DOI: 10.13009/EUCASS2022-7330
9TH EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES (EUCASS)

RAMS as a Crucial Contributor Towards Space Sustainability

Silvana Radu
The European Space Agency (ESA), The Netherlands, silvana.radu@esa.int
Fabrice Cosson
The European Space Agency (ESA), The Netherlands, fabrice.cosson@esa.int
Charles Lahorgue
The European Space Agency (ESA), The Netherlands, charles.lahorgue@esa.int
Laurent Marchand
The European Space Agency (ESA), The Netherlands, laurent.marchand@esa.int

Abstract

Nowadays space vehicles have a wide range of objectives and scopes aiming at accomplishing critical functions in various fields of aerospace engineering such as science, earth observation, navigation, telecommunication, close proximity operations (CPO), etc. The cost of such space missions can range from millions to billions and most of the spacecraft do not allow access for on-board maintenance, thus planning ahead and targeting high reliability is imperative. This latter aspect, becomes even more essential when building missions that may contribute to space sustainability such as Active Debris Removal (ADR) or In-Orbit Servicing (IOS) where two or multiple objects need to operate in close proximity either in a coordinated or uncoordinated manner. The overall Reliability, Availability, Maintainability and Safety (RAMS) analyses need to be thoroughly developed for such missions, in order to ensure safety and, ensure that at the end, the number of debris in protected regions are decreased. This paper's main objective is to highlight the importance of RAMS for unmanned missions that operate in close proximity but also to emphasize on the importance of RAMS in all missions, especially with regards to optimization, cost reduction, schedule, risk and design budgets, while ensuring overall mission success is being maximised.
In a space project, the RAMS assurance program comprises of a number of technical activities that consist of an extensive amount of analyses to be performed at various stages. Sometimes, in projects, it is noticed that the purpose of these analyses is slightly neglected or misunderstood and certain outputs from the RAMS analyses are not properly used. The correct and complete use of RAMS becomes even more critical in the CPO types of missions where safety is of paramount importance and the goal is to contribute to the reduction of debris. Similarly, the use of RAMS analyses are crucial also when deciding for life extension of a satellite and guaranteeing that the reliability of disposal is still met, this in turn contributing to space sustainability. The overall performed work aims at clarifying the interaction and intent of the RAMS analyses though the created RAMS map, especially when tailored for complex missions such as ADR or IOS. The paper will first focus on the RAMS analyses and their scope and definition specified in a general manner for space mission. The existing developed RAMS map which aims at showcasing the interaction between RAMS analyses but also their interdependency with other disciplines such as System Engineering and Fault Detection Isolation and Recovery will be disseminated. Furthermore, a thorough and detailed presentation on how these analyses should be performed and used for unmanned satellite missions will be discussed. Finally, the paper will present the tailoring of the RAMS map on specific types of missions operating in close proximity (ADR and IOS), emphasising on the RAMS delta required, in order to ensure in-orbit safety and mission success. Conclusions and recommendations with regards to RAMS for space missions with particular accent on those missions that aim at improving the overall amount of debris currently in orbit will be highlighted.

DOI: 10.13009/EUCASS2022-7330

DOI: 10.13009/EUCASS2022-7330

NOMENCLATURE

ADR	Active Debris Removal
AOCS	Attitude and Orbit Control System
AR	Acceptance Review
BOL	Beginning Of Life
CDR	Critical Design Review
CIL	Critical Items List
CONOPS	Concept Of Operations
COTS	Commercial Off The Shelf
CPO	Close Proximity Operations
CRR	Commissioning Results Review
ECSS	European Coordination for Space Standardization
ELR	End-Of-Life Review
EOL	End Of Life
FDIR	Fault Detection Isolation and Recovery
FE	Feared Event
FEA	Feared Event Analysis
FM	Failure Mode
FMEA	Failure Modes Effects Analysis
FMECA	Failure Modes Effects (and Criticality) Analysis
FOM	Flight Operations Manual
FR	Failure rate
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GDIR	General Design and Interface Requirements
HSIA	Hardware-Software Interaction Analysis
HW	Hardware
IOS	In-Orbit Servicing
LRR	Launch Readiness Review
OBC	On-Board Computer
ORR	Operational Readiness Review
MBSE	Model-Based System Engineering
MCI	Maintainability Critical Items
MCR	Mission Close-Out Review
MDR	Mission Definition Review
QR	Qualification Review
RAM	Reliability Availability Maintainability
RAMS	Reliability Availability Maintainability and Safety
RBD	Reliability Block Diagram
REX	Return of Experience
RP	Reliability prediction
PA	Product Assurance
PCA	Part-Count Analysis/Method
PDR	Preliminary Design Review
PRR	Preliminary Requirements Review
PSA	Part-Stress Analysis
PSM	Part Stress Method
SDMR	Space Debris Mitigation Requirements
SE	System Engineering
SEE	Single Event Effects
SH	Safety Hazard
SPF	Single Point Failure
SRR	System Requirements Review
SW	Software
WCA	Worst Case Analysis

Copyright © 2022 by First Author and Second Author. Published by the EUCASS association with permission.

DOI: 10.13009/EUCASS2022-7330

1. Introduction

Designing safety-critical systems, especially those concerning in orbit safety, the integrity of the design, development and testing process shall be assured. For space systems such as satellites or spacecraft, this is even more critical than, for example, ground systems, because maintenance cannot be performed at a specific time and thus mission success, minimum autonomy and in some cases survivability, needs to be guaranteed. The quality assurance of the design, development and in some cases testing of such space systems, subsystems and equipment is performed also through reliability, availability, maintainability and safety (RAMS) tools and methodologies. RAMS analyses are tools used as part of the engineering process, aiming at ensuring that the right choices are made from all points of view such as: engineering budgets, cost, safety, survivability, etc. RAMS, or Dependability and Safety, as commonly referred in various standards and publications, represents, for a project life-cycle, an iterative process that starts at very beginning of the project, continues for the period of usage of product and ends once the usage of the certain product is ended. As stated in [1], typically, in engineering, the starting point of view is "what should be achieved" in order to meet the design criteria and accomplish the project successfully while little consideration is being given at the beginning on "what should be assured". RAMS modelling aims at providing a better grasp on the latter in order to contribute to an increase of probabilistic chances of successfulness.

RAMS becomes even more critical when building missions where two or more spacecraft have to operate in close proximity either in a cooperative or uncooperative way. An example of such missions are those that contribute to space debris reduction and increasing space sustainability, such as Active Debris Removal (ADR) or In-Orbit Servicing (IOS) missions. In such cases, RAMS analyses need to be more thoroughly developed in order to ensure safety and that the number of debris in protected regions are not increased. Likewise, RAMS analyses become crucial also when performed in order to decide whether extension of life is possible or disposal would be advisable.

