVA would be required to complete installation of the spare MBSU³. Planning for this contingency EVA was assisted by the FRAT processes that had been developed, such as the post-failure crew and ground timelines and the IOPT analysis development processes. Additionally, the products that had been developed by this point for use after a MBSU failure assisted considerably with the teams being able to rapidly best posture the space station for a Next Worse Failure. Instead of a hurried rush to develop these products, the teams were instead able to review what was already created, determine their applicability for the specific case, and implement the necessary actions to best safeguard the station until the MBSU problems could be resolved.

Another contingency EVA was performed in May 2013. A coolant pump for the photovoltaic system on the port-most (P6) truss started leaking its ammonia coolant. While not a part of the larger external thermal control system of

the ISS, the photovoltaic cooling systems keep the ISS batteries, as well as the avionics that support the batteries, within their operational thermal constraints. Without proper cooling, this equipment would quickly overheat and thus would need to be turned off, resulting in the loss of some of the power storage capability of the space station. It was decided to attempt to replace the only easily accessible component of this cooling system – the coolant pump. For a number of reasons, this EVA needed to occur less than two days after the system leak was reported. It was desired to get the crew to the worksite before all the ammonia had leaked away to help them identify exactly where the leak was occurring. Additionally, three of the six ISS crewmembers were scheduled to return to Earth five days after the leak was reported⁴. The replacement of the coolant pump (a Pump Flow Control Subassembly), which successfully stopped the system leak, was possible in large part due to the work the FRAT had done on developing contingency EVAs. While this particular coolant pump was not on the current “Big 13” FRAT list of hardware, it was on the previous list addressed by the Big 14 team. The information from that work, along with the general processes and templates for preparing for a contingency EVA, proved to be invaluable. The contingency response teams used the FRAT and Big 14 work as a template to decide which analyses were required, which crew training and procedure products were required, and how the timeline leading up to the EVA needed to be orchestrated in order to get the astronauts outside the space station as soon as possible.

VII. FRAT Product Implementation

In December 2013, the flow control valve inside of the Pump Module of the External Thermal Control System’s Loop A failed. This valve was in the pump that had been replaced in the three EVAs in 2010. The valve failure resulted in the loss of cooling control of this thermal loop, not a complete loss of the ability to circulate ammonia. While the pump would still flow ammonia there was no way for the closed loop control of the system to maintain the correct temperature set point. As a result, valves in the interface heat exchangers were closed. This caused the ammonia to bypass these heat exchangers and prevented the heat exchangers from damage or rupture in the event the ammonia got too cold (near or below the freezing point of water). Bypassing the heat exchangers meant that no heat generated by the internal systems and the crew could be rejected to Loop A, necessitating a second series of EVAs to replace the Loop A pump module in order to regain the heat rejection capability. The second series of EVAs was a success and the pump module was replaced in two EVAs. A third EVA to move the failed pump module to a staging location was deferred to a later date. While the pace was fast and the EVA preparation and tasks themselves were still complicated, successful use of the numerous FRAT-generated products made a considerable positive difference in the ability for Team 4 to prepare for the EVA and accurately focus on details specific to this particular failure scenario.

In April 2014, during a routine software load, the redundant external (EXT) MDM did not boot when power was applied. Further troubleshooting was unable to awaken the box and an R&R was required to maintain critical redundancy. This would be the first use of FRAT products to R&R an ORU that had not been previously replaced. Due to the EXT MDM being located in the center of the S0 truss it is in a relatively benign thermal environment. Its electrical inhibits are also simple due to the limited number of connectors. These two factors meant that the total analysis that was required after the failure was minimal. It did, however, reaffirm the work that had gone into the IOPT matrices as no additional work was required in order to perform the contingency EVA. The EVA was successful and was a good test of the FRAT preparation products and approaches. Even though this EVA went smoothly, lessons were still learned. For example, it was realized that a high level document that describes the FRAT’s pre-work and processes was required. This document would be the first reviewed after a critical ORU failure and guide all involved, especially those who were not on the FRAT team, into how to transition from the generic work the FRAT had done into the actual case specific to the failure that had occurred.

When comparing the EXT MDM R&R to the other contingency EVAs, however, it underscored that in order to perform the more challenging EVAs, additional pre-failure analysis must be completed, beyond simply developing IOPT matrices that identify analysis that should be performed.

