UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE CIENCIAS FÍSICAS
DEPARTAMENTO DE FÍSICA APLICADA III (ELECTRICIDAD Y ELECTRÓNICA)

APPLICATION OF INTERNATIONAL QUALITY STANDARDS TO SCIENTIFIC RESEARCH
PRODUCT ASSURANCE IN LARGE SCIENTIFIC INSTALLATIONS

APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE CALIDAD A LA INVESTIGACIÓN CIENTÍFICA
ASEGURAMIENTO DEL PRODUCTO EN GRANDES INSTALACIONES CIENTÍFICAS

TESIS DOCTORAL DE:
TEODORO BERNARDINO SANTOS

DIRIGIDA POR:
JOSÉ MIGUEL MIRANDA PANTOJA

Madrid, 2014

APPLICATION OF INTERNATIONAL QUALITY STANDARDS TO SCIENTIFIC RESEARCH: PRODUCT ASSURANCE IN LARGE SCIENTIFIC INSTALLATIONS

PhD Thesis Project by:
Teodoro Bernardino Santos

Directed by:
Dr. José Miguel Miranda Pantoja

Universidad Complutense de Madrid
Departamento de Física Aplicada III
Electricidad y Electrónica

Madrid, June 2013

Contents

Tables

Figures

Contents

Chapter 1

Introduction

It is often said that science broadens our knowledge of the Universe, while engineering brings these knowledge to our daily life. This document is aimed at presenting a bridge between the engineering standards that drive the industrial processes and the design & implementation of scientific installations.

The development of new scientific installations has always been a challenging task, as usually implies exploring technologies beyond the limit of the actual knowledge. However, it is not only from a technological point of view that the scientific installations are so demanding, they are also huge projects that need an efficient managerial structure, and should be reliable from the point of view of their design, implementation and operation to accomplish their scientific goals.

On the other hand, the engineering of industrial processes has undergone in the last quarter of past century up to present time an evolution of the techniques aimed at providing the most reliable products with the highest efficiency in their development.

On top of that, there is an area which usually deals with both topics, scientific installations and efficient industrial processes: the aerospace sector. Involving three types of different actors: The national -or international- agencies, the scientific committees/institutions and the industry, they are obliged to define rules for the proper definition, implementation, validation of the products as well as the efficient management and coordination of the associated projects to produce them.

This work is aimed at presenting the experience gathered in two different scientific projects, the European Space Agency's PLANCK mission, and the Cherenkov Telescope Array – CTA. The activities carried out in different areas plus the methodologies applied, led to the idea of defining a general Product Assurance procedure which could be applied to any scientific installation.

The goal behind this procedure is to exploit the benefits of the consolidated techniques used throughout the engineering processes in the industry applied to the scientific installations.

1.1 Context

Scientific research is immersed, as almost everything in the world, in a globalization process. The attempt to reach further and further in the nature of the elementary particles, the structure of the Universe, the planetary exploration, etc. demands the development of challenging scientific installations which are more complex, expensive and bigger each time.

The design and implementation of such installations cannot be assumed by a single research institution or even a single country. The magnitude of the effort and cost needed to build them exceeds what can be assumed individually, so the only way to bring them into reality is their internationalization, i.e. the collaboration of several institutions from countries worldwide.

On the other hand, the scientific requirements which shall be accomplished for the installation to provide the desired performances are so demanding that there shall be an excellent collaboration between the scientific and engineering teams to succeed in their construction. This implies, in many cases, that scientific teams are involved in engineering tasks and vice-versa.

The scenario presented above for a so-called **Large Scientific Installation** (LSI) by the previous paragraphs hence faces several problems which shall be properly addressed, among which is worth to mention:

- The definition of the appropriate **managerial structure** to ensure the correct governance of the project during the entire lifetime: concept, design, implementation, operations and disposal.

- The definition of the appropriate **procedures and plans** by the aforementioned managerial structure for the different working groups to devote their activity according to them.
- The definition of internal and/or external **auditing teams** in charge of verifying the correct application of those procedures and plans in the final products.