This paper's main objective is to clarify the RAMS and overall use of RAMS in space with a focus on CPO missions. In the coming chapters, a brief review of currently used body of knowledge will be provided, the use of RAMS analyses in space missions, especially CPO, will be described, the generic RAMS map and RAMS map tailored for CPO will be detailed and provided.

1.1 Definitions from literature

In various existing literature, several definitions are provided for what each of the RAMS acronyms means. In Table 1, a comparison of the definitions found in literature can be seen.

Definitions	Source [1]	Source [10]	Source [4, 5, 6, 7]
Reliability	represents the probability of successful operation or performance of a system (incl. their full chain of equipment that compose the system), with minimum risk of loss or disaster or of system failure.	represents the ability of an item to perform a required function under given conditions and for a given time interval. It is also mentioned that it is generally assumed that the item is in a state to perform this required function at the beginning of this time interval, thus reliability is considered 1 (or 100%) at beginning of life.	represents the ability of an item to perform a function, under given conditions for a given period of time.
Availability	represents the aspect of system reliability that looks at equipment maintainability data, thus designing for availability requires evaluation of the consequences of unsuccessful operation or performance.	represents the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or a given time interval, assuming that the required external resources are provided. It is stated that the ability depends on the combined aspects of reliability and maintainability performance.	represents the ability of an item to perform its required function at a given time or during a given period of time.
Maintainability	represents the aspect of maintenance that looks at the downtime of the	represents the ease of performing maintenance on a product. It is also stated that	represents the ability of an item to be retained or restored to a stated in which it can

DOI: 10.13009/EUCASS2022-7330

	system and it requires an assessment of accessibility and time to repair.	maintainability can be expressed as the probability that a maintenance action on a product can be carried out within a defined time interval, using stated procedures and resources.	perform its required function. Maintainability is the main factor that contributes to the availability of the item.
Safety	is classified into three categories related to personal protection, equipment protection and environmental protection and is being defined as "not involving risks".	represents a state where an acceptable level of risk is not exceeded. In [10] it is also stated that risks relate to fatality, injury/ occupational illness, damage to equipment/system, pollution of environment, damage to public property.	freedom from those conditions that can cause death, injury, occupational illness or damage/loss of equipment or property.

Table 1 Definitions from RAMS literature

Evidently the provided definitions in Table 1 are highly generic and each engineering field and discipline has its own tailored understanding with applicability on the relevant projects of what RAMS is.
RAMS tools and methodologies in space are slightly different than other fields of engineering. Similarly to the provided definitions of scope of RAMS, for space field, RAMS analyses are performed for the same reasons which remain [16]:

- To support design trade-offs through the identification and comparison of design solutions and through the identification of weak points and critical areas;
- To support requirement definition through failure robustness (tolerance and avoidance) and allocation of quantitative reliability and availability objectives;
- To confirm design solutions through the assessment of the performance of the selected design solutions and through the continuation of identification of weak points and critical areas;
- To support and confirm if mission extension is possible or disposal of a certain satellite would be recommended instead;
- To contribute to an assessment of the overall risk.
- To contribute to increasing the chances for mission success

In order to increase reliability, the following aspects are recommended: usage of quality components, ensuring sufficient margin (derating), use of redundancy (through use of trade-offs with respect to mass, volume and cost), design complexity (cross-strapping) and design variety. The following RAMS analyses are typically performed:

FMEA/FMECA analysis used generally for assessment of failure propagation and identification of SPFs. While the analysis can provide a good indication of the qualitative assessment, one of the major limitations of FMEA/FMECA is that it represents a static analysis that focuses on the end failure effects (transient effect before end effect is not identified) and that it assumes the design is free of errors. It is to be noted that FMEA/FMECA may contribute to the identification of design errors but it is not its primary objective. The analysis is typically performed for European Space Missions in accordance with [17].

Reliability prediction is often performed in conjunction with the availability and maintainability analysis as part of the dependability report. The Part-Count Method (PCM) is the method applicable for early mission phases (up to Preliminary Design Review - PDR) when information on the design is not fully available. Part Stress Analysis (PSA) and implicitly Part Stress Method (PSM) are used for later mission phases after the design is frozen (Critical Design Review - CDR and later). The analysis is typically performed for European Space Missions in accordance with [16].

Part-Count Method (PCM) is the method applicable for early mission phases (up to Preliminary Design Review - PDR) when information on the design is not fully available. Thus, performing PCA means that generic part type and information regarding quality, failure rate and environment are used. The equipment failure rate is determined by using generic failure rates and multiplying it by a factor of quality.

Part Stress Analysis (PSA) is applicable when most of the design is completed and a list of parts is available. At RAMS level, it is used to verifying the correct application of the derating requirements.

DOI: 10.13009/EUCASS2022-7330

Part Stress Method (PSM) utilises input from PSA and it is finally used for the reliability prediction at later stages during the mission. The approach is mainly to sum individually the calculated rates of failure for each component and then to add it to the failure rate of the overall unit.

Availability analysis: the scope of the analysis is to verify the conformance of the design with the applicable availability requirements and to provide input in order to support the Operations and Integrated Logistic Support and estimate the life cycle cost of the system. The analysis is typically performed for European Space Missions in accordance with [16, 21].

HSIA is typically performed for European Space Missions in accordance with [17] and represents an analysis generally performed for space systems that aims at ensuring that the software (SW) reacts in an acceptable way to hardware (HW) failures.

Fault Detection Isolation and Recovery (FDIR) analysis is performed in order to assess and combine the information coming from the system engineering with regards to design and the information coming from RAMS with regards to failure modes and compensating provisions as well as effects of HW on SW. The purpose of the analysis is to lead to an FDIR design and process that can be implemented within the flight software. The analysis is typically performed for European Space Missions in accordance with [16, 20].

Feared Event Analysis (FEA) is based on the concept of operations, mission, system and overall objectives. The analysis is used for providing the top events for the FTA, however it makes use of other analyses as well such as FMEA/FMECA, contingency analysis, in-orbit safety mission analysis, FDIR analysis and autonomy concept.

Fault Tree Analysis (FTA) is typically performed for European Space Missions in accordance with [14] and it represents an analysis that showcases a graphical and logical representation and quantification of combination of failures and events occurring in a system that may lead to a top undesired event.

Worst Case Analysis (WCA) is typically performed for European Space Missions in accordance with [16] and aims at demonstrating that the electronic and electrical equipment are performing within specification under the worst conditions such as beginning of life (BOL) and end of life (EOL). The analysis aims at supporting the choice of architecture and components during the design phase.

