Analiza pozdanosti uređaja za servisnu inspekciju vanjskog zavara vakuumske posude

Delaš, Josipa

UNIVERSITY OF ZAGREB
FACULTY OF MECHANICAL ENGINEERING AND NAVAL ARCHITECTURE

MASTER'S THESIS

Josipa Delaš

Zagreb, 2019.

UNIVERSITY OF ZAGREB
FACULTY OF MECHANICAL ENGINEERING AND NAVAL ARCHITECTURE

MASTER'S THESIS

Mentor:

Doc. dr. sc. Stanko Škec, mag. ing.

Student:

Josipa Delaš

Zagreb, 2019.

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgement, the work presented is entirely my own, made by using the knowledge obtained during my undergraduate and graduate studies.

Acknowledgments

Foremost, I would like to express my deepest gratitude and thanks to my thesis supervisor, Doc. dr. sc Stanko Škec, for the guidance, support, encouragement and suggestions he generously offered not only during work on this thesis but also throughout a major part of my undergraduate studies and the entire graduate studies. I am grateful for Your valuable advice, patience and long discussions. Most importantly, thank You for showing me what kind of an engineer I want to be and helping me become one. I could not have imagined having a better advisor and mentor.

Secondly, I would like to thank PhD Pierre-Adrien Itty for granting me the opportunity to write this thesis in collaboration with the company INETEC, as well as numerous INETEC employees who have provided valuable data without which this thesis wouldn't be possible.

Further, my very special thanks goes to my parents, Eva and Marko, to my brother, Mate, and to my sisters, Marija and Nikolina. You have been there for me my entire life, helping and guiding me and always wishing me all the happiness in the world.

My enormous thanks goes to Tajana for being next to me every step of the way and sharing troubles that nobody else could have. Tajana, thank you for your understanding, the long discussions we had over and over again and moral support, especially in the final period of thesis writing.

I would also like to extend my gratitude to my very dear group of friends, penzići. Thank you for every test you got so we could practice together, every coffee break, every seat saved, and for all the fun we had together in the last five years.

And last, but not least...My enormous thanks goes to my boyfriend Dominik. During my studies and especially during the period of thesis work, you showed me unconditional support, encouragement and patience. Thank you for always believing in me, especially when I didn't believe in myself. For the past four years, you have been an amazing listener and amazing friend.

Josipa Delaš

SVEUČILIŠTE U ZAGREBU
FAKULTET STROJARSTVA I BRODOGRADNJE
Središnje povjerenstvo za završne i diplomske ispite
Povjerenstvo za diplomske ispite studija strojarstva za smjerove:
procesno-energetski, konstrukcijski, brodostrojarski i inženjersko modeliranje i računalne simulacije

Sveučilište u Zagrebu Fakultet strojarstva i brodogradnje	
Datum	Prilog
Klasa:	
Ur. broj:	

DIPLOMSKI ZADATAK

Student: **Josipa Delaš** Mat. br.: 0035199554

Naslov rada na hrvatskom jeziku: **Analiza pouzdanosti uređaja za servisnu inspekciju vanjskog zavara vakuumske posude**

Naslov rada na engleskom jeziku: **Reliability analysis of in-service inspection device for vacuum vessel outer field weld**

Opis zadatka:

Analiza pouzdanosti se provodi u okviru razvojnog procesa s ciljem identifikacije, analize i kontrole tehničkih rizika te je nužna za osiguravanje uspješnog razvoja visokokvalitetnih proizvoda. RAMI (*eng. Reliability, Availability, Maintainability, and Inspectability*) analiza predstavlja jedan od najčešće implementiranih postupaka za analizu tehničkih rizika koji bi mogli utjecati ili uzrokovati neispravan rad proučavanog sustava. Iz tog razloga, provodi se kontinuirano i iterativno tijekom cijelog razvojnog procesa, s posebnim naglaskom na ranije faze razvoja s ciljem lakšeg uvođenja korektivnih radnji za smanjenje ili potpuno uklanjanje rizika i pratećih uzroka. U ovom radu potrebno je provesti analizu pouzdanosti koncepcijskih rješenja uređaja za servisnu inspekciju vanjskog zavara vakuumske posude koji se razvija za potrebe sustava ITER.

U radu je potrebno:
- Pregledati stručnu i znanstvenu literaturu vezanu uz metode za analizu pouzdanosti i identifikaciju tehničkih rizika.
- Detaljno opisati postupak provođenja analize pouzdanosti korištenjem RAMI pristupa.
- Prikupiti podatke vezane uz pogreške i kvarove u radu sastavnih dijelova, sklopova i podsustava uređaja te ih povezati s identificiranim funkcijama.
- Provesti RBD (*eng. Reliability Block Diagram*) i FMECA (*eng. Failure Modes, Effects and Criticality Analysis*) analize te prikazati rezultate u standardno predviđenom formatu.
- Usporediti sa sličnim pristupima pronađenim u literaturi i praksi te iznijeti zaključke.
- Interpretirati rezultate analize te predložiti moguća unaprjeđenja konstrukcije uređaja.

Opseg analize i interpretacije rezultata dogovorit će se tijekom izrade rada.

U radu navesti korištenu literaturu i eventualno dobivenu pomoć.

Zadatak zadan:	Datum predaje rada:	Predviđeni datum obrane:
2. svibnja 2019.	4. srpnja 2019.	10., 11. i 12. srpnja 2019.

Zadatak zadao: Predsjednica Povjerenstva:

Doc. dr. sc. Stanko Škec Prof. dr. sc. Tanja Jurčević Lulić

CONTENT

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF SYMBOLS AND UNITS

Latin symbols

Symbol	Unit	Description
A	-	Availability
B_{10}	MioCyc	Statistically expected value for the number of cycles at which 10% of the components have failed dangerously
B_{10d}	MioCyc	Statistically expected value for the number of cycles at which 10% of the components have failed dangerously
MTBF	h	Mean time between failures
n_{op}	-	Number of operating cycles
t	h	Time
R	-	Reliability

Greek symbols

Symbol	Unit	Description
β	-	Shape parameter
γ	h	Location parameter
η	-	Scale parameter
λ	1/h	Number of operating cycles

TABLE OF ABBREVIATIONS

Abbreviation	Description
D	Detection
EP	Equatorial port
ET	Eddy current testing
ETA	Event tree analysis
FFIP	Functional failure identification and propagation
FMEA	Failure mode and effects analysis
FMECA	Failure mode, effects and criticality analysis
FMETA	Failure mode and effect tree analysis
FTA	Fault tree analysis
ICAM	Integrated computer aided manufacturing
IDEF0	Integration definition for function modelling
ISI	In-service inspection
LTM	Long-term maintenance
MECE	Mutually exclusive collectively exhaustive
MTBF	Mean time between failures
MTTR	Mean time to repair
O	Occurrence
RAMI	Reliability, availability, maintainability and inspectability
RBD	Reliability block diagrams
RPN	Risk priority number
S	Severity
UT	Ultrasonic testing
VV	Vacuum vessel
WP	Work package

SAŽETAK

Pouzdanost sustava je vjerojatnost da on izvršava funkcije za koje je predviđen u željenom razdoblju bez kvara i u predviđenoj okolini. Postoji mnoštvo metoda za povećanje pouzdanosti sustava kroz smanjenje tehničkih rizika. Pored metoda koje vrše direktnu analizu tehničkih rizika, postoje i tehnike za procjenu vjerojatnosti rizika. U ovom radu, primijenjena je RAMI (*engl.* reliability, availability, maintainability, inspectability) analiza, koju je definirala ITER organizacija a uključuje kombinaciju IDEF0 (*engl.* Integration definition for function modelling) funkcijsku analizu koja pruža osnovu za provedbu FMECA-e (*engl.* Failure mode, effects and criticality analysis) kao analize tehničkih rizika i RBD analize (*engl*. reliability block diagrams) kao tehnike za procjenu vjerojatnosti rizika. Prvo je proučena zbog upoznavanja sa prednostima i nedostacima ovih metoda, ali i drugih koje nisu primijenjene u radu, u svrhu postizanja boljih rezultata i točne primjene metoda. Nakon toga, u radu je opisana primjena RAMI analize na uređaju za servisnu inspekciju, koji trenutno razvija tvrtka INETEC. Uređaj za servisnu inspekciju se kreće po tračnicama koje su pričvršćene na vanjsku stranu vakuumske posude ITER tokamaka kako bi ispitivao obližnje zavare. Prilikom provedbe analize, poseban naglasak je stavljen na pravilnu dekompoziciju funkcija uređaja i formulaciju IDEF0 funkcijskog modela. Sljedeći korak analize je FMECA u kojoj su definirani mogući načini otkazivanja definiranih funkcija, te pripadajući uzroci i učinci, na temelju prijašnjeg iskustva tvrtke. Prijašnje iskustvo i stručna prosudba su pomogli i pri kvantificiranju ozbiljnosti i učestalosti učinaka i uzroka načina otkazivanja. Posljednji korak je provedba RBD analize za koju su korištene vrijednosti iz FMECA tablice i dekompozicija prikazana u IDEF0 funkcijskoj analizi. FMECA analizom, na temelju vrijednosti kritičnosti, otkrivena su 2 velika rizika, 57 srednjih i 40 malih rizika. RBD analizom dobivena je vrijednost pouzdanosti od 0% nakon 8 sati i dostupnosti od 16,5%. Otkriveno je da na učestalost najveći utjecaj imaju softverske i operatorske greške, a na ozbiljnost, greške koje propagiraju kroz uređaj, poglavito vezane uz tok zraka, vode i struje. Na kraju je izvršena usporedba dobivenih rezultata sa drugim pristupima pronađenih u literaturi i predložene su radnje za smanjenje rizika, odnosno povećanje pouzdanosti i dostupnosti sustava, prema rezultatima opisanih analiza. U daljnjem radu, preporuča se prikupljanje veće količine informacija vezanih u pouzdanost sličnih sustava.

Ključne riječi: RAMI analiza, pouzdanost, ITER, FMECA, RBD

SUMMARY

Reliability is the probability that the system will perform its required functions for desired periods of time without failure, in a specified environment. There are many methods aimed at increasing systems reliability through mitigation of technical risks. Next to methods for direct technical risk analysis, there are also probabilistic risk assessment techniques. In this paper, RAMI (Reliability, availability, maintainability, inspectability) analysis, which was devised by the ITER Organization as a combination of IDEF0 (Integration definition for function modelling) functional analysis to provide the basis for FMECA (Failure mode, effects and criticality analysis) as technical risk analysis and RBD (Reliability block diagrams) as a probabilistic assessment technique, is used. Literature was studied to examine the advantages and disadvantages of these methods, as well as others, to obtain the best possible results and ensure correct application. Afterwards, this paper presents the application of the RAMI analysis to in-service inspection device, which is currently being developed by the INETEC company. In-service inspection device travels inside rails fixed on the outer shell of the ITER tokamak's vacuum vessel in order to inspect adjacent welds. During application, great emphasis was placed on the correct decomposition of functions and formulation of IDEF0 functional model. Next step of the analysis was the FMECA which includes the definition of failure modes for said functions, as well as their causes and effects, based on the company's previous experience. Previous experience combined with expert judgment also helped in quantifying the severity and occurrence of effects and causes of failure modes, respectively. The last step is the RBD analysis which used values from FMECA as an input and the decomposition shown in IDEF0 functional analysis as its basis. FMECA analysis indicated, based on criticality values, 2 major risks, 57 medium and 40 minor risks. RBD analysis showed that the device's reliability achieves 0% after 8 hours and constant availability of 16,5%. The biggest impact on risks occurrence is due to software and operator errors, and on severity is from failures propagating throughout the device, these are mainly air, water and electricity failures. Lastly, a comparison between obtained results and other approaches found in literature was made, and risk mitigations actions were suggested according to the results of the analyses. For future work, more reliability data should be collected from similar systems to get a better reliability model of the device.

Key words: RAMI analysis, Reliability, ITER, FMECA, RBD

1 INTRODUCTION

An important part of the design process is the evaluation of the proposed solution principles during the conceptual design phase that supports correct decision making [1]. Decisions made during the conceptual design phase and its outcomes significantly impact major product characteristics such as performance, reliability and cost since they determine the overall product framework [2]. Since design details are not yet specified, this phase is characterized by uncertainty. If we accept that this uncertainty can lead to outcomes that can negatively affect the project, we are talking about risks [3]. Inadequate consideration of risks can result in cost overruns, time delays and wasted engineering effort. A single defect can cost up to 10 times more to rectify after initial distribution on the market than it would cost to diagnose and repair it early in design [4]. Therefore, reliability techniques should be used early in the design process to discover and remove potential risks that could lead to failures [4].

The initial approach for improving reliability in systems was the 'test and correct' principle. Possible causes of failures were mostly self-evident and resulted in design modification. Another way to reach high levels of reliability was to design extremely robust products that would maintain their performance regardless of possible variations and design parameters [5]. However, designers are becoming constrained by the cost and schedule pressures. This results in the need for advanced approaches to reliability assessment and collection of failure data to support prediction techniques. The experience of poor reliability during exploitation of military equipment throughout the 1940s and 1950s amplified the need for more formal methods of reliability engineering [4]. This gave rise to development of collection approaches of failure information from both the field and from the interpretation of test data. Subsequently, reliability prediction modelling techniques that use the failure information as an input have been developed [4]. Reliability prediction modelling is the process of calculating anticipated system reliability, availability and maintainability from component failure rates. These techniques provide a quantitative measure of how close a proposed design comes to meeting its design objectives and enables comparison between different design alternatives [4]. They include probability theory, reliability of series and parallel system configurations and redundancies.

In complex systems with long development cycles, design methods, reliability predictions during design, reviews and quality methods, as well as test strategies, are all subject to agreement and audit throughout the project [4]. Required reliability for these systems is of such

a high order that even zero failures in a foreseeable time frame are insufficient to demonstrate that the design objective of prolonged continuous operation has been met. In other words, zero failures in 10 equipment years prove very little when to achieve required reliability a mean time between failures of 100 years is needed. Example of such a complex system is ITER.

1.1 ITER

ITER is the first international experimental fusion device. It has to be a highly reliable, efficient and safe device built to produce a 500 MW of fusion power from 50MW of input heating power [6]. To achieve this, 35 nations are collaborating to build the world's largest tokamak (Figure 1), a magnetic fusion device that has been designed to prove the feasibility of fusion as a large-scale and carbon-free source of energy [6].

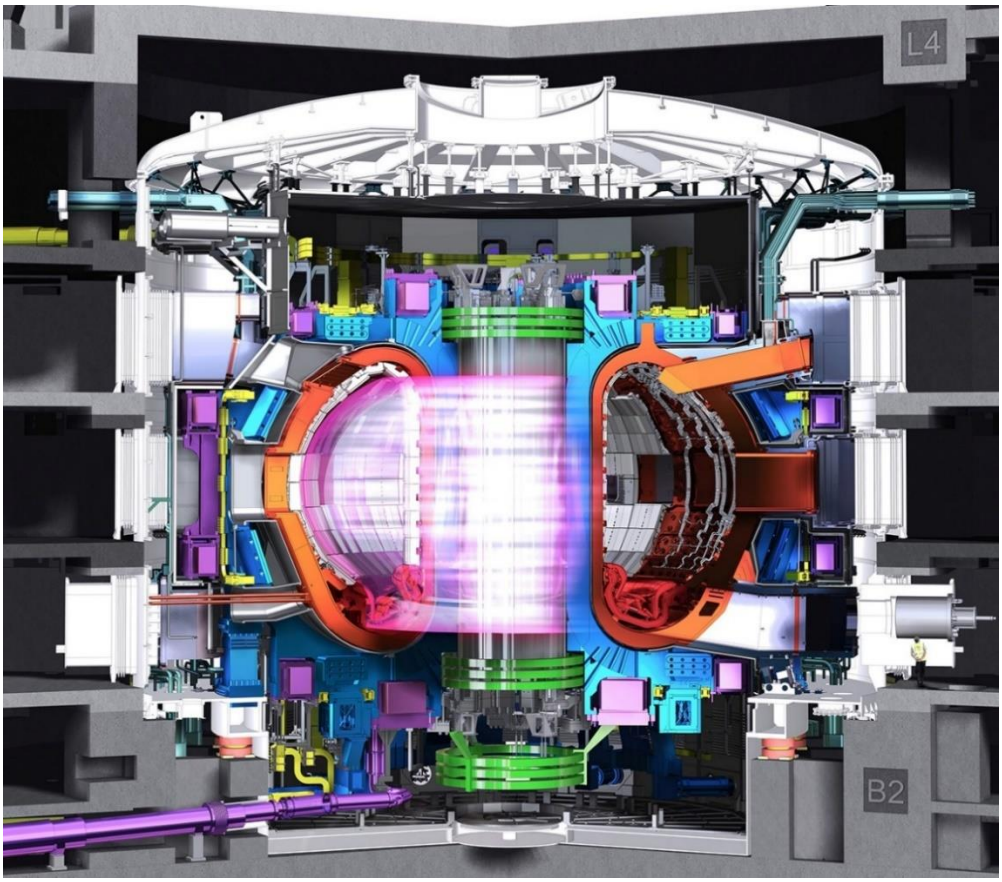


Figure 1: ITER tokamak

The energy produced through the fusion of atoms inside a tokamak is absorbed as heat in the walls of the vessel into manifolds. The fusion power plant will then use this heat to produce steam and then electricity by way of turbines and generators. The centre of a tokamak is a doughnut-shaped vacuum chamber named vacuum vessel and coloured orange in Figure 1. Inside, due to extreme heat and pressure, gaseous hydrogen fuel becomes plasma that enables

hydrogen atoms to fuse and yield energy. The charged particles of plasma can be shaped and controlled by the massive magnetic coils around the vessel, marked in blue and going through the centre of the tokamak [6]. The term "tokamak" itself comes from a Russian acronym that stands for toroidal chamber with magnetic coils.

Product's reliability decreases with number of components (product's complexity) [7]. The ITER tokamak is highly complex due to the sheer number of components, estimated to have over 1 million parts [6], and complex interconnectivity between them [8] which emphasizes the importance of ensuring high reliability of each system.. In addition to technical complexity, the variations in the project schedules from various suppliers that are working on similar parts or parts that interface with parts from other suppliers present an additional challenge. To tackle said problems, the components and their interfaces need to mature at the same pace [8]. It's an integrated approach that involves considering all the components inside the machine as a single system and supports a high degree of collaboration between design teams of major subsystems. In this approach, the designs of all the components are updated periodically. At each development stage, an assessment of how well the configuration works is performed based on feedback obtained from teams working in system development and manufacturing leading to subsequently adjusted designs. The process is, therefore, iterative and includes risk assessment as an essential contributor to design verification.

Various agencies and companies developing or dealing with complex products also recommend dividing projects into different phases [5]. Checkpoints are set after certain phases to review current design and decisions made in previous steps. Knowledge obtained from past phases and reviews are used to redirect the process by making new decisions that will guide the project to its goal [5]. Similarly, in the ITER system, developing a product is divided into three different phases conceptual, preliminary and final design, between which there are major design reviews. The most important parts of those reviews, design analyses and justifications as a part of design verification, must be sufficiently detailed so that a competent person in the subject matter can review and understand the content and verify the adequacy of the results without consulting with the originator [9]. Said phases of ITER product development also include technical risk control, and the requirements that result from it are an essential input in the specifications, design, testing, operation and maintenance of ITER systems [10]. The outputs of the technical risk control should guide designers and engineers towards the optimum system design and proper operation, testing and maintenance programmes [11]. Every ITER supplier that's developing a product for the system will follow the same guidelines for designing and

supply documentation in accordance with written procedures to ensure better communication for resolving interfaces. Despite the fulfilment of all these procedures and set requirements during designing, they cannot guarantee that the system will operate as planned during its entire lifetime. Therefore, suppliers need to provide a maintenance schedule as well as in-service inspection plan that will discover any expected and unexpected material defects and keep track of their propagation in order to prevent failures.

1.1.1 In-service inspection

In-service inspection is required according to the French Order for Nuclear Pressure Equipment [12] since the vacuum vessel as the central piece of the tokamak provides a high-quality vacuum for the plasma and the first containment barrier of radioactive materials [13]. Visual inspection and additional testing will be performed for periodic inspections every 40 months. High priority locations were selected based on VV stress analysis results. These include areas shown on Figure 2 the neck of the inter-modular key (a), triangular support (b), the lower inboard field joints and other components that require removal of the in-vessel components (c) (inter-modular keys, inner field weld and stub keys) [13]. Further on, on the outer side of the vacuum vessel shown in Figure 3, the lower port gussets (a), lip seal welds (b), gravity supports (c) and outer shell welds (d).

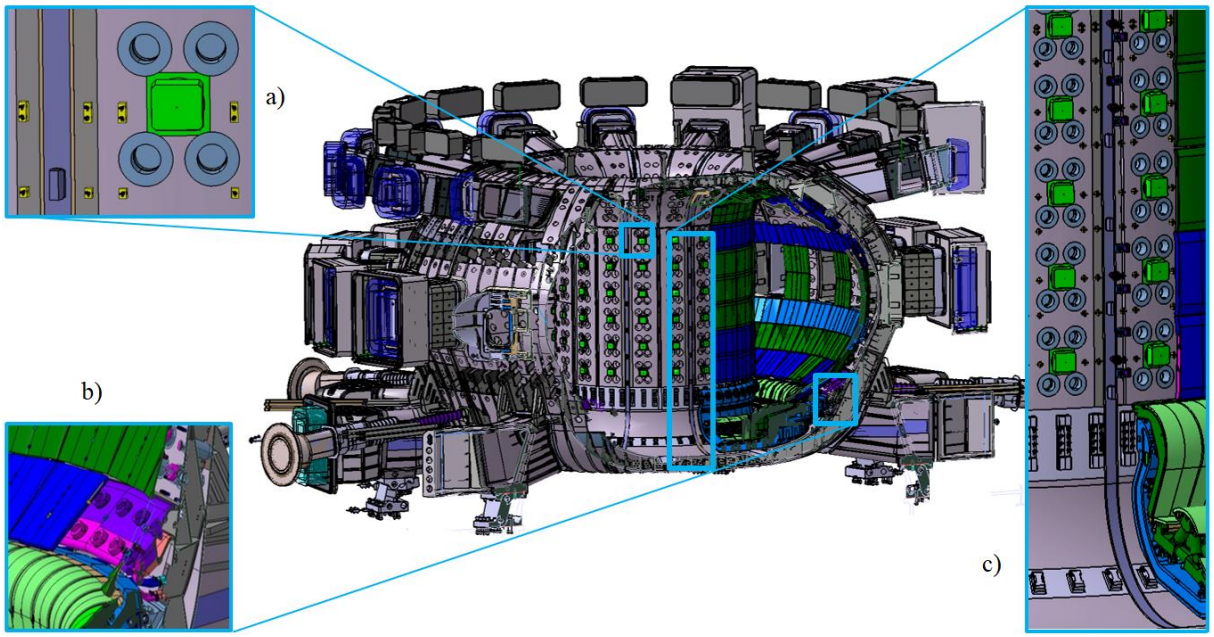


Figure 2: In-service inspection areas inside the vacuum vessel a) inter-modular key, b) triangular support, c) components that require removal of the in-vessel components

The subject of the analysis in this thesis is the outer field weld. Outer field weld consists of two narrow gap welds on each side of the splice plate marked in Figure 3 d) with an arrow. Splice plates are customized to accommodate dimensional differences that result from manufacturing and welding tolerances between the vacuum vessel sectors. Next to these two welds, there are circular flexible housing welds on both sides. All of these welds require visual, surface and volumetric examination to underline the evolution of manufacturing and welding defects or the emergence of new independent operational defects [14]. Manipulator, described in section 4, shall be capable of completing these tasks.

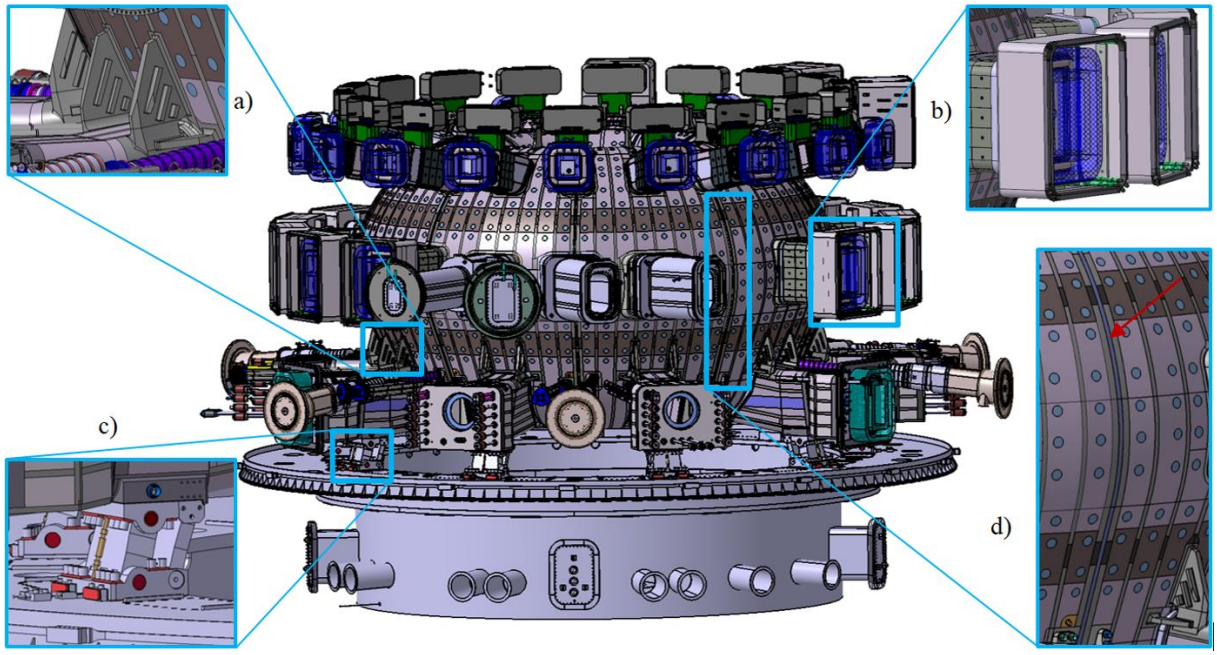


Figure 3: Vacuum vessel outer inspection areas: a) lower port gussets b) lip seal welds, c) gravity supports, d) outer field welds

2 RELIABILITY ENGINEERING

Reliability engineering provides the theoretical and practical tools to predict the probability of systems to perform their required functions for desired periods of time without failure, in a specified environment [7]. Risk refers to the probability of a particular event and the scale of its consequence [4]. We can conclude, from these definitions, that by mitigating risks, we increase the system's reliability. Reliability engineering is intended for studying which type of failures occur and at what time in operating life, collect required data and prepare reliability curves to predict component or system reliability. It also includes the study of the redundancy existing in the system, which indicates whether other elements can take over the function of the failed component, fully or partially [1]. Increasing the reliability in the system is a continuous effort. General guidelines for reliability engineering are as follows [7]:

1. Determine the desired reliability and maintainability that should be designed into the system and allocate the system's goals to its subsystems.
2. Obtain the required failure data and prepare reliability bathtub curves where the failure of the system is plotted versus its age.
3. Conduct Failure modes, effects and criticality analysis (FMECA) to identify which parts of the design should receive priority for redesign, research and development efforts. Study the consequences of failures to determine effects on adjacent parts, profits and human life.
4. Implement design improvement recommendations resulting from FMECA and other studies of failure. Apply general risk mitigation actions (i.e. redundancy, reduce the number of parts, improve quality control, etc.)
5. Predict system's reliability at each design stage.
6. Implement an effective field data collection, analysis, feedback and corrective action system to support future reliability predictions.

