A Method for analog space missions risk analysis

Antonio Del Mastro, Jean Marc Salotti, Giovanni Garofalo

A method for Analogue Space Missions Risk Analysis

Antonio Del Mastro[1], Jean Marc Salotti[2], Giovanni Garofalo[1,3]

1= Mars Planet, **info@marsplanet.org**
2 = Ensc (Ecole Nationale Supérieure de Cognitique, Institut Polytechnique de Bordeaux)
3= ACER-EU (Agency for the Cooperation of Energy Regulators)

Abstract

In this paper, we provide a general risk evaluation method for analogue simulation missions, in terms of the identification of potential hazards and risks which could affect the positive outcome of the mission. The risk analysis method considers the evaluation of the risks of each experiment foreseen in the mission and the evaluation of other general factors which could have an impact on the operation. The scope of this analysis is to ensure that all the operations included in the undertaking are analysed and well defined.

Special attention is paid to the assessment of the safety issues related to the execution of the experiments. The methodology includes elements of the *Fault Tree Analysis* (FTA) and the development of a specific risk-reduction strategy, appropriately scaled and simplified for the space simulation mission scope.

We also introduce the new *Risk Cube* concept, a useful tool that can be applied to other types of Space missions. It is characterized by a higher level of complexity. The added value of the Risk Cube concept is that it is possible to identify all the domains of occurrence of the risks, visualize the interconnection of the different risks and contribute to create a mental map whose aim is to identify all the possible factors and requirements that could have some influence on the outcome of the risk analysis.

Keywords: analogue space simulation, risk analysis, PRA, HRA, FTA, situation awareness

1. Introduction

1.1. Analogue space simulations

Analogue space simulation missions play an important role in the testing of space technology on Earth. Generally, they are carried out whenever it is too expensive to perform an experiment or it is mandatory to validate a cutting-edge technology in Space. Furthermore, analogue simulations missions represent an excellent experience to involve young researchers and people at the beginning of their careers in rewarding challenges and to provide companies with the opportunity to test their products in a space simulated environment. The aspects covered by analogue simulations also consider the simulation of narrow/confined living habitats for the crew, etc. Numerous analogue space simulations have already been carried out in different places on Earth:

1. Hawaii (i.e., HI-SEAS).
2. Utah, USA (i.e., Mars Desert Research Station – MDRS).
3. Israel (i.e., AMADEE Mission experiments).
4. Etc. [6]

All of the above-mentioned sites are desertic and share the characteristics of having a rugged or cratered terrain similar to the Moon or Mars, and remote environments that experience extreme temperatures. Thanks to these realistic features, it is possible to define new requirements and simulate day-to-day operations. In fact, feedback from the testing allows engineers and scientists to develop an improved version of the technology reducing the risk and cost of future space missions [1].

1.1. State-of-the-art: Risk issues connected to scientific activities

The following section analyzes the safety state-of-the-art with regard to the safety standard procedures that can be applied to engineering systems or scientific activities in a hostile or risky environment. The discipline (i.e., System Safety Engineering) employs specialized knowledge in applying scientific and engineering principles, criteria, and techniques to identify hazards and then to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated.

Many institutes and departments have been involved extensively in this type of activity over the years, resulting in the development of multiple standards [2,7,11]. The current approach aims to eliminate hazards when possible, and to minimize risks where those hazards cannot be eliminated.

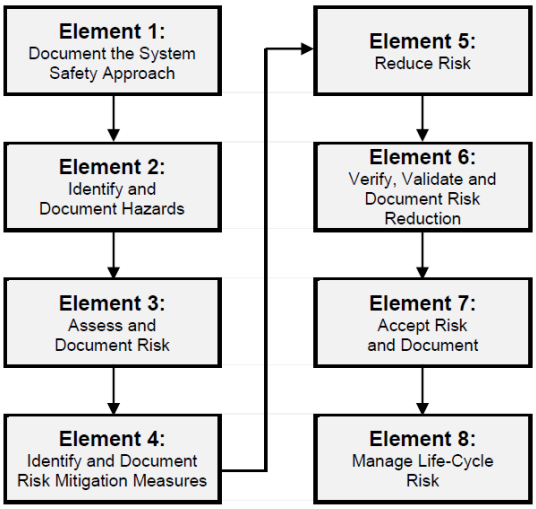


Figure 1 Eight elements of the system safety process. *[2]*

With regard to Figure 1, it is possible to follow the guidelines to achieve an acceptable risk level to reach and its logic sequence. The safety process is required to consists of eight elements, generally. As a requirement, The Program Manager and contractor shall document the system safety approach for managing hazards as an integral part of the process. The minimum requirements for the approach include:

1. Describing the risk management effort and how the program is integrating risk management into the process.
2. Identifying and documenting the prescribed and derived requirements applicable to the system.
3. Defining how hazards and associated risks are formally accepted by the appropriate risk acceptance authority.
4. Documenting hazards with high technology tracking systems.

Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment. The hazard identification process shall consider the entire system life-cycle and potential impacts to personnel, infrastructure, defense systems, the public, and the environment.

Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether. If that is not possible, at least the following passages should be taken into consideration:

1. Reduce risk through design alteration.
2. Incorporate engineered features or safety/warning devices.
3. Incorporate procedures, training, etc.

Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, demonstration, or inspection.

Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority. The user representative shall be part of this process throughout the life-cycle of the system and shall provide formal concurrence before all high risk acceptance decisions.

After having acquired data from reports and experience with similar systems, new hazards may be present or the risk for a known hazard is higher or lower than previously recognized. A single system may require multiple event risk assessments and acceptances throughout its life-cycle. Each risk acceptance decision shall be documented and procedures should be followed accordingly to ensure the personnel is aware of it. If a new hazard is discovered or a known hazard is determined to have a higher risk level than previously assessed, the new or revised risk will need to be formally accepted. [2]

1.2. Risks issues in Moon or Mars analogue terrains and habitats

For low Earth orbit, astronauts follow a training program in specific simulators (e.g., ISS docking simulation [3]), in swimming pools (e.g., Hubble repair mission [4]). On the other hand, for the preparation of missions to the Moon or Mars, simulations have generally been carried out in hostile and prohibitive environments, such as the desert of Utah [5] and Morocco [6].

Whatever the environment, there exist risks linked to the use of complex tools and systems. In this context, failure may occur, resulting in the failure of the experiment (or worse, such as personal injury). It is important to perform an assessment of the risks before the implementation of the mission/experiment, to minimize the number of accidents and failures. Many methods exist for the assessment of risks [7], [8]. It is in generally required to perform a probabilistic risk analysis (PRA) [9]. In the space domain, as the environment becomes extremely dangerous, risk analysis is a critical and fundamental step of the preparatory phase [10].