Contingency analysis aims at assessing the contingency scenarios and/or compensating provisions identified with the FMEA/FMECA, FTA and FEA. For example, in order to ensure that the adopted contingency for a certain undesired event would not lead to collision. The output of the analysis contributes to the Flight Operations Manual (FOM) and requires input from the concept of operations (CONOPS), FDIR, FEA, FTA and FMEA/FMECA. The analysis can dictate over the recovery actions for FDIR. The contingency analysis is typically referred to as an FMEA/FMECA from the operations point of view. The analysis is typically performed for European Space Missions in accordance with [16].

Maintainability analysis is typically performed for European Space Missions in accordance with [16]. The analysis is typically performed at system level and it is used as a design tool to asses and compare design alternatives with respect to specified maintainability quantitative requirements (the time to diagnose item failures, the time to remove and replace the defective item, the time to return the system to its nominal configuration, etc.). The main goal is to compute the probability of repair in a given time [3]. The analysis is typically a standalone document generated mainly for ground system or systems where humans can intervene.

Common-cause analysis is typically performed for European Space Missions in accordance with [16] and represents an analysis that contributes to the identification of the root cause of a failure that may have a potential to negate failure tolerance levels. Generally, the common-cause analysis consists of common mode analysis and zonal analysis and should cover, apart from random failures, also potential errors during design, manufacturing, assembly, operations, etc. Common-cause failures are very important because they are considered large contributors to the unreliability of the system.

RAM Critical Items List (CIL) represents a list of critical aspects (e.g. Items constituting a residual single point failure) that are added into a table for the purpose of tracking items that are considered of risk with respect to RAM. The list is typically built for European Space Missions in accordance with [16, 17].

Safety assurance (in orbit) represents the mission analysis for all in orbit phases in which safety aspects such as collision probability, compliance with safety debris mitigation requirements and re-entry aspects are covered. Moreover, depending the autonomy level of the S/C and the orbital configuration, assessment if S/C is passively safe especially during critical phases is performed. The analysis is typically performed for European Space Missions in accordance with [22, 23] or with inputs and requirements coming from operations authority and safety authority.

DOI: 10.13009/EUCASS2022-7330

Safety Analysis is typically performed for European Space Missions in accordance with [18, 19].

Hazard Analysis is typically performed for European Space Missions in accordance with [19].

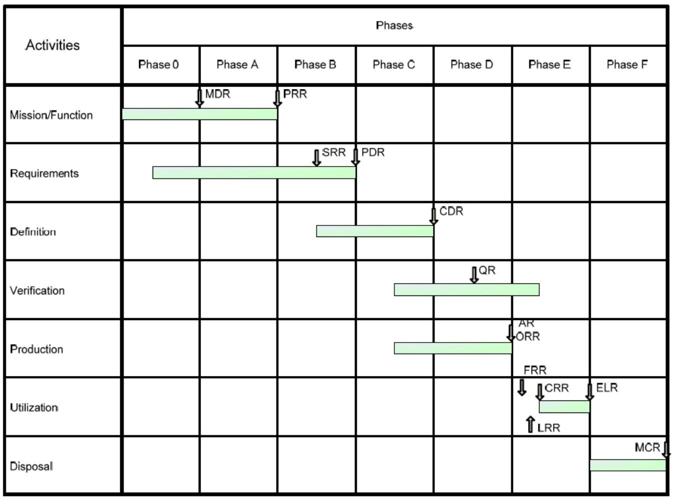
Safety Data Package consists of all safety analyses and safety submission which have their own schedule and depend on the type of mission and launcher. The hazard analysis supports safety submission but does not replace it. The safety submission document is broader and has to consist of the general safety requirements (classes of risks relative to ground activities), specific safety requirements, safety compliance matrix, system overview, hazard overview and launch campaign operations.

Safety Critical Items List similarly to RAM CIL, the Safety CIL tracks the critical and catastrophic items identified with respect to safety. RAM CIL and Safety CIL are merged into RAMS CIL. The list is typically built for European Space Missions in accordance with [16,17,18,19].

Space Debris Mitigation Plan/Report aims at proving compliance with the Space Debris Mitigation Requirements (SDMR) that can be found in [22, 23]. The connection of this report and RAMS is through the calculation of reliability of disposal, casualty risk and accidental break-up which can be applicable in certain types of satellites as per [22].

1.2 Project life cycle and RAMS schedule

While developing a space mission, the following project life cycle is applied as per [24]:



Where the acronyms represent the following:

MDR – Mission Definition Review
PRR – Preliminary Requirements Review
SRR – System Requirements Review
PDR – Preliminary Design Review
CDR – Critical Design Review
QR – Qualification Review
AR – Acceptance Review
ORR – Operational Readiness Review
FRR – Flight readiness Review
CRR – Commissioning Results Review
LRR – Launch Readiness Review
ELR – End-Of-Life Review
MCR – Mission Close-Out Review

Figure 1 Project life cycle

Considering the timeline provided in Figure 1, the following schedule is typically followed for RAMS analyses within a space mission [16, 18]:

DOI: 10.13009/EUCASS2022-7330

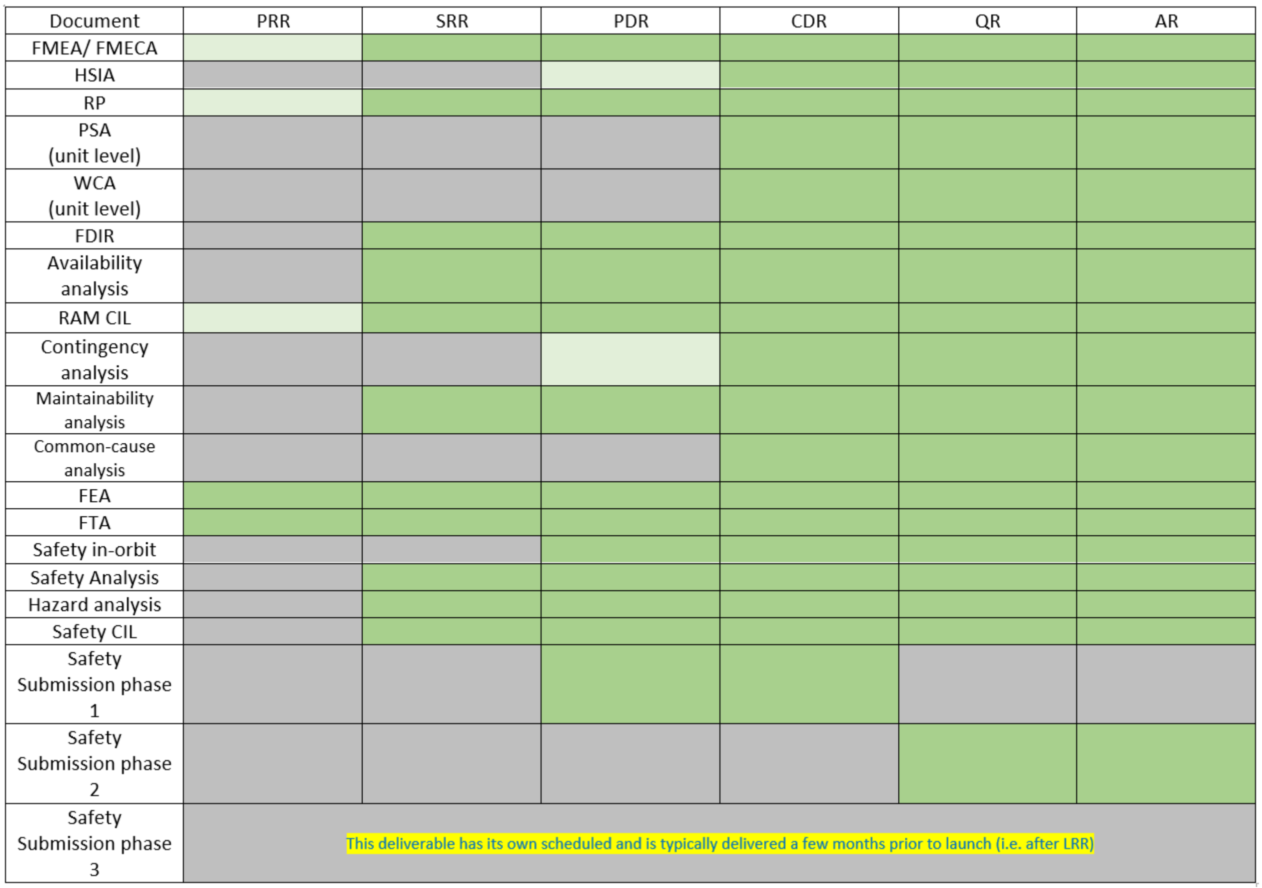


Figure 2 Expected timeline of RAMS analyses

Analysis not required

Analysis could be required if heritage and sufficient information would be available at that stage

Analysis required

DOI: 10.13009/EUCASS2022-7330

2. Generic RAMS map at system level

The first step in a space mission starts with defining the mission requirements, including Reliability, availability and safety requirements. Reliability itself at mission level can be referred to also as mission success. The flow down of requirements for reliability can be also referred to as apportionment of requirements. Based on the RAMS requirements allocated at lower levels, the RAMS analyses can be started and results are compared against those requirements. In Figure 3, a basic diagram shows the flow of the above described steps. It is important to note that having input from system level and equipment level through hardware and software technical specification and design is critical in order to be able to proceed with RAMS analyses. It is also important to note that the information coming from hardware and software technical specification and design towards RAMS is applicable also in the other direction. This is because RAMS analyses, as mentioned before, have as main goal to act as design tools that contribute to trade-offs and identification of weak areas, thus it is common that based on the RAMS results, the design is modified.

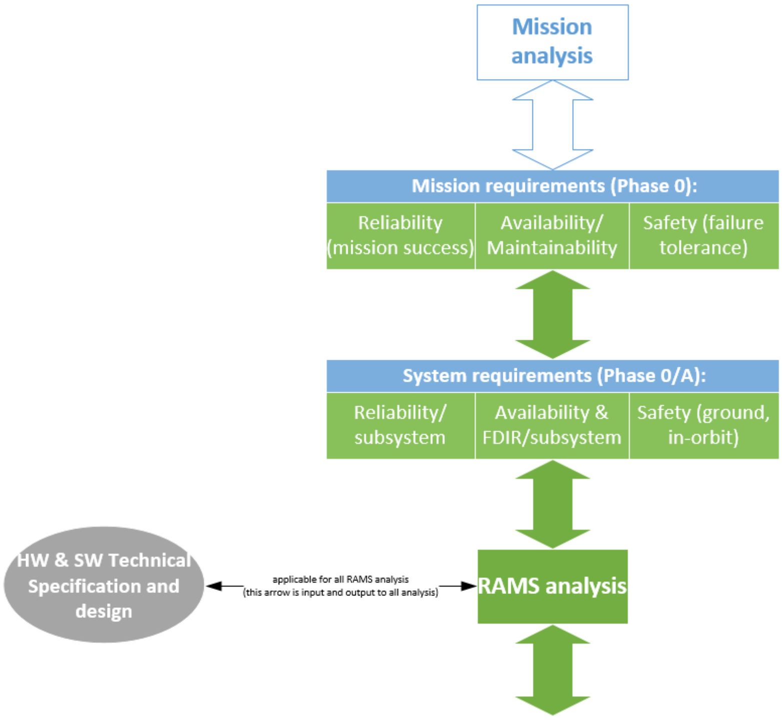


Figure 3 From Mission to RAMS analyses

As previously mentioned, RAMS analyses, their interdependencies and overall flow can be quite complex. Figure 4 aims at demonstrating the various interactions between analyses by specifying what output is used as input from one analysis to another. In Figure 4, grey blocks represent information or results that come from outside of RAMS.