As indicated above, by analyzing failures we can indicate parts of the design where changes would be the most beneficial from the reliability point of view and estimate the required redundancy for achieving specified reliability [7]. Specified reliability defines the desired possibility of failure of the entire system in regards to the system's age. When collecting data, it is crucial to study the effects of age, mission duration, and application and operation stress

levels on reliability. Effects of age relate to the type of failure that the component manifests whose explanations are in the next section. Mission duration is period, usually with high reliability, after which we check the system to ensure it is in proper operating condition before it starts the next mission [7]. However, reliability decreases if the system operates for prolonged periods without interruption. Lastly, as the level of stress increases, failure rate in the early phase of the operation is higher, and the component's total life decreases. Failure data should be continuously collected so that design can be optimized in the future, and corrective actions can be taken substantially in advance of the failure occurring to mitigate potential risks. This data presents an input for various mathematical models to define reliability through individual component failure rates and make these reliability predictions as accurate as possible. These include the multiplication rule, the addition rule, the binomial theorem, Bayes theorem and redundancy rules [4]. The most basic calculation of reliability is as follows [4]:

$$R(t) = exp\left[-\int_0^t \lambda(t)dt\right] \tag{2.1}$$

where *R* depicts reliability, *t* time and $\lambda(t)$ failure rate in specified moment. Reliability methods affect a component or product in their entire lifecycle, from the conceptual phase to disposal, with prime emphasis at the design stage [7].

Aim of every reliable system is to accomplish no-failure performance, which is achieved when the working principle ensures continuous operation according to specifications [1]. This is why reliability theories focus on analyzing specific failure causes and failure distribution in time. From a distribution standpoint, we distinguish three types of failures: early failure, random failure, wear-out failure [7]. Early failures occur early in the operating life of a unit and are characterized by a decreasing failure rate with increasing age. Early failures are costly to correct so their causes should be eliminated with good quality control and worker diligence. These include poor manufacturing and assembly, poor quality control, insufficient burning in, substandard materials, parts failed in storage, etc. Random failures occur unexpectedly in time at irregular intervals. However, their failure rate observed over sufficiently long periods of operation is practically constant. They should be monitored closely to ensure that the achieved failure rate is equal to or less than the set goal and to update failure data and prediction models. Random failure causes are random fluctuations of stress exceeding the component strength, misapplication, human errors during usage and others. Wear-out failures occur mostly late in operating life and are characterized by an increasing failure rate with increasing age. Causes of such failures include wear of mechanical parts, fatigue, corrosion, age, etc.

Most, but not all parts and systems exhibit a failure rate distribution known as the bathtub curve shown in Figure 4 [4]. The reliability bathtub curve presents the sum of three separate overlapping failure distributions. During the burn-in period, usually random and early failures will occur. However, it is also possible for wear-out failures, such as corrosion due to moisture inside packaging, occur in this period. Similarly, during the wear-out period, which corresponds to the latter part of the curve, early failures may occur if the cause is defective material [7]. The middle portion, where failures are mostly random, is useful life [4]. Consequently, the bathtub curve may not look like the ideal one in Figure 4. Useful life is the best period in the life of the equipment, since the overall failure rate is constant and minimum, meaning that the exhibited reliability is at its highest [7]. Bathtub curve tells us about the type of failures we should expect depending on component's or system's operational time.

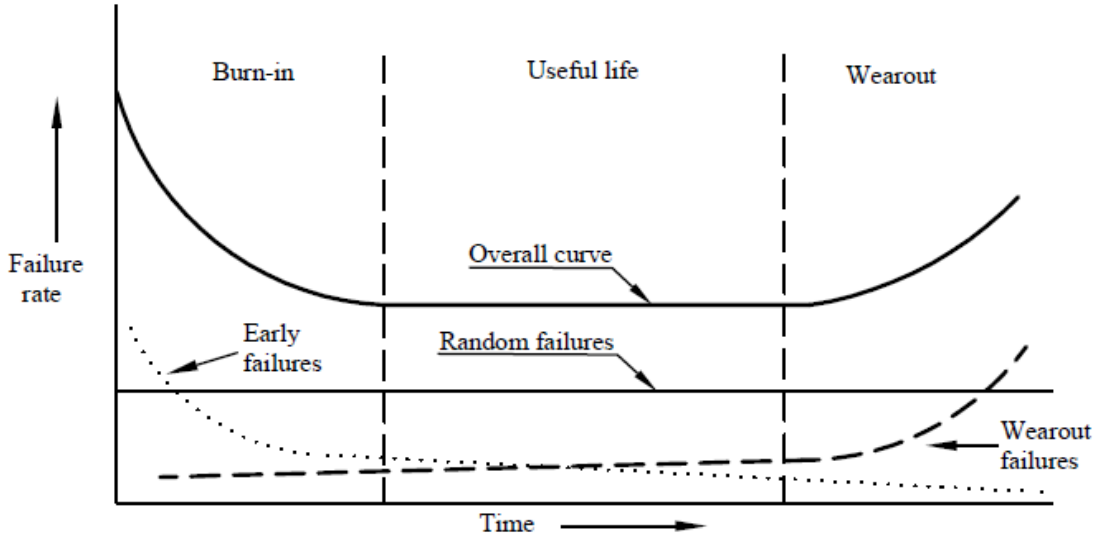


Figure 4: Bathtub curve [4]

Other than the bathtub curve, there are several different distributions for describing component's failure rate in regards to time [4]. The most important one being the Weibull distribution, which will be discussed later on. The aim of these distributions is to accurately depict component's life, meaning that the estimated occurring failures and their causes correspond to the ones occurring in the system [7]. An accurate portrayal of the system failure rates and associated failures enables better and faster risk prioritizing and, as a result, impactful corrective actions [7]. Failure analysis coupled with the determination of the failure type and cause and operational time at which the failure occurred support these efforts. However, in most applications, the failure rate is mostly assumed to be constant throughout the component's lifecycle [4]. This assumption does not diminish the importance of defining failure rates, even if they aren't exact.

2.1 Overview of methods and techniques for increasing reliability

Reliability concepts and methodologies help assure the design that achieves specified reliability. One way to increase reliability is through the mitigation of technical risks, such as the likelihood of component failures and the effect of their failure on the system [3]. Unlike technical risks, project management risks (e.g. schedule and cost risks) will not be considered in this paper. Examples in the literature that deal with technical risks include Failure Mode and Effects Analysis (FMEA), that was used to analyze reliability and determine failure with major consequences of the water distribution system in [15], and Failure Modes, Effects and Criticality Analysis (FMECA) applied for the analysis and improvement of operational reliability of the aircraft equipment [16]. Probabilistic risk assessment techniques, also used for technical risks analysis, such as Fault Tree Analysis (FTA) made for fire and explosion of crude oil during gathering and transportation in [17], Event Tree Analysis (ETA) applied at a preliminary stage of the underwater tunnel excavation to identify potential risks [18] and Reliability Block Diagrams (RBD) for ensuring high reliability of mesh networks [19]. Further on, the application of mentioned methods is shortly explained along with associated advantages and disadvantages.

2.1.1 FMEA and FMECA

Failure mode and effects analysis (FMEA) is an analytical method for systematic identification of possible failures and the estimation of the related risks [1]. Failure mode refers to different events leading to the failure to satisfy a need [5] that represents function fulfilled up to its nominal performance. FMEA is a qualitative tool based on human judgement as a means of ranking risks and involves a direct analysis of failures and their consequences and causes. In an FMEA, the basic process consists of compiling lists of possible component failure modes, that includes all the ways in which a component may fail, gathered from descriptions of each part of the system, and then trying to infer the effects of those failures on the rest of the system [20]. In addition to failure modes and its effects, FMEA also includes causes, possible actions to affect them and metrics for their evaluation, namely severity occurrence and detection. Potential effect of failure is the consequence of its failure on the next higher design or system. In other words, effect refers to the propagation of failure, defined by failure mode, throughout the system. For instance, if a valve has a failure mode *failure to open*, then its effect might be *loss of air supply in the system*. The cause of a design failure mode is the design

deficiency that results in the failure mode. Design deficiencies are features of the design that are defective or prone to failures such as wrong geometry, incorrect material, sensitivity to the environment, design life shorter that service life, and so on [21]. Relationship between the failure mode and the respective causes is not linear or one-to-one, meaning that a single cause can lead to several failure modes. Metrics for evaluating failure modes and associated effects and causes are defined in continuation. Severity is a rating indicating the seriousness of the effect of the potential design failure mode and occurrence is the rating value corresponding to estimated number of failures that could occur due to a given cause [21]. Detection is the estimation of the probability that the failure can be detected before delivery [1]. Severity and occurrence combined with detection provide an overall estimate of risk. Product of these three values is called risk priority number (RPN) and it defines the priority of failure that needs to be tackled. RPN is used to rank potential failure modes. The goal of the FMEA is to reduce risks through a reduction of severity, occurrence and detection [21].

To perform FMEA, one needs to establish the appropriate form, that will contain all of the FMEA data. FMEA's form is not universal or standardized and should be customized according to company needs as the application progresses. Some generally accepted forms can be found in [21], one of which is pictured below (Figure 5). Type of data in defined FMEA firm includes design functions. The engineer defines design functions that correspond to the design's intent, purpose or goal. Designs functions are derived from customer needs but also include safety requirements and compliance with various regulations. They must be identified in detail through a concise, exact and easy to understand the statement [21]. They present a starting point for defining failure modes since failure can be thought of as the loss of a design function. Afterwards, effects and causes are considered for defined failure modes. Next step in standard FMEA procedures is the definition of the rating guidelines [21]. The rating guidelines are also not universal or standardised and are formulated with qualitative and quantitative definition. This results in numerical values that most commonly range from 1 to 10 coupled with short description next to each values to help assign it to a certain failure mode. Once values are assigned, we can calculate RPN and start mitigating risk according to their priority.

Design function	Potential failure mode	Potential effect(s) of failure	∇	SEV	Potential cause(s) of failure	OCC	Detection method	DET	RPN	Recommended action	Individual/ area responsible and completion date	Action results				
												Action taken	SEV	OCC	DET	RPN

Figure 5: FMEA form example [21]

FMEA can be extended to Failure mode, effects and criticality analysis (FMECA) by adding criticality analysis to produce limited quantitative outputs from failure data. FMECA's criticality analysis of the identified failure modes considers the severity and probability of occurrence of the failure modes, by multiplying them to obtain criticality value [21]. However, unlike FMEA, where severity and occurrence values are based on expert judgment, in FMECA, these values are based on actual failure and maintenance data. Determining criticality makes it possible to set more accurate priorities in the measures envisioned to reduce the risk levels.

FMEA is most effective when it is used in sessions with a diverse team and when the team members have experience with the operation of the machine [22]. On the other hand, since the majority of FMEA application stems from expert opinion, so if there is no expert opinion or collected data, FMEA conclusions might not be relevant. Further on, if we analyse new and complex system without the prior knowledge of its behaviour, it is difficult to start and maintain the focus on the most critical failures [22].

2.1.2 RBD

Reliability Block Diagrams (RBD) predict the reliability and availability of each of the system's main functions according to given operating conditions [11]. The RBD approach uses the functional breakdown as a basis, but concentrates on the reliability-wise relationships and represents them by linking the function blocks.

A bottom-up approach is used so there can be several diagrams to describe the multiple levels in the functional breakdown hierarchy. Each block represents a component or a function of the overall system or process that is represented by the RBD [4]. Input data for the function blocks consist of reliability, maintainability and operational parameters. Reliability parameters refer to failure rate distribution, and maintainability parameters include both corrective and scheduled tasks with their detailed descriptions. Maintainability parameters and repair times included in them have a significant impact on availability. Operation parameters refer to duty cycles, component age and number of equal components and their configuration, series or parallel [23]. In a series configuration, failure of a single block causes the failure of other block connected in the same series, whereas block connected in parallel does not affect the failure of other blocks. Parallel definition of a block that represents multiple components is an example of a redundancy arrangement. There are also k-out of–n configurations, where k out of n possible blocks mustn't fail in order for the system to not fail. Redundancy arrangements can also refer to various parallel or k-out of-n configurations, where blocks can fulfil each other's

functions partially and or completely in case of failure. A specific combination of arrangements for a concerned system represents its reliability configuration. Relating this input data to the system reliability is mathematical modelling [4] and will be explained later on. Software is used, due to the great amount of data, to calculate reliability and availability values according to set parameters and blocks configurations. It must be stressed that prediction methods such as this one do not provide a precise measure of reliability. The main benefit of reliability prediction of complex systems doesn't lie in the absolute value predicted but in the ability to test the effect of different repair times and different redundancy arrangements in the design configuration [4]. In other words, a separate RBD model should be made for each proposed design and simulation should be run for each of them. Simulation results, reliability and availability values, can be used to compare said design from their reliability aspect.

An RBD is used to analyze the reliability of a system with a fixed configuration. In some cases, however, a single, fixed configuration does not accurately represent the system's performance over the course of a mission. Aspects of the system may change over time, including the system's reliability configuration; the resources available to the system; or the failure, maintenance and/or throughput properties of its individual components [23]. Therefore, information in the RBDs should be updated during product development to accurately represent system's reliability.

The bathtub curve, explained in previous section, showed that failure rate distributions can involve increasing and decreasing failure rate, as well as random failures. On the one hand, integral from equation 2.1 defines these changes accurately but has a complex nature, and its integration has proven quite difficult. On the other hand, if we consider only random failures, the distribution can be presumed as constant and reliability can be simplified into [4]:

$$R(t) = e^{-\lambda t}, \tag{2.2}$$

but this distribution doesn't take into account all aspects of the failure rate and time relationship. Widely used distribution that has been proven in practice as sufficient for RBD calculations is called Weibull distribution [4]. This technique uses a three-parameter distribution so the reliability can be defined as follows:

$$R(t) = exp - \left(\frac{t-\gamma}{\eta}\right)^{\beta}, \tag{2.3}$$

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1} \tag{2.4}$$

where η is the scale parameter, t is duration and β is the shape parameter and determines whether the failure rate is increasing ($\beta > 1$), decreasing ($\beta < 1$) or the failures are random ($\beta = 1$). Third parameter, γ, is location parameter and it locates the distribution along the abscissa. When $\gamma = 0$ the distribution starts at $t = 0$ or at the origin. Three-parameter version is used only when the two-parameter version is inadequate, which is very rare. In two-parameter version $\gamma = 0$.

RBD is a graphical representation of the system that provides a view of the system close to the modeller, making it more readable and understandable than most other formats, such as FMEA [24]. However, compared to some other analyses, like Markov models and Monte Carlo simulations, RBD is less powerful and its results aren't as correct.

2.1.3 FTA and ETA

FTA and ETA are probability risk assessment techniques that attempt to model events that rarely occur [25]. Once such event occurs, the underlying systems are often changed so that the event cannot occur in the same way again. Fault and event trees are modelling tools used as a part of a quantitative analysis of the system [25]. Other semi-quantitative or qualitative analysis such as FMEA are usually performed in preparation of these more exact analyses. Both methodologies provide a figurative representation of a statement in Boolean logic.

Fault trees use the so-called backward logic. Given a particular failure of a system, called the top event, one analyses the component failures which contribute to the system failure [25]. Combinations of component faults that produce the top event are described using the Boolean operations *and*, *or* and *not* (Figure 6).

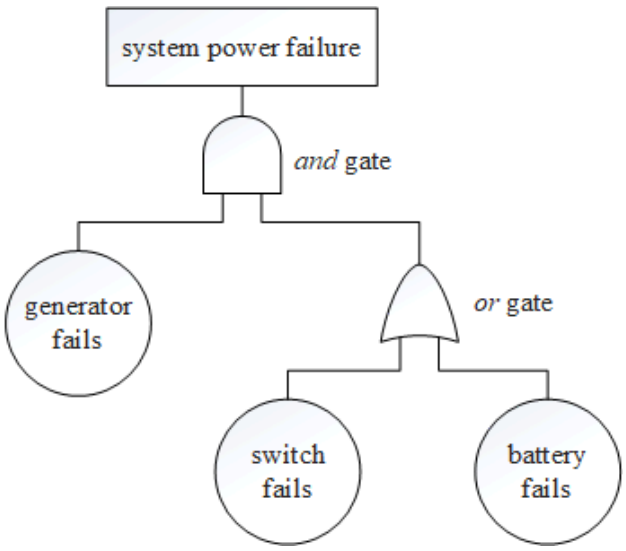


Figure 6: Fault tree example [25]

In fault tree analysis the aim is to develop a description of the occurrence of the top event in terms of occurrence of intermediate events. Intermediate events are also described further until, at the finest level of detail, the basic events are reached. Fault trees are however used together with reliability data for the basic events to make estimates of system reliability [25]. One disadvantage of the conventional FTA is that the basic events are associated with hardware failures only [20].

Event trees use the so-called forward logic. Initiating event (abnormal incident) is propagated through the system by considering all the possible ways in which it can affect the behaviour of the system and subsystems [25]. The nodes of an event tree represent possible functioning or malfunctioning of the subsystem. In other words, each node represents *or* Boolean operation. If a sufficient set of subsystem function normally then the system will return to normal operating conditions. An example of event tree is shown in Figure 7. If either of the safety systems functions normally, it will mitigate the initiating event and the system will return to normal operating conditions. Otherwise an accident occurs.

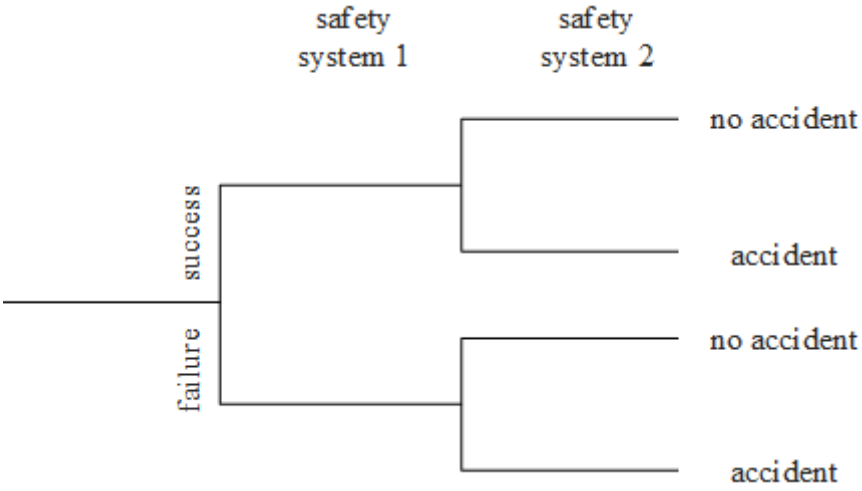


Figure 7: Event tree example [25]

Similar to RBD, advantages of FTA and ETA include its graphical and intuitive representation [17]. Further on, unlike the FMEA which requires expert judgment or statistical data, FTA and ETA are based on a logical analysis [26]. One of the disadvantages of these methods is that significant effort is required to conduct them. As a result, their application is limited to important areas and critical processes [1].

2.1.4 Functional approach

Functional and sequential dependency is important because failure might be caused by more than one mutually dependent event [20]. Sequential dependency refers to the part failures that often results from failure in the higher physical or functional domain of the part. This means that the functional breakdown can be used to track the propagation of failures. Failures of components at the level of the basic function lead to failure of the main function they are related to, and through this main function failure, a specific part or the whole operation of the system can be impacted [11]. However, methods like FMECA lack a description of the hierarchical analysis of physical parameters and functions [2]. In other words, it is difficult to identify the relationships between each part, which could help in identifying causes and effects.

Sequential dependency can be assessed with other methods like FTA. However, such methods usually require a defined system and available failure information. Probabilistic risk assessment methods, including RBDs, also require a lot of information since they are usually done with detailed, high-fidelity models that are not available during conceptual design. A functional model serves to show a design that achieves a given set of functional requirements [27]. Using functional approach can indicate relationships between components and subsystems in the early concept design phases. One such methodology that would analyse risk early on in mechatronic system was suggested in [28]. It is called the Functional failure identification and propagation (FFIP) analysis. In this analysis functional model is used as a basis for analysis of failures by defining failure as the degradation or loss of function.

Functional decompositions use the top-down approach which complements FMEA approach, as well as probability risk assessment methods, one of which is RBD. Even though FMEA isn't suitable for early design phases since it requires a detailed level of system design it can still be a valuable starting point. Failure modes are related to functions, meaning that the relations between functions in the model can be used to track propagation of failure modes allocated to these functions. Thus, functions can be used to develop relationships between future components and define their impact on the system early in the design process. FMEA and its failure modes can be updated as the design progresses but the relations between functions are known early so the effect of any newly added failure mode can be tracked throughout the system. This should reduce efforts and delays required for keeping the analysis consistent with the frequently changing design in the later stages [28].

Certain methodologies have arisen as a combination of the techniques mentioned above to overcome their individual disadvantages. Probabilistic risk assessment techniques are very structured and rely heavily on proper recognition of crucial system failures. Whereas, methods for analysing technical risks are unsuitable for new and complex systems since the failure behaviour is mostly unknown and maintaining the focus of the critical failures is difficult when there's a lack of experience [22]. Traditional practices use FMEA to determine some particular failure of a system, and then use FTA to refine it step by step [26]. Another example of combining methods is Failure Mode and Effect Tree Analysis (FMETA) which conducts system analysis with Axiomatic Design and risk analysis by integrating FMEA and FTA [2]. Axiomatic Design is suitable for reliability-based design [5] because its second axiom leads to the design with the minimum information content. FMEA can be used in combination with RBD to provide input failure data [4]. Another example of combining FMEA and RBD, as well as several other methods is the RAMI analysis.

2.2 Basic principles of RAMI analysis

The RAMI (Reliability, Availability, Maintainability and Inspectability) analysis handles technical risks that have an impact on the availability of the ITER machine operation. The RAMI analysis is devised by ITER Organization because of the need to ensure high availability of a very complex system. There are other examples in literature of similar approaches, such as RAMS – reliability, availability, maintainability and safety-integrity [4], but ITER is the first one to include inspectability and take the functional decomposition as such firm basis for other suggested methods. The RAMI analysis differs from methods suggested in previous sections mainly because it builds on the IDEF0 functional analysis and then combines some of the said methods, namely, FMECA and RBD, to utilize their advantages. The RAMI analysis and its outputs make it possible to have a better guarantee that a device meets the project requirements in terms of [11]:

- Reliability (continuity of correct operation) which emphasizes the scarcity of failures over an interval of time. RAMI approach considers that a function is either fulfilled up to its nominal performance or it is not fulfilled (function failure). In other words, it is important to define what must be fulfilled to make the system reliable.
- Availability (readiness for correct operation) as the probability that the device is in a state to perform a required function under given conditions at a given time assuming that the required resources are provided. The system can have poor availability due

to frequent failures and if the maintenance and repair times are long. Meaning that the availability depends on reliability and maintainability.

- Maintainability (ability to undergo repairs and modifications) as the probability that a given maintenance operation can be accomplished in a given time interval. Maintainability characteristics must be specified and incorporated during system design and concurrent with development.
- Inspectability (ability to undergo visits and controls) as a characteristic of maintainability with a preventive objective. It allows in situ monitoring of equipment performance.

These aspects are achieved through following the RAMI analysis, which begins at the design phase because corrective actions are still possible at this stage [11], mainly in terms of design changes, quality control, the definition of the maintenance frequency and the list of spare parts. The RAMI analysis consists of four major steps [11]:

1. IDEF0 functional analysis
2. Analysing Failure Mode, Effects and Criticality Analysis (FMECA)
3. Calculating reliability block diagrams (RBD)
4. Risk mitigation actions

The analysis should always start with a functional breakdown, based on IDEF0 approach, to set the basis for other methods and to provide insight into which functions affect each other. This is followed by FMECA that will identify possible failures and determine their priority for mitigation. RBD is afterwards used to calculate reliability and availability of specified configuration and enable comparison of these values to the predefined goal. Lastly, once weakness and possible failures in the design are recognized, actions are taken to remove and prevent them in order to decrease risks. These steps are implemented to check, that RAMI analyses of ITER systems are reaching their predefined goals for reliability and availability, throughout the project iteratively. Additional goals for RAMI analysis include providing input to logistic support functions (training requirements, spare part provisions, reliability-centred maintenance) and producing clear and validated documentation to reduce human error [11].

RAMI analysis has proved its worth while being used in ITER project in the past years. Example of good practice that show clear risk reduction includes RAMI analysis for ITER radial X-ray camera system [29]. This paper suggests conducting FMECA prior to RBD calculations and shows the application of such approach. By using this approach, failure data

collected and associated with functions in the FMECA table can serve as an input for RBD, as opposed to rough initial estimations of the failure information of functions directly. Similar approach was also used in preliminary RAMI analysis of DFLL TBS [30], where an important output of the analysis are the suggestions for the system's operation and maintenance plan, which includes the definition of spare parts. Further example of RAMI application is the failure mode analysis of preliminary design of ITER divertor impurity monitor [31] where RAMI analysis revealed that the equipment was lacking a certain design element, such as mirror cleanings, shutter mechanisms and piezo mechanisms. Paper on Korean HCCR TBS to be tested in ITER suggests that FMEA should start by preparing a full and detailed list of all components in the system wherever possible [32]. However, such approach isn't applicable early in the design phase of all products, and it does not comply to ITER suggested procedure.

3 METHODOLOGY

The methodology used in for this study consists of studying the literature, gathering information on failures and application of reliability methods. Literature was studied during the entire case study to gain better insight into reliability-based design and application of specific techniques defining and increasing product's reliability. At the very beginning, it was important to study ITER documentation and requirements set on the device in question to establish the context of the study and ensure the relevance of the analysis. Part of the studied documentation was the RAMI analysis program that defines which methods should be used to ensure the system's reliability and availability conform to ITER objectives. Once it was defined which methods should be applied and in what order, it was necessary to study said methods. This research included the study of other reliability techniques by showing their most significant strengths and weaknesses, based on when and how they should be applied as opposed to the ones used in the RAMI analysis. Comparison of the RAMI analysis to other reliability approaches also enables better understanding of defined methodology. As it was mentioned in the last section, RAMI analysis includes functional analysis, conducting FMEA and calculation of systems reliability with RBDs. An important aspect of conducting the analysis is gathering reliability information throughout the entire application. Lastly, risk mitigation actions are suggested for risks that were recognized by applying said methods. Application of the proposed procedure is shown in section 4.

Steps taken during the application of the RAMI analysis are shown in Figure 8. The first step of the analysis is the functional breakdown of the system. The RAMI approach primary concern is the functions that the product needs to fulfil rather than on physical components that execute them [33]. Advantage of the functional approach is to keep designers from choosing specific embodiment solutions before defining the system and component interaction [27]. Previous functional breakdowns the company made for similar devices were used as a reference. It is important to note that when a failure in the system occurs, the components are the ones behaving differently, not the functions. Therefore, once a sufficient functional breakdown has been achieved, the initial FMECA can be conducted. Afterwards, several iterations of FMECA and IDEF0 should be made to ensure consistency between function and failure modes related to them. Example of an FMEA from the company was used to analyse occurring failures in a similar system. FMECA should identify all failure modes for set

functions, provide a qualitative assessment as well as a quantitative assessment which should serve as an input for RBD diagrams. Functional breakdown structures from IDEF0 analysis form the basis from which the RBDs are derived [29]. Each block in the diagram represents a function of the system, and their configuration often matches the functional breakdown. RBD simulation results of systems availability and maintainability combined with FMECA criticality values should provide an insight into risk levels occurring in the device which is being analysed. Criticality values result from comprehensive research of failure data inside the company and from standard suppliers and handbooks.