The risk is seriously considered in the eventuality of a Mars analogue terrain. For example, the AMADEE-2018 experiments risks (managed by the Austrian Space Forum) have been assessed for all experiments and a dedicated team had to follow every step of the mission for the safety of the people involved in the simulations [13].

In this paper, most of these methods and techniques are addressed as a starting point for our risk analysis technique, connected to the risks issues that can happen in a simulated environment. The purpose is strictly related to the design, preparation, and the performing of the entire analog mission.

2. HRA & Risks classification

2.1 HRA standards

Here we introduce and report some concepts related to the Human Reliability Analysis (HRA) as defined by NASA standards [11]. HRA can be described as a methodology that can support space programs, in which humans operate complex systems. It is possible to evaluate how human actions can negatively impact existing/future systems through HRA, then predict how often these events would occur, and state the potential consequences. Generally, it is possible to identify the key elements of a system's reliability:

1. Hardware.
2. Software.
3. Human (e.g., Ground Crew, Mission Crew).

HRA is related to the last item, and can assist in the identification of human actions that pose significant threats to the mission, to evaluate and compare system upgrades or factors as anomalies and delays, and to assess different scenarios (e.g., accidents or incidents), leading to mission design changes.

As an integral part of a unifying process that considers hardware, software, and human reliability, it is necessary to introduce the PRA (i.e., *Probabilistic Risk Assessment*), which is generally supports performance improvement and costs reduction. It defines an IE (i.e., *Initiating Event*) that could lead to an undesired outcome (e.g., equipment damage), and it is followed by a pivotal event that could consist of a success or a failure.

In general, the HRA process consists of several distinct steps (i.e., problem definition, task analysis, etc.). It is suggested that it should be an integral part of PRA. In this context, pre-existing and post-initiating actions must be evaluated to define what errors are responsible for mishaps. Human error has been assessed to be an IE in 24% of NASA accidents [11]. After an HRA is completed, it is possible to reduce errors or mitigate their effects. Further quantification can be done to verify that the measures are effective in lowering the impact of error on the overall system reliability.

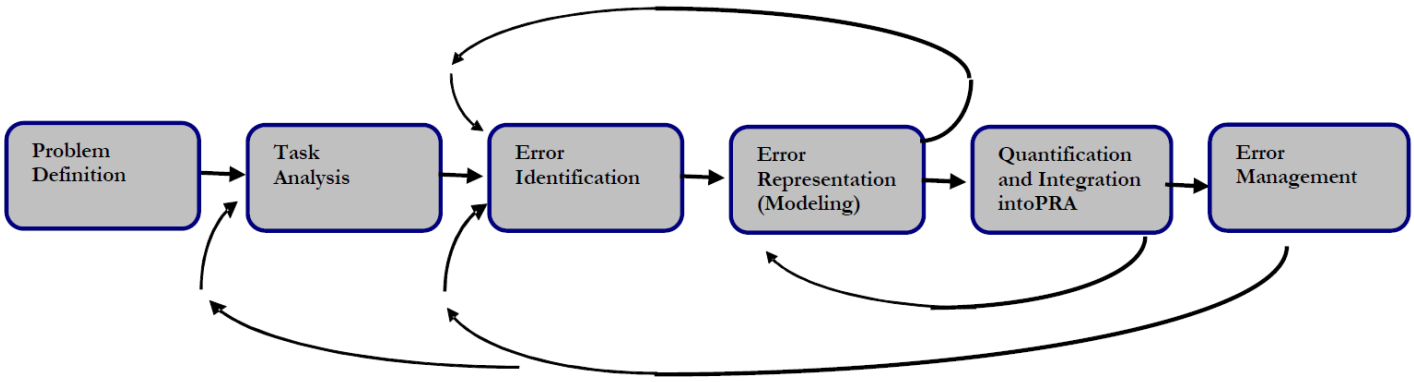


Figure 2 Basic HRA steps *[11]*.

Concerning Figure 1, it is compulsory to define the HRA phases briefly. The *Problem Definition* is the first step to determine what human actions must be evaluated. Two factors affects the analysis:

1. The system's vulnerability to human error, which is dependent upon the complexity of the system and on the amount of man-system interaction.
2. The purpose of the analysis, which can be qualitative or quantitative. Qualitative analyses are more indicated for general processes. Quantitative analyses are more indicated for the definition phase, in which specific human actions are assessed and evaluated.

An optimal system design must be error-tolerant and simple, to provide the capability for the human operator to detect and correct errors.

The second step is the *Task Analysis*, which aims to identify, break down and assess each task into sub-steps that describe the required human necessary activities to achieve the forecast goal. A thorough analysis ensures that the process

has been completely evaluated and all actions have been identified. If the task analysis is being performed to understand the human contribution to the risk at a system functional level, the task analysis should be kept at a higher level (i.e., "*Screening Analysis*"). To further understand a a significant risk, a more detailed analysis is requested.

The third step is the *Human Error Identification*, where human violations can occur, thus having potential contributions to hazardous events. Human actions within a system can be broken down into a cognitive response (i.e., failure to interpret the information correctly) or physical action. The system design (e.g., crew habitable environment) affects the probability that the human operator will perform a task correctly. Consequently, it is important to assess a PSF (i.e., *Performance Shaping Factor*), which is anything that can affect the ability of the person to carry out any task. External PSFs are outside the individual's control. Internal PSFs are human attributes that can be influenced by skills, fatigue, etc. Once PSFs are identified, their influence is determined so that the error rate can be adjusted. However, it would be impossible to list all the possible situations and errors that could happen in a mission, even if it is possible to investigate the most credible circumstances under which human error may occur. In the end, each type of log record (e.g., causal tree record) may turn out to be useful [11].

The fourth step is the *Human Error Representation*, which is conducted to visualize the data, relationships, and inferences that cannot be as easily described with words. Firstly, the system should be evaluated in its standard operating conditions. The analyst must also consider modelling dependencies between different types of human errors (e.g., The likelihood that one human error contributes to or causes another). Within complex systems, it is accepted that very few human errors (seen as IE) can serve as a critical failure function. For each initiating event, a corresponding event flowchart is developed, showing multiple scenarios. After that, it is possible to develop an *Event Tree*[1] in which are stored all the basic initiating events and the occurrence of pivotal events.