DOI: 10.13009/EUCASS2022-7330

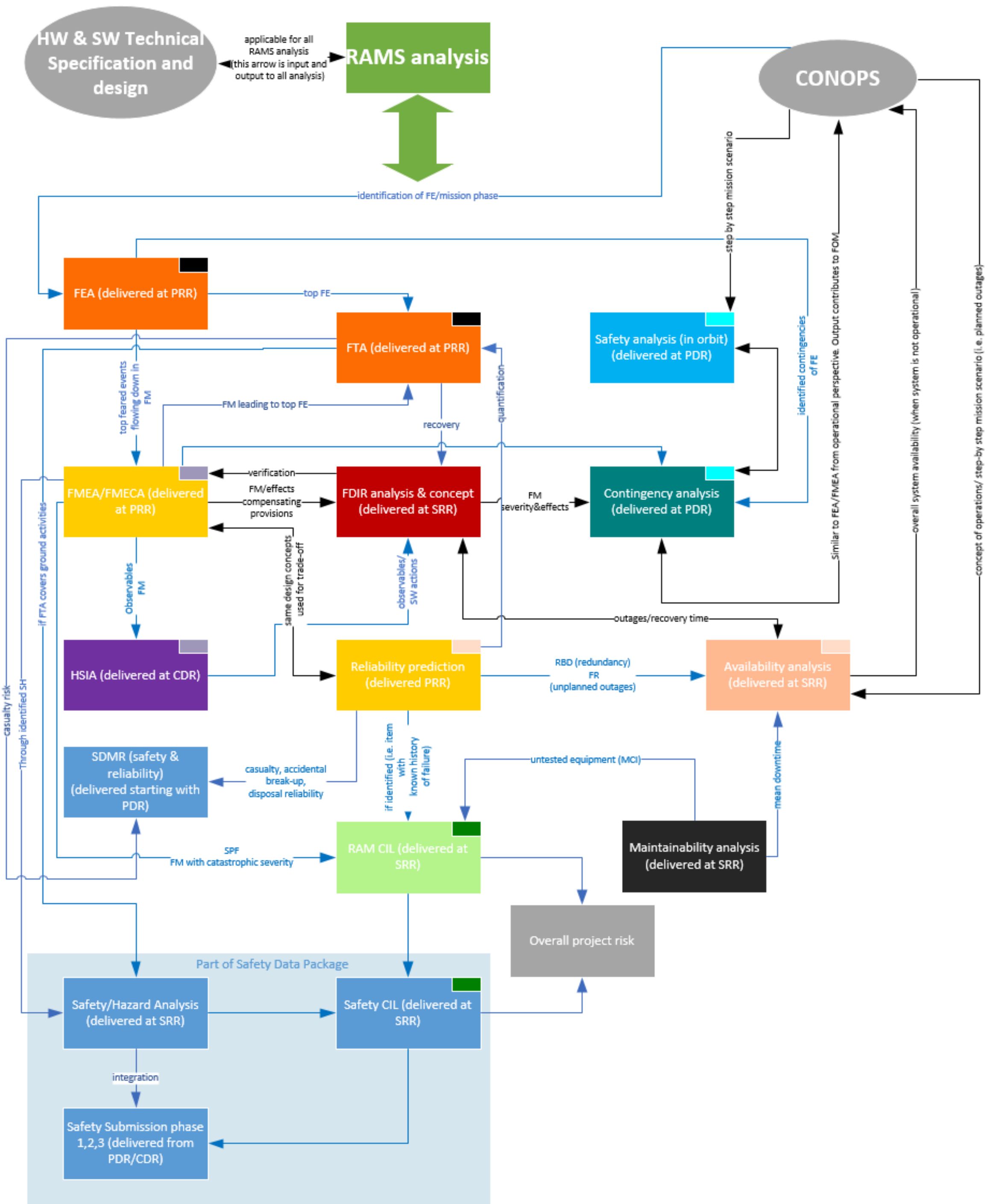


Figure 4 RAMS analyses dependencies

The interdependencies between FEA, FMEA, FTA and Reliability Prediction (RP) are generally obvious but still sometimes performed in practice in an independent manner. The goal of FEA is to identify the top Feared Events (FE) which will then be assessed through FTA, while the goal of FMEA with regards to the FTA is to provide the failure modes (FM) that might lead, either individually or in combination with other FM to one of the top FE. It is to be noted also the importance of the RP that provides input to the FTA through the quantification. The main goal of the FTA is to analyse combinations of failures that may lead to a top FE but also to quantify the probability of failure. The FTA can provide also input to the Hazard Analysis depending on what level the FTA is made. If, for example, the FTA takes into account ground FE, then the FTA would contribute also to the Hazard Analysis. The FEA finally contributes also to the contingency analysis in order to provide input to CONOPS. The FTA can contribute to the FDIR concept through recommendations in terms of recovery/contingency specifically for combinations of failure. These analyses are the main ones that contribute to CPO missions. Based on their use, various risks and top feared events (i.e. collision)

DOI: 10.13009/EUCASS2022-7330

are analysed and quantified. The interdependencies between FMEA/FMECA, HSIA, FDIR, contingency analysis, FTA, availability analysis and CONOPS revolve around the FDIR concept and influence the FDIR design and processes within a mission. FMEA/FMECA contributes to the FDIR through identification of failure modes and effects but also through compensating provisions while in later stages it is used for verification and validation of the FDIR functions. FMEA/FMECA contributes to HSIA through the observables and failure modes while HSIA represents the bridge between FMEA/FMECA and FDIR and contributes through observables and software actions. FDIR and FMEA/FMECA both provide through their output some inputs to the contingency analysis through the failure modes, severity and effects. Availability analysis provides information such as outages and recovery time to FDIR. It is important to note the interaction of availability analysis and CONOPS which comes through providing the overall system availability influences the FDIR. The interdependencies between FMEA/FMECA, reliability prediction, availability analysis, maintainability analysis, RAMS parts from SDMR, RAM CIL and overall project risks represent the core of typical RAMS analyses. The FMEA/FMECA contributes to the reliability prediction and in fact they are analysis performed and reviewed in parallel as they are based on exactly same concepts/designs under trade-off. The reliability prediction is interdependent with the availability analysis through the redundancy scheme and unplanned outages. The reliability prediction contributes to the Space Debris Mitigation Requirements (SDMR) through the computation of the disposal reliability. The disposal reliability computed typically within the reliability prediction report is then compared against the SDMR. Safety shall always be considered in conjunction with dependability, thus it is important to note the interdependencies that exist between the FMEA/FMECA and hazard analysis through identification of safety hazards or the input that the FTA may provide to the hazard analysis through the analysis of ground safety hazards. Furthermore, overall project risk consists, when referring to RAMS, of RAM CIL and Safety CIL which are based on the identified safety hazards. The Hazard and safety analysis, safety CIL and safety submissions are all part of the Safety Data Package.

3. Generic RAMS map at subsystem level

RAMS analyses are not only performed at system level, in fact the approach is generally following the V cycle, first starting with top-down and then continuing with bottom-up. The interdependencies within the analyses is made in a similar manner as for system level. In this subchapter, a description about the interactions that occur between analyses will be provided only for those analyses that were not already tackled in the previous subchapter. It should be kept in mind that the interactions described in this chapter refer to subsystem level. In a similar manner, the grey boxes are inputs coming from other disciplines.

The interdependencies between common-cause analyses and other RAMS analyses depend on external aspects such as system engineering design, detailed hardware design of units/equipment and parameters list. Common-cause analysis is highly dependent on the FMEA/FMECA mainly through information on failure propagation risk between redundant components, however it also interacts with FTA through the support in identification of root cause failure. The common-cause analysis provides information to the availability analysis through unplanned outages.