VIII. FRAT Analysis Review

As the FRAT teams learned from these experiences of performing contingency EVAs between 2010 and 2014, the FRAT also continued putting plans in place to be able to meet Program requirement for the first contingency EVA to always be able to occur within four weeks of a CCE ORU failure, or sooner if at all possible. For eleven of the thirteen ORUs that can lead to a CCE, the portfolio of analyses required to prepare ISS and the crew to execute the repair EVA(s) was finalized by the FRAT. Analyses required to prepare for each CCE were captured in IOPT spreadsheets. As previously explained and illustrated in Figure 4, not all IOPT analyses need to be performed prior to the ORU failing; only the analyses with long lead times or were thought to be necessary to relieve the post failure

workload. The FRAT critically assessed each analysis to determine which must be completed pre-failure to ensure the first EVA can occur within a goal of nine days and a maximum of four weeks of the ORU failure. The final list of recommended pre-failure IOPT analyses for each ORU was approved by the ISS Program Manager in May 2014.

In October 2014 the Space Station Program authorized funding to perform the pre-failure analyses for the Pump Module, the highest priority ORU on the CCE list. The FRAT moved forward to engage the contractor teams to perform the work. Biweekly FRAT leadership meetings coordinated the Flight Operations Directorate, Vehicle Office (and contractor teams), EVA Office, and Safety resources to perform the analyses for the Pump Module.

Also in the October 2014, the ISS Program Risk Advisory Board (PRAB) was presented a schedule that showed final completion of all of the CCE pre-failure IOPT analyses for all ORU types would not occur until 2023. Key factors that impacted the schedule included the capacity of system experts to absorb additional pre-failure analyses workload and the low Technology Readiness Level (TRL) for two CCE cases (micrometeoroid orbital debris penetration and ammonia coolant system leak pinpoint and repair).

The slow pace of performing the CCE pre-failure IOPT analyses, with a schedule extending to 2023 which is very near the projected end of ISS life in 2024, was deemed unacceptable by Program management.

At the December 2014 PRAB, the FRAT team was challenged to assess:

- 1) whether the work currently scoped addresses the correct level of Program risk
- 2) whether the correct and only the necessary analyses were being selected to be able to perform the first EVA quickly
- 3) when the work would really be done (how conservative was the estimate)

Several initiatives were put into motion to address these questions and concerns.

- In January 2015 the Probabilistic Risk Analysis (PRA) Team revisited the risk and likelihood of each of the CCE ORUs failing and confirmed there was no driver to revise the ORU order for performing the pre-failure analyses. The pump module continued to be a high risk. The analyses for the pump module, already started, continued through completion in Fiscal Year 2015.
- The February 2015 PRAB accepted the FRAT recommendation to open separate risks for two of the thirteen ORU failures with low Technical Readiness Level (TRL) so that the PRAB could monitor the progress during bimonthly reviews. This change made it easier for ISS program management to understand the overall readiness level of performing the various contingency EVAs – both those with high readiness levels as well as the two that still had significant development work remaining.
- In February and April 2015 the FRAT Leadership Team continued to refine the remaining IOPT lists to solicit Program approval for a detailed assessment of the pre-failure requirements with the idea that the work list agreed to in May 2014 could potentially be further reduced without significant impact to the overall objective (swift response to a failure and ability to start EVA 1 as soon as possible).
- In April 2015, the ISS Program authorized a special study to optimized the IOPTs to remove duplication of analyses across ORUs, identify areas for a small amount of risk acceptance and thereby leave some the analysis to be performed post-failure, determine where previous analysis and engineering judgment could be used instead of performing new or additional analysis, and streamline work by the safety teams in parallel with the hardware analysis, leaving final integration of the safety assessments for the post-failure timeframe.

In August 2015, the optimized CCE IOPT pre-failure analyses recommendations were presented to the ISS Program. This optimization, which was approved, will result in retirement of the ISS Top Program Risk associated with readiness to perform replacement of eleven of the thirteen ORUs in 2018 instead of 2021 and reduce the pre-failure analysis hours for the remaining ten CCE ORUs by approximately 55%.

IX. Future Plans

The FRAT was chartered in September 2010, as follow-on to the Big 14 work that had concluded in 2008, to provide high-level coordination across a variety of ISS Program organizations to ensure that all CCE failures are adequately developed, provide a centralized location for “shelving” all CCE failure products so the entire team has a consistent starting point when a CCE failure occurs, and serve as the single point of contact to the ISS Program for periodic status reports. This charter remains valid.