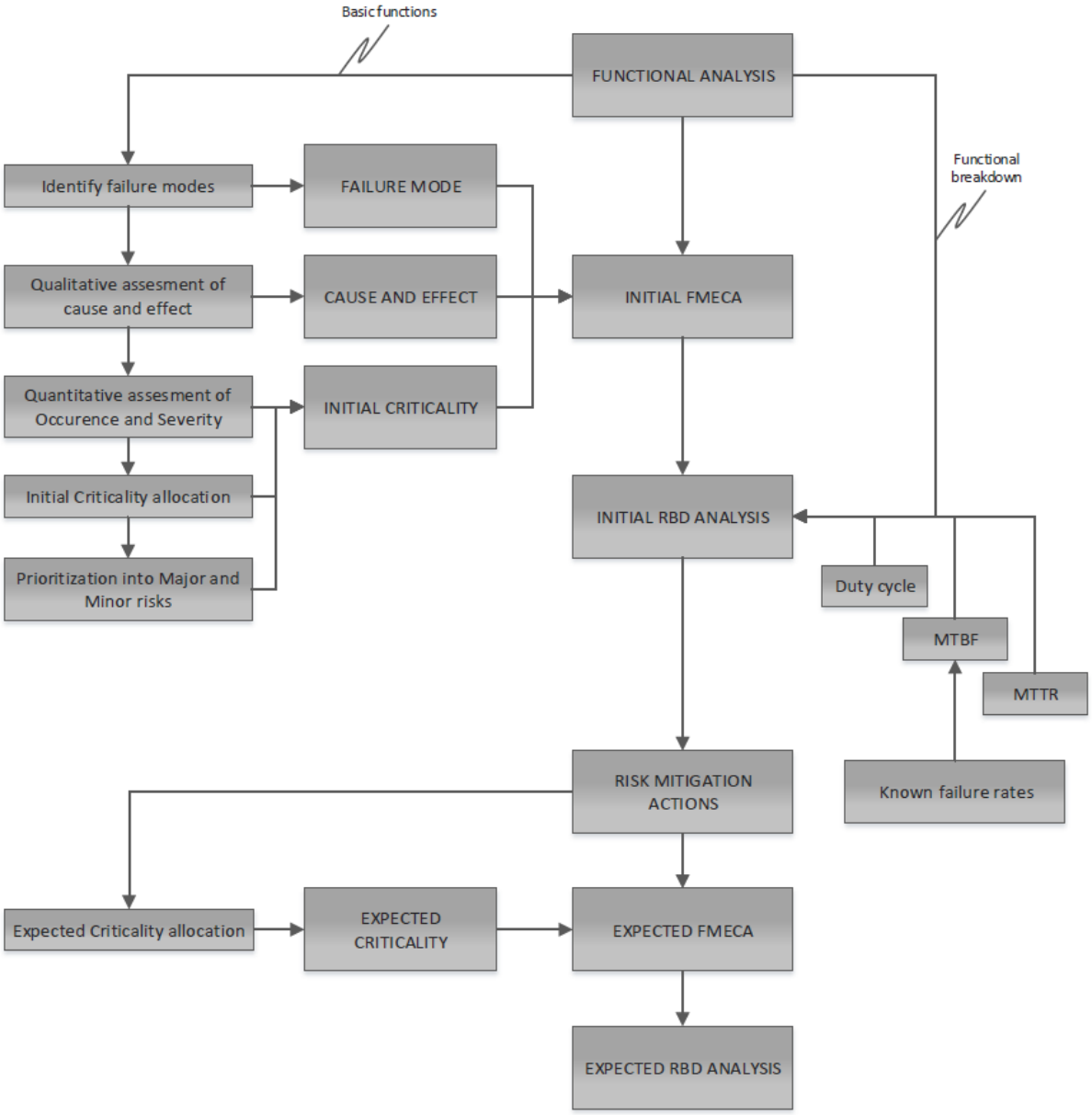


Figure 8: Diagram of RAMI analysis methodology

Afterwards, major risks can be further analysed, and risk mitigation strategies proposed. After risk mitigations actions have been applied, their impact on criticality values is evaluated to check their impact on the devices criticality values. FMECA and RBD can be evaluated again to assess how the system will behave if the proposed actions are conducted. Newly determined criticality values are put back into FMECA and subsequently RBD diagrams to obtain the system's, so-called, expected reliability and availability. Company's previous experience in risk management and design process with similar devices was used as input whenever applicable. If the values obtained from expected RBD analysis are satisfactory, suggested actions should be applied.

3.1 Functional Analysis

Requirements set on the device were compared with those on existing similar devices. Once it was ensured that they are similar, top-level functions that fulfil them were set as top-level functions for the device in this study. However, lower level function served only as a reference to help during decomposition. In RAMI analysis, reliability and availability are considered characteristics that are assigned to the functions of the system [10], with maintainability and inspectability being reflected in the availability [11]. To allocate targeted reliability and availability to each functions, the main functions were decomposed to intermediate and basic functions according to guidelines of the suggested method [Figure 9]. These guidelines defer from those in existing functional decompositions. Finally, intermediate functions were decomposed to basic functions that will be performed by components. During this top-down approach, the list of functions was continually compared to those in other decompositions in the company for similar systems, to ensure that none were overlooked. The procedure was also iterated several times in an effort to achieve mutually exclusive collectively exhaustive (MECE) relationship between upper-level and lower-level functions. Along with MECE, it was important to ensure that none of the basic functions (resulting from different upper-level functions) overlap. It is extremely important that none of the functions overlap to ensure that the following steps of RAMI analysis are performed on a solid and correct basis. In the end, additional effort was put into modelling the diagrams in terms of clarity and consistency between parent and child diagrams. Mistakes in defining functions, including having redundancies in the decomposition, made in this early phase could lead to whole parts of analysis being performed on wrong input data and, subsequently, inappropriate RAMI results and requirements [11]. Wrong input refers to using the same data in multiple blocks or ignoring

some data due to the poor function definition. Further on, wrong input data can mean that failure data was associated with wrong functions later on. The number of arrows was reduced to include only the most relevant ones. Diagrams and function tree were made in Microsoft Visio by using existing ITER template.

In the scope of the RAMI analysis, selected methodology for functional breakdown and representation is the IDEF0 (Integration Definition for Function Modelling) functional analysis [11]. IDEF0 was developed by U.S. Air Force Program for Integrated Computer Aided Manufacturing (ICAM) in the 1970s as a part of a series of techniques, to produce a function model. A function model is a structured representation of the functions, activities or processes within the modelled system or subject area. In the scope of this analysis, IDEF0 will be used strictly to model functions and activities [34]. For new systems, IDEF0 may be used first to define the requirements and specify the functions, and then to design an implementation that meets the requirements and performs the functions. For existing systems, IDEF0 can be used to analyse the functions the system performs and to record the mechanisms (means) by which these are done [34]. Both of these are important for ITER, since the RAMI analysis, and the IDEF0 functional breakdown as its essential part should be started early in the design phase and updated regularly as the system progresses.

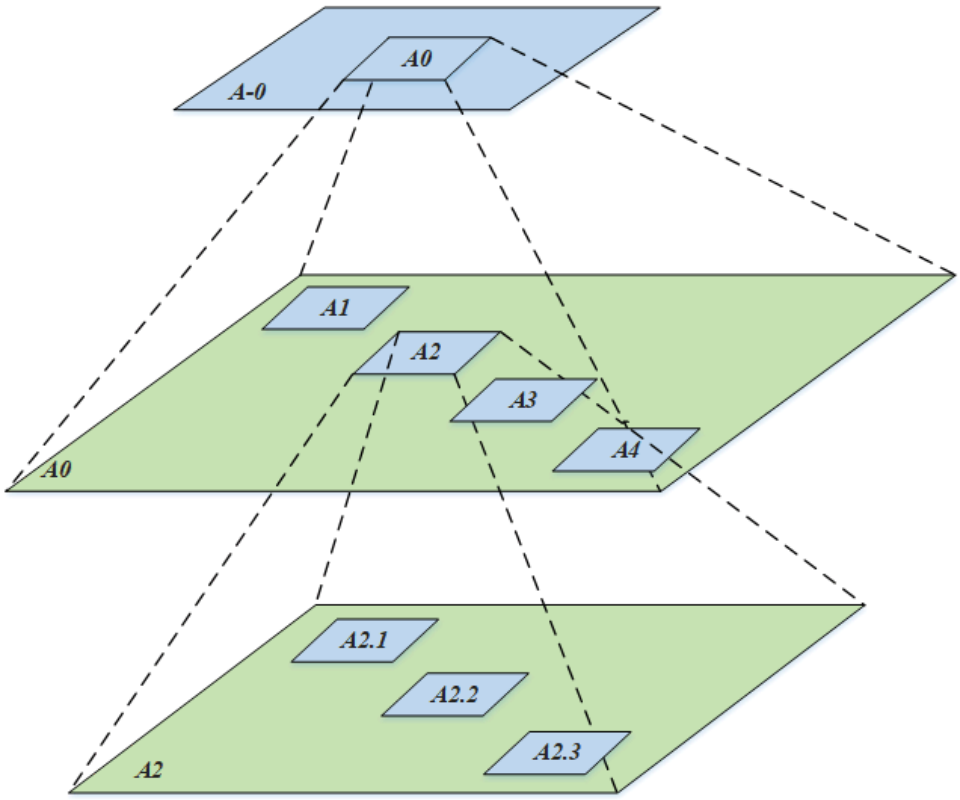


Figure 9: Multiple layers in the IDEF0 hierarchy of functions [11]

3.1.1 IDEF0 Syntax and semantics

The components of IDEF0 syntax are boxes and arrows, rules, and diagrams [34]. Boxes represent functions, defined as activities or transformations. Each box has a name and a number in the lower right corner to identify it. Name is an active verb or a verb phrase that describes the function. Arrows represent data or objects related to functions. An arrow is composed of one or more line segments that may be straight or curved (with a 90° arc), and may have branching configurations. Rules define how the components are used, and diagrams provide a format for depicting models both verbally and graphically.

Semantics refers to the meaning of syntactic components of a language and aids correctness of interpretation. Each side of the function box has a standard meaning in terms of box/arrow relationships [34]as shown on Figure 10. Arrows entering the left side of the box are inputs. Inputs are transformed or consumed by the function to produce outputs. Arrows entering the box on the top are controls. Controls specify the conditions required for the function to produce correct outputs. Arrows leaving the box on the right side are outputs. Outputs are the data or objects produced by the function. Arrows connected to the bottom side of the box represent mechanisms. Upward pointing arrows identify some of the means that support the execution of the function that can be inherited from the parent box. A "squiggle" is an element used to link an arrow with its associated label, for arrows that are too long for the arrow/label relationship to be obvious and for arrows that are between two functions.

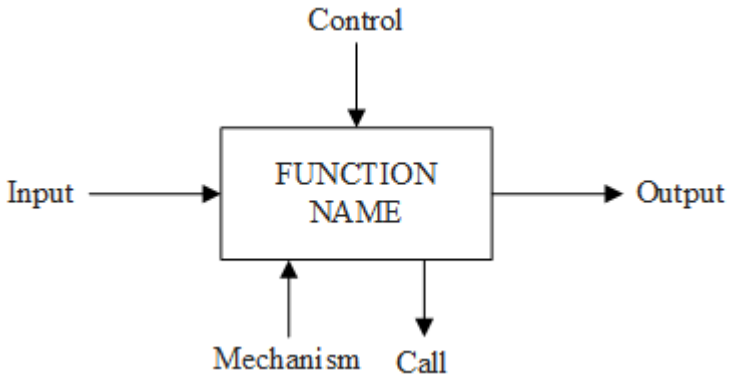


Figure 10: Arrow positions and roles [34]

Functions are decomposed into more detailed diagrams until basic functions have been reached. The context diagram in the model provides the most general or abstract description of the device represented by the model. The single highest-level function represented on the context diagram may be decomposed into its major sub-functions by creating its child diagram. Subsequently, each of these main functions may be decomposed, each creating another, lower-

level child diagram as already shown on Figure 9. At each level, diagrams, except for context diagram, should have from 3 to 6 boxes. There are numerous other rules that provide clarity of interpretation but aren't included in this paper to avoid needless longevity. Detailed overview of mentioned rules, as well as other, can be found in [34].

3.2 Gathering reliability information

Reliability information relevant for this analysis includes the definition of failure rates, their causes and effect and their connection to functions, as well as numerical data like failure rates, MTTR, MTBF, etc. Using past experiences and company archives can improve identification and analysis of possible failure rates due to better knowledge of the possible failures in similar devices [3]. Company provided an insight into frequently occurring failure modes in similar systems and estimations of failure rates that weren't otherwise available. Some failure data was obtained from company's standard suppliers, such as FESTO, LEMO, etc. There are also vast collections of failure data available in data handbooks or databanks, but they must be used with caution because some failure rate data includes items replaced in preventive maintenance, failure rates are affected by the design tolerances, environment in which the component is implemented may not match the one it was tested in, different failure modes are mixed together for the same failure rate value, and so on [4].

3.2.1 Company-based information

Information was obtained from the company by going through archives and interviewing employees. Archives included functional decompositions, FMEA report from the Forerunner project, inspection logs and spare parts lists from other projects, namely Forerunner, Aspira and Orca project.

Functional decompositions were used as a validation of the functional analysis, as was mentioned in section 3.1. Available functional decompositions are decomposed to a very low level and include redundancies. Because of this, it was not possible to use them directly for defining functions but they helped make sure that all of the functions were included in the IDEF0 functional decomposition.

FMEA report, from the company's Forerunner project, was used as a starting point for FMECA as it provided insight into failure modes occurring in a similar device. The Forerunner manipulator inspects the steam generator tubes with the eddy current technique. It can move between the pipes, that require inspection, on its own. The biggest difference is that the

Forerunner doesn't position probes on its own, another system called Usher pushes the probes in the pipes, and doesn't include ultrasonic testing. However, probes required for the ISI device in this paper are rather simple, and the mechanism for ensuring their contact with the surface should be simple too. Effects of the ultrasonic testing on the system's reliability haven't been completely taken into consideration due to the lack of information at this phase. In the FMEA failure modes are related to components, so the initial step was to recognize functions to which the components relate to and then to connect identified failure modes to IDEF0 functions. Severity, occurrence and detection rate values, from Forerunner FMEA, couldn't be reused, because the scale was defined differently and the FMECA requires quantitative data that includes failure rate or MTBF and MTTR.

Inspection logs and maintenance plans with spare parts lists were used as an indicator of failure frequency. They show how often the device malfunctions due to a specific component or how often a component requires replacement, respectively. At first, interviews were conducted with mechanical designers to discuss failure modes and recognized weaknesses of the design. Aforementioned was possible because designers in the company participate in the assembly and testing of the devices. They are also the ones putting together the spare parts list, based on their previous experience and feedback from inspections. Later on, interviews were also conducted with field operators to obtain additional information on failures as well as failure occurrence and detection value. These values were mostly an approximation made on their experience or calculations according to times specified in the inspection logs and maintenance plan. Despite this, they are still applicable to this device since the company uses standard components from the same manufacturers on all projects and because they follow specific guidelines for designing non-standard parts and have all products have a similar architecture. It is also important to note that field operators helped with understanding the inputs in the inspection log since the descriptions in them aren't always extensive.

3.2.2 Other failure data sources

Failure rate data was initially requested from manufacturers that the company usually works with. Some manufacturers provided data which was processed depending on the type of data provided (failure rate, mean time to failure, component life, etc.) in a way described in the next chapter. However, most of the manufacturers don't provide such data. Next step was obtaining failure rates from standard handbooks such as US Military Handbook 217F (MIL-HDBK-217f)[35] and Non-electronic parts reliability data (NPRD) [36]. There are other sources of

reliability data, but they are most pertinent to a specific industry. If there was no failure rate found for a certain failure mode, an estimation was made by experts in the company, based on previous experience of working with such parts. Since the device is still in the stage of preliminary design, functions are decided, but not all of the components are defined yet. Therefore, generic component information can be used in RBD analysis [31], and for the final design, the information will be updated once actual components are defined.

3.3 Failure mode, effects, and criticality analysis (FMECA)

Process of identifying causes and effects for defined failure modes was iterative, to ensure consistency and that all of them are on the same level of detail. It was mentioned before that FMECA should have a specified form to include all of the data in. For this reason, failure modes with associated causes and effects, as well as initial preventive and corrective actions, have been placed in an Excel spreadsheet (Figure 11). Preventive actions are conducted prior to the start of the operation to reduce the possibility of a failure occurring. Corrective actions are applied after the failure occurs in order to eliminate the effect of failure. Quantitative assessment was conducted by using information gathered, as explained in section 3.2. Failure information including severity (S), occurrence (O), detection (D), criticality (C) and risk priority number (RPN) values have been added to said spreadsheet next to associated failure modes.

Function				Failure mode		Possible causes		Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects
cont.	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	

Figure 11: FMECA table layout

Severity values were obtained from MTTR by comparing the severity rating scale meaning (MTTR) with its values (S) according to Table 1. MTTR was obtained strictly from a company expert's approximations. The occurrence was defined in two different ways. Either from failure rate (λ column) directly from Table 2, or from MTBF, approximated in the company or obtained from manufacturers, and replacement time that defines the frequency of preventive component replacement. λ from defines from where was associated failure rate value obtained. This identification is important for the follow up in later phases of the design since a supplier for a certain component might change, or there are newly collected failure data in the company. Detection was also an expert approximation. From S and O information in the table, bubble

plots were made to indicate major risks in a manner explained in the next section. Failure rate (λ column) information in the table was used as an input for blocks in the RBDs.

3.3.1 Qualitative analysis

In RAMI analysis both the functional breakdown and the failure data included in FMECA, namely failure rate and MTTR, will be used as an input for calculating reliability and availability with the RBDs [11]. FMECA starts with the identification of all the failure modes for basic functions defined in IDEF0 diagrams [11]. Failure mode analysis should include all possible failures, however improbable. They can be difficult to predict for new products, which is why some failure modes were taken from Forerunner FMEA. However, this wasn't sufficient since the device in this thesis has some unique features, and it works in a different environment. After these device-specific failure modes have been defined, they are validated by experts. Each basic function can have multiple failure modes. Once failure modes are defined and confirmed, all possible causes for them were defined. Several different causes can result in the same failure mode, and all of them need to be considered since the failure rate differs for them. Lastly, the results of failures due to specific causes were considered. These are called effects, and there can exist multiple effects resulting from the same cause. This procedure of defining failure modes and, subsequently, causes and effects are called qualitative assessment. Causes and effects are related to basic functions because of their association with specific failure modes. Nevertheless, it's important to determine the impact of causes and effects on the main functions of the device and the whole ITER tokamak. For each cause and effect preventive or corrective tasks should be suggested.

3.3.2 Quantitative analysis

The effects and causes are evaluated quantitatively using severity (S) and occurrence (O) rating scales as explained earlier. The product of severity and occurrence is criticality (C). Failure modes are often prioritized according to the risk priority number (RPN) which is the product of severity, occurrence and detection (D) [21]. However, RAMI approach generally doesn't necessarily include detection (it has been included in some reports, but isn't a part of the suggested procedure) and relies on criticality chart, with severity and occurrence as coordinates to highlight the major, medium and minor risks [11]. Bubble plots are used to highlight the distribution of the failure modes into three risk level zones. Major risks (red zone) have criticality value higher than 13 and risk reducing actions are required. For medium risks

(yellow zone) criticality is between 7 and 13 and risk reducing actions are only recommended. Minor risks (green zone) have criticality lower that 7 and corresponding actions are considered optional. Suggested actions aim to reduce risk by decreasing the occurrence of the cause of failure or the severity of the effects [11].

In the ITER project, the severity scale is defined by the time system will remain unavailable. This can be understood as mean time to repair (MTTR) and it consists of [4]:

- Access time – lasting from realization that a fault exists to commencing fault finding
- Diagnosis time – refers to fault finding, including time required to set up testing equipment and interpretation of gained information
- Spare part procurement – time required to take an accessible spare part
- Replacement time – removal of the faulty assembly, followed by connection and wiring of a replacement
- Checkout time – verifying that the fault no longer exists and the system is operational
- Alignment time – result of adjusting a new module or part into the system
- Logistic time – time consumed waiting for transportation of spares, test gear, additional tools and manpower

All aspects of the MTTR must be taken into consideration when defining severity value. If values are obtained from experts, they need to be informed about what is included in MTTR definition. Once MTTR has been defined, it can be translated to severity value according to the scale suggested in Table 1.

Table 1: IO-defined severity rating scale [11]

Value	Description	Meaning
1	Weak <1h	Unavailable less than 1 hour
2	Moderate<1d	Unavailable between 1 hour and 1 day
3	Serious <1w	Unavailable between 1 day and 1 week
4	Severe <2m	Unavailable between 1 week and 2 months
5	Critical <1y	Unavailable between 2 months and 1 year
6	Catastrophic >1y	Unavailable more than 1 year

ITER RAMI program has defined occurrence in terms of failure rate (λ). For constant failure rates, MTBF is the reciprocal of failure rate, so both of them have been shown to relate with occurrence value in the Table 2 below.

In complex engineering products and systems, system failure is not always attributable to the hardware failure of a component part [4]. Failures can occur due to human and environmental factors, combinations of component parameter tolerance, ambiguity in the specification and software elements, etc. Failures can be random hardware failures or system failures. System failures are failures at the system level, which cannot simply be described by reference to individual component failures [4]. In the scope of this thesis, system failures will refer to all other failures that prevent the system from further operation in accordance with specifications. Random hardware failures occurrence is easily approximated numerically by using failure rates, but mentioned systematic failures are difficult to quantify and cannot be predicted with traditional reliability modelling [4]. It was, therefore, necessary to rely on expert opinion for this data.

Table 2: IO-defined occurrence rating scale [11]

Value	Description	Meaning	
1	Very low	$\lambda_{risk} < 5e\text{-}4/y$	$\lambda_{risk} < 5.7e\text{-}8/y$
		MTBF > 2000 years	
2	Low	$5e\text{-}4/y < \lambda_{risk} < 5e\text{-}3/y$	$5.7e\text{-}8/y < \lambda_{risk} < 5.7e\text{-}7/y$
		200 years < MTBF < 2000 years	
3	Moderate	$5e\text{-}3/y < \lambda_{risk} < 5e\text{-}2/y$	$5.7e\text{-}7/y < \lambda_{risk} < 5.7e\text{-}6/y$
		20 years < MTBF < 200 years	
4	High	$5e\text{-}2/y < \lambda_{risk} < 5e\text{-}1/y$	$5.7e\text{-}6/y < \lambda_{risk} < 5.7e\text{-}5/y$
		2 years < MTBF < 20 years	
5	Very high	$5e\text{-}1/y < \lambda_{risk} < 5/y$	$5.7e\text{-}5/y < \lambda_{risk} < 5.7e\text{-}4/y$
		10 weeks < MTBF < 2 years	
6	Frequent	$\lambda_{risk} > 5/y$	$\lambda_{risk} > 5.7e\text{-}4/y$
		MTBF < 10 weeks	

3.4 Reliability Block Diagrams (RBD)

The RAMI approach for RBD uses the functional breakdown as a basis. Meaning that there will be multiple diagrams for lower levels that feed the calculated reliability to the higher level. Almost all of the failure modes will cause the system to fail because the partially fulfilled or unfulfilled function leads to a stop in device operation. When defining RBD diagrams, if one block failure causes system failure, configuration is called series. Since each block in the RBD presents a single basic function, most of the RBDs will be connected in series. There will be as many RBDs as there are main and intermediate functions, since all of the basic functions need to be taken into consideration. From this, we can conclude that the arrangement of the functions in the IDEF0 determines diagrams architecture severely and as a result has a significant impact on the RBD results.

Inputs for blocks required for calculations are MTTR and failure rate taken from FMECA. Even tough used software allows for various models of failure rate distribution, for the purposes of this analysis Weibull two-parameter distribution of failure rate, explained in chapter 2, will be used, mostly with shape parameter set to 1. Shape parameter set to 1 means that the failure rate is constant during component life. This distribution was used for other ITER systems, but it is also the most often used one in practice [4]. Failure rates are used for the calculation of reliability. For the calculation of availability, MTTR is also needed to determine the device's maintainability. Another input for both characteristics is the duty cycle, which defines the percentage of how much the component is in use compared to the total time in which the system is operational. There are marginal differences in specific component operational time, which makes the duty cycle less relevant, compared to other data. Possible exceptions will be stressed in the next chapter. *BlockSim* software calculates the reliability and availability of the system based on reliability, maintenance and operation data in blocks and the configuration of these blocks on each level of the decomposition.

3.4.1 RBD Syntax and semantics

Firstly, one must define what constitutes a system failure, since only then can it be determined which failure modes actually cause the system to fail [4]. If there are several different causes of system failures, so many predictions of the system's reliability are required because each system failure can result in different reliability. System is described as a number of functional blocks (functions taken from IDEF0 decomposition) which are interconnected

according to the effect of each failure on the overall system reliability. This refers to diagram configuration, which can be series, parallel, k-out of-n or a combination as explained in previous chapters. Each block contains reliability and maintenance values as well as other failure rate and operation information. Blocks can be connected in a series, where the failure of a single block causes the failure of all blocks in the same series, and in parallel (redundancy), where the failure of a single block is insufficient to cause system failure [4]. These configurations can be seen on Figure 12. As the complexity of the system increases it is possible to have combination of series and parallel and k-out of-n configuration wherein k number of blocks needs to fail to cause system failure.

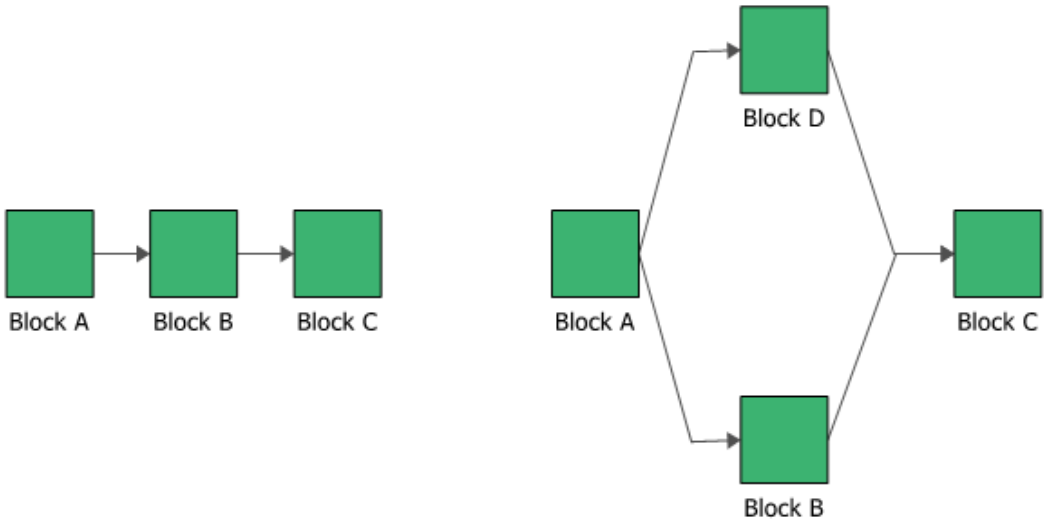


Figure 12: Series configuration (left) and parallel configuration (right) [23]

There are some additional general rules such as [4]: if the same function needs to be implemented multiple times, each block should represent the maximum number of those implementations in order to simplify the diagram, in those cases each function needs be defined as a whole number of blocks, block shouldn't contain any significant redundancy within, etc. Failure rates and MTTR which are the input for RBD calculations are provided by FMECA occurrence and severity values, respectively. If there are multiple failure modes for a single function, block will have a failure rate predicted from the sum of failure rates for given function on the FMECA worksheet [4]. In addition to this input data, duty cycle which specifies a component's usage in the concerned system (i.e. component does not operate continuously, subject to greater loads than those rated), is defined. Establishment of relations between block failure rates and the system reliability is done through mathematical modelling of failure rate. It was already explained in chapter 2, that there are many ways to model failure rate distribution. RBDs can be configured as analytical diagrams, which use the exact algebraic equation for the

system model, or a simulation diagram, which provides more modeling options and results but requires analysis with discrete event simulation [23]. In analytical diagrams, only the failure rate distribution model is relevant, and all maintenance information specified in the block is ignored during analysis. Maintenance information is ignored because it doesn't affect system's reliability, which is the output of analytical diagrams. In simulation diagrams, the failure rate distribution model, as well as maintenance tasks are relevant, meaning that all of the defined information in the blocks is considered during the simulation. Since all of the available information is considered, the output of simulation diagrams is the system's availability. Hence, both the analytical and simulation diagrams need to be used to obtain both reliability and availability values of the system. It is important that both of the diagrams have the same configuration of RBDs on all levels and that they have the same input data. The only thing that differentiates them is the processing of the data in the blocks.

4 APPLYING RAMI ANALYSIS TO IN-SERVICE INSPECTION DEVICE FOR VACUUM VESSEL OUTER FIELD WELD

To comply with regulations for nuclear equipment and to ensure ITER total availability and maintainability, it is necessary to inspect recognized critical parts of the vacuum vessel to keep track of predicted and possible failures and ensure their maintenance. For these operations, an eight-month scheduled downtime, including two months for preparatory activities for opening the vacuum vessel and getting the machine back online, will be allocated on average every two years as major shutdown (long-term maintenance state, LTM) [10]. In this LTM period, allocated time for the inspection of welds on vacuum vessel outer shell with the device described below is two weeks. However, the system should be able to conduct the planned inspection in under a week, and the second week will be used only if something unforeseeable happens and the device is unable to complete inspection in planned time.