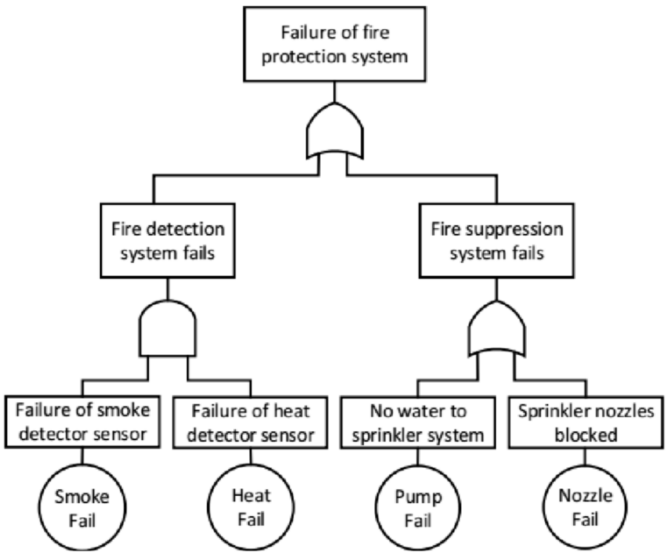


Figure 3 Fault Tree Analysis representation. *[12]*

The last two points of the HRA flowchart regard the *Quantification and Integration* and *Error Management.* The first one assignes probabilities to human errors to determine which ones are the most significant. The data must be sufficient to allow the analyst to estimate the frequency with which the errors may occur. The purpose of the screening is to limit the number of human actions to evaluate.

If the remaining potential human errors are still significant risk contributors to overall system reliability and safety, then the system should automatically detect and correct the error or provide the human with the capability to detect and correct it. If the error cannot be corrected, then the system should at least mitigate its negative effects.

The following table defines the classical HRA Method Selection Criteria and features that must be followed to perform a thorough analysis.

Criteria and Attributes	Description
Applicability to existing aerospace design	The HRA method must apply to existing aerospace designs.

[1] It relates to the FTA method. The *Fault Tree Analysis* is a top-down approach used to analyse, virtually display and evaluate failure paths in a system, thereby providing a mechanism for effective system level risk evaluation. Its fundamental concept relies on the easy logic visualization of an event. The logic segment provides a method for qualitative evaluation of an action or a methodology. [21]

Applicability to existing aerospace design (conceptual phase)	The HRA method must apply to aerospace system designs in the early conceptual design phase.
Human error probability (HEP) quantification	The HRA method must include procedures for error modelling and result in human error probability (HEP) quantification.
Screening capability	The method requires significant details to perform the analysis.
Model capacity updating	Update the model to provide a detailed analysis of human actions.
Guidance on task decomposition	It must be possible to break down human activities into different subtasks. It requires guidelines.
Flexible PSF list	It is compulsory to specify a set of PSFs based on the tasks.
Coverage of error sources	Provide a broad estimation of errors (e.g., omission, failure to respond in time, failure to complete a task).
Procedures for error identification, modelling, and quantification	Users are not HRA experts, the procedure should be straightforward.
Address errors omission and commission	HRA is essential for both nominal and emergency operations.
Guidance on the treatment of error recovery	The method should include explicit treatment of error recovery.
Explicit treatment of task/error dependencies	Identify and address task dependency and recovery within HEP estimates.
Uncertainty bound estimation	Provide instructions to assess HEP uncertainty bounds.
Validation	The risk-related human tasks are to be modelled inside the PRA model. In current practice, error identification is typically performed when developing the PRA models.
Reliability and reproducibility	The error analysis, identification, and error probabilities in the HRA method should have good reliability and reproducibility.
Low sensitivity	The HRA method mustn't yield large changes in the HEP calculated when only small changes were made in the PSFs.
Multiple data source	The HRA method should adapt to data from a wide variety of sources, including simulators, and human performance studies. minor changes should not have a large effect on the error probability computed.
Broad-based experience	This indicates the degree to which the method can be applied to different space mission areas.
Usable by a non-HRA expert user	In HRA, there are three levels of HRA-related knowledge people: 1. HRA Specialist: Many years of experience. 2. HRA Analyst: About one year of experience in HRA practice. 3. PRA Analyst: Capable of performing general engineering analysis by following instructions.
Minimal expenditure of resources	HRA methods can be divided into three required levels of effort: 1. Low: Requires a few hours of effort. 2. Medium: Requires a few days, up to one week of effort. 3. High: Requires a few weeks to a few months.
Available with reasonable cost	The HRA method must be available for immediate use. The method should be usable by an analyst who is not an expert in HRA, and the method should not require significant amounts of training to yield reliable, reproducible results between analysts. Some methods require certain costly tools for analysis.

Table 1 HRA Method features. *[11]*

2.1. Analogue space simulation risk assessment

According to this approach, the following table describes a potential set of main risk type group that can be a source of error during the preparation and execution of an analogue mission. Some of the examples might be repeated, due to the impossibility of disjointing them.

Risk type	Examples
Logistics	• Driver Shortage & Retention. • Government Regulations. • Environmental Issues.
Financials	• Transportation costs. • VISA and permits. • Fuel costs.
Planning	• Unexpected delays. • Overlapping schedules. • Disorganization. • Shift Swapping.
Crew capabilities	• Lack of technical skill. • Lack of behavioural skills. • Lack of cooperation. • Cultural issues.
Crew training	• Insufficient training. • Inappropriate training.
Experiment Execution	• Unclear procedure. • Technical issue.
Mission control supervision	• Unable to address the unexpected event. • Unable to understand the current state of the experiment.
Communication	• Loss of communication. • Misunderstanding.
Data	• Loss of data during or after the experiment. • Important data not stored.

Table 2 Risk types.

2.2. Analogue space simulations example experience & Performance Metrics

As already stated before, analog field testing results are vital for the assessment of the risks connected to equipment failure in hostile environment, where problems can be hard to solve. By learning from mistakes and improving the procedures, it is possible to gather and use the information to make reliable systems and procedures. Often these analogs may reveal unexpected issues for further development.

Thus, the general reader shall be provided evidence of the potential risks a crew can encounter while on a mission and how it should be prepared for unexpected events. The following example refer to one analog mission [1] conducted in a hostile environment by NASA with the aid of CSA[2] operators whitin the premises of Mauna Kea during the years 2008 – 2010, and has been part of technology prototype testing of ISRU[3].

[2] Canadian Space Agency.
[3] In-Situ Resource Utilization.

During the 2008 field test, high winds kicked up volcanic dust at the site, creating a surprise analog for dust mitigation in hardware systems. Planetary dust is a major concern for space exploration. Dust mitigation techniques were used on some hardware and worked well during the test, but dust issues caused several resets of drilling electronics that were not properly protected. With regard to the situation, it is possible to refer to Table 1 to identify the risks types which were evidence for this mission and their consequences:

1. Mission Control Operation (Unable to address the unexpected event initially).
2. Crew Training (insufficient/inappropriate training).
3. Experiment Execution (technical issues due to the dust).
4. Data (loss of data during or after the experiment).

Issues with system integration led to another lesson learned. At the 2010 field test, NASA and CSA successfully integrated several hardware. However, the testing uncovered non-optimized man – machine interfaces.