Key FRAT roles that will remain for years:

- Guide Program resources to complete the CCE pre-failure analysis per agreed-to planned schedules.
- Recommend additional hardware to the Program for deployment to improve the CCE failure and Next Worse Failure risk postures.
- Serve as a focal point for the Program for input that may affect CCE failure response plans.
- Provide regular status reports to the Program.
- Adjust FRAT-related priorities as new information becomes available.

Currently, all identified pre-failure analysis for the Pump Module has been completed. The FRAT is concluding the incorporation of the analysis work into operations products such that when the next pump module R&R is required, there should not be any additional analysis work required before the EVA can be completed unless the unique failure case is something the generic pre-failure assessments did not anticipate. As the analysis work for other ORUs is completed, the work of updating operations products will be completed as well.

The FRAT team is currently assessing other ways to mitigate the need for contingency EVAs through additional electrical jumpers which would reroute power through the space station when installed. There are still two major reasons that an MBSU is on the list of contingency EVAs. The first is providing power to the Russian segment and the second is providing power to the station's robotic arm. The FRAT team has identified jumpers that can be used to mitigate the risk to the arm. The production of these jumpers is currently being evaluated by the ISS Program. With the delivery of the MLM module to the Russian segment (planned for 2018), there will be capability on the Russian segment to reroute power in the event of an MBSU failure. If the identified jumpers for the robotic arm are flown to the station and once the MLM's capability is established, there should be no need for a contingency EVA in the event of a MBSU failure.

The FRAT is also working with the ISS stochastic safety and probabilistic risk assessment team to refine the likelihood of failure for each of the contingency EVAs. Two of the contingency EVAs, Ammonia Tank Assembly (ATA) and Nitrogen Tank Assembly (NTA), would only be performed in the event that a Flex Hose Rotary Coupler failure occurred and the ammonia lines in that rotating ORU could not be isolated. In that case, it is possible that enough ammonia and nitrogen will leak from the system to require the ETCS to be completely refilled. A complete refill would require more ammonia and nitrogen that can be supplied by a single ATA and/or NTA and would thus need to be replaced after its use to refill the system. The FRAT is evaluating this scenario as the likelihood of failure may lead to a conclusion that it is non-credible to have a failure which would require an ATA and NTA R&R. This could eventually lead to removing the ATA and NTA from the list of CCE ORUs, reducing the amount of resources required to fully develop those EVAs.

Early in the development of contingency responses, the use of the space station's primary robotic arm and its additional, smaller dexterous manipulator was ground-ruled out due to the lack of experience performing critical ORU R&Rs robotically. Since that time, multiple R&Rs of non-critical ORUs have been performed robotically, as well as numerous robotic installations and removals of payload experiments. In the months ahead, the FRAT team will be reassessing the use of the robotic systems to R&R critical ORUs as alternative to EVA.

Analysis in support of CCEs will continue through 2018. Once that analysis is completed, one of the major reasons for chartering the FRAT team will be complete. In the absence of newly identified contingency EVAs, the effort of the team will be reduced in scope to an effort of sustaining the contingency responses already developed. At this point the top ISS program risk associated with being unable to respond to a critical failure can be retired.

X. Conclusion

While the efforts to prepare for critical contingency EVAs prior to the Pump Module failure in 2010 were well thought out and developed, putting the plans into practice for the first time revealed several key areas that needed additional focus for future contingency EVAs. While this is true, it should not be overlooked that the series of EVAs in 2010 was entirely successful in replacing the failed pump and the ability to perform this repair in relatively short order was due in significant part to the work of the Big 14 team.

Reviews after the 2010 replacement revealed that additional focus was needed in the areas of generation of engineering analysis prior to failure whenever possible and practical, clearer documentation of assumptions both at the Programmatic and operational levels, and development of plans, procedures, and hardware to best fortify the space station to withstand a second significant failure after the first failure has occurred.

It should not be overlooked that the Big 14 team effort, prior to the 2010 failure, was performed without additional, specific funding. This project was absorbed as part of 'standard work' by the teams involved. To that

end, very little engineering analysis was performed during that timeframe. Rather, the teams worked to identify the analytical work that would need to be performed once the failure occurred. Leaving all the analysis to be performed 'post failure' proved to be a primary driver for the timing of when the first – and subsequent – repair EVAs could be performed. As another lesson learned from the 2010 EVAs, the ISS Program realized it would need to fund dedicated pre-failure analyses for all of its contingency EVA replacements in order to help ensure as short a time as possible between failure and the repair EVAs.