The vacuum vessel comprises of nine sectors that are welded together sequentially. The connection between sector 3 and 4 is welded last. All of the manufacturing and welding deviations will be added up in this area. These dimensional differences are eliminated with customized splice plates produced and welded between said sectors. Weld on the outer side of the vacuum vessel, connecting splice plate with the sector, is called outer field weld. Outer field welds are located between the rails in Figure 13. In addition to these, the in-service inspection device should also inspect the welds in their immediate proximity. These include circular welds for flexible housings and poloidal T-rib welds. To enable access to these welds rails will be fixed on the outer wall of the vacuum vessel. Rails opening, marked on the left side of Figure 13, is outside of the cryostat, where the instruments and other necessary inspection equipment will be. The opening is shown in its closed state on the picture and cryostat is excluded for clarity of the picture. This is also the point where the operator inserts the device into the rails, and after which it will be controlled remotely.

The in-service inspection device is being developed by INETEC – Institute for nuclear technology. It needs to be capable of moving along the rails, lock its position for inspection of flexible housings, move the inspection devices into position for inspecting, adjust them to vacuum vessel surface and conduct inspection. The manipulator needs to be remotely operated, equipped with cameras for supervision and robust positioning assemblies. Concept of such manipulator can be seen in Figure 14.

To achieve above-mentioned operations, manipulator should have 5 degrees of freedom: moving along the rails, rotation of the entire arm, the tilt of the entire arm, the extension of the arm, sled rotation. The arm needs to be tilted to pass through bends and go over the rails. Extension of the arm is required for flexible housing and T-rib welds set at a varying distance from the rails. Inspection of T-rib and flexible housing welds requires certain degrees of freedom to be locked. It is also important to ensure proper cable management that will prevent cables from getting stuck or damaged. Another limitation of the system is the radiation of 5mSv/h. The amount itself is insignificant but, if the system operates for a long period of time, the accumulated dose can, damage electrical components, including cameras.

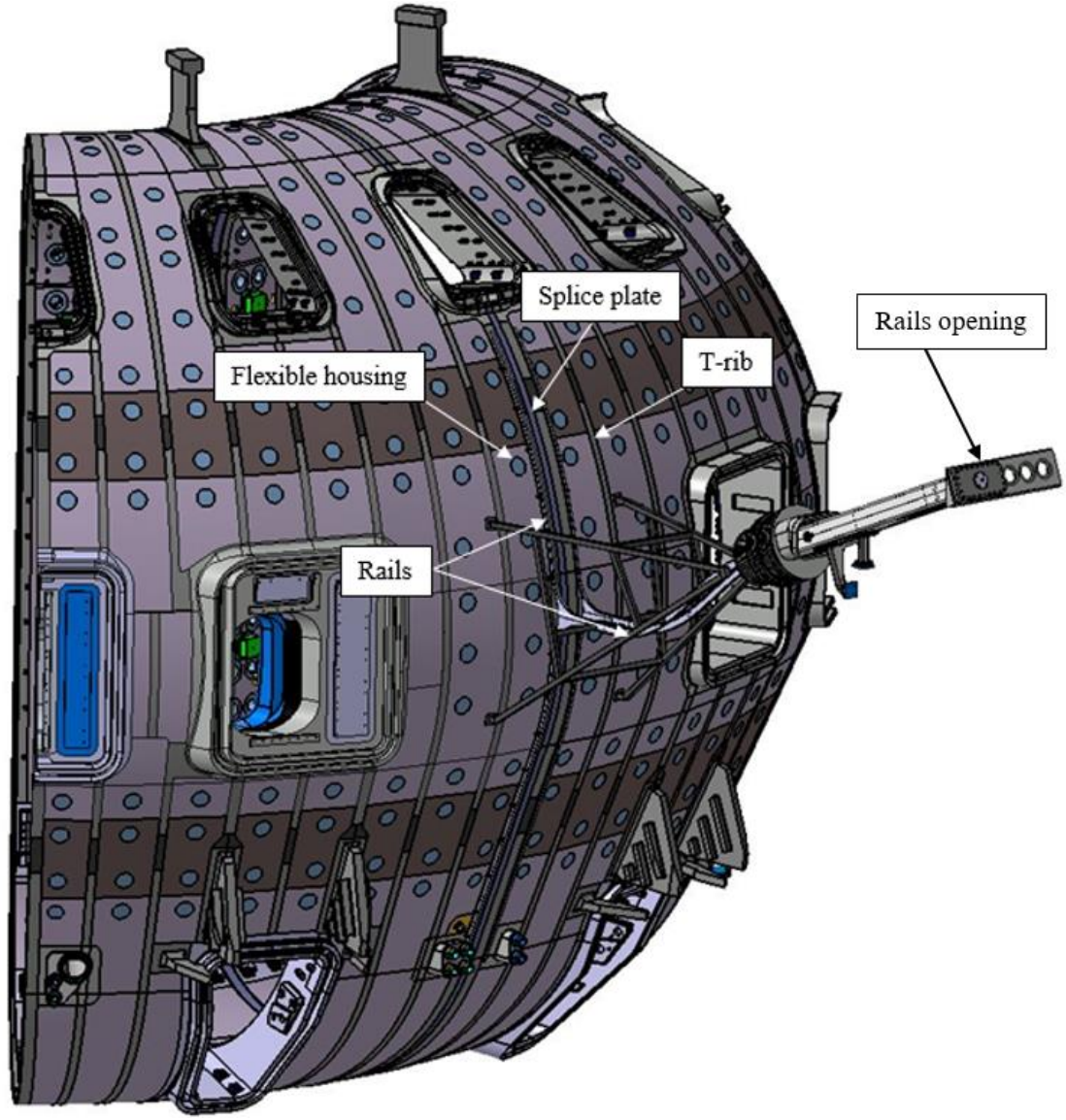


Figure 13: Outer connection of sector 3 and 4 of the vacuum vessel with rails

Apart from the manipulator, the system includes rescue equipment, instruments for inspection, control box and cable reel near the opening of the rails. Service equipment to enable maintenance and storage are in a different building, and operator control unit is 40 meters away in a safe area.

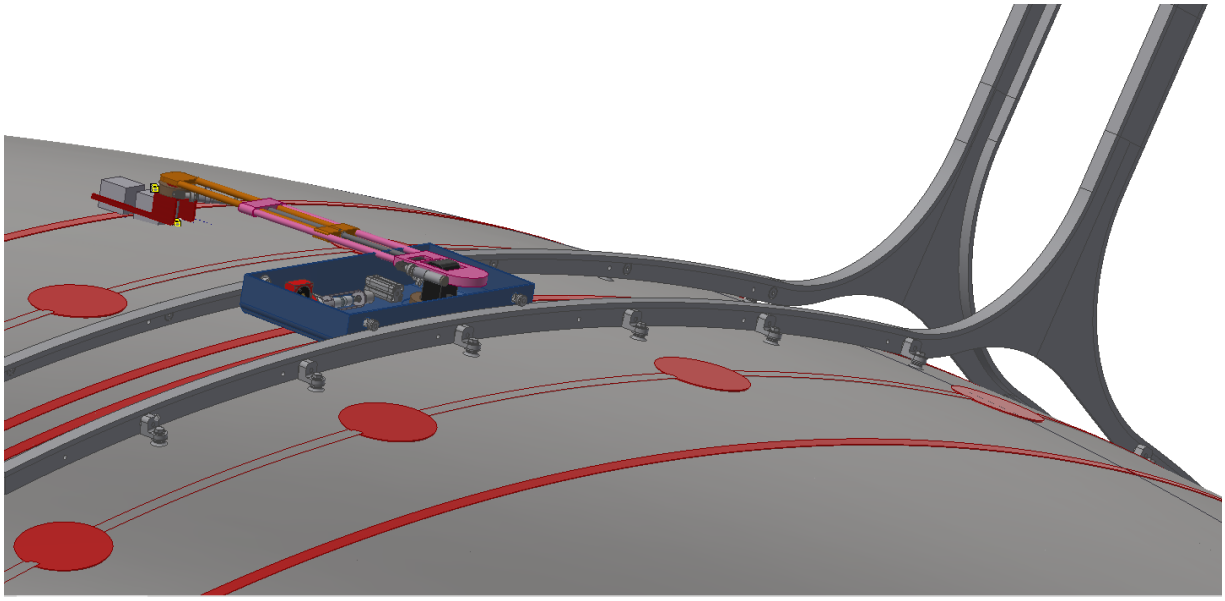


Figure 14: Concept of the manipulator in inspection area

Lastly, manipulator's dimensions are restricted by rails and the thermal shield marked in purple in Figure 15. Due to thermal shield oscillations, the maximum permissible height of the device is 120 mm. The cross-section also shows rails profile, the distance between two welds and distance from weld to rail, all of which present a problem for inspecting welds. Welds are inspected volumetrically with ultrasonic methods which require coupling fluid, visually with cameras and with Eddy current testing which is a technique for surface inspection.

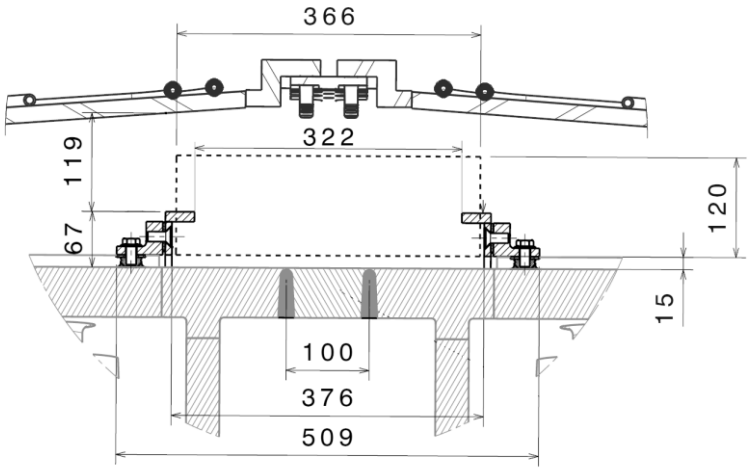


Figure 15: Cross-section of space reservation for the manipulator

In the current concept shown in Figure 16, moving along the rails, arm tilt, rotation and extension and sled rotation will be realized with electric motor drives and gear transmission, where required. Arm needs to extend due to the great distance between T-rib weld and the rails. Each of the degrees of freedom will have its position measured by an encoder. Pneumatic elements ensure contact between probes and surface. Pneumatic elements lock degrees of freedom in such a way that the loss of air unlocks them. Cable management and other design aspects, have yet to be decided and the radiation impact is reduced by excluding all possible electronic components from inside the device, by placing them in the control box.

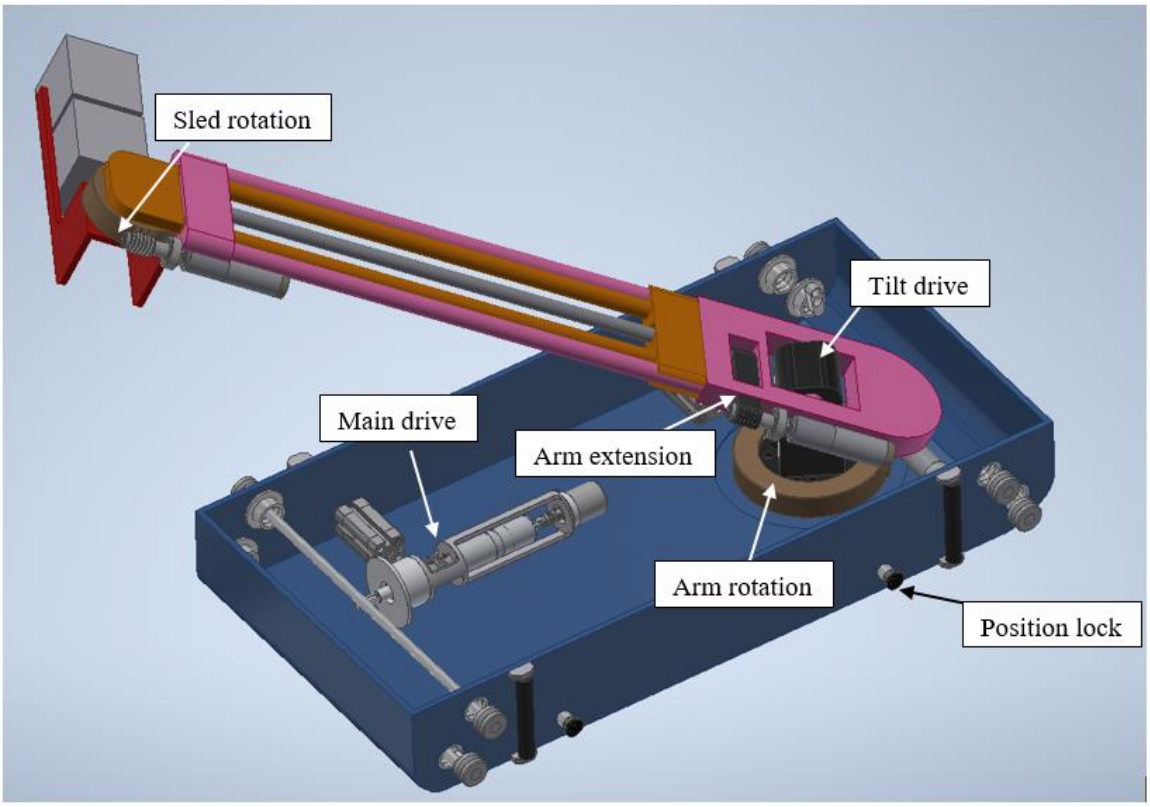


Figure 16: Conceptual representation of the ISI device

4.1 IDEF0 Functional Analysis

Four main functions were identified based on the requirements that the in-service inspection (ISI) equipment need to fulfil:

A1 To control

A2 To provide support functions for WP3/1 equipment

A3 To ensure positioning in inspection area

A4 To conduct visual, surface and volumetric inspection.

From these 4 main functions, 2 intermediate and 27 basic functions were decomposed. "To control" has 6 subfunctions referring to user interface, managing inspection procedures, system supervision and supply of electricity, air and water for the probes. "To provide support functions for WP3/1 equipment" includes rescue operations, maintenance and storage. Intermediate function "To enable rescue operations" (A2.1) is decomposed to 2 basic functions: "To activate fail safe mechanism" (A2.1.1) and "To enable manipulator extraction" (A2.2.2). Having only two subfunctions doesn't comply with the usual IDEF0 modelling procedure but, nevertheless, it was used to emphasize a two-step rescue procedure used for the manipulator. "To ensure positioning in inspection area" includes all functions necessary for manipulator and probe positioning. That makes 6 sub-functions, including intermediate function "To drive degree of freedom" (A3.3) which also consists of 6 subfunctions, in this case all basic functions. The last main function (A4) is decomposed into 6 basic functions which include recording with cameras and their lighting, scan with ET and UT probes and transfer of inspection data. In addition to these, A4 main function also includes "To prevent loss of coupling fluid" (A4.3), which is one of the most important functions since the system must prevent the leakage of the fluid during inspection. Function tree with all functions listed can be seen in Appendix A.

Figure 17 shows the representation of the top-level functions for the ISI device. The main inputs are VV welds that require inspection, desired operational parameters, manipulator ready for operation and energy sources. Outputs are inspected welds and inspection data, reaction forces, and successfully managed (stored, maintained, driven, rescued) manipulator. Colours are used to simplify diagram interpretation. Red signifies control regarding set parameters, green is also control but related to the device and equipment environment, blue is used for energy relations, brown for mechanisms located outside the inspection area, and purple for the ones in inspection area. Standard IDEF0 guidelines don't define the use of various colours for various connections. This approach and specific colour codes, namely red and green, are generally accepted for usage by ITER and can be found in existing functional analyses for various ITER systems.

We can see that the IDEF0 method is not only used for identifying functions but also to define the interactions between each of them. A good example is function *A1 - To control* setting operational parameters as the control for all the other main functions. Although only the main function level is shown, lower levels down to the basic functions have been established in a similar way and are available in Appendix A and include diagrams A1, A2, A2.1, A3, A3.3 and A4. Diagram label can be found in its lower left corner.

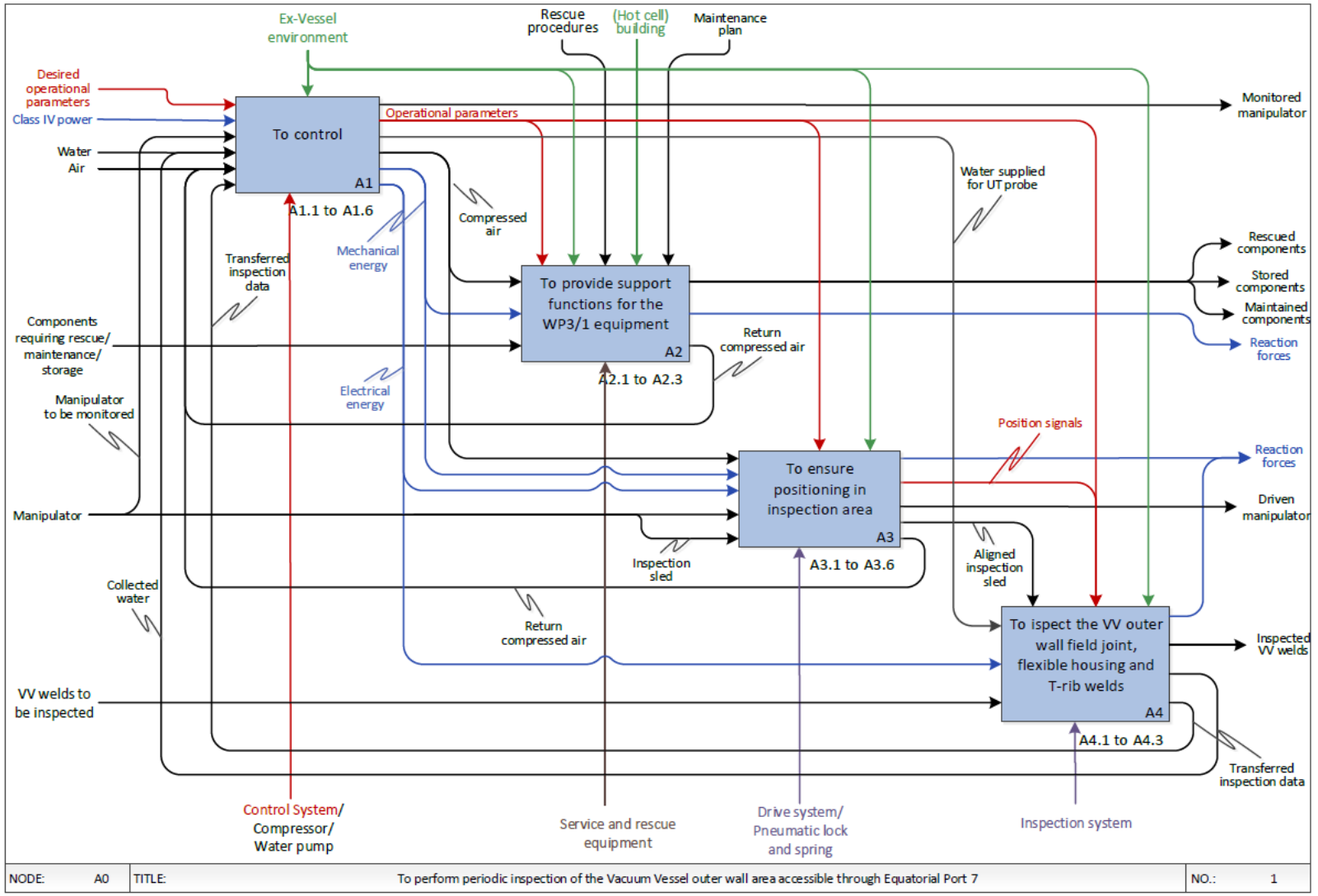


Figure 17: Top IDEF0 diagram (A0 level: To perform periodic inspection of the VV outer wall area accessible through EP7)

4.2 Gathering reliability information

One of the more valuable inputs was the previously in-house conducted FMEA analysis for a manipulator for in-service inspection of a steam generator. In this FMEA, failure modes were related to components, but these components could be connected to corresponding functions in reverse. This was important, because not all of the functions are shared by both manipulators. Therefore, some failure modes in the existing FMEA had no relevance in this analysis. The most relevant data obtained, was related to the electronic parts of the system because the company uses the same or similar parts from the same suppliers as before. This made using manufacturer provided data valid. Even though, severity, occurrence and detection data couldn't have been directly used in the analysis, RPN number still provided a valuable input into system's weakest aspects. In other words, previously conducted FMEA indicated which design solutions to avoid.

Example of data obtained from manufacturers is shown on **Error! Reference source not found.**. It is an example of a pneumatic valve with defined service life value. MTTF and, subsequently, failure rate can be calculated from this value by using the following equation:

$$MTTF = \frac{B_{10d}}{0{,}1 \cdot n_{op}} = \frac{2 \cdot B_{10}}{0{,}1 \cdot n_{op}} \tag{4.1}$$

where B_{10d} indicates the mean number of cycles until 10% of the components have failed dangerously [37] and n_{op} specifies the number of cycles the component has been submitted to.

FESTO usually specifies B_{10} value which is statistically expected value for the number of cycles at which 10% of the components have exceeded the limit values under specific conditions [38]. By considering the recommended ISO assumption $B_{10d} = 2 \cdot B_{10,}$ equation 3.1 achieves its final form. For some components, FESTO specifies failure rate in which case no calculations are needed. LEMO company provides shelf life information for their products. HPC gears company provides hours of life [39], this number was divided by the number of hours a component was operational to obtain a more realistic failure rate. Rotary and linear motion sensors (RLS) company provides MTTF information [40].

Other suppliers that INETEC usually orders from don't provide reliability information. Some, for instance Maxon motor, suggest that they use standard handbook information to calculate failure rate for their components [41]. Therefore, using failure rate information from handbooks for standard components presents the next step in obtaining reliability information.

For standard components Non-electronic parts reliability data handbook and US Military handbook 217F. Most of the information was taken from the NPRD handbook [36]. Since the handbooks provide several failure rate values for the same components, it was important to determine the operational conditions that are similar to those of the ISI device. These are called application environments and describe the conditions of field operation. The NPRD application environments are consistent with those in MIL-HDBK-217f [35]. The one applied for the ISI device is GM – ground mobile and refers to equipment installed on wheeled or tracked vehicles [36]. For the components where such distinction wasn't provided common failure rate was used.

Table 3: Product reliability information example – FESTO [42]

FESTO	Datasheet product reliability
Part	Pneumatic valve VUWG-L10-B52-M7 No. 573825

Feature	Value
Well-tried component	Yes
Service-life value B_{10}	10 MioCyc

Lastly, for nonstandard components and assemblies and for standard components for which there was no available data, an estimation of MTBF data was made. If it wasn't possible to define MTBF due to preventive maintenance, frequency of component replacement was used. This frequency was obtained mostly from maintenance plans that include spare parts list, while the MTBF was based on inspection logs and expert opinion. Estimations were made by engineers that design and test the devices, as well as the field workers that use similar devices. These estimations can be found in Appendix B FMECA table in the MTBF column. Estimations that were used to calculate failure rates are marked with the INETEC label in the λ column.

MTBF and frequency of preventive component replacement were also estimated for some standard parts with known failure rate data from other sources. This is useful because it indicates failure in nuclear power-plant conditions. Existing preventive actions must be taken into consideration in RAMI results, and all analyses used for obtaining them.

4.3 Failure mode, effects, and criticality analysis (FMECA)

The first step of FMECA is the identification of failure modes. In RAMI analysis, failure modes are thought of in relation to basic functions from IDEF0 decomposition. Any inconsistencies and overlaps in the basic functions noticed during identification of failure modes required alteration of the functional decomposition. An example of an overlap of functions would be separating drives on the manipulator and drives on the arm. Even though they have a different purpose, for moving the manipulator and ensuring sufficient contact between VV surface and the probes, respectively, their drives consist of identical or similar parts which would cause unnecessary redundancies in failure modes. After identification of initial failure modes, FMECA was cross-checked with previously mentioned FMEA of a similar system. This resulted in a rephrasing of failure modes or the addition of new ones. For instance, failure mode defined in Forerunners FMEA was *The PCB screws are not tightened*, which was rephrased into *Loose PCB* with cause *Screw connections loosened by vibrations*. This cause is possible only if the screws weren't sufficiently tightened during assembly. Example of a newly added failure mode is *Probes are worn out* which wasn't considered in the Forerunner analysis. Finally, identified failure modes have been shown to company field experts, to ensure that none have been overlooked and to check validity of identified ones.

4.3.1 Qualitative analysis

Basic functions defined under *A1 To control* have a total of 21 failure modes. Under this main function are included software errors which have high occurrence, many operator errors and other failure modes whose effect propagates through the entire system, such as damaged cables, connectors, air leakage, etc. Failure mode or effect of some function can propagate in the system and present a cause of failure to some other function. This can be explained through potential issues with function *A1.5 To supply air*. Failure of several different parts (cause) can cause air leakage (failure mode). Air leakage results in reduced or no airflow (effect). Reduced or no airflow (cause) is the reason why a pin for locking the position (A3.2) won't extend (failure mode). If the pin doesn't extend, position of the manipulator cannot be secured and scheduled inspection cannot be conducted (effect).

A2 To provide support functions for the WP3/1 equipment has only 4 failure modes. These failure modes and causes are important because they can have large severity value if the spare parts aren't envisioned. Some of the basic functions can never fails partly because that would mean the manipulator is irretrievable which is forbidden.

Further on, main function *A3 To ensure positioning in inspection area* has the modes failure modes, in total 26. *A3.3.5 To transfer mechanical energy* is the basic functions with the most failure modes (7). This is because a lot of components fall under this basic functions, and all of them have a failure mode. Cause for most of these failure modes is the overload. Basic function *A3.6 To align inspection* sled to VV surface has only 1 failure mode but 5 causes which is the most any other failure mode has. It is important to point out that most of the failures in the main function A3 are the result of failure in A1. Especially, operator and software error that can cause clashes of the manipulator with the environment.

Lastly, the functions related to inspection methods, under *A4 To conduct visual, surface and volumetric examinations*, are subject to radiation damage, namely cameras, and wear, ET probes. Other causes don't have such a significant impact. UT probe failure modes haven't been completely defined because no proper solution has been proposed so far. Also, there is a weak magnetic field, outside of the vacuum vessel, that could affect the signal. There are no solutions for this problem, either. In the current functional decomposition, surveillance cameras are separated from cameras for inspection, because they have a different purpose and different characteristic. However, some of the failure modes are still applicable to both, and some of the failure data also. In later stages, further effort should be made to either make a more significant distinction or include them both under one function to avoid redundancies.

Figure 18 shows an excerpt from the FMECA table, the rest of which is available in the Appendix B. The first column contains functions, and the second column lists the failure modes identified for said functions. Causes of these failure modes are in the third column, and subsequently defined effects in the fifth column. Fourth and sixth column contain suggested preventive and corrective actions for causes and effects. For example, insufficient cooling of the motor (cause) affects the function, *A3.3.1 To control the drive,* by causing overheating (failure mode) which can result in damage to electric components (effect). A single failure mode can have multiple causes or effects. For instance, air leakage can result from the failure of any of the components in the pneumatic chain. To avoid excessive longevity of the document only more critical failure modes have been thoroughly considered. These failure modes were distinguished by discussing with experts and studying failure rate data. For instance, under normal operational conditions, the bearing can last much longer than necessary for the inspection. This resulted in only taking into consideration bearing failure due to abnormal operational conditions, such as overload.

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects
A3 To ensure positioning in inspection area					
A3.1 To ensure sufficient traction force	Slipping	Insufficient normal force	Increase pressure/ Test mechanism operation before inspection	Loss of precision for positioning	Reposition and repeat inspection
	Wheels cannot spin	Excessive applied force	Decrease pressure/ Test mechanism operation before inspection	Manipulator stuck inside the rails	Decrease pressure/ Emergency removal
	No force applied	Pneumatic mechanism assembled inaccurately	Training of people involved in assembling/ Test mechanism operation before inspection	Manipulator can't move	Check for and repair damage after inspection/ Reassemble mechanism
		Reduced/ No airflow	Test mechanism operation before inspection	Manipulator can't move	Emergency removal and repair/reassembly
A3.2 To lock position in rails	Pin doesn't extend	Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Position cannot be secured	Replace damaged part and redo inspection
	Pin extends at the wrong time	Operational parameters set incorrectly	Test mechanism operation before inspection	Manipulator operation abrupted	Retract pin and continue inspection
A3.3 To drive degrees of freedom					
A3.3.1 To control the drive	Connector between the motor and the PCB is damaged	Mishandling during assembly	Training of people involved in assembling/ Use higher quality connectors	Drive not working	Replace connector
	Loose PCB	Screw connection loosened by vibrations	Check screw connections during assembling	Possible damage to electronic components and cables	Use industrial glue for connecting the screw again
	Overheating	Insufficient cooling of the motor drive	Use thermal grease between the motor drive and the housing surface	Damage to electronic components	Pause inspection/ Replace damaged components

Figure 18: Excerpt from FMECA table

In other words, all of the components and their failures have been taken into consideration, but not all of them have been analysed in detail since some of them have no significant impact on system's reliability and availability. On the other hand, operator and software errors have been taken into consideration due to their frequency. Operator errors are based partially on inspection logs and partially on field operators experience. Software failures have been grouped together since tracking of their causes is very difficult, and the techniques for software reliability are still being developed. The most significant input for software failure rate is the inspection logs.