This schematic description of how the biggest scientific installations are made is obviously too simplistic. Actually, it is not the goal of this introduction to deeply analyse the different types of problems which could face a Large Scientific Installation, but to define to context to which the work of subsequent chapters apply.

The industrial production is driven by a set of procedures, methods and checks which compose the so-called Product Assurance. That methodology is not so deeply integrated in the design and implementation of the scientific installations, which usually define a completely new management policy for each project. This becomes a huge task in Large Scientific Installations when international consortiums defined *ad-hoc* manage the projects. The coordination of such consortiums usually has to deal with boundary conditions that impose important constraints completely different from the technical aspects of the project: Political issues, competition between team members instead of cooperation, lack of understanding between the scientific committee in charge of defining the project's objectives and the technical team in charge of implementing it, etc.

In the aerospace sector, this scenario already occurs, with the major advantage that there is a top management organization which usually drives the development of the projects. Considering the three types of actors involved which were defined previously, the organization in a scientific mission in the aerospace sector is as follows:

- The **National or International Agencies** (e.g. ESA[1], NASA[2], CNES[3], DLR[4], etc.) are the higher managerial structure of these projects, coordinating both the scientific committees and the industries.

[1] ESA: European Space Agency (Europe)
[2] NASA: National Aeronautics and Space Administration (United States)
[3] CNES: Centre Nationale des Etudes Spatiales (France)

- The **Scientific Institutions/Committees** are in charge of defining and supervising the scientific objectives of the mission, and co-operates with the industry in the design and production of the scientific payload.
- The **Aerospace Industry** is mainly composed of private owned companies in charge of designing and developing specific elements of the mission, under the supervision of the National/International Agencies and in collaboration with the Scientific Institutions/Committees.

Apart from the pre-defined managerial structure with the different actors involved, the aerospace sector has entire sets of norms, standards and procedures for almost every aspect of its activities.

In the general industry, as explained before, the Product Assurance management is driven by international standards that define the minimum requirements that a single company / institution must comply for a pre-defined level of certification (for instance, ISO standards).

In the aerospace sector, these international standards have been augmented to cover specific areas of aeronautics, navigation, manned space flights, etc. For instance, the European Coordination for Space Standardization (ECSS) maintains the so-called ECSS standards which are applicable to all ESA projects.

In the case of a Large Scientific Installation, it is common to start from "scratch", hence defining the applicable rules for Product Assurance at the same time as the managerial structures of the project are been consolidated. This may lead to a lack of "time to market" in the provision of the needed procedures & rules to the different working groups during their activities.

At these early development stages of Large Scientific Installations, mainly in those that stem from an ad-hoc international consortium, the core of the manpower is mainly composed of scientists that deal with scientific, industrial and managerial aspects of the project. This scenario may lead to inefficiently tackling the provision of the predefined set of Product Assurance rules, as the scientists are mainly talented people with an absolute knowledge of the scientific aspects of the project, but not so of the industrial processes involved in its development.

This situation is the one intended to be overcome with the proposed solution: The definition of an entire procedure for Product Assurance applicable to almost any Large Scientific Installation that allows speeding up the internal settlement of the rules that will drive its development, with a significant reduction of the associated effort & time needed to prepare them.

[4] DLR: Deutschen Zentrums für Luft- und Raumfahrt (Germany)

1.2 Background experience

A new entire procedure for the management of Product Assurance is presented. It is intended to be flexible enough as to fit the needs of any Large Scientific Installation with very small modifications, as will be summarized in section 1.3

The procedures proposed for the aforementioned disciplines is the result of joining the experience gathered in two different projects: ESA's PLANCK mission and CTA, at two different levels:

1.2.1 The PLANCK mission

The European Space Agency PLANCK mission is the third medium-sized mission (M3) of the Horizon 2000 scientific programme. It was conceived for the detection of the anisotropies of the Cosmic Microwave Background (CMB) radiation, remnant of the Big Bang and the major source of experimental data for testing cosmological models. It contains two instruments on board:

- The High Frequency Instrument (HFI), covering the frequency range from 100 to 845 GHz.
- The Low Frequency Instrument (LFI), with three channels at 30, 44 and 70 GHz.