A dedicated team – the FRAT – is now a part of the ISS Program. This team continues to manage and help integrate the ongoing analysis efforts for the critical contingency EVA hardware. This includes finalizing and storing analyses, operations products, assumptions, and next worst failure products in locations that are easily and readily accessible should they be needed. The team also continues to work with experts across the Program to assess additional ways to protect against Next Worst Failures, either through development of new hardware or adapting hardware, software, and procedures already onboard. The work of both the Big 14 and the FRAT teams has shown that success requires input and expertise across a number of disciplines. Thus the FRAT continues to ensure members from the ISS Program, Flight Operations, Engineering, Safety, EVA, and contractor teams remain involved in the continuation and finalization of the FRAT work. The FRAT work completed to date has shown usefulness not only directly in the response to critical hardware failures but also in response to other failures not formally designated 'critical' that needed swift response in order to ensure ISS could continue its primary mission.

It should be noted that little mention has been made regarding the repair of ammonia system leaks or micrometeoroid debris penetration in the ISS pressure shell. Both of these items are on the Critical Contingency EVA list as items that definitely need rapid response should they occur. Unfortunately, the means and methods to pinpoint leak or penetration locations, let alone successfully repair them, are still in development. These have been in development for years and have proven to be both difficult and costly to accomplish. Until the designs for such systems and tools are finalized and launched to orbit, the readiness to perform contingency EVAs is low.

As the ISS Program continues its mission of first class scientific and exploration research that can only be performed off-planet, the on-going work of the FRAT and development of readiness to perform the next Critical Contingency EVA will help ensure a swift and successful response to the next hardware failure to ensure ISS can continue its mission for the next ten years or longer.

Acknowledgments

The authors of this paper would like to thank the following personnel for their support of the multiple meetings, discussions, testing, validation, and research that was required to complete the work documented in this paper: Bob Levy, Matt Scudder, Bruce Harkness, Kirt Chapman, Olga Vassiliev, Larry Turner, Tim Bond, Richard Morton, Gary Rankin, Dana Weigel, Kevin Window, Phillip Mortillaro, Ryan Prouty, Ginger Kerrick, Theresa Castillo, John Yasensky, Andrew Willis, Lawrence Thomas, Ankur Desai, Mike Lammers, Scott Stover, David Gruntz, Dina Contella, Courtenay McMillan, Holly Ridings, and Kieth Johnson. The authors would also like to specifically thank Jackie Kagey for her assistance in developing this paper.

References

1. Smith, L. N. and Van Cise, E. A., "Contingency Planning for Removal and Replacement of Critical Equipment During Stage Extra-Vehicular Activity," AIAA-2008-3287 SpaceOps 2008 Conference
2. Prouty, R., et al., "ISS Contingency EVA Failure Response Assessment Team: Lessons Learned from Loop A Pump Module Recovery," April 2011 (unpublished White Paper).
3. Stephenson, Haley. "The Toothbrush Hack." *APPEL Academy of Program Project Engineering Leadership*. NASA Academy of Program Project Engineering Leadership, 8 Feb. 2013. Web. 13 Sept. 2015. <<http://appel.nasa.gov/2013/02/08/the-toothbrush-hack/>>.
4. Kauderer, Amiko. "Astronauts Complete Spacewalk to Repair Ammonia Leak, Station Changes Command." *NASA International Space Station Status*. NASA, 12 May 2013. Web. 13 Sept. 2015. <http://www.nasa.gov/mission_pages/station/expeditions/expedition35/e35_051113_eva.html>.
5. "Assembly Sequence Critical Failures - Final Report," March 1998 (unpublished).
6. "Increment Definition and Requirements Document for Increments XX and YY Standard Blank Book," NASA SSP 54004 Revision F, August 2013.
7. "Generic Groundrules, Requirements, and Constraints Part 1: Strategic and Tactical Planning," NASA SSP 50261-01 Revision G, August 2012.
8. Gerstenmaier, W. H. and Greene, J. H., "EPS Inhibits for IVA and EVA," NASA MA2-88-170, February 2000.