4.3.2 Quantitative analysis

Basis for the quantitative analysis is a valid qualitative analysis. Only when all failure modes and their relations to causes and effects have been defined, can we start assigning reliability values to these failure modes. A certain component can have several different failure rates depending on the failure mode. This distinction is important for the gathering and assigning reliability information. It was explained in earlier sections, namely 3.2, 3.3 and 4.2, how reliability information is gathered and related to failure modes. Distinctions were made on type of failure data (failure rate, MTBF, MTTR and replacement time) obtained from different in-house sources (inspection logs, maintenance plans) and experts (field operators, mechanical designers). It was established that most of the medium risks result from operator and assembly errors. Medium risks with higher criticality (closer to major risks) and major risks are the ones with high severity in terms of propagation throughout the system which requires replacement of multiple parts or makes the detection difficult.

Software failure modes have been grouped together since the extrapolation of software test failure rates and failure modes into the field has not yet established itself as a reliable modelling technique [4]. Inspection logs of past inspections provided the best insight into problems regarding software and enabled their quantification. Further on, operator failure rate has also been deduced entirely from company's previous experience. Other failure data has been collected in the manner described in section 2.1.1. Figure 19 shows the continuation of the table presented in Figure 18. This part of the table presents failure data used for determining risk priorities and as an input for RBD analyses.

MTTR values were gathered in the company by interviewing employees in a way explained in section 3.2 and 3.3. Of all the listed times that the MTTR comprises of, the diagnostic time has the biggest impact. MTTR values have been translated into severity values by using the rating scale suggested in Table 1.

Next, occurrence values were determined. These values stem from failure rates. The procedure for determining failure rates has already been explained in section 3.3.2. The only thing that is important to emphasize is the determination of values resulting from the company experience. Some of the values that the company provided are occurrence observed directly in inspections, but other values are derived from replacement frequency. For example, operator error has an MTBF of approximately 12h and represents directly defined occurrence while signal cable damages have an MTBF of 5 years, but here it refers to replacement frequency since there is a higher probability that the component will be replaced rather than fail.

There are many parts inside the manipulator that are replaced before their failure. This is done to prevent damage to other parts of the manipulator, that can be caused by the failure of said components. Also, multiple components in the system lose their quality due to ageing and long exposure to radiation. This means that some of the values in the FMECA table aren't actually failure rates but are used as an indicator of what the failure rate would possibly be if there was no preventive maintenance. This includes cables and connectors, some pneumatic elements such as cylinders and hoses, failure modes related to the PCB and others. It is acceptable to use such values since they are more conservative than what the actual failure rates would be. Criticality values are then calculated as the product of corresponding occurrence and severity values.

Even though the severity values of failure modes recognized in the manipulator are mostly low, rating table suggested by ITER was used because it shows its potential impact within the scope of the wider project. It allows comparison with other similar systems and emphasizes the low impact that the manipulator has on the entire ITER machine. Severity values are obtained from MTTR which is a maintainability measure. Low severity values result in high maintainability due to quick replacements, and since availability considers the system's maintainability, it will also increase the system's availability. Occurrence values for the ISI device are high, partly because the components are movable and cannot be over-dimensioned due to space reservations. ITER suggested rating scale is very rough and doesn't provide distinctions, that might be relevant for such a system, but it was used, nevertheless.

Function	Failure mode	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A3 To ensure positioning in inspection area											
A3.1 To ensure sufficient traction force	Slipping	1	0,5h	4	2,854E-05	INETEC	4y	1	4	4	1,259E-04
	Wheels cannot spin	1	0,5h	4	2,854E-05	INETEC	4y	1	4	4	
	No force applied	2	3h	4	2,854E-05	INETEC	4y	3	8	24	
		2	3h	4	4,032E-05	FESTO	4y	3	8	24	
A3.2 To lock position in rails	Pin doesn't extend	2	3h	4	4,032E-05	FESTO	4y	3	8	24	3,017E-03
	Pin extends at the wrong time	1	0,5h	6	2,976E-03	INETEC	14d	2	6	12	
A3.3 To drive degrees of freedom											
A3.3.1 To control the drive	Connector between the motor and the PCB is damaged	2	12h	4	2,854E-05	INETEC	4y	3	8	24	8,562E-05
	Loose PCB	2	12h	4	2,854E-05	INETEC	4y	4	8	32	
	Overheating	2	12h	4	2,854E-05	INETEC	4y	2	8	16	

Figure 19: Excerpt from FMECA table continued

Risk mitigation actions should be aimed at reducing the occurrence because it directly affects the system's reliability. Figure 18 shows the distribution of risks recognized for the manipulator. The bubble chart has minor risks marked in green, medium ones in yellow and major risks are in red. Occurrence and severity are multipliers, and their product, criticality, lies in the intersection of the lines. In other words, wherever a certain product of a specific occurrence (e.g. 3) and a specific severity (e.g. 4) exists, a bubble is placed in the intersection to represent existing criticality value (yellow bubble with number one). Each bubble contains a number which indicates the number of failure modes that have the specified criticality. For example, if the number inside the bubble is 18, it means that there are 18 instances inside the FMECA table that have associated criticality.

Bubble charts are an excellent way of visualizing which risks and how many of them need to be mitigated. There are in total 40 minor risks, 57 medium risks and 2 major risks. Minor risks are those that can be mitigated in a very short period, but often have high occurrence. There are 18 of them with highest possible occurrence. These sort of risks affect reliability very negatively. Minor risks include incorrectly set operational parameters, insignificant water and air leakages, etc. As was already pointed out before medium risks are mostly related to operator errors such as mishandling of connections during assembly, increased cable or hose tension, and so on. These risks should be mitigated with training of the operators, clear assembly instructions and design that prevents mishandling. There are only two major risks, bending of the air hose (C=18) that prevent air flow and failure of the spring (C=16) that needs to ensure manipulator extraction. Bending of the air hose is problematic because it might be difficult to detect the exact point where it is happening, and also might me difficult to correct once the product is finished if there wasn't enough space envisioned. Meaning, that it could be fairly easy to mitigate if the designers keeps this in mind in the later stages of product development. Spring envisioned for enabling manipulator extraction needs to be included in preventive measures. Springs are subject to deterioration due to age and radiation. Even though there are only two major risks in the manipulator, an additional effort should be made to reduce system's occurrence. It is suggested by ITER to increase system's reliability, rather than availability.

Last column of the Figure 19 contains failure rate predicted from the sum of the failure rates for corresponding basic function in the FMECA worksheet. These values present an input for corresponding blocks.

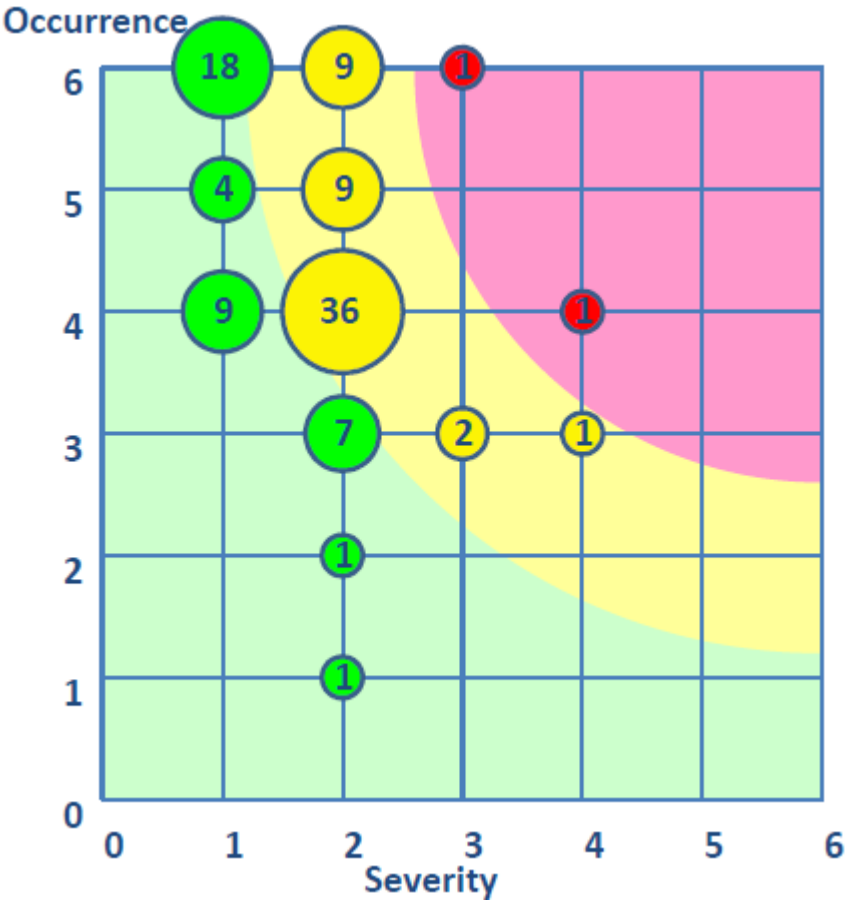


Figure 20: Bubble chart for criticality

4.4 Reliability Block Diagrams (RBD)

System failure is defined as the inability to conduct the inspection. Some functions aren't required for the system to be operational, such as *A1.4 To provide system supervision*. However, inspection requires appropriate supervision to help the operator conduct a valid inspection. Therefore, it was concluded that every basic functions needs to be fulfilled in order to conduct inspections. Since failure of a single function would result in what is defined as the system failure, diagrams are set as series at all levels.

The functional breakdown from section 0 was used as the basis for modelling the diagrams. Each main or intermediate function represents a subdiagram, six of them in total, and each basic function represents a block. Each lower-level diagram calculates reliability and availability of specified configuration and feeds this input into associated block on the higher level. Figure 21 shows the top level diagram and the decomposition on the main functions. The diagram logic will be explained on the function *A3 To ensure positioning in inspection area*. We need to start on the lowest level, meaning that the software first calculates the reliability or availability of

the series of blocks A3.3.1 to A3.3.6. Once the value is calculated, it is assigned to the block A3.3. Next, calculation of reliability or availability is calculated for series of blocks from A3.1 to A3.6. Obtained value is assigned to the block A3. Finally, series of blocks A1 to A4 is calculated to obtain system's total reliability or availability. Of course, the same logic applies to all the other subdiagrams. If blocks on the lower levels aren't properly defined, calculations cannot be made.

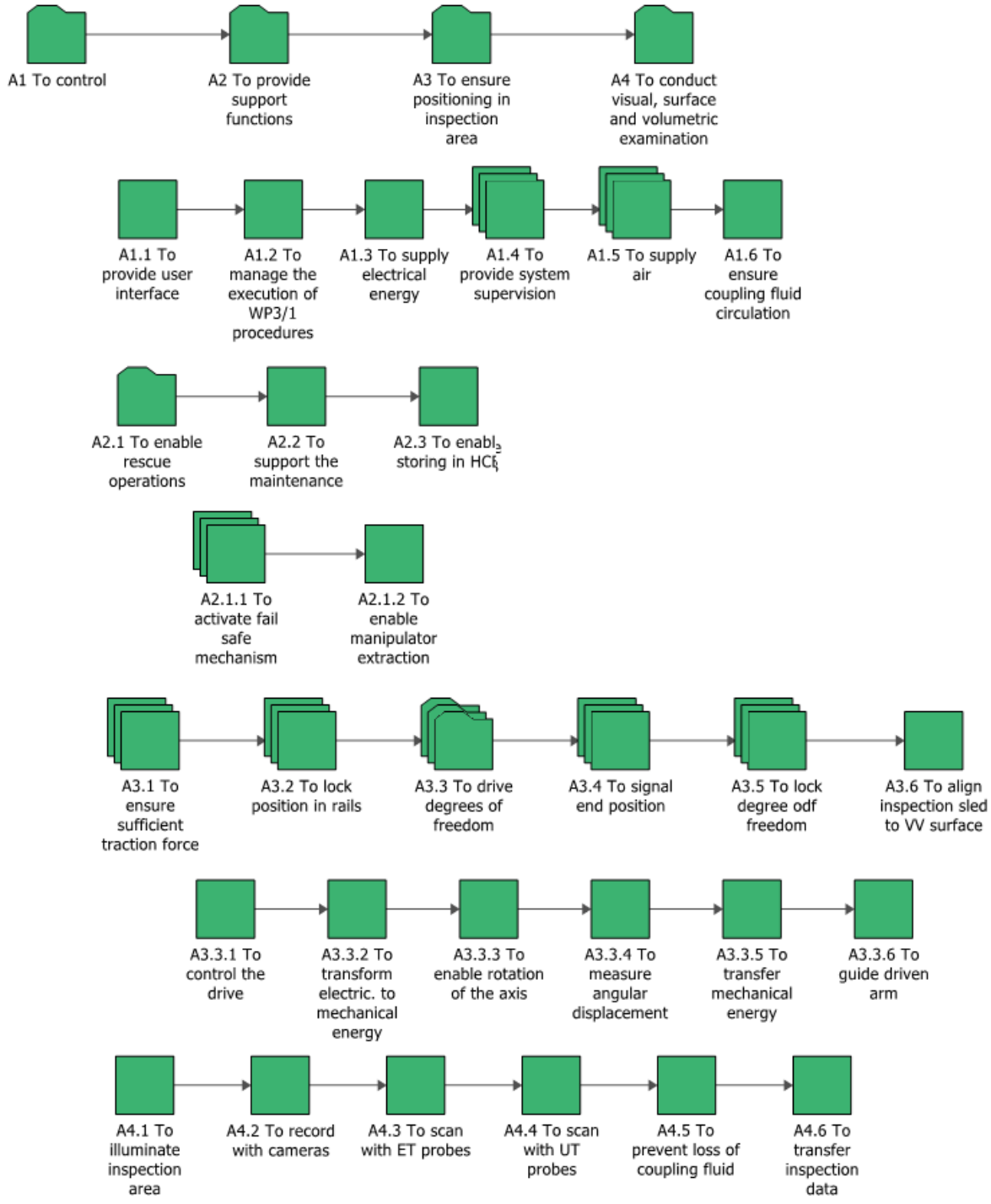


Figure 21: RBD structures in BlockSim software

Some blocks represent multiple ones. It was mentioned earlier in section 3.4.1. that the same function can occur multiple times in the same system. Block that describes such instance is called multiple block type and can be defined either as a series or as a parallel. Example of such block is A3.3 To drive degrees of freedom which represents a series of 5 drives since each of them needs to work to make the inspection possible.

Block properties contain reliability distributions, corrective task and operation information that includes duty cycle and defining the block as multiple type if necessary. Reliability distributions have initially all been set as fixed. This means that in applied 2-parameter Weibull distribution, the shape parameter (β) set to 1, and the scale parameter (η) assumes the value of the reciprocal failure rate. Further research should be put into determining the effects of wear, ageing and radiation on reliability distribution. Early failures are eliminated through calibration, factory acceptance and site acceptance test. Corrective tasks refer to the worst case scenario of the function, by taking the largest value of the MTTR of said function.

Duty cycle is set as 1 for most functions because most of the system are operational during entire inspections. Exceptions include *A2 To provide support functions*, since they are only used when the manipulator isn't conducting inspection or in emergency removal situations, and functions relating to inspections themselves. The manipulator conducts visual and Eddy current inspection simultaneously or just the ultrasonic inspection at a given time. Analyses are run bottom-up and thus cannot be conducted unless all of the blocks have been properly defined.

Both the simulation and the analytical diagrams have the same configuration of blocks. Simulation diagrams are used to show systems availability (A). Figure 22 shows system initial availability analysis converging to the value of 16,5%.

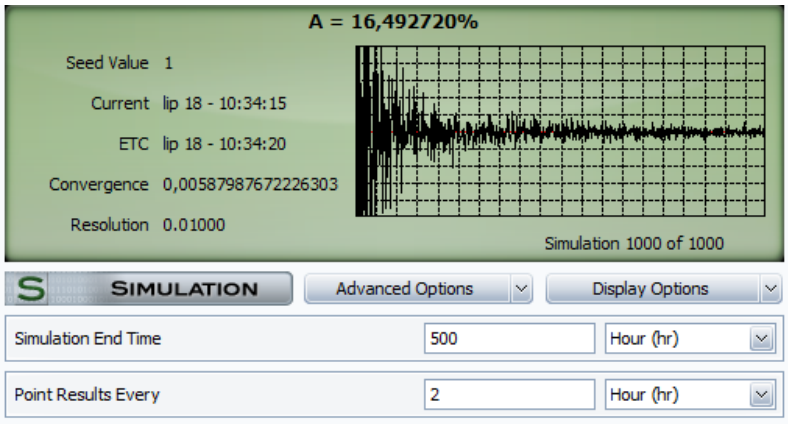


Figure 22: Results of the simulation diagram – availability

The RAMI analysis program suggests an operational availability of up to 50% for systems that are operational for about 2 weeks [11]. However, inspection devices are used only during LTM

in which the ITER machine isn't operational, meaning that the allowed availability could be slightly lower. Nevertheless, availability should be aimed at 50 % because of the limited period in which the system is scheduled to be used. Simulation end time was set to 500 hours since the system won't be operational for a longer period of time.

Analytical diagram is used to show system's reliability (Figure 23) and how it changes over time. This indicates that the system's reliability after only 8 hours drops to zero. In other words, there is no way for the system to operate for a period longer than 8 hours without failing. This is unacceptable for the system that should be operational for 2 weeks (336 hours). Reliability improvement should be the main priority of risk mitigation actions.

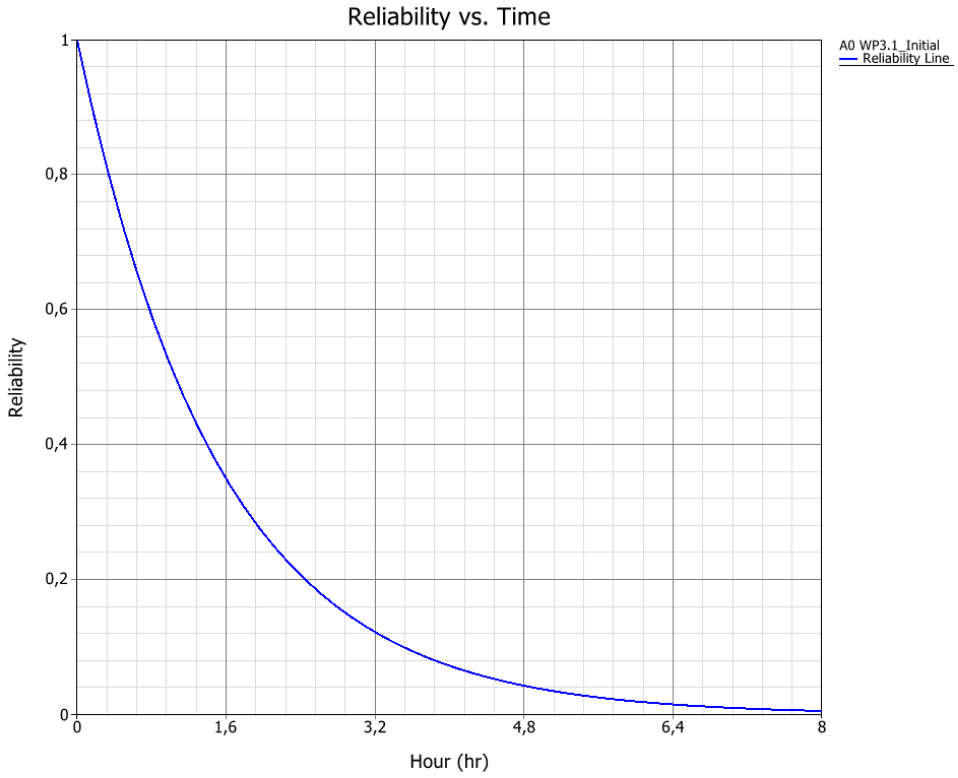


Figure 23: Results of the analytical diagram - reliability graph

On the next page in Figure 24, comparison of each subdiagram graph has been shown. These graphs also show the reliability vs time plot. To make them comparable, all graphs have been plotted for 336 hours. This can indicate which subfunctions and, consequently, which failure modes have the biggest impact on the obtained low reliability. *A1 To control* has very low reliability due to failure modes related to frequent operator and software errors. *A2 To provide support functions* has very high reliability. This is caused by the very low duty cycle and also because some of the function block are set never to fail (storage). It is important to point out that this function has extremely high reliability and seems satisfactory from the point of RBD analysis. However, this function contains one of two major risks, spring failure

discussed in previous section, that must be mitigated. This shows the importance of applying different methods to check for system's reliability. *A3 To ensure positioning in inspection area* has low reliability because of the current serial nature of the configuration. Specifically, A3.3 block is set as a series of 5 drives. Which means that the already low reliability was multiplied 5 times. Another reason for this diagrams low output reliability is the *A3.6 To align inspection sled to VV surface that has very high failure rate*. There is only one failure mode specified for this function and that is inspection sled lift off. We can then observe the most critical cause of this failure mode and that would insufficient water under the probe. Special attention should be given to this mechanism during the design to make it robust.

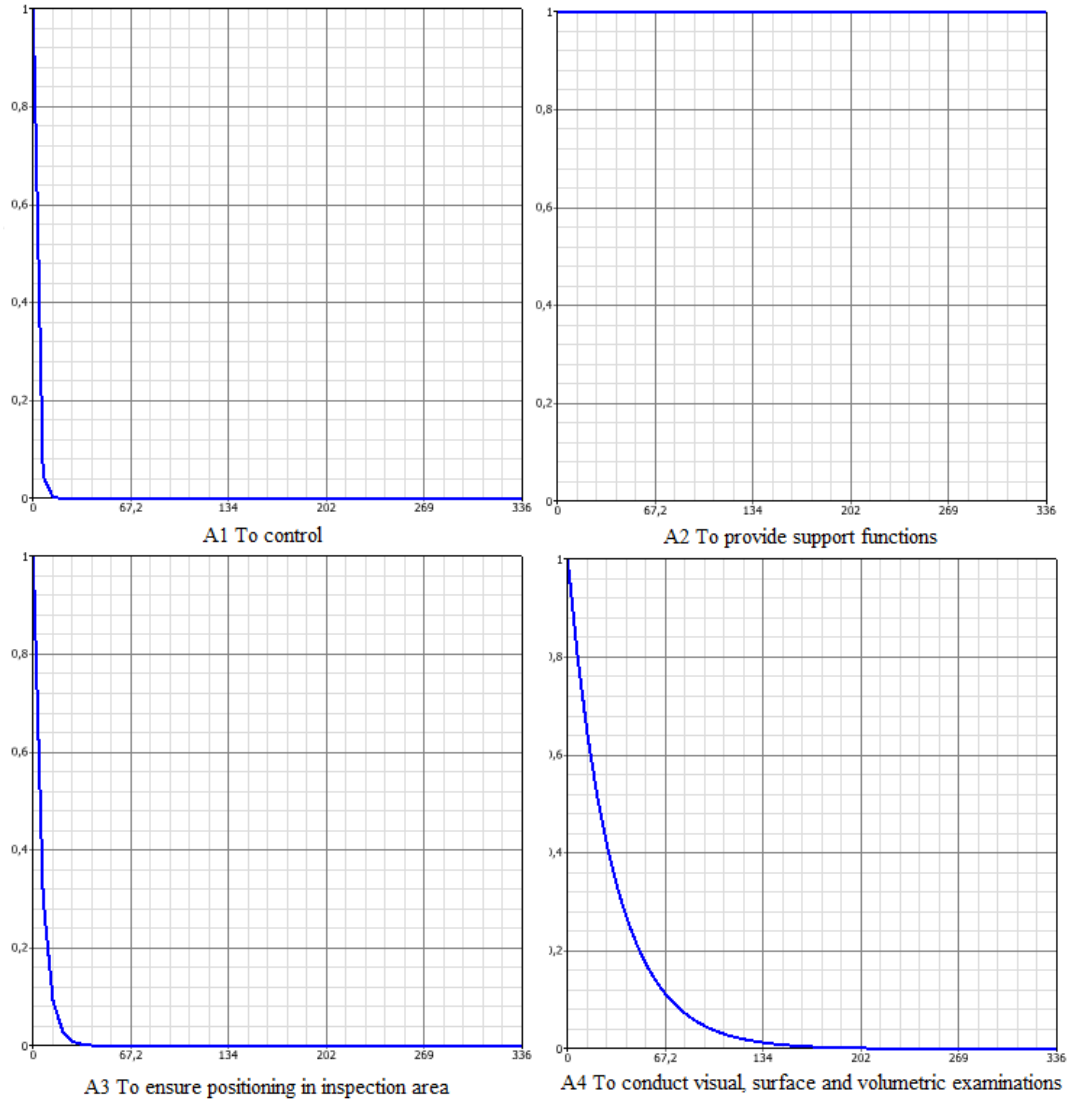


Figure 24: Comparison of the subdiagrams reliability

Reliability values of the subdiagram *A4 To conduct visual, surface and volumetric examinations* are the most difficult to affect because the inspection probes have very short life span. However, decreasing operator and software related errors will result in increased reliability.

5 DISCUSSION

RAMI analysis has provided an insight into the greatest weaknesses of the ISI device in this thesis, as well as similar devices existing in the company. This analysis and its results can be used as a starting point for future reliability analyses and models made inside the company. Analyses conducted in the company so far have been qualitative in nature, as opposed to this one, which is both qualitative and quantitative. From the perspective of quantitative analysis, information received from the company was very limited. Unfortunately, the company doesn't have any written procedures for measuring equipment's performance in the field, which would include the collection of failure data. Inspection logs usually contain information on when did the failure occur, and mitigation action, including mean time to repair, but don't contain detailed descriptions of failures. Failure rates relate to specific failure modes, and since failure modes aren't specified in inspection logs, failure rates derived from them are less accurate. Accuracy was increased using expert assessment. In addition to inspection logs and expert approximations, failure rate data was obtained from manufacturers. Extreme care should be taken when using failure data from manufacturers since they don't test the components in the exact same environment as their implementation might be in [4]. Nevertheless, for the conceptual design phase, this level of accuracy should be sufficient. However, further effort should be put into collecting field data, especially because the company is often the one using it in the field and could control the entire process of gathering failure data. Once more data is gathered, the precision of reliability prediction and risk detection will be increased. This data can also be further improved by applying adjustment factors, for operating temperature, radiation damage and vibrations, according to [43] for the exact environment they will be implemented in. These adjustment factors represent a ratio between failure rate manifested in the environment suggested for a part and the environment in which it will be used. Qualitative input from the company was much more significant since it included information at every step of the analysis. The most helpful was the functional approach that the company practices. Similar to quantitative input, written failure information was scarce. To compensate for the lack of written information, interviews were conducted with various company employees.

The company makes a functional analysis for every project at its beginning. In total three functional decompositions were analysed, for projects Aspira, Orca and Forerunner. The focus of the existing functional analyses was the mechanical perspective of the device with the

addition of electronic functions for parts embedded in the device. The mechanical aspect of the system is divided into subfunctions, which are then detailed to very low-level functions. Most of these low-level functions weren't used for the decomposition in this thesis to achieve conciseness. The electronic functions are usually at a high level of abstraction, but the flows, of energy, material and signal, between it and the mechanical part provided valuable insight for further decomposition. Electronic aspect refers to control and flow of the signal. The syntax of studied functional decompositions differs from the IDEF0 one, but many of the functions could be used after being slightly reformulated. For instance, *Measuring rotational position of the lower axis* was changed into *To measure angular displacement*. Function reformulated in this way can relate to measuring of position of multiple drives and not just the lower axis, which is in accordance with ITER suggestions for functional decompositions. Avoiding redundancies this way is the main difference between the two functional approaches, since the company's functional analysis show every degree of freedom separately. Some functions were grouped together to define a higher level function in IDEF0. Best example of this is a set of functions for leading the air to a certain component that were grouped into *To supply air*. This function needs to include all of the failure modes related to functions that have been grouped. So far the functional approach in the company ignored all the other aspects of the system, such as control and its software, instruments for inspection, compressor, and so on. Nevertheless, it was sufficient to conduct the IDEF0 functional analysis.