Within this context, the Austrian Space Forum (OeWF), has recently proposed an algorithm with which to compare analog missions through complexities/fidelities performance indicators to improve the scientific output and mission safety and maximize the efficiency of analog missions [13]. The algorithm requires a combination of distinct objective data sets to perform a weighted metric of the complexity and fidelity of a mission. Afterwards, the identified numerical outcomes are compared with reference missions, which yield strengths and weaknesses in mission planning.

This tool is used by key decision-makers to understand how and to what extent the inputs are enabling progress toward outputs and outcomes. However, the parameters cover a wide variety of elements of analog research. The OeWF defined three main sections of the *Analog Mission Performance* (AMP) metrics as follows: Level of representativeness of the test site, Dichotomous, and Quantitative sections. For the first two sections, the main key performance indicators (KPIs) that characterize an analog mission are complexity and fidelity. This is based on the assumption that analog missions aim to simulate future planetary surface operations in a scenario, which is as representative to actual flight missions as possible and hence have maximum complexity and fidelity. The AMP metrics algorithm specifically excludes: small-scale tests with low fidelity in terms of operations, computer simulations that include virtual reality, and actual flight missions.

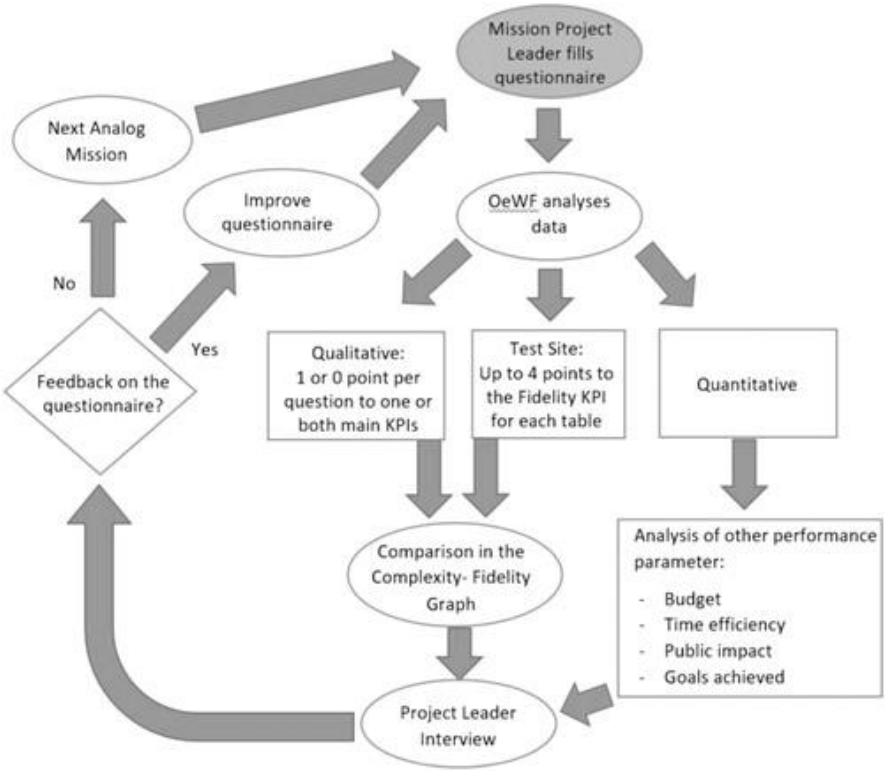


Figure 4 Deployed workflow for the AMP metrics evaluation. *[13]*

3. Risks reduction strategy

In the case of an analogue simulation mission, the above-described methodology must be appropriately scaled and simplified according to the dimension of the simulation mission. Nevertheless, the risk-reduction strategy eventually identified in this analysis wants to be an overall process of risk reduction, reported in the following figure, which starts from the definition of the main mission concepts and requirements and ends with the evaluation of the risk prevention measures undertaken by the crew and by the crew support organization.

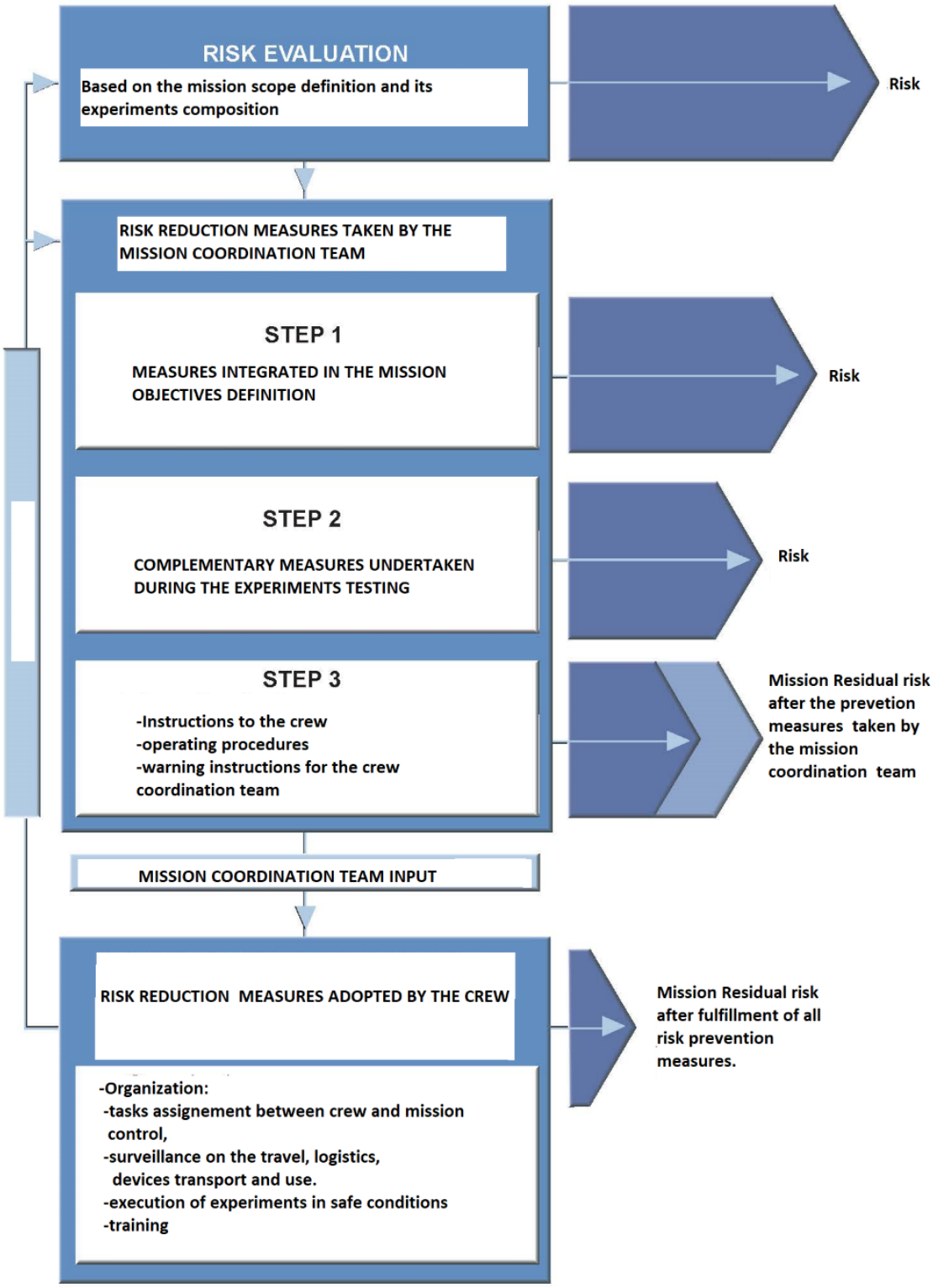


Figure 5 Mission risk reduction strategy.

