IAC-17-B3.9-GTS.2

REVIEW OF SIGNIFICANT INCIDENTS AND CLOSE CALLS IN HUMAN SPACEFLIGHT FROM A HUMAN FACTORS PERSPECTIVE

Jackelynne Silva-Martinez, Richard Ellenberger, Jonathan Dory
NASA Johnson Space Center, United States
jackelynne.p.silva-martinez@nasa.gov, s.r.ellenberger@nasa.gov, jonathan.r.dory@nasa.gov

This project aims to identify poor human factors design decisions that led to error-prone systems, or did not facilitate the flight crew making the right choices; and to verify that NASA is effectively preventing similar incidents from occurring again. This analysis was performed by reviewing significant incidents and close calls in human spaceflight identified by the NASA Johnson Space Center Safety and Mission Assurance Flight Safety Office. The review of incidents shows whether the identified human errors were due to the operational phase (flight crew and ground control) or if they initiated at the design phase (includes manufacturing and test). This classification was performed with the aid of the NASA Human Systems Integration domains. This in-depth analysis resulted in a tool that helps with the human factors classification of significant incidents and close calls in human spaceflight, which can be used to identify human errors at the operational level, and how they were or should be minimized. Current governing documents on human systems integration for both government and commercial crew were reviewed to see if current requirements, processes, training, and standard operating procedures protect the crew and ground control against these issues occurring in the future. Based on the findings, recommendations to target those areas are provided.

Keywords: human spaceflight, significant incidents, human factors, human systems integration, space, safety, mission assurance.

I. INTRODUCTION TO SIGNIFICANT INCIDENTS TOOL

The Significant Incidents and Close Calls in Human Spaceflight graphic in Figure 1 presents a visual overview of major losses and close calls throughout the history of human spaceflight. The chart focuses primarily on those incidents that happened with crewed missions for suborbital, orbital, and lunar missions. The incidents are organized by flight phase: those occurring in ground, during launch, flight (ascent and descent), entry, landing, and post-landing. Each box includes the name of the mission, date in which the incident occurred, and a brief description. The colors of the boxes signify the types of events: loss of crew (red), crew injury (light orange), and related or recurring events (yellow). This chart was created and is currently maintained by the NASA Johnson Space Center Safety and Mission Assurance Office. It was put together with the purpose of providing awareness of the risks inherent in human spaceflight, and to encourage continued vigilance for current and new missions. It is a tool for sharing lessons learned to prevent future tragedies [1].

This graphic led to the development of an interactive tool where the user can click on provided classifications, such as the type of event, human error, vehicles, country, systems, and lessons learned [2]. These classifications allow a user to narrow down the incidents, and then click on the interested event to see a slide with more information about the incident, with links to references. This interactive tool was used to perform an in-depth analysis from a Human Systems Integration (HSI) perspective, looking at human error occurring in the operational phase [3,4]. From there, we were able to derive classifications of human error and provide recommendations that will be discussed in the next sections.

II. ANALYSIS OF SIGNIFICANT INCIDENTS IN HUMAN SPACEFLIGHT

II.I. Assumptions for Analysis

Human error can occur anywhere in a System of Systems. For example, an error in software code is also a human error since a human is the one developing it. Similarly, an error in the process is also a human error given that humans were the ones creating the process [4]. However, to scope this analysis, the following assumptions were made:

a) Human errors included in this analysis were cases when the errors led to an incident or close call.

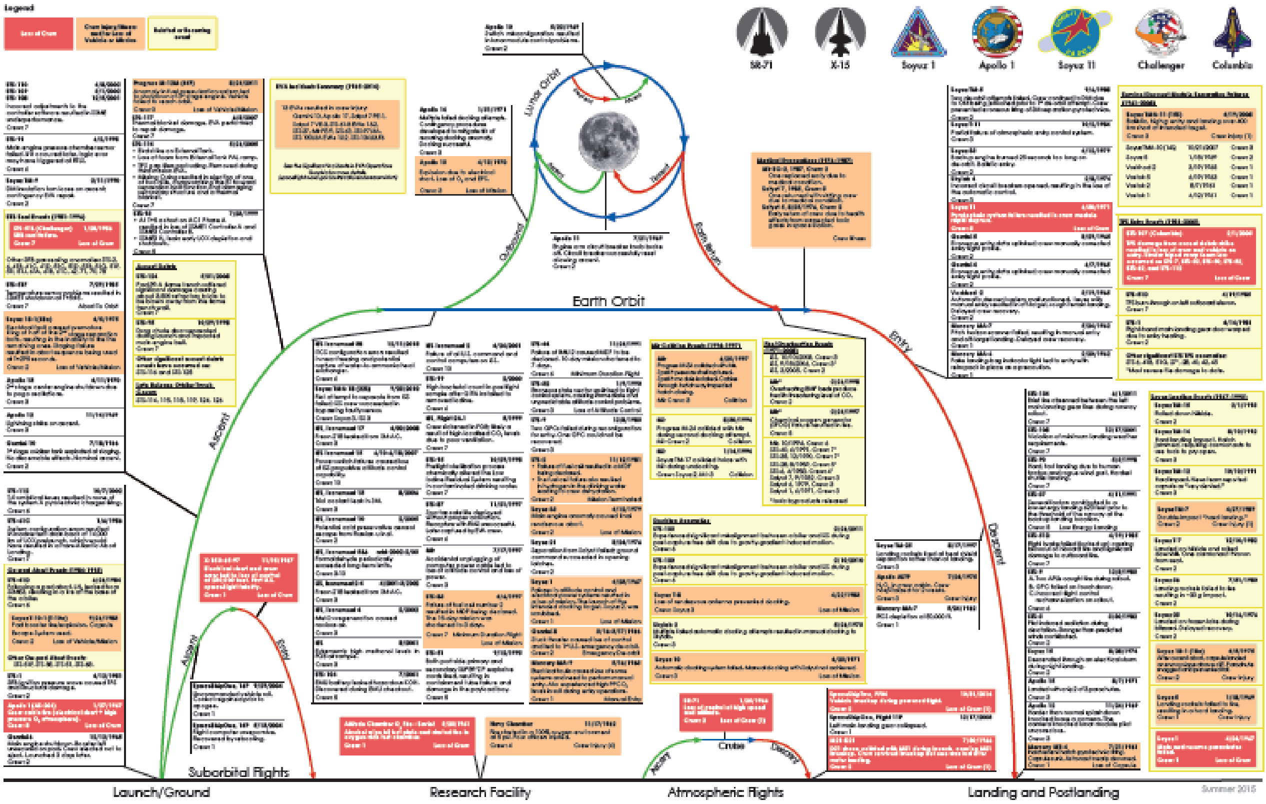


Fig. 1. Significant Incidents and Close Calls in Human Spaceflight (NASA, 2015) [1].

b) Although everything can be attributed to human error at some point, this classification focuses on human error at the operational level, and whether it was a design-induced error. Design-induced errors occur when the task or action did not meet its intended function due to design issues.

c) All medical evacuations are described as being due to medical conditions. Private health information is unavailable for this study and we cannot be sure whether the medical condition was caused by design-induced error or operational error.

d) EVA incident summaries were excluded from this review as they are documented in a separate graphic called “Significant Incidents and Close Calls in Human Spaceflight: EVA Operations” [5].

II.II. Description of Analysis

The in-depth exploration of the significant incidents related to human error was performed using Microsoft Excel, in which a table was created to address different factors for this analysis. This file can be used as a tool to easily search for lessons learned related to human factors. If users want to investigate further a particular incident, they can follow up with the Significant Incidents tool with incorporated recommendations made in this paper. The tabs included are (shown in Figure 2):

- Project Summary
- Assumptions
- Classification
- To-add SpaceShip 2
- To-add EVA 23
- Recommendations for Tool Updates

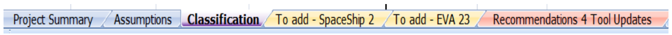

Project Summary | Assumptions | Classification | To add - SpaceShip 2 | To add - EVA 23 | Recommendations 4 Tool Updates

Fig. 2: Screenshot of Excel file showing tabs of Classification Tool

The first two tabs are introductory items for the user that include a project description and high level summary of findings. The Classification tab is explained in the next section. The tabs with To-add Spaceship2, and To-add EVA23 provide a summary of findings and references for these two main events that did not make it to the Significant Incidents tool. The last tab includes general recommendations for tool updates, and these will be described in a later section.