The RAMI analysis must include mentioned aspects of the system, at every stage, because their operation also affects the overall system's reliability. Non-mechanical aspects of the system that are developed in the company but fall under the jurisdiction of different departments include electronic elements outside of the device, software and probes. Interfaces between these various subsystems are resolved personally between a member from each department once the design is at the relevant level of detail. Meaning that there is no written trace of their resolution. This made the gathering of failure information about the entire equipment, especially in the later phases, additionally difficult. To facilitate this, next to studying inspection logs, Forerunner FMEA and maintenance plans, interviews were conducted with company employees from various departments. The most important input was received from employees that have conducted inspections with the company's devices because they witness failures. Because of the early development stage of the in-service inspection device, no interviews were conducted with the software department. The extrapolation of software failure rates from the field has not yet established itself as a reliable modelling technique, even in the later stages of

product lifecycle [4]. Therefore, all of the software failures were grouped together under a single failure mode, and its failure rate is derived from inspection logs and personal experience of field operators.

Interviews with mechanical designers were helpful in defining the functions and failure modes with associated causes and effects. They confirmed that all possible risks are taken into account, but also provided information on how some of the risks are currently being mitigated. This information was included in FMECA under corrective and preventive tasks. Interviews with mechanical designers were important because they emphasized previous errors in their designs. However, this information could not have been obtained in any other way. Collection of this type of data should also be addressed in the future. Interviews conducted with field operators provided additional input for quantitative data. For proposed failure modes, they suggested MTTR and MTBF values along with explanations. They were much more certain in values of failure modes that occur often, then in rarely occurring failure modes. Actually, for the components that fail rarely, such as pneumatic cylinders, they provided time between replacements rather than MTBF. Collection of data through interviews was rather difficult. Employees were reluctant to provide assessments because they weren't sure they could provide accurate ones from memory. This is partly because the ITER scale isn't appropriate for the device. Employees would easily provide severity assessment of a specific failure mode if they were given a choice to choose a number from 1 to 5 because it is always easier to provide comparative value, rather than an absolute one. Instead, they were asked for exact periods, in which the system fails or could be repaired. It should also be considered that this probably affected the accuracy of obtained values negatively.

The main advantage of conducting the RAMI analysis for this device is the definition of the major risks in the system. It underlines some risks, that the company was probably aware of, but wasn't aware of their severity. For example, the company was aware that most of the errors are related to software and operator, but they weren't aware of the total effect it had on the manipulator's operation time. Other advantages include setting the basis for determining systems reliability and availability throughout its development and early consideration of risks. The latter is important since the mental effort required for setting up a reliability model helps the designer understand the product's architecture and can be as valuable as the numerical outcome [4].

There are some drawbacks of RAMI analysis when analysing systems like the one in this thesis. First of all, the occurrence and severity scales aren't suited for the device because it is

used for a short period of time and the failures occurring cannot have such a significant impact. Also, goals set for reliability and availability of the entire ITER aren't directly relevant since the device isn't used during normal ITER operation, meaning that the failure of the device doesn't directly affect ITER's availability. In order words, the system is still subject to a strictly defined schedule, but the scales aren't adjusted for it. ITER hasn't set a specific goal values on reliability and availability for inspection system. The RAMI analysis documentation suggests availability of 50% for systems operating for about two weeks during ITER operation. ISI device should be operational for two weeks, but during LTM, meaning that this value can be accepted but doesn't necessarily need to be fulfilled. Further on, there is no possible way for the in-service inspection device to harm the ITER tokamak. This means that the considered risks have lower severity, as was shown in the previous chapter. Additionally, the device and its behaviour are dynamic in nature, unlike most of the other ITER systems. This dynamic nature wasn't taken into consideration in the analysis. Part of this problem is the fact that some parts are short-lived. Best examples are the probes since they scrape the vacuum vessel surface and rapidly wear out. In order to replace the probes, the system needs to stop and return to the point of entry in the rails. Which means that the operation without failures isn't possible, which is the goal for the most of other ITER static system. Lastly, ITER procedure suggests keeping the functional breakdown on the higher level to map all the system's main functions and to avoid redundancies. From the company's point of view, it would probably be better if the functions are decomposed to lower levels for the following reasons. First, because all of the documentation in the company is done with very low-level functional analysis and having reliability model adjusted for it would simplify the application on existing projects that might be improved in the future. Second, because it would make the connection of collected data to the reliability model would be easier. The single function would be related to fewer components, and the reliability model would be more detailed. Changes would be easier to track since the lack of function would result in its exclusion from the model, not in altering other elements of the model. Third, it would be easier to make comparisons between various systems' reliabilities, especially in the later stages of the design. It would be possible to directly compare the reliability of two different embodiment designs fulfilling the same functions in two different systems.

One of the aspects that lack in this analysis is connection between failure modes and components. In this analysis, failure modes are related to function, which is also important, but functions are intermediaries between intention and reality without physical manifestation and

thus cannot have failure modes [27]. Relating failure modes to functions is the standard approach [21], but relating them to specific components would provide an even better output. One of the reasons for this is because there are many different ways to embody chosen solution for a specific function [1]. An additional shortcoming of this approach is the lack of analysis of failure propagation through the system. Currently, it relies on functional decomposition, which can provide only a partial insight. The best way to analyse propagation is to implement FTA analysis on the most critical elements of the system recognized through FMECA [26]. FTA has an opposite approach to RBD. Even though RBDs are important for ITER because they provide the results of the total worst case scenario, this might not be the best approach for the device in question. Unlike most of the system's in ITER, ISI device is quickly repaired, and it doesn't affect the tokamak's operation. In analytical RBDs, every malfunction reduces system reliability. This is technically true, but might not be as relevant as it is for other ITER systems since the device will nevertheless complete the task in scheduled time. Efforts should be made to determine the propagation of major failures and prevent them, rather than increase systems reliability through several separate minor risks that have little effect on the system.

It should be noted that it is very difficult to accurately predict product reliability in the initial design phase for complex products [2]. However, results obtained from this analysis are in accordance with inspection logs and interview information of similar systems, meaning that the analysis has provided a relevant model for device's reliability and maintainability. Once the design is more detailed and specific, it should be updated with more data obtained from previous stages and components used, in the same layout and under the same conditions, in some other devices.

5.1 Risk mitigation actions

Risk mitigation is often the most appropriate strategy for treating identified risks in projects such as this one where the design organization has direct control over the risks [3]. For every credible major technical risk that would compromise the required operational capability of ITER, mitigation actions and/or provisions for recovery are defined in terms of design changes, tests, operation procedures and/or maintenance/spares plan with the objective to mitigate the risk or reduce its criticality level below the limit defined for the major risks [10]. ITER set the limit for major risks at the criticality of 13. In cases where the risk level cannot be sufficiently reduced, specific provisions are defined for recovery including failure detection, localization repair and verification, in addition to an inspection plan to be able to prevent the failures.

Reliability and maintainability can be increased through activities in three main areas: design, manufacture and field use. An important part of all three areas is the feedback of failure information to provide reliability growth. There are three characteristics of the design that have proven to increase products reliability [4]:

1. Minimal complexity: Reduction of the number of component parts and the types of materials used in the. Failures that arise from the interaction of many parts with various tolerances, rather than a single component, are more difficult to predict.
2. Duplication/replication: The use of redundant parts whereby a single failure does not cause the overall system failure. However, this method adds capital cost, weight, maintenance and power consumption.
3. Excess strength: Deliberate design of components to withstand stresses higher than anticipated. This applies equally to mechanical and electrical items.

Controlling reliability in manufacturing is limited since it is outsourced. In field use, it is important to provide adequate operating and maintenance instructions, proof test to reveal dormant failures and use replacement and spares strategies (e.g. early replacement of items with known wear out characteristic) [4].

5.1.1 Risk mitigation proposals

There are risk mitigation actions suggested in the FMECA table are based on information obtained in interviews and Forerunner FMEA and show how these problems have been solved in the company so far. Risk mitigation actions are divided into preventive actions for recognized causes and preventive and corrective actions for recognized effects of defined failure modes. Preventive actions have priority over corrective actions because they increase reliability. By examining these suggested preventive actions, it becomes evident that almost all of them relate to human operator actions. These include checking components before installation, testing operations and assemblies after installation and training of operator prior to inspection. This indicates that providing a thorough operation manual and proper training of the operator can significantly lower risks. Nevertheless, operators shouldn't be solely responsible for the product's reliability. It should be the responsibility of the mechanical designer to a certain extent, especially since they can affect risks early in product development and they are partially included in the process of assembling and testing. Meaning that they receive feedback for the design they produce. This is also the type of reliability information that would be helpful if it

was written down but currently isn't. In addition to operator actions, preventive measures include adding cable protection and redesign of mechanisms that have proven unreliable in previous designs. All of these measures are regularly applied in the company. However, most of these preventive actions are still in the late stages of product development. Risks should be recognized and mitigated early, which is why a bigger emphasizes should be put on a redesign based on previous experience and using reliability predictions. Preventive measures also included in replacement and spare strategies in the form of scheduled part replacements before they fail. These strategies are made more accurate with more data to indicate their replacement. Corrective actions include replacement of failed components during the inspection, reassembly, repeating of the inspection, emergency removal and subsequent repair. It is obvious that these actions increase the device's downtime and should be avoided, especially in the early stages of the design when it is possible to suggest preventive measures. To mitigate these risks operator manuals should be as clear as possible and operators should be trained prior to operating the device. Currently, manuals provide instructions for these corrective actions. For the case where these corrective actions cannot be avoided, such as replacement of the probes after wear out, designers should enable easy access and replacement of components that require action. To decrease required downtime during corrective actions, systems are usually equipped with diagnostic elements which eliminate the need for the operator to search the cause of failure on his own. For instance, manometers are placed in several places to directly indicate where the loss of air occurred. Once the operator knows where the air leakage is located he can quickly check and repair its cause.

Another thing that the FMECA shows is the high occurrence of software errors. Errors in software that affect control can cause significant damage to mechanical parts by inducing clashes with the environment. For instance, manipulator's arm rotates before it is lifted above the rails, causing it to hit the rails and possibly damage the drives and probes on it. Software should limit operator's possibility of error, by not allowing certain actions, such as stopping the systems if it's supposed to clash, and loading of the wrong inspection file. Conceptual design phase might be too early for the discussion of software, but it is, nevertheless, something to keep in mind during product development.

To ascertain the effect of both the software and operator error, RBD simulation was run, under the assumption that the occurrence of these errors is zero. In other words, if there were no errors, mechanical and electrical components would display the reliability shown in Figure 25. By comparing Figure 25 with Figure 24 we can conclude that a significant portion of

system's unreliability lies in software and operator error. To be more precise function A1 is almost 10 times more reliable, when software and operator errors are excluded, and the function A3 has doubled its reliability. Functions A2 and A4 aren't affected by operator and software errors. Total reliability has been increased from reaching 0 reliability in 8 hours to reaching 0 reliability in 35 hours, which is still low but a significant improvement. By mitigating software and operator error risks with high occurrence (6), and low severity (1) will be eliminated, in total 12 out of 18 of them. The other 6 out of 18 with high occurrence are caused by radiation and increased cable tension of probes during inspection. Radiation can be mitigated only with shielding, which often causes more risks because it increases device's weight significantly. Therefore, it should be further studied if it is better to replace components when they fail or try to mitigate occurrence without affecting other elements. Cable tension should be prevented in the design stage by ensuring sufficient space for the cable to bend and sufficient length during all positions of inspection sled.

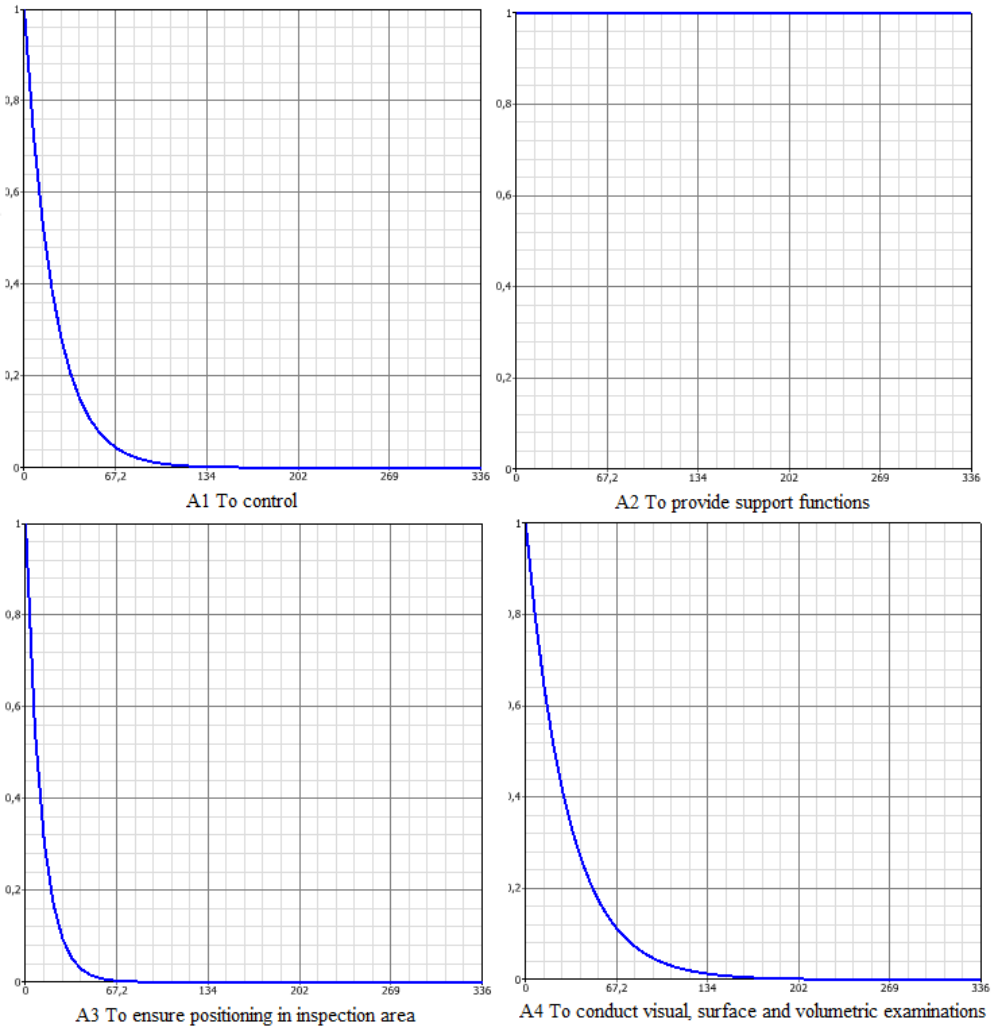


Figure 25: Reliability of the ISI device without human and software errors

When it comes to maintenance, there should be left no room for the operator to make a mistake. In other words, the device should be designed in such a way that the replacement and assembly of parts is simple and intuitive. If the replacement and assembly aren't intuitive, very clear instructions should be made. Another important part of the risk mitigation is the spare parts list Currently, spare parts lists are defined based on the expert opinion of which parts might fail and how often. If the company had an infrastructure for collecting failure data, required spare parts could be determined with greater accuracy. This would eliminate the need of having excessive spare parts on site, and at the same time, it reduces the severity, since spares of all of the parts that could possibly fail would be available.

Major risks according to FMECA are the bending of the pneumatic hose and spring failure of the arm retraction systems. Unfortunately, both the spring and pneumatic hoses age, so their failure rate cannot be completely mitigated, but certain improvements can be made. For the pneumatic hose it is important to envision its position during the design leave sufficient space for it, and avoid sharp objects in the area next to it. Spring failure can be avoided with regular maintenance and replacements. Also, this part of the design should be made robust because of its importance. If the spring fails, extraction of the manipulator could result in its major damage. Design should be proposed that would ensure arm retraction even in the case of spring failure. Example of such design would be a single-acting cylinder that retracts when there is a lack of air. This solution presents a redundancy in the system, since one component can fulfil the function of another in case of failure.

Another significant problem for the system could be water leakage both inside (C=10) and outside (C=12) of the device. To prevent this double containment of all water hoses and seals should be ensured. Further on, even though predicted temperature is 20 °C, it can range from 10 °C to 50°C which is why appropriate cooling should be envisioned for all electronic components that might stop working due to overheating. The cooling fan should be attached to all PCBs, and if this isn't sufficient, another one with an independent power source should be attached on the housing directed at the PCB. This preventive action would mitigate two criticalities with the value 8 and one criticality with the value of 12. 36 failure modes have the criticality of 8. These criticalities are related to failures that occur in hard to reach parts of the system and propagate, which extend the time required for their repair. These include failures occurring near the drive, such as overheating, cable damage, loose connections are failures related to overload. They can be mitigated by making this area of the device accessible, which is a challenge due to space reservations, and careful assembly and operation.

Some risk mitigation actions already exist in the company due to experience with similar systems. Company ensures that every possibly required spare part is on-site and ready to be replaced. Replacement time is also diminished by ensuring easy access to various parts of the manipulator, especially the ones requiring frequent maintenance. Another aspect of ensuring fast maintenance is a modular design. The modular design needs to be implemented in areas where a high possibility of failure of multiple components exists. These multiple components should be grouped together in a removable assembly that requires less time to replace than the total time of replacing each failed component separately. Example of modular design is the inspection sled. In the case of clashing with the environment, sled might get damaged and lose proper contact with inspection surface. The entire sled with probes is then replaced, as opposed to replacing every component separately. Figure 26 suggests a solution to simply connect and disconnect the sled with probes. The probes aren't disconnected from the sled. Connection between the sled and the worm wheel is quadratic to ensure the transmission of power, and the connection between the arm and sled is cylindrical with a plain bearing to enable free rotation in regards to the arm. At the end of the cylindrical part of the sled is a thread for the nylon nut, which is used to prevent loosening of the connection. Cylindrical plate was placed between the bearing and the nut. In case the sled or the probes are damaged, it is replaced with a spare sled with probes. While the other one is used for inspections, the first, damaged, sled can be repaired.

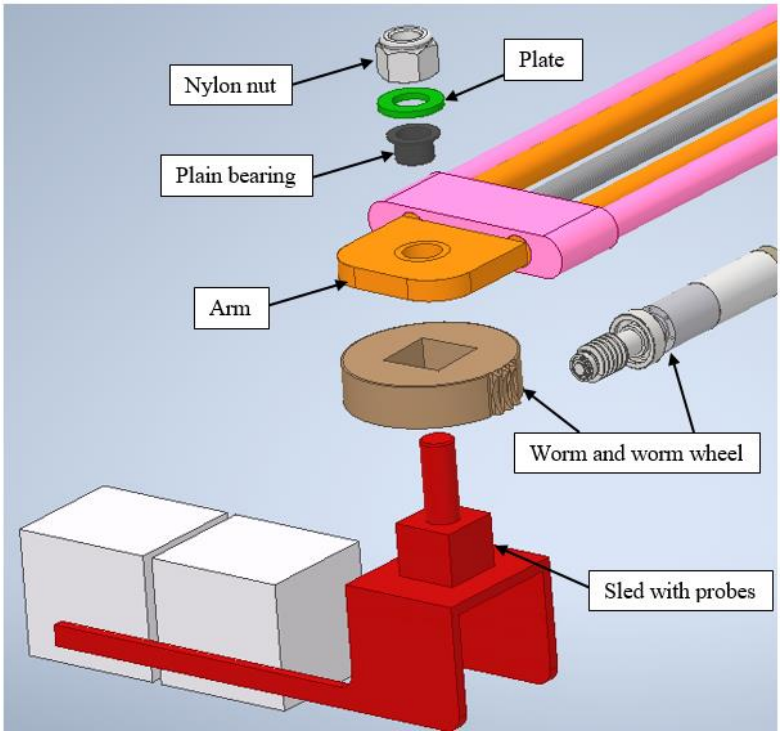


Figure 26: Modular design of the sled

6 CONCLUSION

RAMI analysis is an approach, devised by ITER, for increasing reliability, availability, maintainability and inspectability throughout the product development. Said analysis provides an insight into major, medium and minor risks in design and ensures their mitigation through timely recognition. Current conclusions and input values are based on the company's previous experience in developing similar devices and data obtained from manufacturers. The results of the conducted RAMI analysis for the ISI device show that the device's reliability is 0 after only 8 hours and constant availability of 16,5%. To gain more precise reliability and availability values, more failure data should be gathered in the future. It is very important to emphasize that the failure rate, on which the reliability prediction models, such as this one, are based, is probably the least precise engineering parameter, and these predictions are limited. That being said, values obtained in this analysis are in compliance with those identified during interviews, which makes the model obtained within this thesis relevant to this device. Currently, FMECA analysis relates failure modes to functions, which is not the approach suggested in literature. Usually, failure modes, with associated causes and effects, are related to the components, which stresses the importance of their regular updates as the design progresses. Results of the FMECA analysis recognize 2 major risks, 57 medium risks and 40 minor risks. According to ITER guidelines, major risks must be resolved and for medium risks mitigation actions are recommended. Even though minor risks are usually acceptable, in this device, some of them that have very high occurrence should be mitigated. This high occurrence is mostly the result of frequent operator and software errors. By eliminating them, total system reliability increases by four times. Additional risk mitigation actions are suggested in the previous chapter. Since the design is still in its early stages, preventive risk mitigation actions should have priority over corrective actions. RBD analysis also provides important insight into system's weaknesses and possible risks. It shows that the functions *A1 To control* and *A3 To ensure positioning in inspection area* have the biggest impact on systems reliability. Meaning that if two failure modes, one from function A3 and the other from A4, have the same criticality, the one from A3 should be prioritized in risk mitigations. In the future, suggested risk mitigation actions should be applied and their impact on the system's reliability and availability evaluated. Also, additional effort should be made for collecting reliability information inside the company to ensure more precise reliability prediction models.

LITERATURE

[1] G. Pahl, W. Beitz, J. Feldhusen, and K.-H. Grote, *Engineering Design*, 3rd ed. Springer-Verlag, 2007.

[2] B. Goo, J. Lee, S. Seo, D. Chang, and H. Chung, "Design of reliability critical system using axiomatic design with FMECA," *Int. J. Nav. Archit. Ocean Eng.*, vol. 11, no. 1, pp. 11–21, 2019.

[3] C. Hsiao, R. Malak, I. Y. Tumer, and T. Doolen, "Empirical Findings about Risk and Risk Mitigating Actions from a Legacy Archive of a Large Design Organization," *Procedia Comput. Sci.*, vol. 16, pp. 844–852, 2013.

[4] D. J. Smith, *Reliability, Maintainability and Risk Practical Methods for Engineers*, 9th ed. Butterworth-Heinemann, 2017.

[5] E. M. Benavides, *Advanced engineering design: An integrated approach*. Woodhead Publishing Limited, 2012.

[6] "What is ITER?" [Online]. Available: https://www.iter.org/proj/inafewlines.

[7] D. Kececioglu, *Reliability Engineering Handbook, Volume 1*. Lancaster: DEStech Publications, 2002.

[8] A. Martin and A. Saenz, "Managing complexity with good processes," 2015. [Online]. Available: https://www.iter.org/newsline/-/2171.

[9] Z. Zhanwei and F. Nadine, "ITER Quality Assurance Program (QAP), ITER D 22K4QX," 2017.

[10] S. Chiocchio, B. De Gentile, and M. Shute, "Project Requirements, ITER D 27ZRW8," 2014.

[11] D. van Houtte, K. Okayama, and F. Sagot, "ITER RAMI analysis programme, ITER D 28WBXD," 2012.

[12] P. Order *et al.*, "Order of 12/12/2005 on Nuclear Pressure Equipment," no. March 1978, pp. 1–23, 2005.

[13] K. Ioki *et al.*, "In-service Inspection and Instrumentation for ITER Vacuum Vessel," *2013 IEEE 25th Symp. Fusion Eng.*, pp. 1–6, 2013.

[14] L. Dimitar, "Technical Specification for Lot 1 (WP3/1) of the VV ISIS procurement, ITER D U5TS7H," 2017.

[15] L. Tuhov, M. Tauš, and T. Kučera, "The Assessment of the Technical Condition of the Water Distribution Systems," *Procedia Eng.*, vol. 89, pp. 1420–1427, 2014.

[16] L. Jun and X. Huibin, "Reliability Analysis of Aircraft Equipment Based on FMECA Method," *Phys. Procedia*, vol. 25, pp. 1816–1822, 2012.

[17] X. Zhao-mei, "Research on FTA of Fire and Explosion in the Crude Oil Gathering-transport Comination Station," *Procedia Eng.*, vol. 11, pp. 572–582, 2011.

[18] E. Hong, I. Lee, H. Shin, S. Nam, and J. Kong, "Quantitative risk evaluation based on event tree analysis technique : Application to the design of shield TBM," *Tunn. Undergr. Sp. Technol. Inc. Trenchless Technol. Res.*, vol. 24, no. 3, pp. 269–277, 2009.

[19] C. Lin, H. Teng, C. Yang, H. Weng, M. Chung, and C. Chung, "A Mesh Network Reliability Analysis Using Reliability Block Diagram," no. July, 2010.

[20] R. K. Sharma and P. Sharma, "Qualitative and quantitative approaches to analyse reliability of a mechatronic system: A case," *J. Ind. Eng. Int.*, vol. 11, no. 2, pp. 253–268, 2015.

[21] D. H. Stamatis, *Failure Mode and Effect Analysis FMEA from Theory to Execution*, 2nd ed. ASQ Quality Press, 2003.

[22] J. F. W. Peeters, R. J. I. Basten, and T. Tinga, "Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner," *Reliab. Eng. Syst. Saf.*, vol. 172, pp. 36–44, 2018.

[23] ReliaSoft, "User's guide: BlockSim," no. March, 2018.

[24] S. Distefano and A. Puliafito, "System modeling with dynamic reliability block diagrams," *Saf. Reliab. Manag. Risk*, pp. 141–150, 2006.

[25] D. V. Lindley, T. Bedford, and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*, vol. 86, no. 506. 2008.

[26] X. Han and J. Zhang, "A Combined Analysis Method of FMEA and FTA for Improving The Safety Analysis Quality of Safety-Critical Software," *2013 IEEE Int. Conf. Granul. Comput.*, pp. 353–356, 2013.

[27] D. C. Jensen and I. Y. Tumer, "Modeling and Analysis of Safety in Early Design,"

Procedia Comput. Sci., vol. 16, pp. 824–833, 2013.

[28] S. Sierla, I. Tumer, N. Papakonstantinou, K. Koskinen, and D. Jensen, "Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework," *Mechatronics*, vol. 22, no. 2, pp. 137–151, 2012.

[29] S. Qin *et al.*, "RAMI analysis for ITER radial X-ray camera system," *Fusion Eng. Des.*, vol. 112, pp. 169–176, 2016.

[30] D. Wang, R. Yuan, J. Wang, F. Wang, and J. Wang, "Preliminary RAMI analysis of DFLL TBS for ITER," *Fusion Eng. Des.*, vol. 112, pp. 192–197, 2016.

[31] S. iti Kitazawa and H. Ogawa, "Failure mode analysis of preliminary design of ITER divertor impurity monitor," *Fusion Eng. Des.*, vol. 112, pp. 74–80, 2016.

[32] M. Y. Ahn, S. Cho, H. G. Jin, D. W. Lee, Y. H. Park, and Y. Lee, "Preliminary failure modes and effects analysis on Korean HCCR TBS to be tested in ITER," *Fusion Eng. Des.*, vol. 98–99, pp. 1715–1718, 2015.

[33] D. van Houtte, K. Okayama, and F. Sagot, "RAMI Approach for ITER," *Fusion Eng. Des.*, vol. 85, no. 7–9, pp. 1220–1224, 2010.