The risk analysis and the risk-reduction process both require the removal or the reduction of the perils which could jeopardize the mission completely. This process is undertaken to employ multiple evaluations, which can be classified as follows:

1	**Removal of the danger or reduction of the risk employing mission definition**
2	**Risk reduction measures are undertaken by the mission support and organization team**

3	**Risk reduction measures are undertaken by the crew in all the steps of the mission**
4	**Mission Residual risk**

Table 3 Risk reduction process.

4. Identification of mission hazards and risk

As a first step of the risk analysis, it is necessary to identify the possible risks that could occur in an analogue mission. We suggest using a formatted table as Tab. 4, which reports a list of hazards that might occur during the various moments of the mission preparation and operations. the columns specify if the described hazard is detected during the mission or in the various stages of its preparation, development, and completion.

Legend:

E - Experiment Definition
F - Financial
L - Logistics
T - Experiments Testing before the mission
Mo - Mission operations
Mc - Mission controls
C - Crew management
S - Safety

No.	Risk Description	Situation Detected						
		E	**F**	**L**	**Mo**	**Mc**	**C**	**S**
1	Example	☐	☐	☐	☐	☐	☐	☐
2	Example	☐	☐	☐	☐	☐	☐	☐
3	Example	☐	☐	☐	☐	☐	☐	☐
4	Example	☐	☐	☐	☐	☐	☐	☐
5	Example	☐	☐	☐	☐	☐	☐	☐

Table 4 Checklist for mission risk identification.

5. Risk evaluation according to the risk matrix

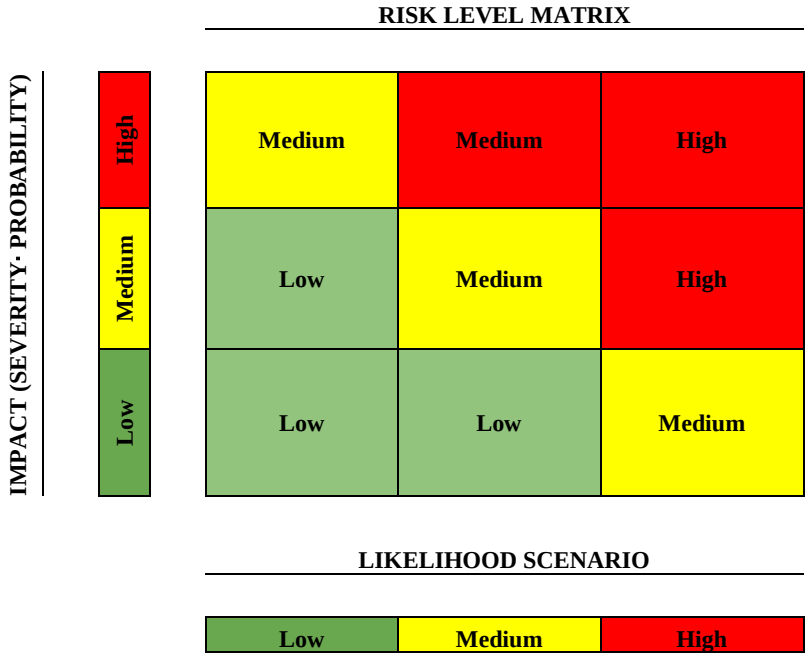
The used risk evaluation method is described in the following risk matrix. At first, the qualitative type method is applied to the risk evaluation of the single experiments, and after a complete analysis, it is reported in this document.

Priority	Experiment risk impact definition
High	*It involves non-compliance with regulations and disruption of goods and services to end-users.*
Medium	*Interruption of goods and services to end-users*
Low	*End users will probably not notice the failure*
Priority	**Likelihood**
High	*Certain to fail*

Medium	*Occasional failure likely*
Low	*Very unlikely, but not impossible*

Table 5 Risk evaluation.

This classification gives rise to the following matrix:



When the evaluation is in the red area, measures must be undertaken to reduce the mission risk. The element in this area poses significant threats to the mission. Therefore, the plan must be thought in a different and disruptive way.

When the evaluation is in the yellow area, Some features of the current plan may threat significantly the outcome of the mission. The implementation of measures is recommended to reduce the mission risks further.

When the evaluation is in the green area, the mission risk has been properly assessed and reduced. Therefore, no substantial changes are needed for the current mission approach.

Figure 6 3X3 Risk Matrix (OHSAS 18001[4] Model).

6. Risks List

The risk evaluation method used in this analysis is the one described in the following risk matrix. The method is applied in the risk evaluation of each experiment of the mission and the results are reported in a single comprehensive table.

Date:	Prepared:	Checked:	Approved:	-
Requirement	**Type**	**Likelihood**	**Impact**	**Risk level**
Example	Example	Example	Example	Example

[4] The acronym OHSAS stands for "Occupational Health and Safety Assessment Series" and identifies an English standard for a worker health and safety management system. A specific guide to this standard was published in 2008. The latter was revised in 2008.

With the publication of an international standard (ISO 45001 - "Occupational Health and Safety Management Systems - Requirements with guidance for use") in March 2018, BS OHSAS 18001 was withdrawn and replaced by BS ISO 45001. OHSAS 18001, starting from 1 October 2021, has been definitively replaced by ISO 45001. The ISO Standard has a “High Structured Level” (HSL) format, and it is divided in ten sections. [20]

Table 6 List of risk identification.

7. Risk Mitigation / Contingency Plan

A C*ontingency Plan* regards identified risks onlys. It is not developed to prevent errors or dangers from happening, but to define a rapid countermeasure that could immediately respond to the escalating situation. On the other hand, a *Mitigation Plan* attempts to decrease the chances of higher risks and their subsequent impact on the mission. It has to be developed and implemented in advance. It is common for the stakeholders involved to encounter the following challenges [14]:

1. Contingency planning is seen as a low priority (it can lead to mission failure).
2. Team members tend to be over-confident about the best-case scenario.
3. Lack of planning and enterprise can hinder further plan implementation.
4. Not spending enough time identifying all the risks.