The Classification tab contains most of the information relevant to this analysis. The full list is shown in Appendix A: Requirements addressing significant incidents with design-induced and operational errors. It is divided into the following 6 parts.

1. **Incident Description:** Provides the mission name, date, type, and short description. This description varies from the one given in the Significant Incidents tool, as it pertains mainly to the human factors aspect of the incident.

2. **Human Errors (Classification):** This classification answers the following questions:
   - Did the Significant Incidents tool flag the incident as human error?
   - Should it have been flagged as such or does it need to be changed?
   - Were the human errors at operational level design-induced or operational errors?
   - Were the identified human errors at operational level the primary cause or contributing factors to the incident or close call?

3. **Human Factors Design:** For those incidents where human factors design was the primary cause or a contributing factor, poor human factors design decisions that led either to an error-prone system or did not facilitate crew making the right choices were identified.

4. **HSI Discipline Responsible:** Each incident is assigned to at least one NASA HSI discipline. Given that HSI operates as part of the Systems Engineering System of Systems, each incident corresponds to at least one domain [4]. HSI domains are added as the responsible groups that need to ensure current and future missions are addressing the incident's issue. These groups may not necessarily be involved in the design itself, but are responsible for asking the right questions during their participation in preliminary design reviews, critical design reviews, test readiness reviews, or other systems engineering reviews throughout the lifecycle of a mission, so as to prevent them from becoming incidents or close calls again.

5. **Recommendations:** This section includes recommended updates for the interactive tool for a particular incident, and recommended actions that could have been done during the design, operational, or training phases to prevent the incident from occurring.

6. **Review of Documents:** Requirements in four main documents were reviewed as a way to ensure we in fact have learned our lesson, and appropriate requirements addressing these incidents in human spaceflight were incorporated [6,7,8,9]. Those include:
   - NASA-STD 3001 Volume 2
   - NASA SP-2010-3407 Handbook
   - MPCV 70024 HSIR
   - CCT-REQ-1130

   These documents were chosen as they cover current crew modules in development. This section of the tool also includes a 'recommendations for documents' column in case some of those requirements need to be clarified or added.

II.III. Human Factors Classification of Significant Incidents

The developed Microsoft Excel file shows the Human Factors Classification of Significant Incidents and Close Calls in Human Spaceflight. The tool shows the six parts that were described in the previous section. Here we will describe insights to the classification with the use of a few examples.

The first assessment made was for those events that were classified as 'human error' in the Significant Incidents tool. As mentioned earlier, the graphic and tool were prepared by the Safety and Mission Assurance group with no participation of the Habitability and Human Factors group, which is the group that mainly deals with the minimization of human error for crew tasks. This analysis was an attempt to fill that gap. The intent was to verify that these events were actually human error at the operational level.

During the analysis we realized that perhaps the term 'human error' was not appropriate for these classifications. There were a couple of instances that were classified as human error, yet these were design-induced errors. One was for Soyuz TM-25 that dealt with landing rockets being fired at heat shield separation instead of at landing. During the conceptual phase, this design should have accounted for possible environmental conditions, such as high humidity levels in the atmosphere that may affect the connectors. In other cases, the events were not flagged as human error but should have been, so a change is recommended for those cases. For example, Apollo-Soyuz Test Project (ASTP) caused a crew injury that happened with the Earth Landing System auto/manual when switching back to auto. In this case, the displays did not have a visual cue for the pilot to realize that he was still operating in manual mode. This was a poor human factors design decision that did not facilitate the crewmember to make the right choice.

Therefore, the recommendation for the interactive tool is to change this classification to “design-induced error” (pertaining to direct interfaces of human and equipment), and “operational error” (pertaining to human error as opposed to hardware or software operational malfunction).

Once this classification was done, NASA HSI domains related to the incident were added. Those included Human Factors Engineering, Training, Maintainability and Supportability, Habitability and Environment, Operations Resources, and Safety. For example, the Mir Progress M-24 collision occurred during the second docking attempt. The primary cause was human factors design, as there was a failure of control equipment in the software design. The domains involved are Human Factors Engineering (usability evaluations of the software could have been helpful), Systems Safety (quality assurance to minimize risk personnel was needed), and Training (more ground simulations could have helped).

In many of the incidents, there were several factors acting either as causes to the incident or as a consequence of the first incident; in both cases they contributed to the failure. Those are documented in the column of “other causes synergistic in causing the failure”. Main observations from this part of the tool are summarized in the next two points:

- Many synergistic causes are process related
  - We tend to overestimate the ability of processes to catch problems.
  - The speed of a human’s thought process is overestimated (one crewmember may take more time to think about a way to proceed).
  - We need to understand flaws in the process and how they propagate.
  - Make changes to the process as needed.

- Training
  - It is hard to assess the best way to train; we need to have specific metrics to verify that something was learned.
  - For any training there is a list of tasks and some requirements; if you can show you did the task, it is complete. What if the person did not go through that one event during the on the job training (OJT) time to show that he/she is capable of handling it; how is that measured?
  - In spaceflight, OJT is hard to assess, as we cannot account for every possible scenario. Human judgment leads one to follow procedures except when it is unsafe.

II.IV. Recommendations for Significant Incidents and Preventive Measures

The Human Factors Classification of Significant Incidents tool contains a recommendations section, which includes updates for the Significant Incidents tool that are specific to each incident; and preventive measures during design, training, and operational phases to avoid the incident. For example, Soyuz TM-5 close call was acknowledged to be a combination of incorrect actions of the crew commander and mission control personnel. Since this was related to training, the recommendation for preventive measures was to provide appropriate training to crewmembers, and to perform more ground simulations of possible burns. The recommendation for the tool itself was to add a reference that includes this close call report, add a specific root cause and how the event was addressed in later flights.

The SpaceShipTwo (SS2) loss of crew incident had minimum information, which may be due to it being a recent event during the last update of the Significant Incidents tool. The recommendations include several sources that detailed the findings from the investigation report. In addition, a separate tab was created in the Excel file called “To add – SpaceShip2”, which has a summary of the findings of the SS2 accident based on the above sources. These can be found in Appendix B. Recommended preventive measures include:

a) During the requirements development, it is necessary to include the participation and authority of a human factors expert in the lifecycle of the mission.
b) During the design phase, use a HSI approach and do not use the operator as a single-point failure or the responsible party for fixing a known possible design issue.
c) During the operational phase, use the buddy system, also known as error trapping, for executing steps. This should even be part of the procedures.

Summarizing the findings from other incidents and close calls, the following mission lifecycle recommendations are provided:

1) Automation can be a big aid to managing human errors during flight missions. Designers of advanced tools will need to ensure whether they are going for effectiveness or efficiency in the tasks they want to see accomplished by the operator. Given that automatic tools can help minimize errors, it can also prompt the user to get distracted with other activities. A human-centric design for spaceflight needs to provide functionality to astronauts while addressing their individual needs [10].

2) Many human errors are found in the manufacturing operations phase because proactive steps are not considered during the design phase. Workload must be better planned and distributed, leaving sufficient time for manufacturing operations to reduce work pressures, stress, and fatigue. If there are organizational changes, management needs to clearly explain the changes in the organization structure, people's new roles, procedures, and all which could affect normal manufacturing operations [11].