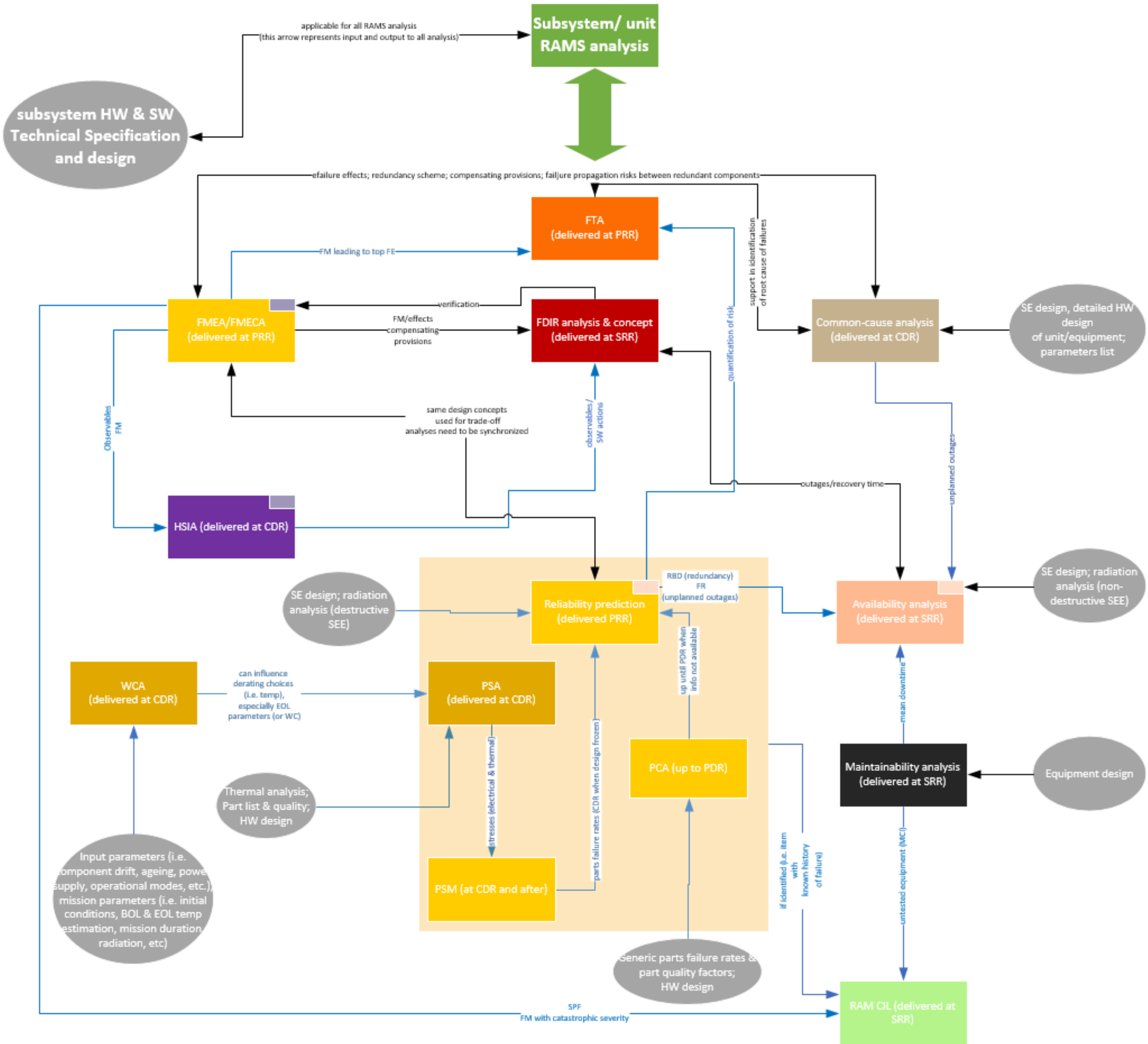


Figure 5 RAMS at Subsystem level

4. RAMS analyses tailored for CPO

There are various types of CPO missions that could be identified, such as: active debris removal, in-orbit servicing, rendezvous, etc. For the purpose of this paper an example of ADR mission for which RAMS analyses have been tailored will be provided:

An Active Debris Removal mission consist of a servicer that has to perform capture of an uncooperative object (target) and bring it into a lower orbit in order to dispose it in a timeframe that is in accordance with the SDMR [22]. Such a mission is highly complex and risky due to potential collision with the target and/or generating more debris. Depending on the spacecraft composition and the altitude at which it operates, the RAMS process is rather complex and complete. FTA analysis is critical in this case as the main interest is to assess if any of the combinations of failures may lead to the top feared events. For ADR missions, catastrophic/critical (with high safety risk) consequences can be identified as FE: collision and debris generation, impossibility of controlling the stack (servicer and target), impossibility to actuate accordingly the capture mechanism (depending on the type – robotic arm, magnetic plate, etc.) and other. The maintainability analysis would not be needed, however it is to be noted that parameters of maintainability are needed for the availability analysis. It is interesting to note that there are other close proximity operations types of missions for which maintainability analysis would be needed, such as for In-Orbit Servicing (i.e. servicer performing

DOI: 10.13009/EUCASS2022-7330

maintenance/repair/refuelling on a spacecraft). Thus, the RAMS analyses that are typically followed for such a mission are provided can be seen in the following table:

Analysis	Performed	Not Performed	Partially Performed	Justification
		System level		
FEA	X			
FTA	X			Performed because of high risk of collision during close proximity operations (CPO).
FMEA/FMECA	X			
HSIA	X			
FDIR analysis & concept	X			
Reliability prediction	X			
Availability prediction	X			Mainly required for the critical phases (i.e. rendezvous, capture, etc.)
Maintainability analysis		X		Applicable only to ground systems and systems for which humans can intervene. Some maintainability parameters are still required for the availability analysis (mean downtime)
SDMR	X			All SDMR requirements would need to be demonstrated [22, 23] as an ADR mission would have to orbit in the protected region (i.e. area where objects are not naturally compliant with the 25 years requirement on natural decay and re-entry) if it aims at disposing a debris
Safety (in orbit) part of mission analysis	X			Similar to mission analysis and collision probability computation
Contingency analysis	X			
RAM CIL	X			
Safety/Hazard analysis	X			
Safety Submission	X			
Safety Data Package	X			
Safety CIL	X			
		Subsystem or lower level		
FMEA/FMECA	X			
FDIR concept	X			
FTA	X			
Common-cause analysis	X			
HSIA	X			Typically performed at system level, however sometimes can be performed at lower levels - On-Board Computer (OBC)
Reliability prediction	X			
PSA	X			
PSM	X			
PCM	X			
WCA	X			
Availability analysis	X			
RAM CIL	X			
Hazard Analysis	X			Generally input for system level
Safety CIL	X			

Table 2 ADR RAMS analyses

DOI: 10.13009/EUCASS2022-7330

ADR RAMS system level (example of RAMS map):