It would be useful to follow the following guidelines to prevent unhappy outcomes:

1. Identify the trigger event for the execution of the plan's implementation.
2. Cover each step of the plan (e.g., what will happen, the key actors involved, etc.)
3. Define clear guidelines for the operators who have to follow them and define a communication plan.
4. Monitor the plan regularly to ensure it is up to date.

We suggest identifying risk mitigation/contingency plans during the different risks evaluation steps. A simple risk mitigation/contingency plan can be executed according to the following table:

Risk ID	Risk Event	Mitigation Plan	Likelihood	Impact	Risk Level	Contingency Plan
R1	Example	Example	Example	Example	Example	Example
R2	…	…	…	…	…	…
…	…	…	…	…	…	…
R_n	…	…	…	…	…	…

Table 7 Risk mitigation & Contingency Plan.

8. Situation Awareness demons' evaluation

Maintaining situation awareness (SA) can be difficult when systems are complex and there is a great deal of information to keep up with (or changes rapidly), and when it is hard to focus on multiple feedbacks [15]. The problem cannot be limited to technical facilities or cockpits. The amount of information we are subjected to is growing rapidly day by day, and it has become very difficult to just focus on the needed information, especially when systems are not divided into sub-domains (impossible to manage without having reached a certain grade of automation in the process). The capacity of the individual in terms of sorting and understanding the useful correct amount of information can result in a thorough success for the mission (e.g., any kind of manned mission). Thankfully, success involves more than just data. It mainly requires that data is sorted, processed, and ultimately transformed into useful information in a reasonable amount of time. It happens frequently that someone might get in touch only with just scraps of data in most situations, therefore needing to judge the situation and consequently decide how to act in a short period.

Most of the errors and catastrophic outcomes have been labelled as "Human errors" over time. This misleading term has resulted in the development of more complex systems to prevent humans from being able to respond to any

problem that might arise or comprehend it thoroughly. But the operator cannot be considered as the main source of failure; instead, it should be viewed as the final ground for inherent problems and difficulties in the technology we have created. In this context, SA (i.e., *Situation Awareness*) can be defined as an internalized mental model of the current state of the operator's environment. It is essential to develop systems that can help us cope with information, or at least identify the key points necessary to dam errors of every kind [16,17,19]. The successful improvement of SA through design or training programs requires the guidance of a clear understanding of SA requirements in the domain, the individual, the system, and environmental factors that affect SA, and a design process that specifically systematically addresses SA [16].

The Situation Awareness (SA) demons introduced in the classical studies of Endsley are here applied to evaluate the performance of the simulation mission. The scope of the SA demons' evaluation is also to perform a statistical analysis regarding the type of demons identified during the execution of analogue missions as well as during other types of space simulation missions. The joint use of the risk reduction strategy and method above described and SA DEMONS identification will provide a complete view of the risks involved in the simulation missions. In this manner, the risk analysts in charge of simulation missions risk evaluation will have at disposal a general flexible method with different components whose application can be sized and tailored according to the nature, dimension and time pipeline of the simulation mission.

The SA demons' definitions and their occurrences during the simulation of a mission are reported in the following table. A brief description is provided in the last column of Table 7. The Completion of the table is executed for each experiment and each activity foreseen during the simulation mission.

SA Demon	Definition & Description	Demon ID
Attentional tunnelling	It is important to be focused on complex domains. Multiple pieces of information may be given/processed by the operator to perform a particular task. The "attentional tunnelling" demon occurs when an operator strongly focuses on a specific problem, locking in on certain aspects or features of the environment he/she is trying to process, leaving out of the big picture other important parameters, which must be scanned properly to avoid unwanted situations or an accident.	ID No.1
Out-of-the-loop syndrome	The demon is related to system automation. If the automation loop fails, and the system suddenly gives back feedback about it, the personnel responsible for it might not be able to detect the problem instantly and subsequently correct it, therefore this situation leads to misinterpretation of the current situation and to the potential inability to solve it.	ID No.2
Errant mental model	A mental model is essential to analyse information. An "errant mental model" may lead the operator to the misinterpretation of that same information and be the cause of an accident or an unwanted outcome in high responsibility contexts. It might be due to inappropriate inferences derived from observations. The phenomenon can be reduced through standardization.	…
Complexity creep	The "complexity creep" demon typically occurs along with the "data overload" phenomenon. It can interfere with the ability of the operator to interpret information correctly, resulting in a catastrophic outcome. If the rules that govern a system's behaviour are complex, and many sub-systems are involved, someone could experience some difficulties in managing it.	…
Misplaced salience	In many complex systems, the operator seeks out relevant information for the achievement of a general goal. Simultaneously, he/she could be sensitive to other pieces of information (e.g., noises). "Misplaced salience" can be the root cause of a failure (e.g., if a system interface is designed to maximize the perception and attention of the user on a specific device, while the salience of an event prevents being focused on it).	…
Data overload	It defines the rapid rate at which information is given outpaces the operator's ability to process a large amount of data, resulting in significant and frequent lapses that might jeopardize the mission or negatively affect the task's outcome. The problem can be reduced by organizing, adjusting, and subsequently slowing the stream of data to be given.	…

Requisite memory	Related to the operator short-term memory while processing working information. The phenomenon can occur when many subtasks must be performed, and the operator forgets one of them.	…
Workload, fatigue, or stress	In this context, self-esteem, career advancement, or high-consequence events are involved. "stressors" can also natural (e.g., noise, vibration). Relying on working memory during these situations might affect the operator's ability to process peripheral information, resulting in attentional tunnelling and eventually being the cause of an accident.	ID No.N

Table 8 SA Demons mission identification.

9. SA-Oriented Design and enhancement

It is a real challenge to determine what aspects of a situation are important for the operator's SA [17,19]. It usually follows a thorough analysis, in which major goals and subgoals are identified. The requirements to perform the analysis focus on data as well as other dynamically integrated information. This goal-oriented analysis helps define the decision-making process in a complex environment. The goals may be all active at once, even if the priority of tasks must be considered. About the procedure, the design referent does not need to understand how the information is gathered or acquired by the operator since it can vary from person to person. The analysis seeks instead to determine what operators would ideally like to know to meet each goal since they often operate in incomplete information territories. Static knowledge (e.g., rules and procedures), on the other hand, cannot be considered to perform a SA requirements analysis, because it does not focus strictly on the dynamic knowledge that affects the operator's response to a certain situation.