3) Crew Resource Management (CRM) is the effective use of all available resources: human resources (people), hardware (technology), and information (process) (FAA AC120-51E, 2004) [12]. As observed in the analysis, the most frequent causes for human error at the operational level included fatigue, complacency, lack of attention, unclear directions, and organizational restructure [13]. Most CRM techniques are successfully being used in the aviation industry. They include organizational factors, decision making, leadership, communication, teamwork, workload planning and distribution, and training. CRM provides a set of skills that can be applied for better error detection and efficient error management [14]. Although human spaceflight applies some of these concepts, it would help to follow the structure these techniques provide. HSI covers these concepts through the NASA domains.

4) Increase participation of the manufacturing group in early stages with derivation of requirements, design reviews, drawings, and test plans to identify and address risk for error proactively.

5) Early testing at the element or subsystem levels to minimize risk for errors during assembly and test of the entire system.

6) Decomposition of requirements into many specifications can create more confusion if not written clearly.

7) Even when the same drawings or procedures of a legacy/heritage program are used, there is no guarantee the same results will be obtained for follow-on missions. Materials, technology, equipment, techniques, and people constantly change [15].

8) For the medical incidents, as we go into deep space, despite all countermeasures, we can provide the aid of an on-site medical doctor with experience on major surgeries that would be beneficial for the survival of the crew [16].

9) Leadership skills are important to help with quick and smooth adaptation to the new environment, and to ensure a successful mission. The selected crew must have demonstrated leadership skills to be able to embrace change, make decisions, motivate the rest of the crew, be open to different ideas, and be fair. Leadership mainly helps with the psychological health of the crew living together for an extended period of time and promotes healthy work and life/survival performance [16].

10) The designer's role in view of the full system life-cycle now also includes that of an observer and analyst of actual working practices of human operators, adding to efforts by researchers in anthropology, ethnography and human-computer interaction. "The aim is to understand both user requirements and organizational pre-requisites for design and operations, in order to intervene in systems in the middle of their life cycle or feed into requirements generation and development of future systems" [17].

II.V. General Recommendations for Significant Incidents Tool

The Significant Incidents Tool provides a great platform to find information about loss of crew, crew injury, loss of vehicle or mission, and related or recurring events in the history of human spaceflight. It is understood that this is a continuous work in progress tool, and we would like to contribute with some recommended updates to the tool.

1) Although this study excluded EVA significant incidents because of its maintenance in a separate tool, it was noted that the list of incidents listed in that chart is missing the information from a recent close call during EVA 23, with EVA 35 as a related event. A separate tab called “To add – EVA 23” was added providing a summary of the findings for EVA 23 that can be used in the Significant Incidents tool, along with references. Refer to Appendix C for a description and summary of findings of this dangerous EVA incident.

2) Add legend for incidents that do not have colored boxes, like close calls.

3) Move boxes of sources away from the bottom of the page (in presentation mode at the bottom left, these sources boxes interfere with presentation buttons to move forward and back, which do not allow one to click on them).

4) Classification of "system" could be a little bit misleading, as we want to get people to acknowledge that "humans" are part of the system. It is understood that in Human Spaceflight we typically call the technical groups “systems”; so if that is too big of an organizational/cultural change, it is ok to keep "systems" as a separate category. But maybe perhaps "technical systems"?

5) Consider changing "Human Error" classification to something else; anything done whether on the systems or by the operator can be attributed to human errors (e.g. humans also develop SW). Perhaps a good classification method instead of human error and systems would be "design-induced errors" and "operational errors".

6) Consider adding a category for "organizational factors" to include decisions made at the top level that created a series of errors in the system (human, software, and hardware).

7) Change "Lessons Learned" tab to "Lessons Learned Summary" and move it to the right side, as it is not a classification.

8) Recommend dividing classifications in Main Page into three sections, as follows:

Classification 1 – Incidents

Keep classification for:
○ Loss of Crew
○ Crew Injuries
○ Related or Recurring Events

Add:
○ Close Calls

Classification 2 – Various

Make another box or section (maybe by color) of second classification:
○ Space Vehicles
○ Country (not sure you need this but ok)
○ Systems (see recommendation 4, maybe rename to "technical system")

Classification 3 - Human Factors

Make another classification just for Human Factors Errors, or better yet for HSI. Also, distinguish from other classifications by color of box. Suggested Classification:
○ Human Factors Design-Induced Errors
○ Operational Errors/Factors
○ Design Errors/Factors
○ Organizational Errors/Factors

9) Add keywords to each incident so it is easily searchable and related to other events.

10) Add corresponding classification to each incident slide.

11) Create another category for unmanned vehicles (e.g. Progress).

12) Add number of crewmembers in each incident slide.

13) For incidents/failures during same mission, add a link in slides to jump to those events (e.g. Soyuz 1 during orbit, Soyuz 1 during re-entry).

14) Separate "related events" from "recurring events". Related events do not necessarily have to be highlighted. If the intention is to show that same thing happened (in other words we did not learn our lesson) perhaps another category will need to be added.

15) For each incident, it would be good to divide description in 3 parts:
Part 1: Brief description of incident
Part 2: Reason/causes/consequences
Part 3: Solutions (methods in place resulting from incident investigations, if any)

III. GOVERNING DOCUMENTS REVIEW

Governing documents refer to specifications, standards, and all requirement documents mainly at the parent level that parts and subassemblies would be designed under. Before getting into their review, it is important to learn some history for governing documents that have been used with respect to human systems. The Shuttle and ISS programs used the NASA-STD-3000 Man Systems Integration Standards (1985). This evolved into the currently used NASA-STD-3001 Space Flight Human Systems Standards, which has two volumes. Volume 1 focuses on Crew Health, and Volume 2 focuses on Human Factors, Habitability & Environmental Health [6,18]. This governing document is supported by the NASA/SP-2010-3407 Human Integration Design Handbook, which details different HSI requirements developed from lessons learned in past human spaceflight missions. The process is required by NPR 8705.2B Human-Rating Requirements for Space Systems, and NPR 7120.11 Health & Medical Technical Authority Implementation [7,19].

New human spaceflight programs use NASA-STD-3001 to make a program-specific set of requirements. For example, ISS created the SSP 50005 ISSP Flight Crew Integration Requirements; and Constellation developed the CxP 70024 Human Systems Integration Requirements. After the cancellation of Constellation, the latter document was updated with a new version that corresponded to the Multi-Purpose Crew Vehicle (MPCV) program [20].

Orion has addressed human errors in the MPCV 70024 Human Systems Integration Requirements (HSIR) [8]. The HSIR contains topics such as anthropometry, biomechanics, and strength; natural and induced environments; architecture, crew functions and interfaces; flight and ground maintenance; and extravehicular activity (EVA). Human systems requirements that assess the design against measurable objective human performance ratings to prevent the occurrence of errors are included in HS7066 Crew Interface Usability, HS7080 Crew Cognitive Workload, and HS7003 Handling Qualities.

The current Commercial Crew Program (CCP) has developed a Commercial Human Systems Integration Processes (CHSIP) document, which traces down to a reference document called Human Systems Integration Processes (HSIP). Some of those processes include human error analysis, design for human physical characteristics, capabilities, and population variation, crew survivability, net habitable volume, and other requirements.

One of the most important requirements applicable to our human error analysis is documented in HS7066 and CTS335. In order to verify that the spacecraft will not be susceptible to human error, crew interfaces have to be certified to “a maximum of 5% erroneous task steps per participant, where each erroneous task step is committed by 10% or fewer participants” [21,22].

III.I. Have we learned our lesson?

This part of the review closes the circle of the significant incidents analysis from a HSI perspective. Knowing what the incident was, what the primary cause or contributing factor was, and what could have been done to prevent the incident, we can verify if we actually learned our lesson and are taking the necessary steps to minimize human error at the operational level. Using the classification and analysis described in Section 4, several governing documents were reviewed to ensure that they incorporate requirements that protect against these incidents from occurring in the future.

This was done for those incidents that were classified as design-induced error and operational human error, 23 out of 113.