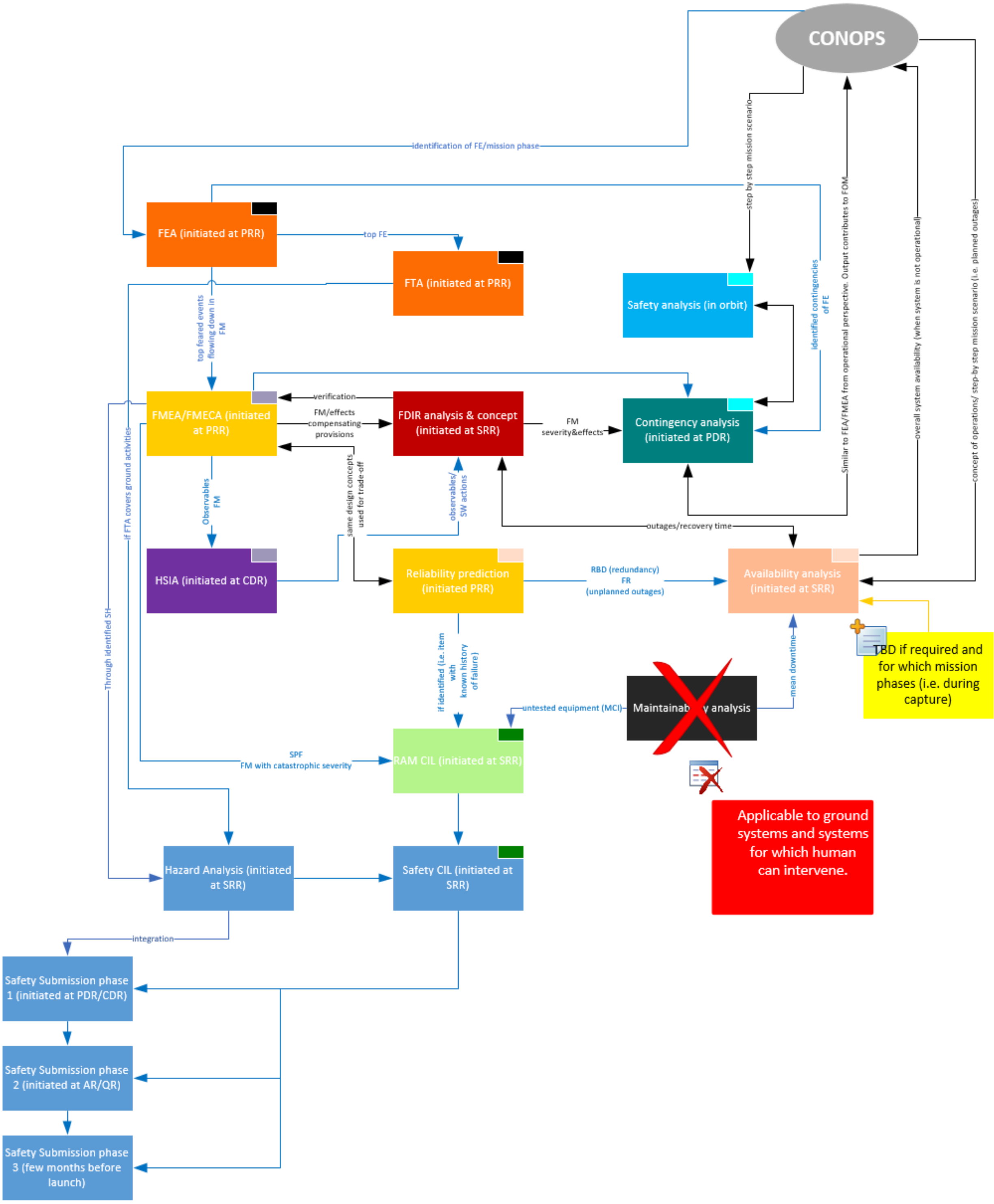


Figure 6 ADR RAMS system level

DOI: 10.13009/EUCASS2022-7330

ADR RAMS subsystem level (example of RAMS map):