A set of design principles have been developed based on the theoretical model of the mechanisms and processes involved in acquiring and maintaining SA in dynamic complex systems. These guidelines feature support for limited operator resources, including:

1. Direct presentation of higher-level SA needs, rather than supplying only low-level data that operators must interpret manually.
2. Goal-oriented information displays should be provided and organized so that the information needed for a particular goal is co-located and directly answers the major decisions associated with the goal.
3. Support for global SA, which provides an overview of the situation across the operator's goals and enables efficient and timely goal switching and projection.
4. Critical cues need to be determined and made salient in the interface design. Those cues that will indicate the presence of prototypical situations will be of primary importance and will facilitate goal switching in critical conditions.
5. Alien information not related to SA needs should be removed.
6. Support for parallel processing, such as multi-modal displays should be provided in data-rich environments.

One of the key benefits of looking at SA is that it tells us how data needs to be combined and understood. A structured approach is required to incorporate SA considerations into the design process, including a determination of SA requirements, designing for SA enhancement, and measurement of SA in design evaluation. [16]

10. Flowchart and Risks cube

The Risk Management Process can be summarized in Figure 4.

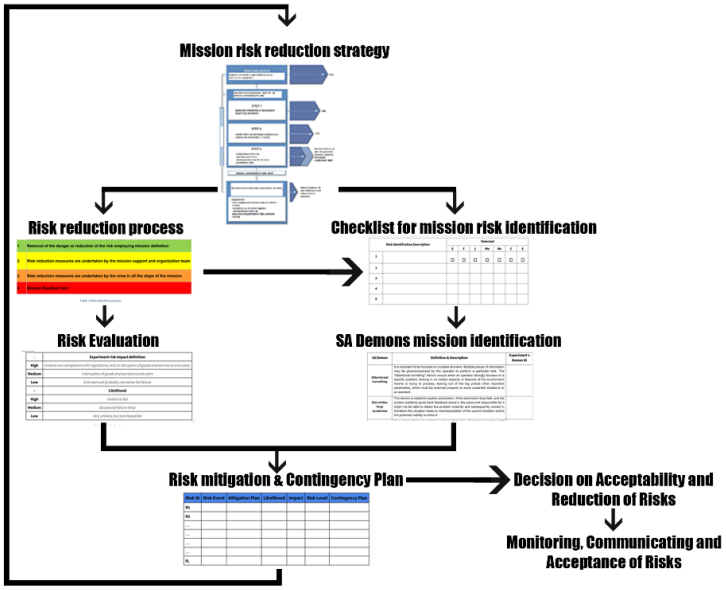


Figure 7 Overall risk evaluation process Flowchart.

Given the assessed risks at hand (according to the flowchart), the entire process leads to a situation in which it is possible to verify and control the identified risks. A periodic reassessment of those (possibly carried out through predictive maintenance and JIT techniques) is needed to operate in safety. As a general rule, new implementations in the mission lead to new risks, and to the updating of suitable changes afterwards in a neverending cycle of updates. The risks must be communicated to the project team members, while the residual ones must be accepted on a management level. Among the general tasks that the Management must ensure/execute, it is possible to list:

1. Gather all the possible information on the project.
2. Define a risk policy.
3. Follow the various project phases.
4. Consider the proportionate countermeasures.
5. Communicate every variation or risk information with the stakeholders and/or team members quickly.

Subsequently, we suggest here to visualize the various risk procedures and tools like different faces of a “Risks Cube” shown in Figure 5 since the previously analysed risk tools must not be considered as steps of a standard procedure, but pieces of a flexible risk management activity.

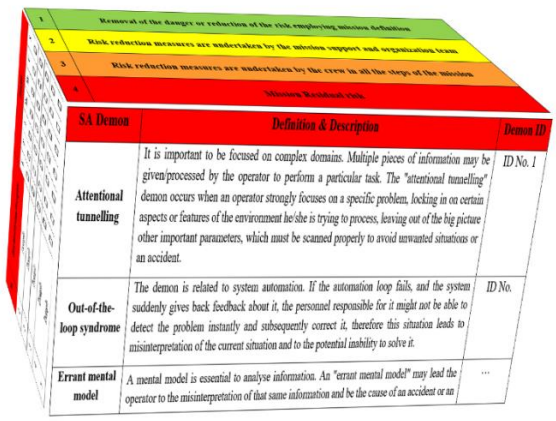


Figure 8 The " Risks Cube" (see also Figure 6 for the unfolded version).