Appendix A shows the specific requirements that address a particular incident or close call. In some cases, there is more than one requirement that addresses other parts of the incident causes, and those found are stated in each cell. The last column, "Recommendations for Documents," detail recommendations to either clarify or add to those requirements listed in the governing documents. It was found that all of them have at least one requirement that address an incident. However, as mentioned earlier, some incidents occurred due to several factors, and once they happened, other issues arose that also became issues. Alternate solutions should be implemented in current designs for all of these cases. After consulting with NASA subject matter experts, we found that some of those requirements are documented in parent requirement documents, or even lower level documents. There is also a NASA Lessons Learned Database for Human Spaceflight, where the incidents in these analyses could be found. However, this site is currently under construction and a massive reorganization is currently in the works. Hence, we have not used this database other than to check the incidents are also listed there. Another source to check as future work is the NASA Human Factors Analysis and Classification System (HFACS), which is led by an Agency's Mishap Program Working Group.

Let us take the STS-3 close call as an example -- the pilot induced oscillation during de-rotation, where stronger than predicted winds contributed to the issue. The primary cause was human factors design -- the transition between autoland and manual was not fully evaluated in the control design. This was related to the Human Factors Engineering, Training, and Operations Resources NASA HSI domains. The requirements found in the documents are as follows:

- NASA-STD-3001 Volume 2:
  10.6.1.5 Automation Levels (V210104), addresses minimal automation of manual control [6].

- SP-2010-3407 Handbook:
  10.10.2.4 Levels of Automation, addresses the necessity of manual control [7].

- MPCV 70024 HSIR:
  HS7004 Manual Control, and HS7063C Protection for Flight Actuated Critical Controls.
  HS7004 addresses manual control but does not specify that it is required when automation is used, as in the other documents [8].

- CCT-REQ-1130:
  Both 3.2.6.1 and 4.3.2.6.1 Manually Override Software, address manual override capability for automation systems [9].

These requirements are the most proximate to address the STS-3 incident, but there may be other requirements specified in top level documents. For instance, NPR 8705.2B has a requirement related to transition between autoland and manual, and feedback status of automation and inhibits. Some other requirements may be verified at lower level documents; for example, the HS7063C is called out and will be verified by analysis and demonstration in the 72242 Orion Display Format Standards [23]. This may be the case for other incidents as well.

IV. FINAL REMARKS

Overall, from this analysis we conclude that most of the issues encountered in the significant incidents and close calls in human spaceflight are being covered by requirements in the governing documents. NASA is doing its best to mitigate and minimize human error. It would be useful to specify certain requirements addressing these significant incidents, and those are noted in the recommendations sections. Discussions with the standards team within the Habitability and Human Factors Branch, the division, and among other organizations at the Johnson Space Center would be beneficial to ensure the lessons are covered somewhere in the process/procedures and there is a responsible group verifying those are addressed. Addressing these possible risks earlier in the mission life cycle process, during requirements development, design, and manufacturing/testing phases, would contribute to having better error management and its minimization at the operational level.

ACKNOWLEDGMENTS

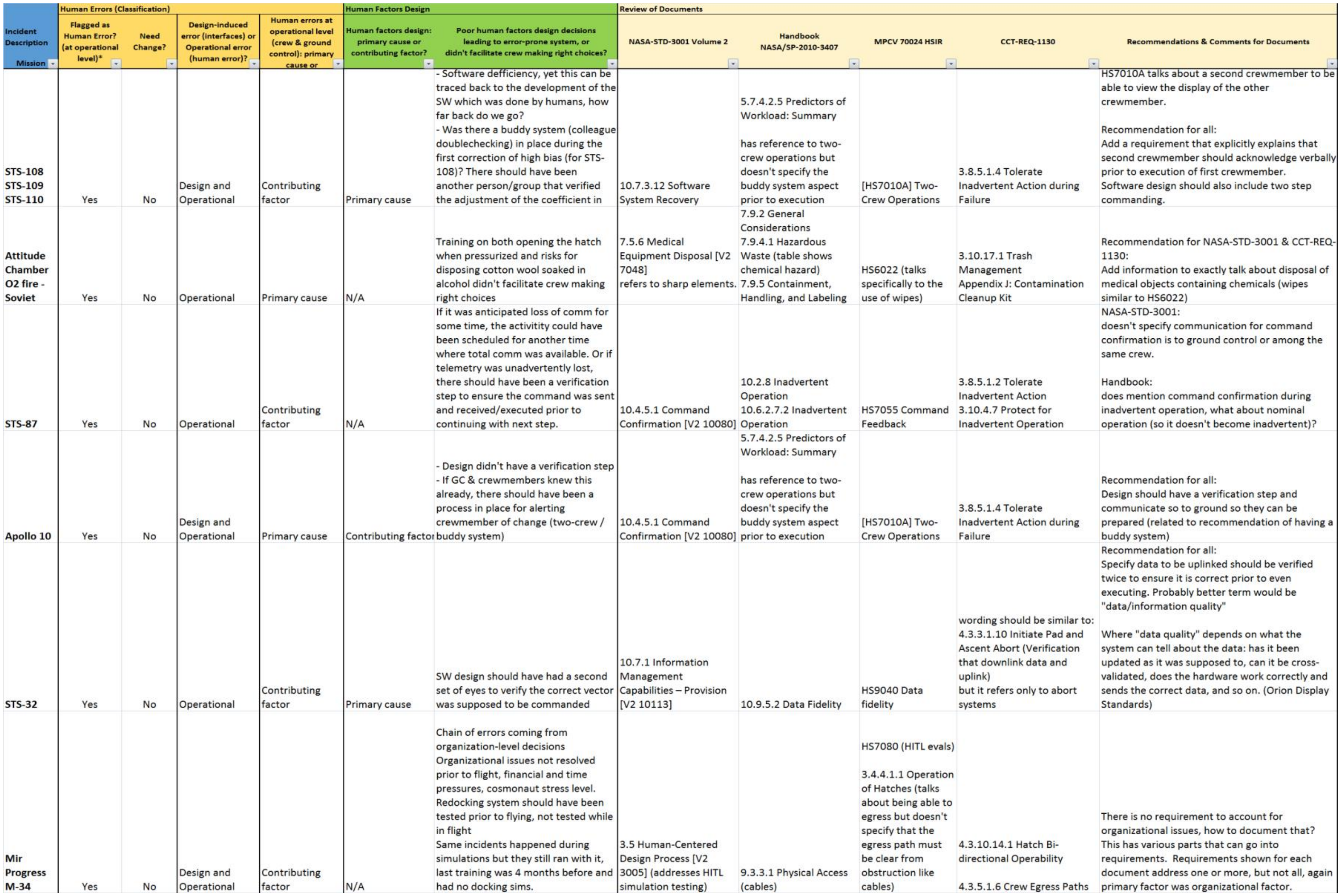
The authors would like to thank the Habitability and Human Factors Branch of the Human Health and Performance Directorate at NASA Johnson Space Center for providing the expertise to perform this research. The authors would also like to thank Dr. Nigel Packham and the Safety and Mission Assurance Directorate at NASA Johnson Space Center for the development of this important tool that helps by reducing close calls and significant incidents in human spaceflight, and which served as the platform for this study.