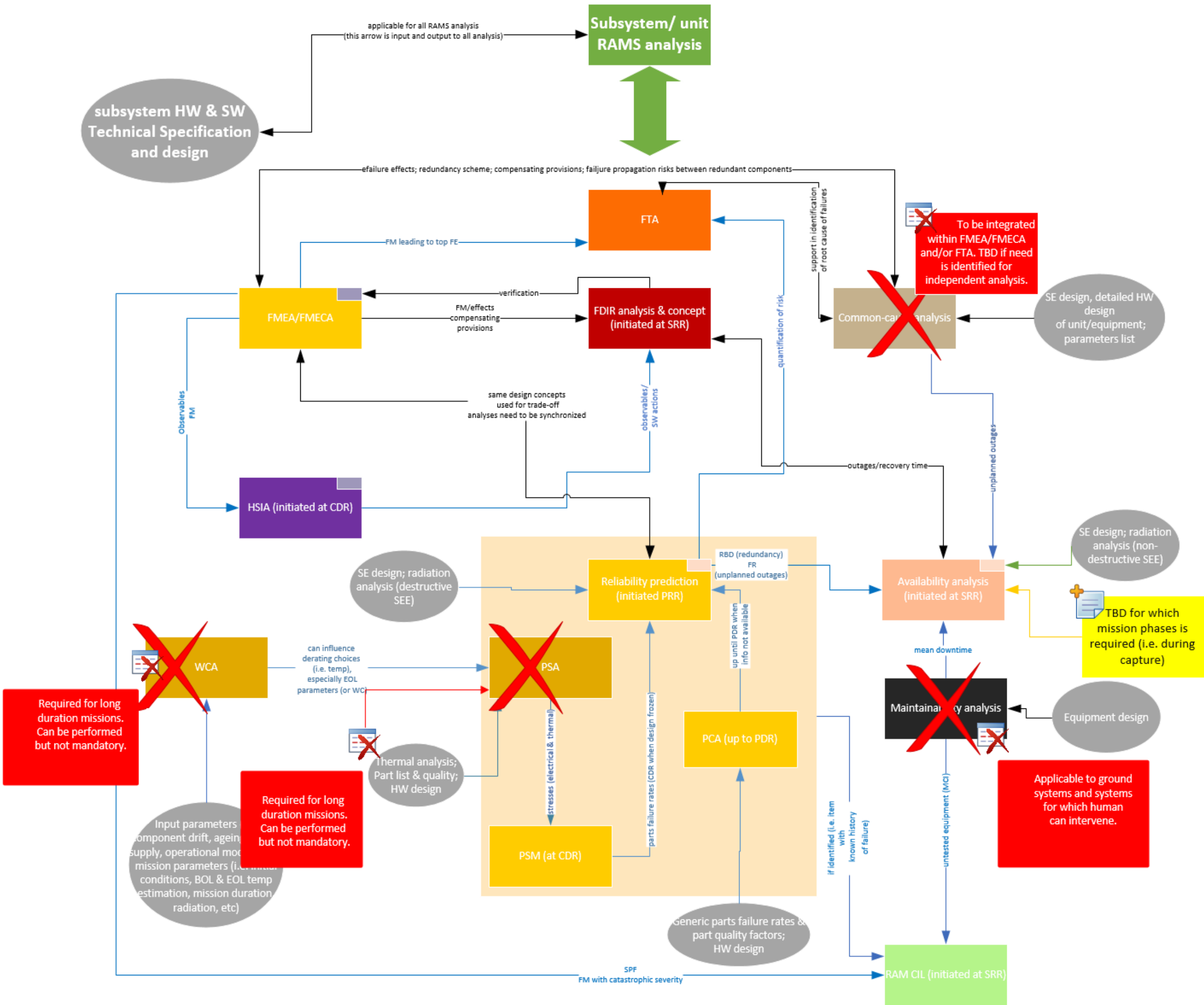


Figure 7 ADR RAMS subsystem level

5. Conclusions

The RAMS discipline could be referred to as the bridge between System engineering and FDIR. There are challenges associated with RAMS analyses, in particular as it is a transversal discipline, and the RAMS Map presented in this paper aims at clarifying relationship between disciplines in interface and also the phasing of the analyses. However, RAMS analyses remain the main tools to identify and mitigate potential technical risks that could affect mission objectives to an acceptable level for the mission. The overall goal is to quantify those risks based on the outcomes of RAMS analyses combined with expert judgment and heritage and identify and implement mitigations that are meant to prevent the risks from happening. RAMS analyses are crucial for safety-critical missions in which a failure may lead to collision and generation of debris and as such, the proper performance of these analyses can lead to a more sustainable space if performed properly. Moreover, it is to be noted that RAMS analyses contribute to space sustainability indirectly, through their use for decision making between if the lifetime and mission duration of a conventional mission (e.g. earth observation, telecommunications, navigation, etc.) should be extended, or it would be advisable, based on the new predicted reliability, to decide for disposal.
This paper aimed at providing an introduction to RAMS with the purpose of showing the importance and complexity of this discipline is, especially for CPO missions, in order to ensure space sustainability. The paper also provided a detailed description of what it is expected from each RAMS analyses both in a generic manner but also with regards to CPO and highlighted through tables and diagrams the main differences between generic approach and the approach adopted for safety-critical missions such as CPO. Another objective of the paper was to explain the different interactions between various fields with RAMS but also between various RAMS analyses and this was done through the RAMS Map. The RAMS Map represents a complex diagram that explains various dependencies between different

DOI: 10.13009/EUCASS2022-7330

analyses and engineering fields that are used for space missions, mainly targeting spacecraft, and for this particular paper, CPO missions. The RAMS Map presents the ways in which various analyses should be used and what output of each analyses serves as input for other analyses, thus it can provide valuable information on how to perform RAMS in an effective and fruitful manner, especially when tailored per type of mission. Another positive aspect of the RAMS Map is that it can provide a view on various hierarchical levels of implementation, from system to subsystem and/or lower levels (not presented in this paper), showing what should be performed at each level.

6. References

References must be numbered in the text in the following style [3] and listed at the end of the paper in the following way.

[1]	Rudolph Frederick Stapelberg, Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design, 2009, Springer (DOI 10.1007/978-1-84800-175-6)
[2]	Military Handbook – Reliability prediction of electronic equipment, MIL-HDBK-217F Notice 2, 2 December 1991
[3]	Dr. David J. Smith, Reliability maintainability and risk – Practical methods for engineers, Sixth edition 2001, Butterworth-Heinemann
[4]	Marvin Rausand, Arnljot Hoyland, System Reliability Theory Models and Statistical Methods, second edition 2004, Wiley
[5]	Quality management and quality assurance – vocabulary ISO 8402:1994 - withdrawn, definitions now used from IEC 60050-192, International electrotechnical vocabulary — Part 192: Dependability
[6]	BS 4778-3.1:1991 – Quality vocabulary, availability, reliability and maintainability terms. Guide to concepts and related definitions
[7]	MIL-STD-882D , Department of Defense Standard Practice, 10 February 2000
[8]	IEC60300-1:2014 – Dependability management – Part 1: Guidance for management and applications
[9]	J.C. Laprie, Dependability: Basic Concepts and Terminology, 1992, Springer
[10]	European Cooperation for Space Standardization, Glossary of terms ECSS-S-ST-00-01C, ECSS Secretariat, ESA-ESTEC, 10 October 2012, Noordwijk, The Netherlands
[11]	Fides Group, Reliability Methodology for Electronic Systems, FIDES guide 2009, Edition A, September 2010
[12]	NSWC-11, Reliability prediction handbook for mechanical equipment, logistics, technology support, May 2011
[13]	IEC 610251 edition 2.0 Fault Tree Analysis (FTA) International Standard, 2006, IEC Geneva Switzerland
[14]	European Cooperation for Space Standardization, Space product assurance, Fault Tree Analysis – Adoption notice ECSS/IEC 61025 ECSS-Q-ST-40-12C, ECSS Secretariat, ESA-ESTEC, 6 March 2009, Noordwijk, The Netherlands
[15]	NUREG-0492 Fault Tree Handbook, U.S. Nuclear Regulatory Comission, 1981
[16]	European Cooperation for Space Standardization, Space product assurance, Dependability ECSS-Q-ST-30C, ECSS Secretariat, ESA-ESTEC, 15 February 2017, Noordwijk, The Netherlands
[17]	European Cooperation for Space Standardization, Space product assurance, Failure modes, effects (and criticality) analysis (FMEA/FMECA) ECSS-Q-ST-30-02C, ECSS Secretariat, ESA-ESTEC, 6 March 2009, Noordwijk, The Netherlands
[18]	European Cooperation for Space Standardization, Space product assurance, Safety ECSS-Q-ST-40C, ECSS Secretariat, ESA-ESTEC, 6 March 2009, Noordwijk, The Netherlands
[19]	European Cooperation for Space Standardization, Space product assurance, Hazard Analysis ECSS-Q-ST-40-02C, ECSS Secretariat, ESA-ESTEC, 15 November 2008, Noordwijk, The Netherlands
[20]	SAVOIR FDIR Handbook issue 2, ESA ESTEC, 01/11/2019
[21]	European Cooperation for Space Standardization, Space product assurance, Availability analysis ECSS-Q-ST-30-09C, ECSS Secretariat, ESA-ESTEC, 31 July 2008, Noordwijk, The Netherlands
[22]	ISO 24113 Second Edition, Space Systems – Space debris mitigation requirements, 2011-05-15.
[23]	European Cooperation for Space Standardization, Space sustainability, Adoption notice of ISO 24113: Space Systems – Space debris mitigation requirements ECSS-U-AS-10C Rev.1, ECSS Secretariat, ESA-ESTEC, 3 December 2019, Noordwijk, The Netherlands
[24]	European Cooperation for Space Standardization, Space project management, project planning and implementation ECSS-M-ST-10C Rev 1, ECSS Secretariat, ESA-ESTEC, 6 March 2009, Noordwijk, The Netherlands