[34] Computer Systems Laboratory National Institute of Standards, "Integration Definition for Function Modeling (IDEF0)," *Draft Fed. Inf. Process. Stand. Publ. 183*, vol. 4, no. June 1981, pp. 1–128, 1993.

[35] D. of Defense, "US Military Handbook 217F: Reliability prediction of electronic equipment." Washington DC, 1991.

[36] W. Denson, G. Chandler, W. Crowell, and R. Wanner, "NPRD-91 Nonelectronic Parts Reliability Data," p. 632, 1991.

[37] "Product Service Life at Festo," 2013. [Online]. Available: https://www.festo.com/net/SupportPortal/Files/293239/Product_Service_Life_at_Festo_135502_EN_0.

[38] "FESTO products." [Online]. Available: https://www.festo.com/cat/hr_hr/products.

[39] H. Gears, "Worm / Wheel Reduction information." p. 1.

[40] "What is the MTTF for linear and ring encoders?" [Online]. Available: https://www.rls.si/en/faq/#What-is-the-MTTF-Mean-Time-To-Failure-for-linear-and-ring-encoders_78.

[41] J. Wagenbach, "Reliability analysis, Failure rate, MTBF," 2019. [Online]. Available:

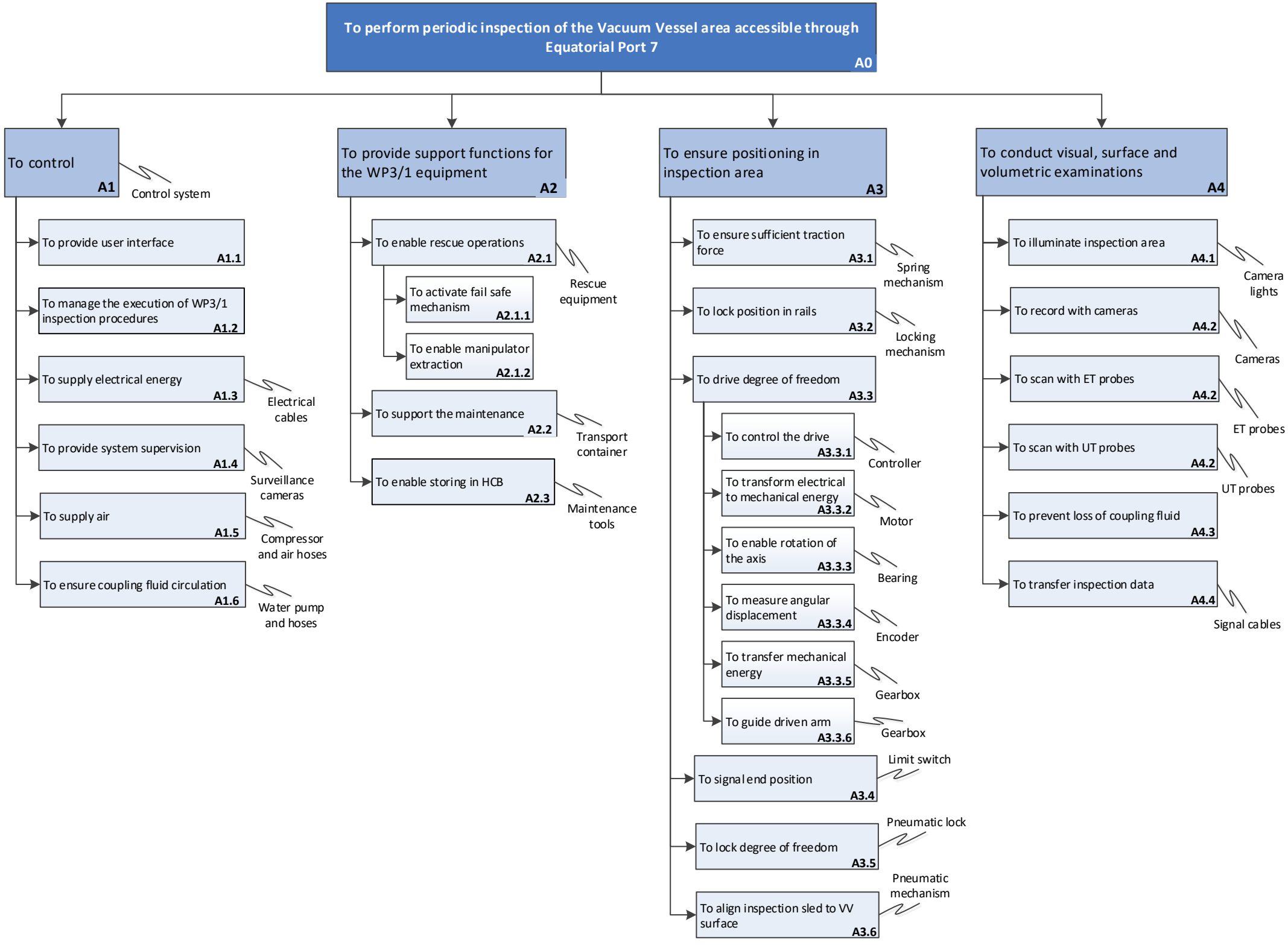
https://support.maxonmotor.com/hc/en-us/articles/360017808654-Reliability-analysis-Failure-rate-MTBF.

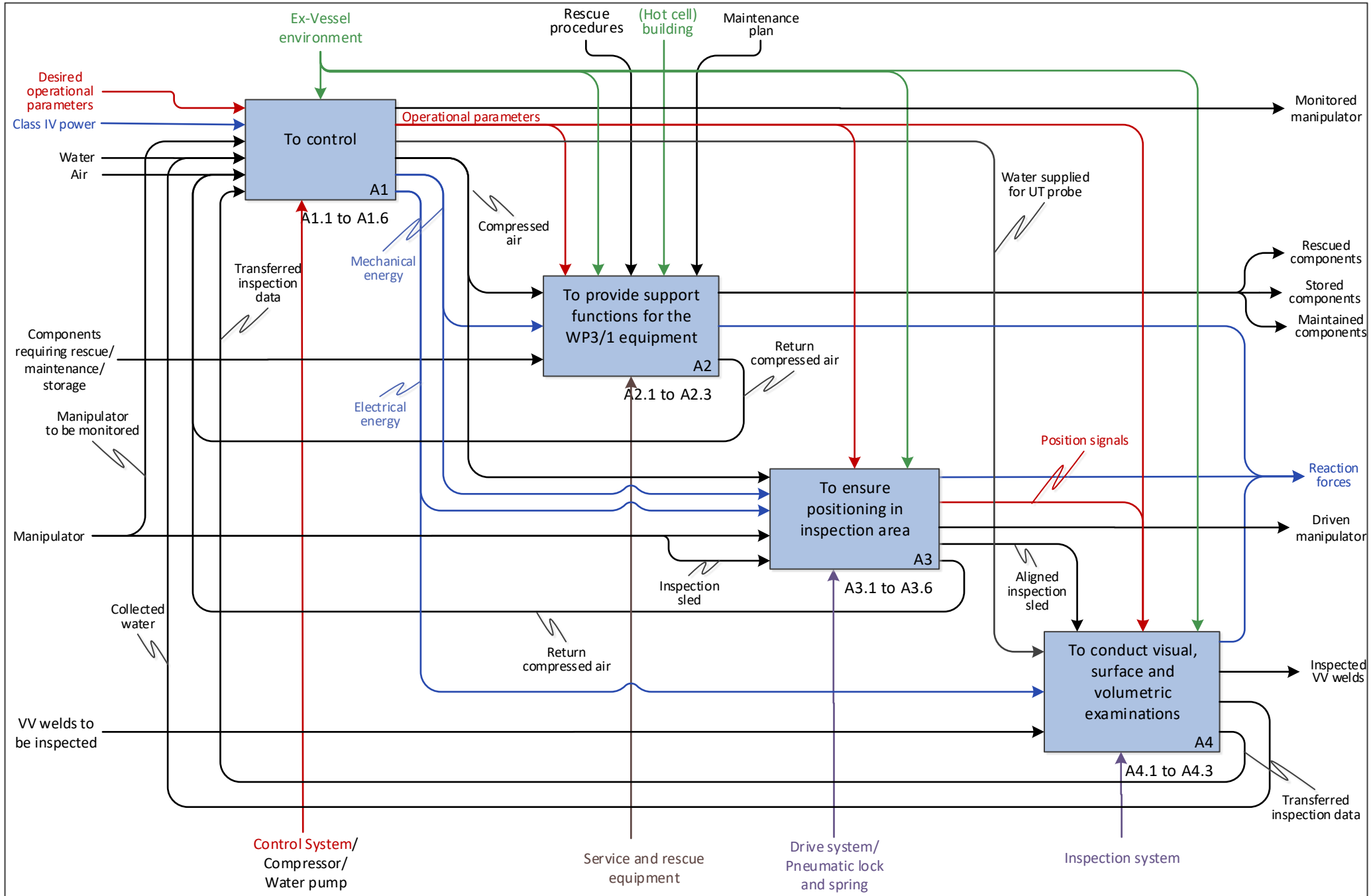
[42] FESTO, "Pneumatic valve VUWG-L10-B52-M7, Datasheet product reliability," 2019. [Online]. Available: https://www.festo.com/eap/en-gb_gb/ReliabilityDatasheet/start.do?partno=573825.

[43] L. C. Cadwallader, "Failure Rate Adjustment Factors for High Technology Components," pp. 3–5, 2013.

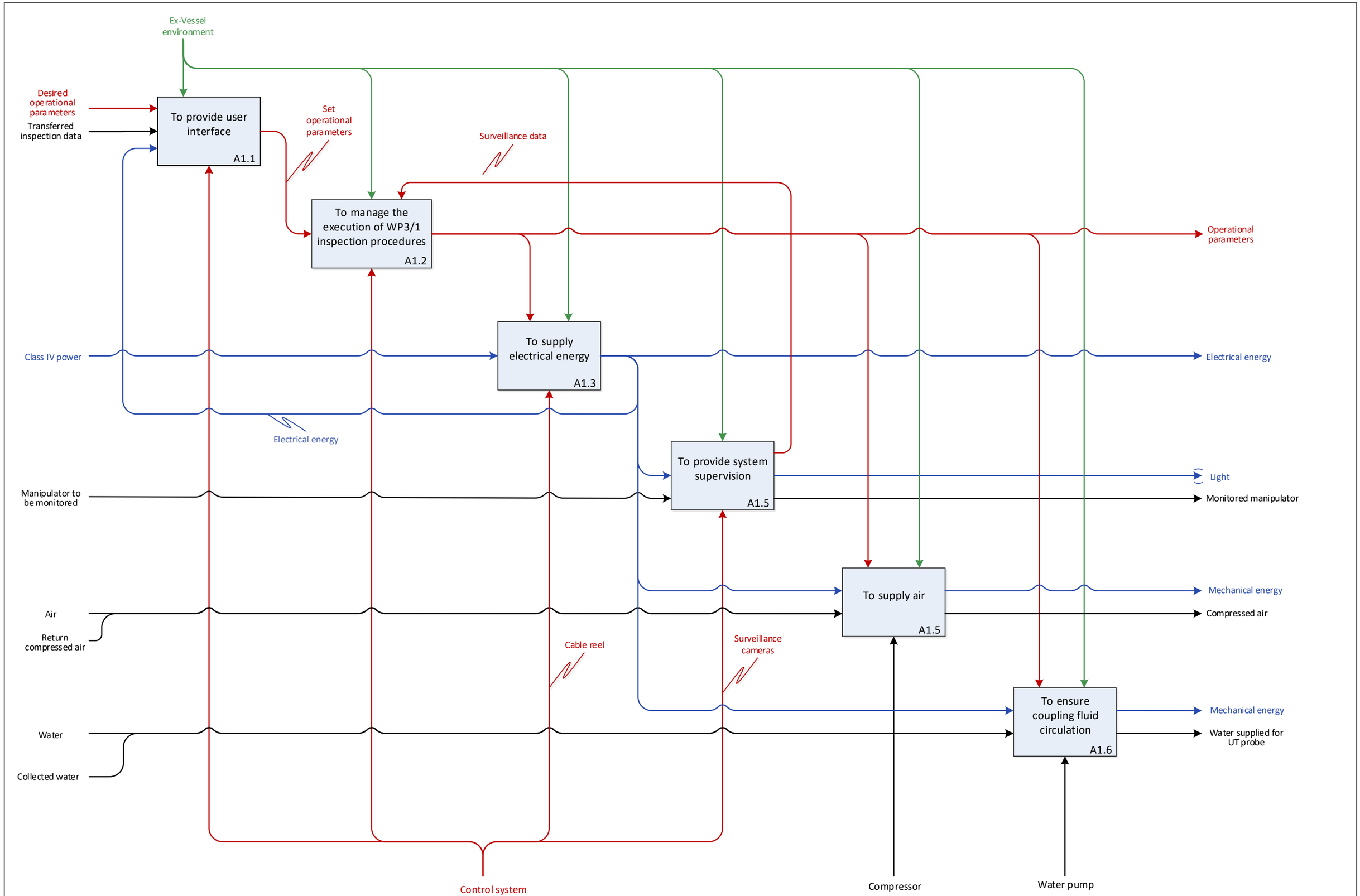
APPENDIX A: IDEF0 Functional breakdown

Functional breakdown includes function tree at the beginning as an overview of the decomposition, even though IDEF0 analysis usually shows this hierarchy with a node tree. Underneath some of the boxes, at the right side, is a call to child diagram if it exists. This call specifies how many subfunctions are in the child diagram.

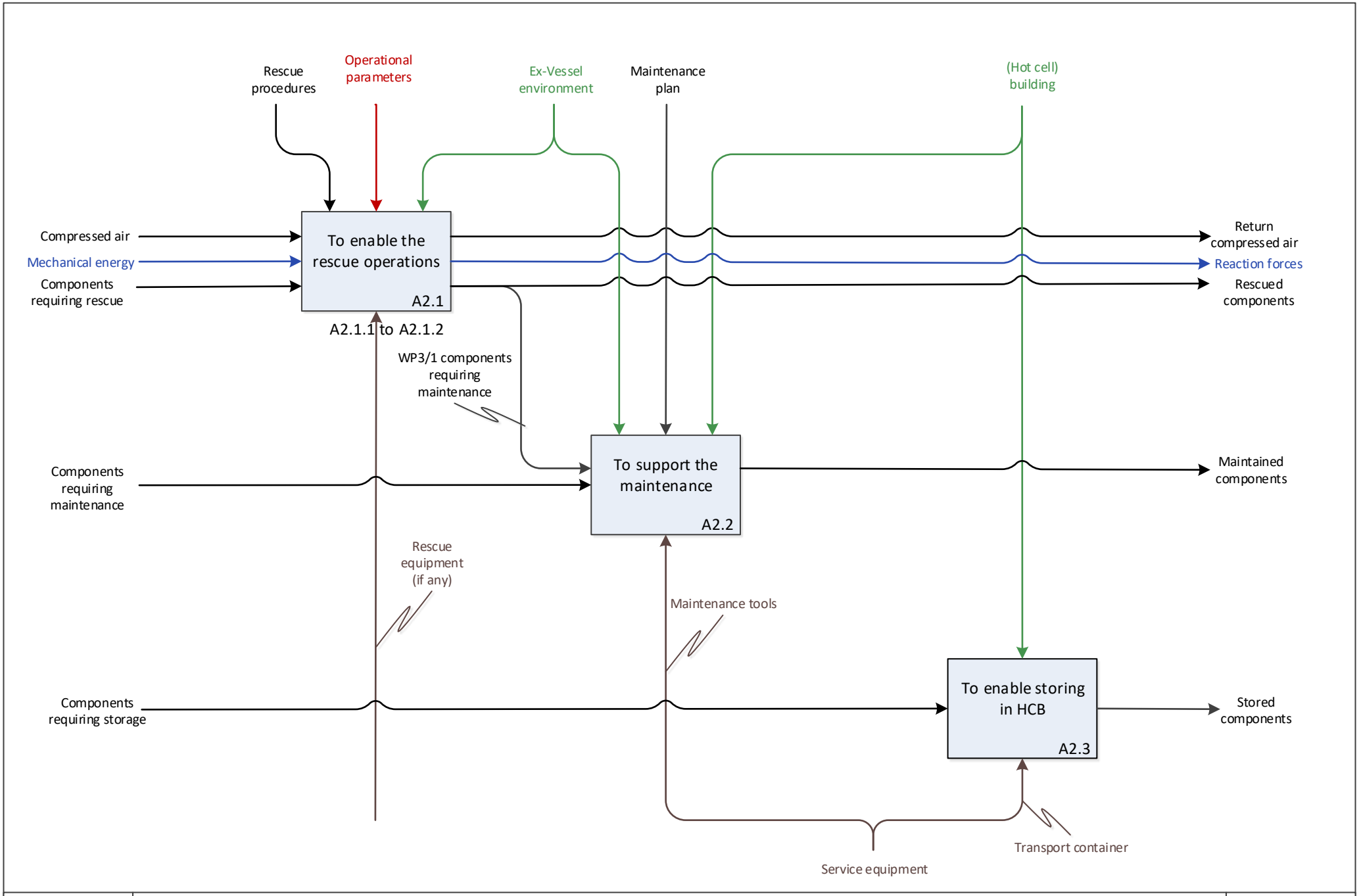

To perform periodic inspection of the Vacuum Vessel area accessible through Equatorial Port 7
A0
To control
A1
Control system
To provide user interface
A1.1
To manage the execution of WP3/1 inspection procedures
A1.2
To supply electrical energy
A1.3
Electrical cables
To provide system supervision
A1.4
Surveillance cameras
To supply air
A1.5
Compressor and air hoses
To ensure coupling fluid circulation
A1.6
Water pump and hoses
To provide support functions for the WP3/1 equipment
A2
To enable rescue operations
A2.1
Rescue equipment
To activate fail safe mechanism
A2.1.1
To enable manipulator extraction
A2.1.2
To support the maintenance
A2.2
Transport container
To enable storing in HCB
A2.3
Maintenance tools
To ensure positioning in inspection area
A3
To ensure sufficient traction force
A3.1
Spring mechanism
To lock position in rails
A3.2
Locking mechanism
To drive degree of freedom
A3.3
To control the drive
A3.3.1
Controller
To transform electrical to mechanical energy
A3.3.2
Motor
To enable rotation of the axis
A3.3.3
Bearing
To measure angular displacement
A3.3.4
Encoder
To transfer mechanical energy
A3.3.5
Gearbox
To guide driven arm
A3.3.6
Gearbox
To signal end position
A3.4
Limit switch
To lock degree of freedom
A3.5
Pneumatic lock
To align inspection sled to VV surface
A3.6
Pneumatic mechanism
To conduct visual, surface and volumetric examinations
A4
To illuminate inspection area
A4.1
Camera lights
To record with cameras
A4.2
Cameras
To scan with ET probes
A4.2
ET probes
To scan with UT probes
A4.2
UT probes
To prevent loss of coupling fluid
A4.3
To transfer inspection data
A4.4
Signal cables



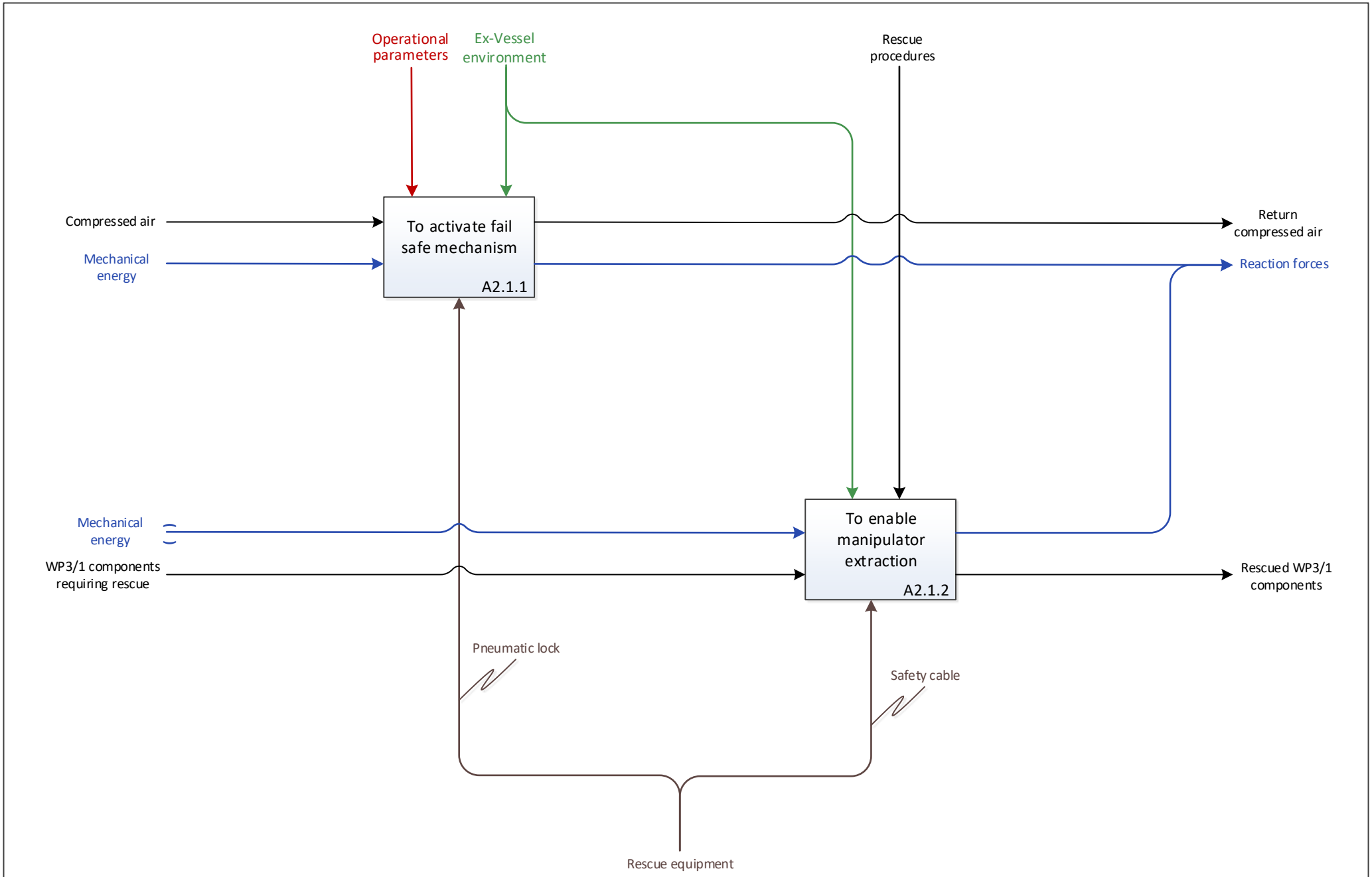
NODE: A0	TITLE: To perform periodic inspection of the Vacuum Vessel outer wall area accessible through Equatorial Port 7	NO.: 1



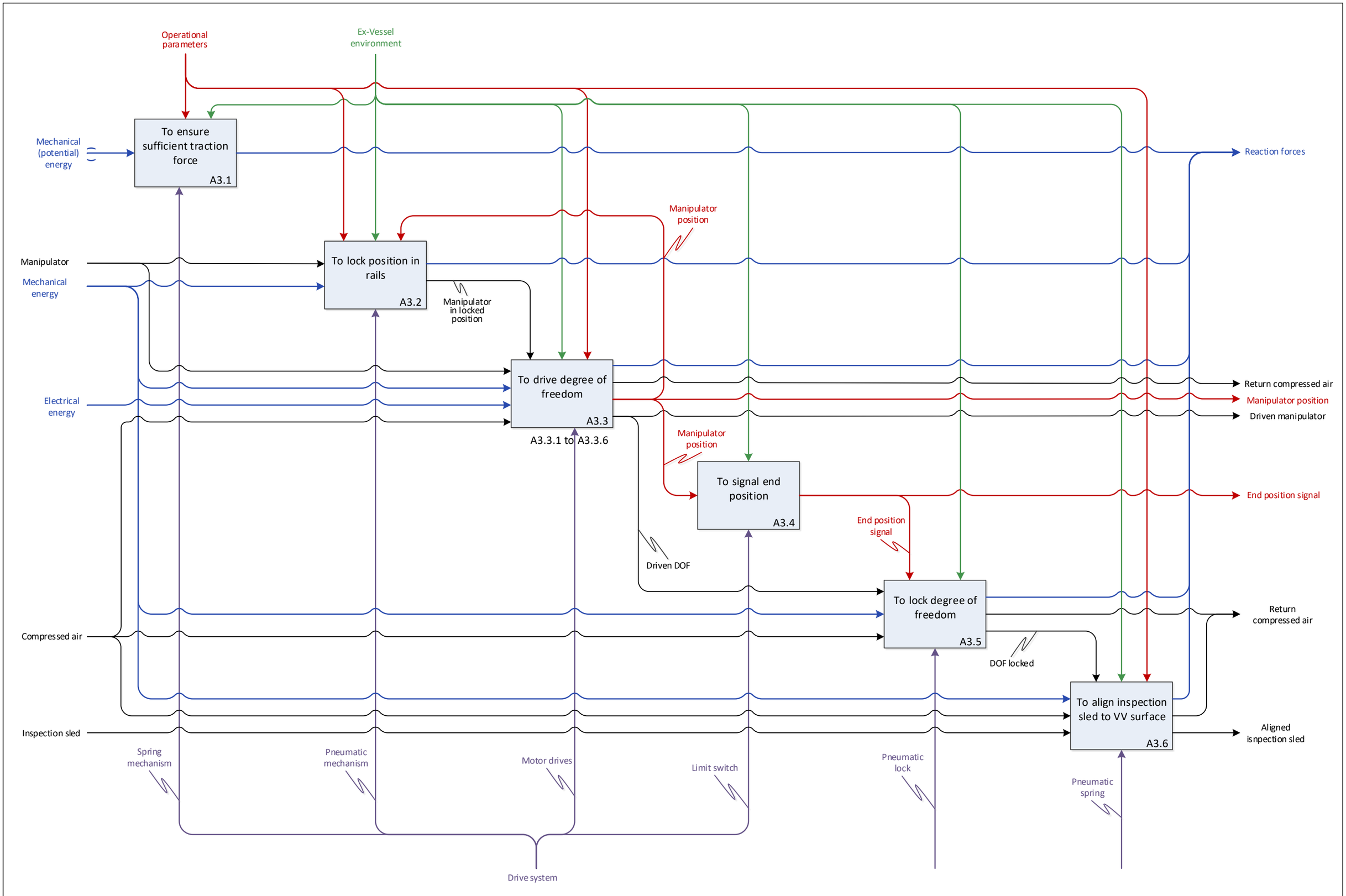
NODE: A1	TITLE: To control	NO.: 2



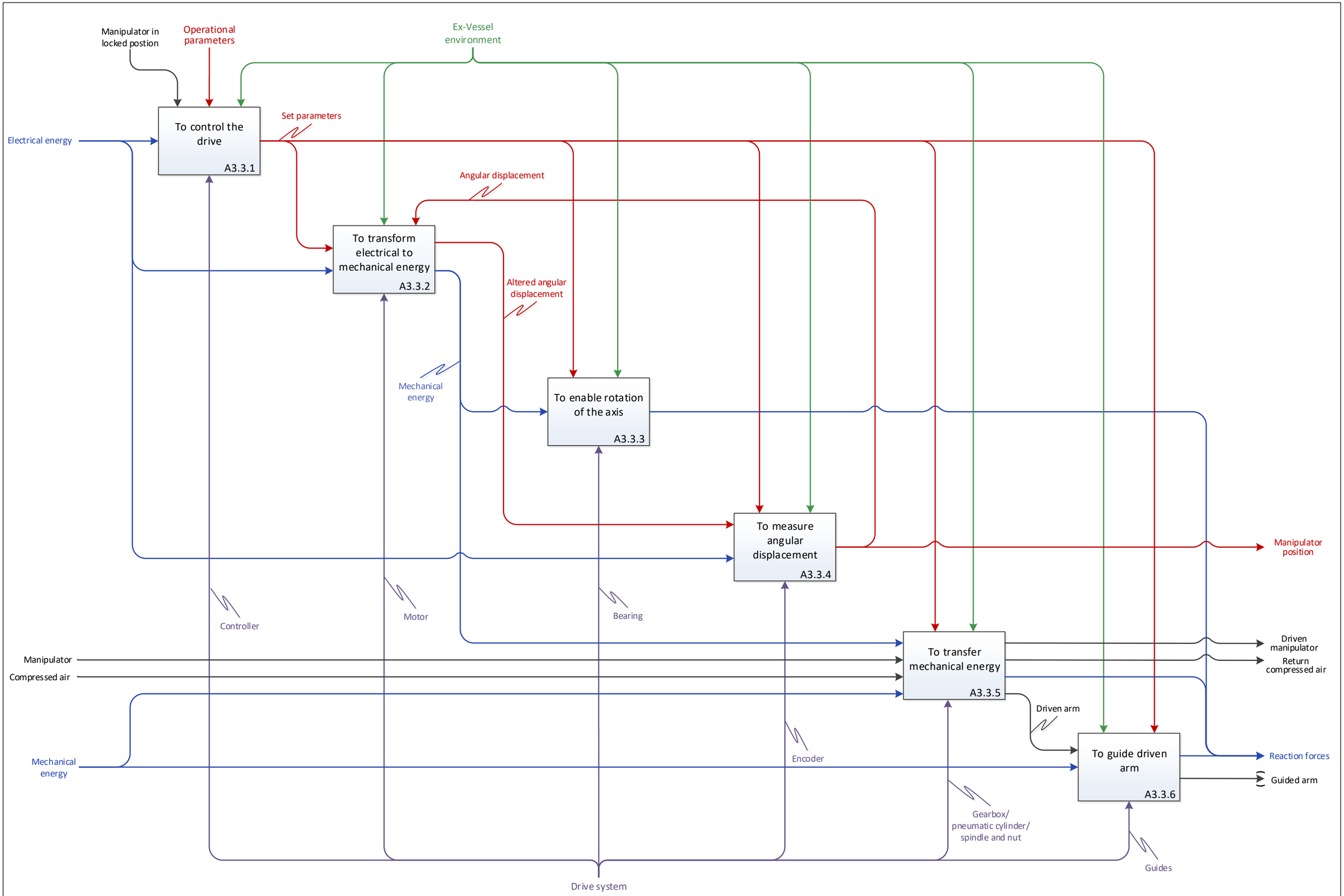
NODE: A2	TITLE: To provide support functions of the WP3/1 equipment	NO.: 3