REFERENCES

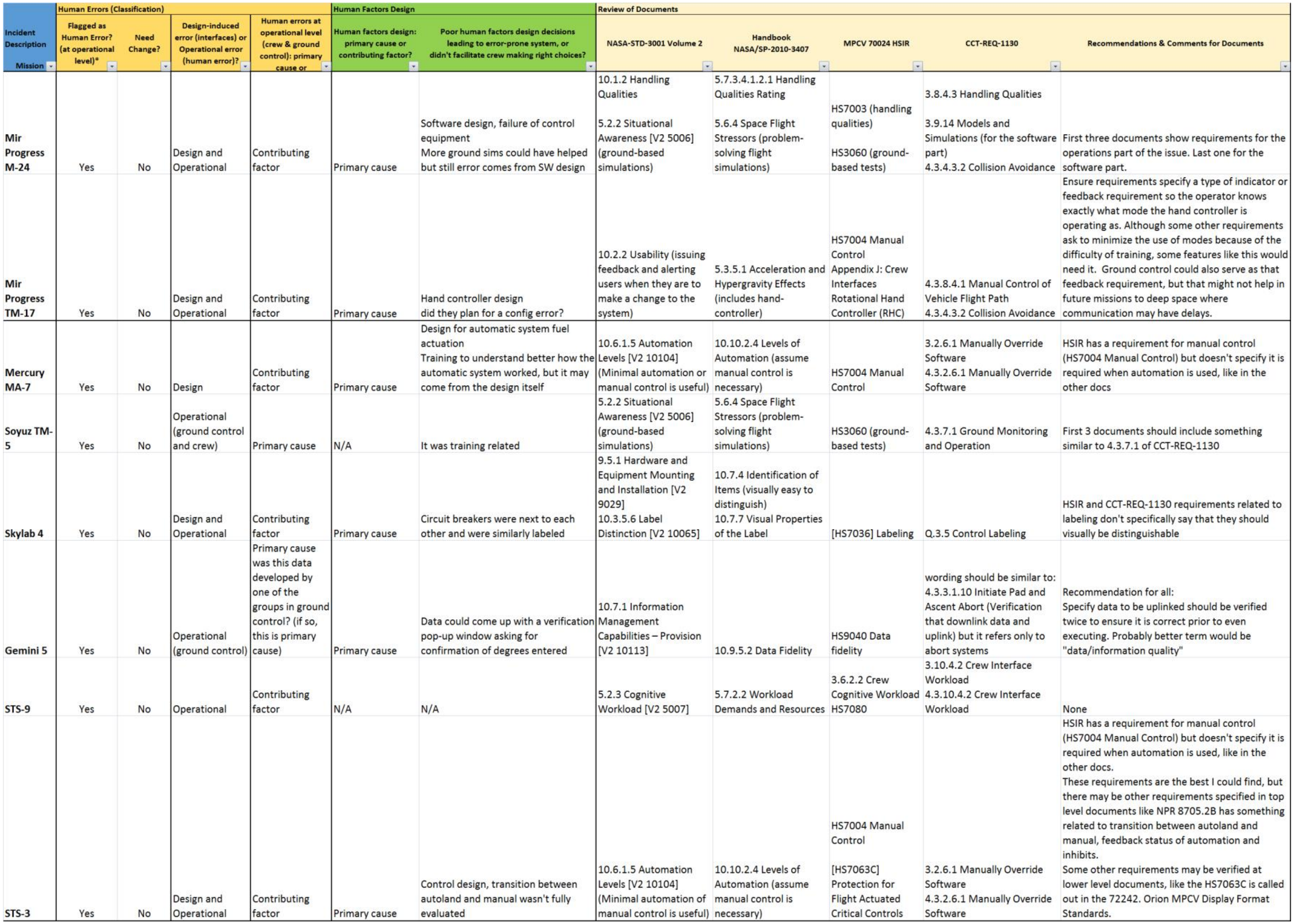
1. NASA (2015). Significant Incidents in Human Spaceflight. Johnson Space Center Safety and Mission Assurance Flight Safety Office. Retrieved from: http://spaceflight.nasa.gov/outreach/Significant_Incidents_Zcard2015.pdf [Accessed July 2016].
2. NASA (2017). Significant Incidents and Close Calls in Human Spaceflight Interactive Edition. Johnson Space Center Safety and Mission Assurance Flight Safety Office. Retrieved from: https://spaceflight.nasa.gov/outreach/SignificantIncidents/index.html [Accessed February 2017].
3. NASA (2015). NASA/SP-2015-3709 Human Systems Integration (HSI) Practitioner's Guide, NASA Johnson Space Center, November 2015.
4. Silva-Martinez, J. (2016**).** Human Systems Integration: Process to Help Minimize Human Errors, a Systems Engineering Perspective for Human Space Exploration Missions**,** Journal REACH - Reviews in Human Space Exploration. Volume 2, Issues 2–4, Pages 8-23, December 2016, Published by Elsevier.
5. NASA (2017). Significant Incidents and Close Calls during EVA Operations Interactive Edition. Johnson Space Center Safety and Mission Assurance Flight Safety Office. Retrieved from: https://spaceflight.nasa.gov/outreach/SignificantIncidentsEVA/index.html [Accessed March 2017].
6. NASA (2015). NASA-STD-3001, NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health, 12 February 2015.
7. NASA (2014). SP-2010-3407 Rev1 Human Integration Design Handbook. 5 June 2014.
8. NASA (2015). MPCV 70024 Orion Multi-Purpose Crew Vehicle Program: Human Systems Integration Requirements (HSIR), 4 March 2015.
9. NASA (2015). CCT-REQ-1130 ISS Crew Transportation Certification and Services Requirements Document, Revision D-1, 23 March 2015.
10. Silva-Martinez, J., Martinez, V. (2015). Using a Human-Centric Design Process for the Implementtion of Advanced Computer-Based Tools in Space Programs. 66th International Astronautical Congresss 2015. IAC-15,E5,1,6,X28356, Jerusalem, Israel.
11. Silva, J. (2012). Management's Role on the Application of Human Factors in the Aerospace Industry: Satellite Design and Manufacturing. ICES, San Diego, CA.
12. FAA AC120-51E (2004). Crew Resource Management Training Advisory Circular. US Department of Transportation.
13. Salas, E., Maurino, D. (2010). Human Factors in Aviation. Academic Press.
14. Silva-Martinez, J. (2015). Application of Crew Resource Management Techniques in the Aerospace Industry. IEEE Aerospace Conference 2015. 8.5 Human Factors & Performance.8.0504. Big Sky, MT.
15. Silva, J. (2013a). Incorporating Human Concepts in the Lifecycle of Aerospace Systems, INCOSE International Symposium, Philadelphia, PA.
16. Silva, J. (2013b). Crew Health for Space Vehicles in a Mars mission. Space 2013 Conference & Exposition. San Diego, CA.
17. Peldszus, R. Silva, J., Imhof, B. (2014). Contemporary Human Technology Interaction Issues in Space Architecture. 65th International Astronautical Congress 2014. IAC-14-E5.3.1.25092. Toronto, Canada.
18. NASA (2015). NASA-STD-3001, NASA Space Flight Human-System Standard Volume 1, Revision A: Crew Health. 12 February 2015.
19. NASA (2008). NPR 8705.2B Human Rating Requirements for Space Systems, 6 May 2008.
20. NASA (2012). CxP 70024 Constellation Program Human-System Integration Requirements, Revision E, 19 November 2010.

21. Holden, K., et al. (2013). Human Factors in Space Vehicle Design, Acta Astronautica, Volume 92, Issue 1, Pages 110-118.
22. NASA (2015). MPCV 72557 Orion Multi-Purpose Crew Vehicle Program Human Error Analysis, 29 April 2015.NASA (2010).
23. CxP 72242 Rev A Orion Display Format Standards, 8 September 2010.