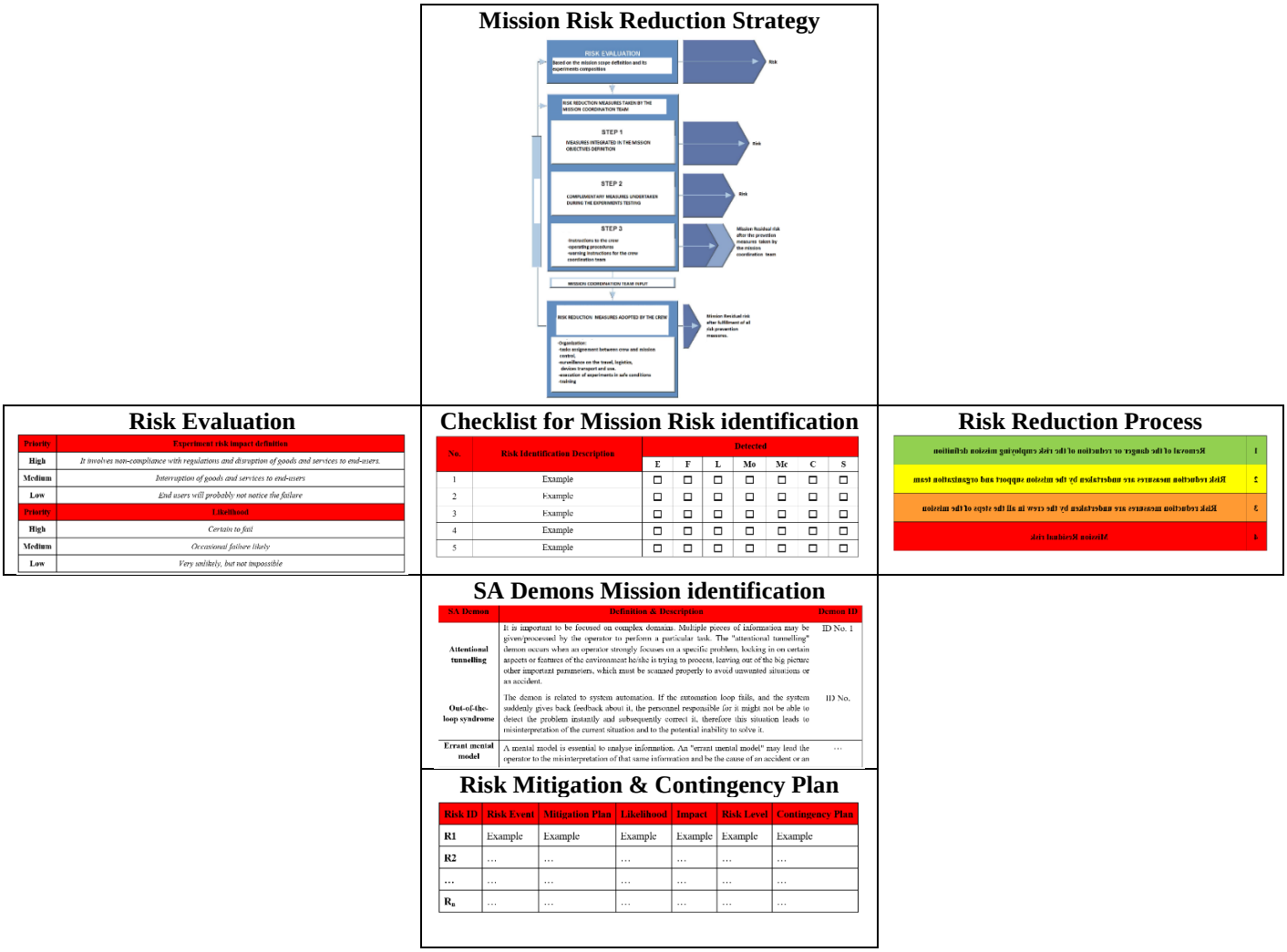


Figure 9 Unfolded Risk Cube.

We want to highlight that the risk analyst can choose to employ all the six faces of the Risks Cube or only some of them, that better fit the situation under analysis. It would be helpful to visualize all the Risk Cube faces (representing the above-mentioned procedures). The operator can look at the single risk management activity as part of a more general issue-identification during the space simulation mission and the necessary countermeasures to undertake to keep the overall mission risk to an acceptable level.

11.Conclusion

In this paper, we provided a general risk evaluation method for analogue simulation missions to analyse the circumstances that could affect the positive outcome of the mission. The risk analysis method considers the evaluation of the risks of each experiment foreseen in the mission, and the evaluation of other general factors. The scope of this analysis is to ensure that all the operations included in the simulation mission are analysed and well defined.
The method includes different well-known risk analysis tools and procedures, such as the evaluation based on situation awareness demons', that can be used totally or partially according to the level of complexity of the simulation mission. The Risk cube concept is introduced to visualize the interconnection of the different risk analysis tools that, taken all together, can identify all the domains of occurrence of the possible risks. Finally, it is worth noting that the suggested

method, including the Risk Cube concept, can be applied with appropriate changes to other types of Space missions characterized by a higher level of complexity.

References

[1] National Aeronautics and Space Administration: Langley Research Center, NASA's Analog Missions: Paving the Way for Space Exploration, Hampton, VA: NASA, 2010.

[2] D. o. Defense, “MIL-STD-882E: System Safety Standard Practice,” Department of Defense, Fort Belvoir, VA, 2012.

[3] J. D. Mitchell, “Integrated Docking Simulation and Testing with the Johnson SPace Center Six-Degree-of-Freedom Dynamic Test System,” in *AIP Conference Proceedings*, 2008.

[4] T. N. Arnesen, “Stress Assessment During a Simulated EVA,” in *55th International Astronautical Congress on the International Astronautical Federation, the International Academy of Astronautics, and the International Institute of Space Law*, 2004.

[5] V. Pletzer, “Crew Time utilisation and Habitat interface investigations for future planetary habitat definition studies: field tests at MDRS,” in *38th COSPAR Scientific Assembly* , 2010.

[6] G. Groemer, “The AMADEE-15 Mars Simulation,” *Acta Astronautica,* vol. 129, pp. 277-290, 2016.

[7] T. Aven, “Reliability and Risk Analysis,” *Elsevier Applied Science,* 1992.

[8] H. Fukuyama, E. Fernandes and N. F. F. Ebecken, “RIsk Management in the Aeronautical Industry: Results of an Application of Two Methods,” in *6th International Conference on Computer Simulation Risk Analysis and Hazard Mitigation*, 2008.

[9] T. Bedford and R. Cooke, “Probabilistic Risk Analysis Foundations and Methods,” *Cambridge University Press,* 2001.

[10] J.-M. Salotti and S. Ephraim, “Manned Missions to Mars: Minimizing Risks of Failure,” *Acta Astronautica,* vol. 93, pp. 148-161, 2014.

[11] F. T. Chandler, J. Y. Chang,, A. Mosleh, J. L. Marble, R. L. Boring and D. I. Gertman, “Human Reliability Analysis Methods,” NASA Headquarters Office of Safety and Mission Assurance, Washington, DC 22039, 2006.

[12] InfraSpeak, “Fault Tree Analysis (FTA): Definition, Applications and Benefits,” InfraSpeak, 18 December 2021. [Online]. Available: https://blog.infraspeak.com/fault-tree-analysis-fta/. [Accessed 18 December 2021].

[13] S. Gruber, G. Groemer, S. Paternostro and T. L. Larose, “AMADEE-18 and the Analog Mission Performance Metrics Analysis: A Benchmarking Tool for Mission Planning and Evaluation,” *Astrobiology,* vol. 20, no. 11, pp. 1295-1302, 2020.

[14] Project Management Guide, “What is a Contingency Plan in Project Management?,” 2021. [Online]. Available: https://www.wrike.com/project-management-guide/faq/what-is-contingency-plan-in-project-management/.

[15] M. R. Endsley and D. G. Jones, Designing for Situation Awareness: An Approach to User-Centered Design, Boca Raton, FL: Taylor & Francis Group, 2004.

[16] M. R. Endsley and G. Marietta, “Designing for Situation Awareness in Complex System.,” in *Proceedings of the Second intenational workshop on symbiosis of humans, artifacts and environment, Kyoto, Japan.*, Kyoto, 2014.

[17] J.-M. Salotti and E. Suhir, “Degraded situation awareness risk assessment in the aerospace domain,” *HAL,* pp. 1-6, 2019.

[18] K. Kireev, A. P. Grishin and G. L. Dowell, “Medical Issues Associated with Winter Survival Training,” *Aerospace Medicine and Human Performance,* pp. 677-680, 2021.

[19] S. Gruber, “AMADEE-18 and the Analog Mission Performance Metrics Analysis: a Benchmarking Tool for mission planning and evaluation,” *Astrobiology,* pp. 1295-1302, 2020.

[20] International Standard Organization, *UNI ISO 45001:2018 - Sistemi di gestione per la salute e sicurezza sul lavoro - Requisiti e guida per l'uso,* Genève: International Standard Organization, 2018.

[21] C. A. Ericson II, “Fault Tree Analysis - A History,” in *Proceedings of the 17th International Safety Conference*, Seattle, Whashington, 1999.