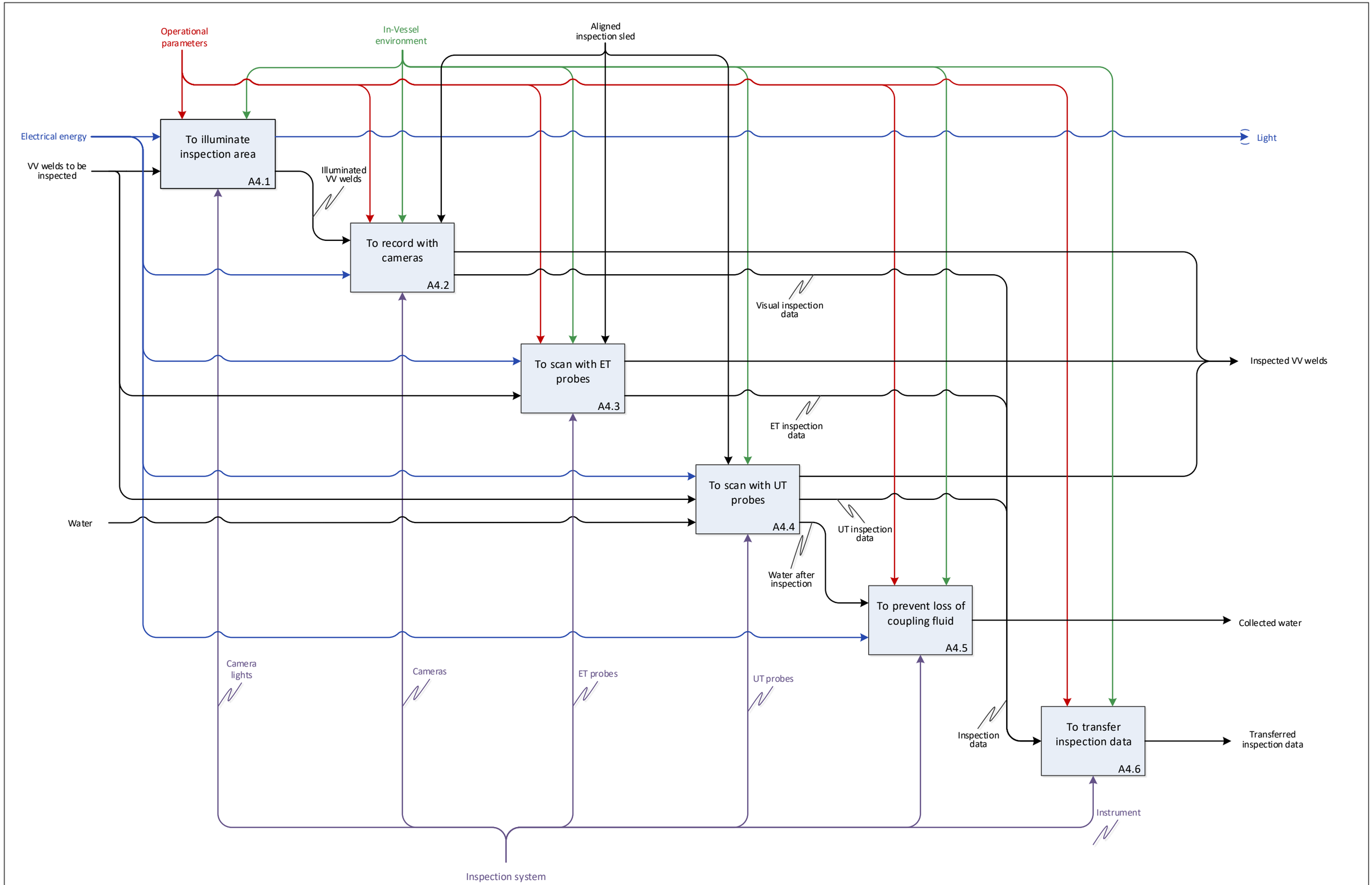
NODE: A2.1	TITLE: To enable rescue operations	NO.: 4



NODE: A3	TITLE: To ensure positioning in inspection area	NO.: 5



NODE: A3.3	TITLE: To drive degree of freedom	NO.: 6



NODE: A4	TITLE: To conduct visual, surface and volumetric examinations	NO.: 7

APENDIX B: FMECA table

This appendix contains the entire FMECA table for the in-service inspection device. To facilitate visualization, every other function and its corresponding failure modes, are coloured differently.

FMECA Analysis of the in-service inspection															
Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A1 To control															
A1.1 To provide user interface	Computer not working	Cable damage	Use appropriate cable protection/ Ensure adequate storage	Inability to conduct inspection	Replace cable	1	1h	4	2,283E-05	INETEC	5y	1	4	4	2,740E-05
		Hardware damaged during transportation	Ensure adequate storage	Inability to conduct inspection	Replace damaged hardware	2	8h	3	4,566E-06	INETEC	25y	1	6	6	
A1.2 To manage the execution of the WP3/1 inspection procedures	Operational parameters set incorrectly	Wrong inspection file loaded	Train operator prior to inspection/ Check loaded file before inspection	Faulty inspection data	Repeat inspection after correcting the error	1	≤0,5h	6	8,333E-02	INETEC	12h	1	6	6	3,014E-01
		Operator error	Train operator prior to inspection	Faulty inspection data	Repeat inspection after correcting the error	1	0,5h	6	8,333E-02	INETEC	12h	2	6	12	
		Software malfunction	Test operation before inspection	Faulty inspection data	Restart computer and repeat inspection	2	6h	6	8,333E-02	INETEC	12h	1	12	12	
	Software reports an error	Tripped circuit breaker	Test operation before inspection	Inability to continue inspection	Reset circuit breaker	1	0,5h	6	1,389E-02	INETEC	3d	3	6	18	
		Overload	Avoid collision when driving manipulator	Possible damage to electronic components	Troubleshoot error and continue inspection after fixing it	2	12h	6	2,083E-02	INETEC	2d	3	12	36	
		Incorrect positioning information received	Calibrate positioning assembly before inspection	Faulty inspection data	Repeat inspection after correcting the error	1	0,5h	6	8,334E-03	A3.3.4	5d	2	6	12	
		Incorrect positioning information received	Calibrate positioning assembly before inspection	Collision with Ex-Vessel Environment	Check for and repair damage after inspection	1	0,5h	6	8,334E-03	A3.3.4	5d	2	6	12	
A1.3 To supply electrical energy	Amplifier not working	Overheating	Use appropriate cooling	Inability to continue inspection	Replace amplifier/ Reset circuit breaker/ Restart amplifier after cooldown	2	3h	6	2,976E-03	INETEC	14d	3	12	36	3,265E-03
	Converter not working	Overheating	Use appropriate cooling	Tripped circuit breaker	Reset circuit breaker	2	3h	4	3,805E-05	INETEC	3y	3	8	24	
	Cable gets stuck	Excessive length of cable pushed	Inrease tension of cable/ Check tension during pushing	Manipulator stuck inside the rails	Emergency removal	1	1h	5	1,142E-04	INETEC	1y	1	5	5	
		Cable reel not spinning	Test operation before inspection	Manipulator stuck inside the rails	Emergency removal/ Pause inspection to fix cable reel	2	16h	4	2,283E-05	INETEC	5y	1	8	8	
	Connector is damaged	Increased cable tension	Reduce tension of cable/ Check tension during pushing	Power supply cut off	Replace connector	2	12h	4	2,283E-05	LEMO	5y	3	8	24	
		Mishandling of connection	Train operator prior to inspection/ Simplify connections	Power supply cut off	Replace connector	2	12h	4	2,283E-05	INETEC	5y	3	8	24	
	Cable disconnects	Connector is damaged	Check connection after installation	Power supply cut off	Reattach connector and glue if neccessary	2	12h	4	2,283E-05	LEMO	5y	3	8	24	
	Cable is damaged	Increased cable tension	Reduce tension of cable/ Check tension during pushing	Power supply cut off	Replace cable	2	6h	4	2,283E-05	LEMO	5y	3	8	24	
		Damage due to collision with Ex-Vessel environment	Use appropriate cable protection	Power supply cut off	Replace cable	2	12h	4	2,283E-05	INETEC	5y	3	8	24	

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A1.4 To provide system supervision	No signal from camera	Signal cable is damaged	Use appropriate cable protection	Inability to supervise inspection	Replace cable	2	2h	4	2,283E-05	INETEC	5y	3	8	24	9,309E-03
		Signal cable is disconnected	Check connection after installation	Inability to supervise inspection	Reattach connector and glue if neccessary	2	2h	4	2,283E-05	INETEC	5y	3	8	24	
		Signal cable connector is damaged	Reduce tension of cable/ Train operator prior to inspection/ Simplify connections	Inability to continue inspection	Replace connector	2	2h	4	2,283E-05	LEMO	5y	3	8	24	
		Power supply cut off	Train operator prior to inspection	Inability to supervise inspection	Replace malfunctioned part	2	2h	6	3,265E-03	A1.3	5y	3	12	36	
	Poor image quality	Radiation damage to camera	Shield camera/ Use camera with higher radiation resistance	Inspection supervision is only partial	Pause the inspection/ Replace camera or camera part	2	3h	6	2,976E-03	INETEC	14d	1	12	12	
	No signal from camera	Radiation damage to camera	Shield camera/ Use camera with higher radiation resistance	Inability to supervise inspection	Replace camera or camera part	2	3h	6	2,976E-03	INETEC	14d	3	12	36	
		Mechanical damage to cameras	Change position of the camera on the manipulator to avoid clashes with Ex-Vessel geometry	Inability to supervise inspection	Replace damaged part	2	3h	4	2,283E-05	INETEC	5y	3	8	24	
A1.5 To supply air	Pneumatic hose is bent	Wrongly positioned during assembly	Test airflow after installation	Reduced or no airflow	Reassemble pneumatic installations	1	0,5h	4	2,854E-05	INETEC	4y	3	4	12	4,189E-02
		Not enough space envisioned during design	Test airflow after installation/ Redesign surrounding components in oder to avoid bending	Reduced or no airflow	Reposition hose if possible	3	2d	6	4,167E-02	INETEC	24h	3	18	54	
	Air leakage	Damage of pneumatic hose	Check hose before and after installation/ Reposition hose to avoid sharp components	Reduced or no airflow	Replace damaged hose	2	2h	5	8,064E-05	FESTO	4y	3	10	30	
		Valve leaks	Test airflow after installation	Reduced or no airflow	Replace damaged valve	2	2h	4	2,016E-05	FESTO	4y	3	8	24	
		Cylinder leaks	Check the cylinder before and after installation	Reduced or no airflow	Replace cylinder	2	2h	4	2,016E-05	FESTO	4y	3	8	24	
		Seal leaks	Check the seal before and after installation	Reduced or no airflow	Replace seal	2	2h	4	1,418E-06	NPRD	4y	4	8	32	
	Valve doesn't open/close	Valve anchor failure	Check valve operation before and after installation	No airflow	Replace damaged valve	2	2h	4	2,016E-05	FESTO	4y	2	8	16	
	Pneumatic hose is disconnected	Increased tension of pneumatic hose	Check connection after installation	No airflow	Reconnect pneumatic hose/ Replace connector	1	0,5h	5	5,708E-05	INETEC	2y	1	5	5	

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A1.6 To ensure coupling fluid circulation	Water leaks inside the device	Damage of water hose	Check water hose before installation/ Use appropriate cable protection	Short circuit on electronic components	Seal off electronic components	3	30h	3	1,746E-06	NPRD	4y	1	9	9	2,018E-04
		Valve leaks	Test flow after installation	Short circuit on electronic components	Seal off electronic components/ Replace malfunctioned components	2	0,5h	4	2,621E-05	NPRD	5y	4	8	32	
		Seal leaks	Check the seal before and after installation	Short circuit on electronic components	Seal off electronic components/ Replace malfunctioned components	2	0,5h	3	1,418E-06	NPRD	4y	4	6	24	
	Water hose is clogged	Particles from VV surface are collected together with water from under the probe	Redesign assembly to include a filter	Inability to conduct volumetric inspection	Replace clogged hose/ Unclog the hose	2	2h	3	1,746E-06	NPRD	4y	3	6	18	
	Water hose is bent	Wrongly positioned during assembly	Check flow after instalation	Inability to conduct volumetric inspection	Reassemble hydraulic installations	2	2h	4	2,854E-05	INETEC	4y	3	8	24	
	Water hose is disconnected	Increased tension of water hose	Check connection after installation	Water leaks outside the device	Improve/test sealing on the housing	4	1w	3	1,746E-06	NPRD	4y	1	12	12	
		Increased tension of water hose	Check connection after installation	Water leaks inside the device	Seal off electronic components/ Replace malfunctioned components	2	2h	5	1,142E-04	A3.6	4y	3	10	30	
	Valve doesn't open/close	Valve anchor failure	Check valve operation before and after installation	Inability to conduct volumetric inspection	Replace damaged valve	2	3h	4	2,621E-05	NPRD	5y	2	8	16	
A2 To provide support functions for the WP3/1 equipment															
A2.1 To enable rescue operations															
A2.1.1 To activate fail safe mechanisms	Manipulator arm not retracted	Spring failure	Test airflow before inspection/ Troubleshoot	Manipulator stuck inside the rails	Emergency removal (despite the arm breaking)	4	1w	4	2,385E-05	NPRD	-	3	16	48	1,733E-04
		Plastic deformation of the guides	Avoid collision when driving manipulator	Difficulties during manipulator extraction	Emergency removal	2	4h	4	1,142E-05	INETEC	10y	1	8	8	
	Sled not lifted	Spring failure	Test airflow before inspection/ Troubleshoot	Manipulator stuck inside the rails	Emergency removal (despite the sled breaking)	2	4h	4	2,385E-05	NPRD	-	3	8	24	
	Manipulator arm retracts before the sled lifts	Operator/Software error	Redesign mechanism/ Test mechanism operation before inspection	Difficulties during manipulator extraction	Emergency removal (despite the sled breaking)	2	4h	4	5,708E-05	A1.2	2y	1	8	8	
		Operator/Software error	Redesign mechanism/ Test mechanism operation before inspection	Mechanical damage to the sled	Replace sled after damage	2	4h	4	5,708E-05	A1.2	2y	1	8	8	
A2.1.2 To enable manipulator extraction	None					1	-	1	-	-	-	1	1	1	
A2.2 To support the maintenance	Mechanical damage	Mishandling	Train operator prior to inspection	Inability to continue inspection	Replace damaged part	1	0,5h	5	5,708E-05	INETEC	2y	1	5	5	5,708E-05
A2.3 To enable storing in HCB	None					1	-	1	-	-	-	1	1	1	

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A3 To ensure positioning in inspection area															
A3.1 To ensure sufficient traction force	Slipping	Insufficient normal force	Increase pressure/ Test mechanism operation before inspection	Loss of precision for positioning	Reposition and repeat inspection	1	0,5h	4	2,854E-05	INETEC	4y	1	4	4	1,259E-04
	Wheels cannot spin	Excessive applied force	Decrease pressure/ Test mechanism operation before inspection	Manipulator stuck inside the rails	Decrease pressure/ Emergency removal	1	0,5h	4	2,854E-05	INETEC	4y	1	4	4	
	No force applied	Pneumatic mechanism assembled inaccurately	Training of people involved in assembling/ Test mechanism operation before inspection	Manipulator can't move	Check for and repair damage after inspection/ Reassemble mechanism	2	3h	4	2,854E-05	INETEC	4y	3	8	24	
		Reduced/ No airflow	Test mechanism operation before inspection	Manipulator can't move	Emergency removal and repair/reassembly	2	3h	4	4,032E-05	FESTO	4y	3	8	24	
A3.2 To lock position in rails	Pin doesn't extend	Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Position cannot be secured	Replace damaged part and redo inspection	2	3h	4	4,032E-05	FESTO	4y	3	8	24	3,017E-03
	Pin extends at the wrong time	Operational parameters set incorrectly	Test mechanism operation before inspection	Manipulator operation abrupted	Retract pin and continue inspection	1	0,5h	6	2,976E-03	INETEC	14d	2	6	12	
A3.3 To drive degrees of freedom															
A3.3.1 To control the drive	Connector between the motor and the PCB is damaged	Mishandling during assembly	Training of people involved in assembling/ Use higher quality connectors	Drive not working	Replace connector	2	12h	4	2,854E-05	INETEC	4y	3	8	24	8,562E-05
	Loose PCB	Screw connection loosened by vibrations	Check screw connections during assembling	Possible damage to electronic components and cables	Use industrial glue for connecting the screw again	2	12h	4	2,854E-05	INETEC	4y	4	8	32	
	Overheating	Insufficient cooling of the motor drive	Use thermal grease between the motor drive and the housing surface	Damage to electronic components	Pause inspection/ Replace damaged components	2	12h	4	2,854E-05	INETEC	4y	2	8	16	
A3.3.2 To transform electrical to mechanical energy	Cable damage	Mishandling during assembly	Use appropriate cable protection	Drive not working	Replace cable	2	12h	4	2,283E-05	INETEC	5y	3	8	24	1,218E-04
		Sharp objects inside the housing	Redesign housing/ Reposition cable	Drive not working	Replace cable	2	12h	4	2,283E-05	INETEC	5y	3	8	24	
	Motor stopped working	Overload	Avoid collision when driving manipulator	Drive not working	Replace motor	2	12h	5	7,610E-05	INETEC	1,5y	3	10	30	
A3.3.3 To enable rotation of the axis	Plastic deformation of the bearings	Overload	Avoid collision when driving manipulator	Operating difficulties due to increased friction	Replace bearing	2	12h	4	7,996E-06	NPRD	5y	3	8	24	7,996E-06
A3.3.4 To measure angular displacement	Inaccurate distance from encoder reading head to the magnetic ring	Encoder failure	Quality control of components after assembly	Wrong values on drive absolute encoder	Reassemble/ replace encoder	2	12h	3	7,61E-07	RLS	5y	3	6	18	8,334E-03
	Backlash in manipulator drive assembly	Measuring is performed on the side of the motor, not the load	Reduce the backlash and elasticity of the mechanism	Software receives incorrect positioning information	Use a different encoder/ Incorporate total backlash in the software	2	12h	6	8,333E-03	INETEC	5d	3	12	36	

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A3.3.5 To transfer mechanical energy	Backlash in manipulator drive assembly	Abrasive wear	Test mechanism operation before inspection	Software receives incorrect positioning information	Replace damaged component	2	12h	4	1,598E-06	HPC	10y	3	8	24	1,225E-04
	Damaged gear/belt	Overload	Avoid collision when driving manipulator	Drive not working	Replace damaged component	2	12h	4	2,283E-05	INETEC	5y	3	8	24	
		Abrasive wear	Use grease	Backlash in manipulator drive assembly	Replace damaged component	2	6h	4	1,598E-06	HPC	10y	4	8	32	
	Damaged shaft	Overload	Avoid collision when driving manipulator	Drive not working	Replace damaged component	2	12h	3	6,199E-07	NPRD	5y	3	6	18	
	Damaged clutch/ shaft key	Overload	Avoid collision when driving manipulator	Drive not working	Replace damaged component	2	12h	4	9,988E-06	NPRD	5y	3	8	24	
	Plastic deformation of the cylinder for arm extension	Overload	FEM analysis of component before production/ Avoid collision when driving manipulator	Arm locked at current length	Redesign component or use material with higher tensile strength/ Replace cylinder	2	12h	1	never fails	INETEC	5y	1	2	2	
	Pneumatic cylinder cannot extend	Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Arm locked at current length	Replace damaged part and redo inspection	2	12h	5	8,064E-05	FESTO	5y	3	10	30	
	Spindle nut is stuck	Abrasive wear	Test mechanism operation before inspection	Arm locked at current length	Emergency removal/ Replace component	2	12h	2	4,762E-07	INETEC	4y	1	4	4	
		Particles from VV surface enter spindle nut	Training of people involved in assembling	Operating difficulties due to increased friction	Replace component	2	6h	3	4,762E-06	INETEC	5y	3	6	18	
A3.3.6 To guide driven arm	Plastic deformation of the guides	Overload	FEM analysis of component before production	Operating difficulties due to increased friction	Redesign component or use higher strength material	2	12h	3	5,708E-06	INETEC	20y	1	6	6	5,708E-06
A3.4 To signal end position	Cable is damaged	Mishandling during assembly	Use higher quality connectors	Limit switch not transmitting signals	Replace cable	1	12h	4	2,283E-05	INETEC	5y	2	4	8	8,802E-05
		Damage due to exploitation	Secure limit switch cables away from moving and sharp parts	Limit switch not transmitting signals	Replace cable	1	12h	5	6,519E-05	FESTO	5y	2	5	10	
A3.5 To lock degree of freedom	Plastic deformation of the locking pin	Overload	FEM analysis of component before production	Operating difficulties due to increased friction	Redesign component or use higher strength material	3	12h	3	4,566E-06	INETEC	25y	1	9	9	2,465E-04
	Position od the arm isn't locked	Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Arm rotates during inspection	Redo inspection after repairing rotation lock	2	12h	5	8,064E-05	FESTO	∞	3	10	30	
		Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Arm retracts during inspection	Redo inspection after repairing extension lock	2	12h	5	8,064E-05	FESTO	∞	3	10	30	
	Position od the sled isn't locked	Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Sled rotates during inspection	Redo inspection after repairing sled lock	2	12h	5	8,064E-05	FESTO	∞	2	10	20	
A3.6 To align inspection sled to VV surface	Inspection sled (probes) lift off	Insufficient amount of water under the probe	Reduce the amount of lifting during inspection/ Improve circulation mechanism	Poor quality of inspection data	Redign surrounding components to adjust the probe to surface/ Repeat inspection	2	0,5h	6	8,333E-02	INETEC	12h	1	12	12	1,282E-01
		Damage due to clashes with Ex-Vessel environment	Avoid collision when driving manipulator/ Change material of inspection sled	Inability to conduct inspection	Replace damaged parts	2	3h	6	2,976E-03	INETEC	14d	1	12	12	
		Increased speed	Train operator prior to inspection/ Decrease speed	Poor quality of inspection data	Redo inspection	1	0,5h	6	4,167E-02	INETEC	24h	1	6	6	
		Strained cables connected to probes	Test mechanism operation before inspection	Inability to conduct inspection	Reposition cables and redo inspection	2	3h	5	1,142E-04	INETEC	1y	1	10	10	
		Reduced/ No airflow	Test airflow before inspection/ Troubleshoot	Inability to change sled height	Replace damaged component	2	3h	5	8,064E-05	FESTO	4y	3	10	30	

Function	Failure mode	Possible causes	Preventive Action on Possible Causes	Effects	Corrective or Preventive Action on Effects	Si	MTTR	Oi	λ	λ from	MTBF/ replac.	Di	Ci	RPN	λ(SUM)
A4 To conduct visual, surface and volumetric examinations															
A4.1 To illuminate inspection area (with dimming effect)	Light on the camera not working	Cable damage	Use appropriate cable protection	Poor quality of inspection data	Replace light and/or cable	1	2h	6	3,265E-03	A1.3	4y	2	6	12	7,589E-03
	Dimming effect not working	Cable damage	Use appropriate cable protection	Poor quality of inspection data	Replace camera and/or cable	1	2h	6	3,265E-03	A1.3	4y	2	6	12	
		Potentiometar failure	Avoid collision when driving manipulator	Poor quality of inspection data	Replace/adjust potentiometar	1	2h	6	1,059E-03	NPRD	2y	2	6	12	
A4.2 To record with cameras	No signal from camera	Signal cable is damaged	Use appropriate cable protection	Poor quality of inspection data	Replace cable	1	2h	6	3,265E-03	A1.3	5y	2	6	12	1,579E-02
		Signal cable is disconnected	Check connection after installation	Poor quality of inspection data	Reattach connector and glue if neccessary	1	2h	6	3,265E-03	A1.3	5y	2	6	12	
		Signal cable connector is damaged	Reduce tension of cable/ Train operator prior to inspection/ Simplify connections	Poor quality of inspection data	Replace connector	1	2h	4	2,283E-05	LEMO	5y	2	4	8	
		Power supply cut off	Train operator prior to inspection	Poor quality of inspection data	Replace malfunctioned part	1	2h	6	3,265E-03	A1.3	5y	3	6	18	
	Poor image quality	Radiation damage to camera	Shield camera/ Use camera with higher radiation resistance	Poor quality of inspection data	Pause the inspection/ Replace camera or camera part	1	2h	6	2,976E-03	INETEC	14d	2	6	12	
	No signal from camera	Radiation damage to camera	Shield camera/ Use camera with higher radiation resistance	Poor quality of inspection data	Replace camera or camera part	1	2h	6	2,976E-03	INETEC	14d	3	6	18	
		Mechanical damage to cameras	Change position of the camera on the manipulator to avoid clashes with Ex-Vessel geometry	Poor quality of inspection data	Replace damaged part	1	2h	4	2,283E-05	INETEC	5y	3	4	12	
A4.3 To scan with ET probes	Cable is damaged	Increased cable tension	Reposition cable to reduce tension	Inability to conduct inspection	Replace cable	1	2h	6	1,389E-02	INETEC	3d	3	6	18	2,780E-02
	Connector is damaged	Increased cable tension	Reposition cable to reduce tension	Inability to conduct inspection	Replace connector	1	2h	4	2,283E-05	LEMO	5y	3	4	12	
	Probes are worn out	Friction between probes and VV surface	Use higher quality probes	Poor quality of inspection data	Replace probe	1	3h	6	1,389E-02	INETEC	3d	2	6	12	
A4.4 To scan with UT probes	Cable is damaged	Increased cable tension	Reposition cable to reduce tension	Inability to conduct inspection	Replace cable	1	3h	6	1,389E-02	INETEC	3d	3	6	18	1,391E-02
	Connector is damaged	Increased cable tension	Reposition cable to reduce tension	Inability to conduct inspection	Replace connector	1	3h	4	2,283E-05	LEMO	5y	3	4	12	
A4.5 To prevent loss of coupling fluid	**TBD**														
A4.6 To transfer inspection data	Noise in the signal	Motor is in contact with housing	Redesign housing to avoid contact	Poor quality of inspection data	Repeat inspection	2	12h	4	2,283E-05	INETEC	5y	3	8	24	2,283E-05
		Magnetism	Shield cable	Poor quality of inspection data	Repeat inspection	3	-				-	3	0	0	