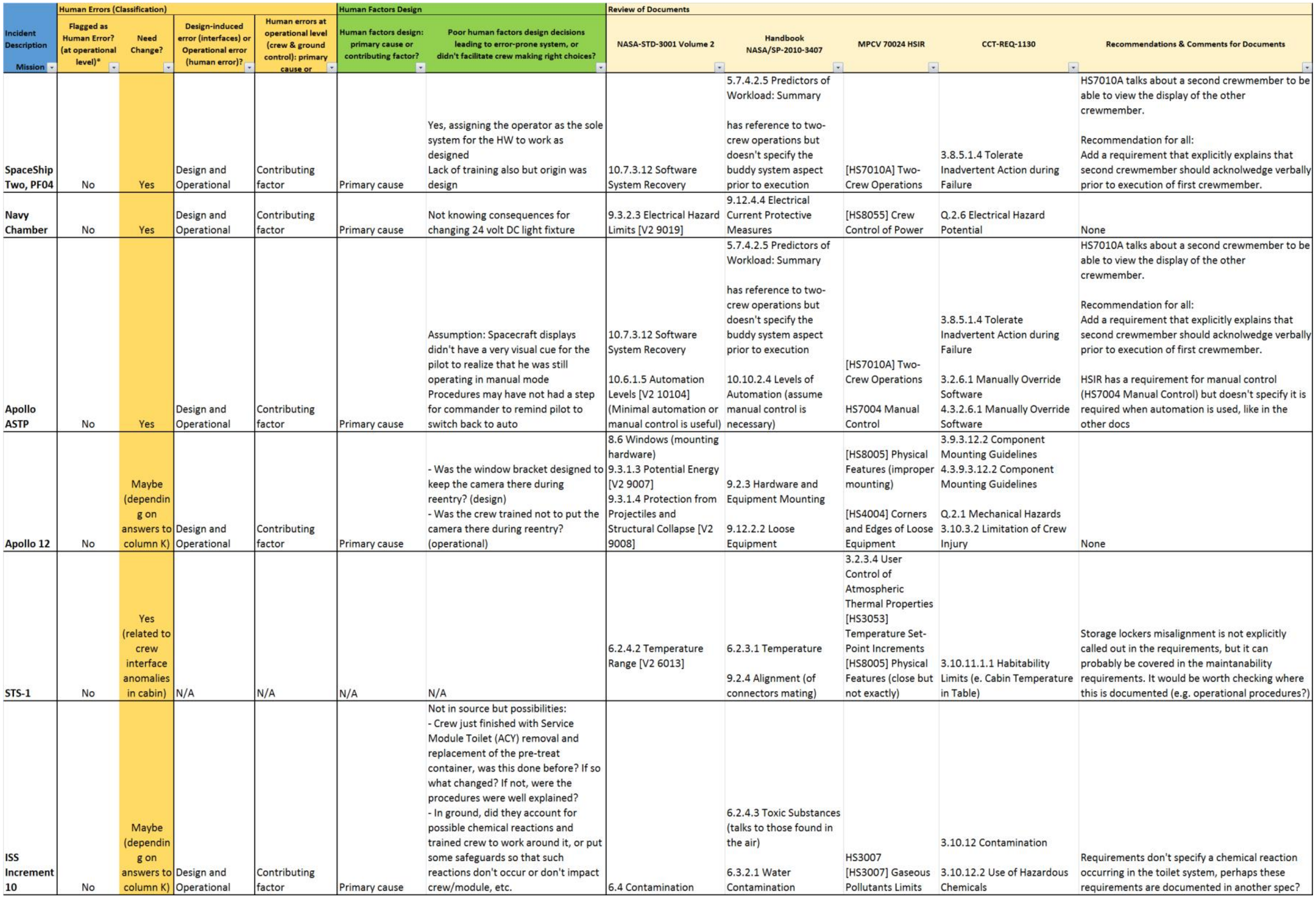
Appendix A: Requirements Addressing Significant Incidents with Design-induced and Operational Errors



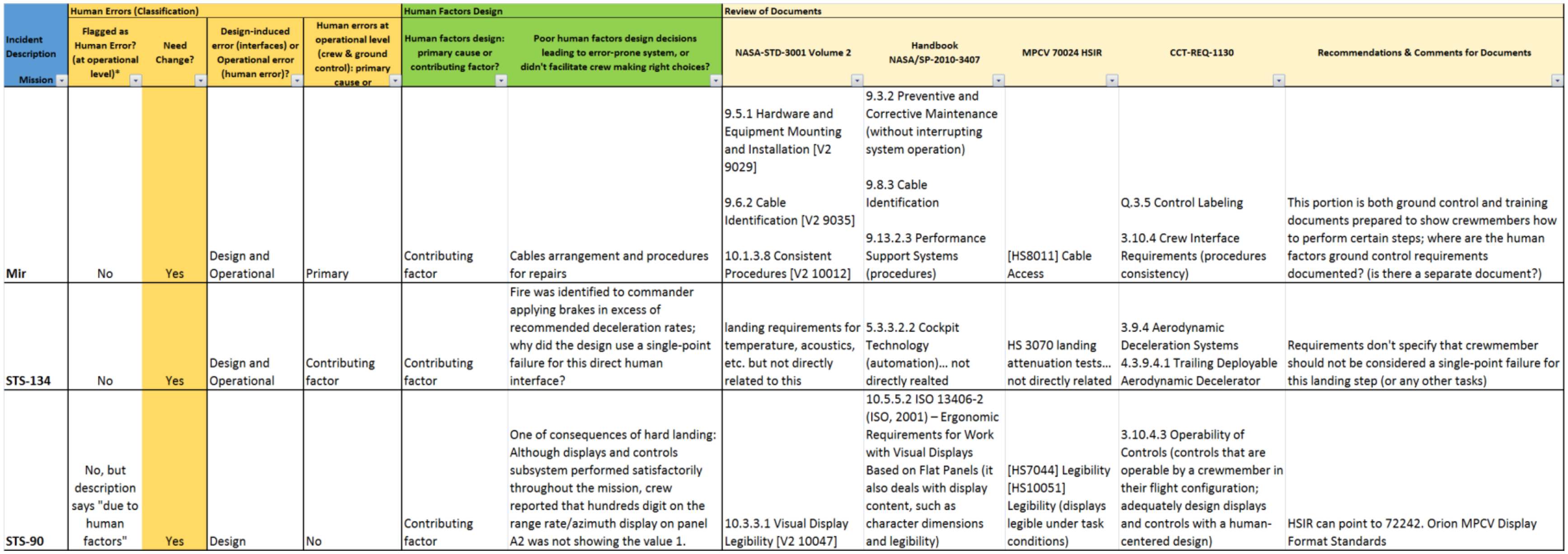
	Human Errors (Classification)				Human Factors Design		Review of Documents				
Incident Description Mission	Flagged as Human Error? (at operational level)*	Need Change?	Design-induced error (interfaces) or Operational error (human error)?	Human errors at operational level (crew & ground control): primary cause or	Human factors design: primary cause or contributing factor?	Poor human factors design decisions leading to error-prone system, or didn't facilitate crew making right choices?	NASA-STD-3001 Volume 2	Handbook NASA/SP-2010-3407	MPCV 70024 HSIR	CCT-REQ-1130	Recommendations & Comments for Documents
STS-108 STS-109 STS-110	Yes	No	Design and Operational	Contributing factor	Primary cause	- Software defficiency, yet this can be traced back to the development of the SW which was done by humans, how far back do we go? - Was there a buddy system (colleague doublechecking) in place during the first correction of high bias (for STS-108)? There should have been another person/group that verified the adjustment of the coefficient in	10.7.3.12 Software System Recovery	5.7.4.2.5 Predictors of Workload: Summary has reference to two-crew operations but doesn't specify the buddy system aspect prior to execution	[HS7010A] Two-Crew Operations	3.8.5.1.4 Tolerate Inadvertent Action during Failure	HS7010A talks about a second crewmember to be able to view the display of the other crewmember. Recommendation for all: Add a requirement that explicitly explains that second crewmember should acknowledge verbally prior to execution of first crewmember. Software design should also include two step commanding.
Attitude Chamber O2 fire - Soviet	Yes	No	Operational	Primary cause	N/A	Training on both opening the hatch when pressurized and risks for disposing cotton wool soaked in alcohol didn't facilitate crew making right choices	7.5.6 Medical Equipment Disposal [V2 7048] refers to sharp elements.	7.9.2 General Considerations 7.9.4.1 Hazardous Waste (table shows chemical hazard) 7.9.5 Containment, Handling, and Labeling	HS6022 (talks specifically to the use of wipes)	3.10.17.1 Trash Management Appendix J: Contamination Cleanup Kit	Recommendation for NASA-STD-3001 & CCT-REQ-1130: Add information to exactly talk about disposal of medical objects containing chemicals (wipes similar to HS6022)
STS-87	Yes	No	Operational	Contributing factor	N/A	If it was anticipated loss of comm for some time, the actitivity could have been scheduled for another time where total comm was available. Or if telemetry was unadvertently lost, there should have been a verification step to ensure the command was sent and received/executed prior to continuing with next step.	10.4.5.1 Command Confirmation [V2 10080]	10.2.8 Inadvertent Operation 10.6.2.7.2 Inadvertent Operation	HS7055 Command Feedback	3.8.5.1.2 Tolerate Inadvertent Action 3.10.4.7 Protect for Inadvertent Operation	NASA-STD-3001: doesn't specify communication for command confirmation is to ground control or among the same crew. Handbook: does mention command confirmation during inadvertent operation, what about nominal operation (so it doesn't become inadvertent)?
Apollo 10	Yes	No	Design and Operational	Primary cause	Contributing factor	- Design didn't have a verification step - If GC & crewmembers knew this already, there should have been a process in place for alerting crewmember of change (two-crew / buddy system)	10.4.5.1 Command Confirmation [V2 10080]	5.7.4.2.5 Predictors of Workload: Summary has reference to two-crew operations but doesn't specify the buddy system aspect prior to execution	[HS7010A] Two-Crew Operations	3.8.5.1.4 Tolerate Inadvertent Action during Failure	Recommendation for all: Design should have a verification step and communicate so to ground so they can be prepared (related to recommendation of having a buddy system)
STS-32	Yes	No	Operational	Contributing factor	Primary cause	SW design should have had a second set of eyes to verify the correct vector was supposed to be commanded	10.7.1 Information Management Capabilities – Provision [V2 10113]	10.9.5.2 Data Fidelity	HS9040 Data fidelity	wording should be similar to: 4.3.3.1.10 Initiate Pad and Ascent Abort (Verification that downlink data and uplink) but it refers only to abort systems	Recommendation for all: Specify data to be uplinked should be verified twice to ensure it is correct prior to even executing. Probably better term would be "data/information quality" Where "data quality" depends on what the system can tell about the data: has it been updated as it was supposed to, can it be cross-validated, does the hardware work correctly and sends the correct data, and so on. (Orion Display Standards)
Mir Progress M-34	Yes	No	Design and Operational	Contributing factor	N/A	Chain of errors coming from organization-level decisions Organizational issues not resolved prior to flight, financial and time pressures, cosmonaut stress level. Redocking system should have been tested prior to flying, not tested while in flight Same incidents happened during simulations but they still ran with it, last training was 4 months before and had no docking sims.	3.5 Human-Centered Design Process [V2 3005] (addresses HITL simulation testing)	9.3.3.1 Physical Access (cables)	HS7080 (HITL evals) 3.4.4.1.1 Operation of Hatches (talks about being able to egress but doesn't specify that the egress path must be clear from obstruction like cables)	4.3.10.14.1 Hatch Bi-directional Operability 4.3.5.1.6 Crew Egress Paths	There is no requirement to account for organizational issues, how to document that? This has various parts that can go into requirements. Requirements shown for each document address one or more, but not all, again primary factor was organizational factor.



	Human Errors (Classification)				Human Factors Design		Review of Documents				
Incident Description Mission	Flagged as Human Error? (at operational level)*	Need Change?	Design-induced error (interfaces) or Operational error (human error)?	Human errors at operational level (crew & ground control): primary cause or	Human factors design: primary cause or contributing factor?	Poor human factors design decisions leading to error-prone system, or didn't facilitate crew making right choices?	NASA-STD-3001 Volume 2	Handbook NASA/SP-2010-3407	MPCV 70024 HSIR	CCT-REQ-1130	Recommendations & Comments for Documents
Mir Progress M-24	Yes	No	Design and Operational	Contributing factor	Primary cause	Software design, failure of control equipment More ground sims could have helped but still error comes from SW design	10.1.2 Handling Qualities 5.2.2 Situational Awareness [V2 5006] (ground-based simulations)	5.7.3.4.1.2.1 Handling Qualities Rating 5.6.4 Space Flight Stressors (problem-solving flight simulations)	HS7003 (handling qualities) HS3060 (ground-based tests)	3.8.4.3 Handling Qualities 3.9.14 Models and Simulations (for the software part) 4.3.4.3.2 Collision Avoidance	First three documents show requirements for the operations part of the issue. Last one for the software part.
Mir Progress TM-17	Yes	No	Design and Operational	Contributing factor	Primary cause	Hand controller design did they plan for a config error?	10.2.2 Usability (issuing feedback and alerting users when they are to make a change to the system)	5.3.5.1 Acceleration and Hypergravity Effects (includes hand-controller)	HS7004 Manual Control Appendix J: Crew Interfaces Rotational Hand Controller (RHC)	4.3.8.4.1 Manual Control of Vehicle Flight Path 4.3.4.3.2 Collision Avoidance	Ensure requirements specify a type of indicator or feedback requirement so the operator knows exactly what mode the hand controller is operating as. Although some other requirements ask to minimize the use of modes because of the difficulty of training, some features like this would need it. Ground control could also serve as that feedback requirement, but that might not help in future missions to deep space where communication may have delays.
Mercury MA-7	Yes	No	Design	Contributing factor	Primary cause	Design for automatic system fuel actuation Training to understand better how the automatic system worked, but it may come from the design itself	10.6.1.5 Automation Levels [V2 10104] (Minimal automation or manual control is useful)	10.10.2.4 Levels of Automation (assume manual control is necessary)	HS7004 Manual Control	3.2.6.1 Manually Override Software 4.3.2.6.1 Manually Override Software	HSIR has a requirement for manual control (HS7004 Manual Control) but doesn't specify it is required when automation is used, like in the other docs
Soyuz TM-5	Yes	No	Operational (ground control and crew)	Primary cause	N/A	It was training related	5.2.2 Situational Awareness [V2 5006] (ground-based simulations)	5.6.4 Space Flight Stressors (problem-solving flight simulations)	HS3060 (ground-based tests)	4.3.7.1 Ground Monitoring and Operation	First 3 documents should include something similar to 4.3.7.1 of CCT-REQ-1130
Skylab 4	Yes	No	Design and Operational	Contributing factor	Primary cause	Circuit breakers were next to each other and were similarly labeled	9.5.1 Hardware and Equipment Mounting and Installation [V2 9029] 10.3.5.6 Label Distinction [V2 10065]	10.7.4 Identification of Items (visually easy to distinguish) 10.7.7 Visual Properties of the Label	[HS7036] Labeling	Q.3.5 Control Labeling	HSIR and CCT-REQ-1130 requirements related to labeling don't specifically say that they should visually be distinguishable
Gemini 5	Yes	No	Operational (ground control)	Primary cause was this data developed by one of the groups in ground control? (if so, this is primary cause)	Primary cause	Data could come up with a verification pop-up window asking for confirmation of degrees entered	10.7.1 Information Management Capabilities – Provision [V2 10113]	10.9.5.2 Data Fidelity	HS9040 Data fidelity	wording should be similar to: 4.3.3.1.10 Initiate Pad and Ascent Abort (Verification that downlink data and uplink) but it refers only to abort systems	Recommendation for all: Specify data to be uplinked should be verified twice to ensure it is correct prior to even executing. Probably better term would be "data/information quality"
STS-9	Yes	No	Operational	Contributing factor	N/A	N/A	5.2.3 Cognitive Workload [V2 5007]	5.7.2.2 Workload Demands and Resources	3.6.2.2 Crew Cognitive Workload HS7080	3.10.4.2 Crew Interface Workload 4.3.10.4.2 Crew Interface Workload	None
STS-3	Yes	No	Design and Operational	Contributing factor	Primary cause	Control design, transition between autoland and manual wasn't fully evaluated	10.6.1.5 Automation Levels [V2 10104] (Minimal automation of manual control is useful)	10.10.2.4 Levels of Automation (assume manual control is necessary)	HS7004 Manual Control [HS7063C] Protection for Flight Actuated Critical Controls	3.2.6.1 Manually Override Software 4.3.2.6.1 Manually Override Software	HSIR has a requirement for manual control (HS7004 Manual Control) but doesn't specify it is required when automation is used, like in the other docs. These requirements are the best I could find, but there may be other requirements specified in top level documents like NPR 8705.2B has something related to transition between autoland and manual, feedback status of automation and inhibits. Some other requirements may be verified at lower level documents, like the HS7063C is called out in the 72242. Orion MPCV Display Format Standards.



Incident Description Mission	Human Errors (Classification) Flagged as Human Error? (at operational level)*	Need Change?	Design-induced error (interfaces) or Operational error (human error)?	Human errors at operational level (crew & ground control): primary cause or	Human Factors Design Human factors design: primary cause or contributing factor?	Poor human factors design decisions leading to error-prone system, or didn't facilitate crew making right choices?	Review of Documents NASA-STD-3001 Volume 2	Handbook NASA/SP-2010-3407	MPCV 70024 HSIR	CCT-REQ-1130	Recommendations & Comments for Documents
SpaceShip Two, PF04	No	Yes	Design and Operational	Contributing factor	Primary cause	Yes, assigning the operator as the sole system for the HW to work as designed Lack of training also but origin was design	10.7.3.12 Software System Recovery	5.7.4.2.5 Predictors of Workload: Summary has reference to two-crew operations but doesn't specify the buddy system aspect prior to execution	[HS7010A] Two-Crew Operations	3.8.5.1.4 Tolerate Inadvertent Action during Failure	HS7010A talks about a second crewmember to be able to view the display of the other crewmember. Recommendation for all: Add a requirement that explicitly explains that second crewmember should acknolwedge verbally prior to execution of first crewmember.
Navy Chamber	No	Yes	Design and Operational	Contributing factor	Primary cause	Not knowing consequences for changing 24 volt DC light fixture	9.3.2.3 Electrical Hazard Limits [V2 9019]	9.12.4.4 Electrical Current Protective Measures	[HS8055] Crew Control of Power	Q.2.6 Electrical Hazard Potential	None
Apollo ASTP	No	Yes	Design and Operational	Contributing factor	Primary cause	Assumption: Spacecraft displays didn't have a very visual cue for the pilot to realize that he was still operating in manual mode Procedures may have not had a step for commander to remind pilot to switch back to auto	10.7.3.12 Software System Recovery 10.6.1.5 Automation Levels [V2 10104] (Minimal automation or manual control is useful)	5.7.4.2.5 Predictors of Workload: Summary has reference to two-crew operations but doesn't specify the buddy system aspect prior to execution 10.10.2.4 Levels of Automation (assume manual control is necessary)	[HS7010A] Two-Crew Operations HS7004 Manual Control	3.8.5.1.4 Tolerate Inadvertent Action during Failure 3.2.6.1 Manually Override Software 4.3.2.6.1 Manually Override Software	HS7010A talks about a second crewmember to be able to view the display of the other crewmember. Recommendation for all: Add a requirement that explicitly explains that second crewmember should acknolwedge verbally prior to execution of first crewmember. HSIR has a requirement for manual control (HS7004 Manual Control) but doesn't specify it is required when automation is used, like in the other docs
Apollo 12	No	Maybe (depending on answers to column K)	Design and Operational	Contributing factor	Primary cause	- Was the window bracket designed to keep the camera there during reentry? (design) - Was the crew trained not to put the camera there during reentry? (operational)	8.6 Windows (mounting hardware) 9.3.1.3 Potential Energy [V2 9007] 9.3.1.4 Protection from Projectiles and Structural Collapse [V2 9008]	9.2.3 Hardware and Equipment Mounting 9.12.2.2 Loose Equipment	[HS8005] Physical Features (improper mounting) [HS4004] Corners and Edges of Loose Equipment	3.9.3.12.2 Component Mounting Guidelines 4.3.9.3.12.2 Component Mounting Guidelines Q.2.1 Mechanical Hazards 3.10.3.2 Limitation of Crew Injury	None
STS-1	No	Yes (related to crew interface anomalies in cabin)	N/A	N/A	N/A	N/A	6.2.4.2 Temperature Range [V2 6013]	6.2.3.1 Temperature 9.2.4 Alignment (of connectors mating)	3.2.3.4 User Control of Atmospheric Thermal Properties [HS3053] Temperature Set-Point Increments [HS8005] Physical Features (close but not exactly)	3.10.11.1.1 Habitability Limits (e. Cabin Temperature in Table)	Storage lockers misalignment is not explicitly called out in the requirements, but it can probably be covered in the maintanability requirements. It would be worth checking where this is documented (e.g. operational procedures?)
ISS Increment 10	No	Maybe (depending on answers to column K)	Design and Operational	Contributing factor	Primary cause	Not in source but possibilities: - Crew just finished with Service Module Toilet (ACY) removal and replacement of the pre-treat container, was this done before? If so what changed? If not, were the procedures were well explained? - In ground, did they account for possible chemical reactions and trained crew to work around it, or put some safeguards so that such reactions don't occur or don't impact crew/module, etc.	6.4 Contamination	6.2.4.3 Toxic Substances (talks to those found in the air) 6.3.2.1 Water Contamination	HS3007 [HS3007] Gaseous Pollutants Limits	3.10.12 Contamination 3.10.12.2 Use of Hazardous Chemicals	Requirements don't specify a chemical reaction occurring in the toilet system, perhaps these requirements are documented in another spec?



Incident Description	Human Errors (Classification)				Human Factors Design		Review of Documents				
Mission	Flagged as Human Error? (at operational level)*	Need Change?	Design-induced error (interfaces) or Operational error (human error)?	Human errors at operational level (crew & ground control): primary cause or	Human factors design: primary cause or contributing factor?	Poor human factors design decisions leading to error-prone system, or didn't facilitate crew making right choices?	NASA-STD-3001 Volume 2	Handbook NASA/SP-2010-3407	MPCV 70024 HSIR	CCT-REQ-1130	Recommendations & Comments for Documents
Mir	No	Yes	Design and Operational	Primary	Contributing factor	Cables arrangement and procedures for repairs	9.5.1 Hardware and Equipment Mounting and Installation [V2 9029] 9.6.2 Cable Identification [V2 9035] 10.1.3.8 Consistent Procedures [V2 10012]	9.3.2 Preventive and Corrective Maintenance (without interrupting system operation) 9.8.3 Cable Identification 9.13.2.3 Performance Support Systems (procedures)	[HS8011] Cable Access	Q.3.5 Control Labeling 3.10.4 Crew Interface Requirements (procedures consistency)	This portion is both ground control and training documents prepared to show crewmembers how to perform certain steps; where are the human factors ground control requirements documented? (is there a separate document?)
STS-134	No	Yes	Design and Operational	Contributing factor	Contributing factor	Fire was identified to commander applying brakes in excess of recommended deceleration rates; why did the design use a single-point failure for this direct human interface?	landing requirements for temperature, acoustics, etc. but not directly related to this	5.3.3.2.2 Cockpit Technology (automation)… not directly realted	HS 3070 landing attenuation tests… not directly related	3.9.4 Aerodynamic Deceleration Systems 4.3.9.4.1 Trailing Deployable Aerodynamic Decelerator	Requirements don't specify that crewmember should not be considered a single-point failure for this landing step (or any other tasks)
STS-90	No, but description says "due to human factors"	Yes	Design	No	Contributing factor	One of consequences of hard landing: Although displays and controls subsystem performed satisfactorily throughout the mission, crew reported that hundreds digit on the range rate/azimuth display on panel A2 was not showing the value 1.	10.3.3.1 Visual Display Legibility [V2 10047]	10.5.5.2 ISO 13406-2 (ISO, 2001) – Ergonomic Requirements for Work with Visual Displays Based on Flat Panels (it also deals with display content, such as character dimensions and legibility)	[HS7044] Legibility [HS10051] Legibility (displays legible under task conditions)	3.10.4.3 Operability of Controls (controls that are operable by a crewmember in their flight configuration; adequately design displays and controls with a human-centered design)	HSIR can point to 72242. Orion MPCV Display Format Standards