From the point of view of the work devoted to the PLANCK mission and the experience gathered for the purpose of the procedures presented in the final solution, the major highlights are listed below:

- PLANCK is an excellent example of a Large Scientific Installation developed in the frame of the aerospace sector, with its three actors clearly identified:
    - ESA being the International Agency leading the project,
    - The scientific committee being a group of Universities and Research centres led by Nazzareno Mandolesi, from Istituto di Astrofisica Spaziale e Fisica Cosmica (INAF - IASF) in Bologna (Italy) for the Low Frequency Instrument and Jean-Loup Puget, from Institut d'Astrophysique Spatiale (IAS - CNRS) in Orsay (France) for the High Frequency Instrument.
    - Finally, the industries in charge of manufacturing the satellite were managed by an industrial consortium led by Alcatel Space Industries (France), with Astrium GmbH (Germany) and Alenia Spazio (Italy) as main contractors.
- The work devoted to PLANCK was carried out at Instituto de Física de Cantabria (IFCA - CSIC) in Santander (Spain) and focused in:
    - The development of a physical model of the radiometers at 30 and 44 GHz of the Low Frequency Instrument, to obtain the equations that described their susceptibility to the variations in the environmental conditions of operation as a function of adjustable parameters [34].
    - The development of two modules of the software for the ground calibration of the radiometers, Radiometer aNAlyzer (RaNA): the RaNA_Oft to characterize

the zero-point offsets and dark signals, and the RaNA_Susc to characterize the parameters of the susceptibility model previously described.

- The further support to the LFI calibration activities [27], [28], [29], [30], [31].

A more detailed description of the PLANCK mission and the work devoted to it which helped in the preparation of the proposed solution will be provided in chapter 2.

1.2.2 The Cherenkov Telescope Array

The Cherenkov Telescope Array (CTA) is, by far, the most challenging project in astroparticle physics ever [32], [33]. CTA is aimed at constructing two observatories in the Northern and Southern hemispheres, with unprecedented resolution, sensitivity and dynamic range of energies covered. Both observatories will be composed of up to four different types of Imaging Air Cherenkov Telescopes (IACT's) covering each a different range of energies. An IACT does not observe the night sky objects directly, but the cascade of particles disintegrations produced in the higher layers of the atmosphere when an incident very high energy particle (a gamma-ray photon) impacts on it.

Now switching to the work devoted to CTA observatory, it is the seed of the procedures proposed in chapters 4 to 8. While PLANCK mission is a clear example of an aerospace LSI with a very well consolidated structure as per the actors identified in section 1.2.1, CTA is, on the contrary, an excellent example of a LSI started from "scratch" and coordinated by a newly defined international consortium.

The work devoted to CTA project was done at UCM_ELEC group. UCM_ELEC is the acronym for Universidad Complutense de Madrid, High Frequency Electronics group (http://pendientedemigracion.ucm.es/info/electron/CTA/), which belongs to Departamento de Física Aplicada III (Electricidad y Electrónica) of Facultad de Ciencias Físicas. Among the different tasks carried out in CTA which served as the ultimate origin of the procedures proposed, it is worth remarking:

- The contribution to the CTA Product Assurance Plans [35], [36], [37], [38], [46], [47].
- The contribution to the RAMS assessment in the different technical work packages [39], [40], [42], [43], [45].
- The contribution to the organization of the Product Assurance managerial structure [41], [44].
- The contribution to the review of the seismological risk assessment in the document for CTA-North Spanish SITE candidate proposal [22].

A more detailed description of the CTA observatory is provided in chapter 3, along with the details on the work carried out there.

1.3 The proposed solution

As a result of the experience gathered in the two LSI's presented, it was identified a clear drawback in LSI's managed by an *ad-hoc* International Consortium compared to the ones managed by an existing International Agency, as in the case of the aerospace sector examples. This drawback was reflected in:

- Lack of consensus to define the Project Plans, including the Product Assurance ones. As a result, their approval and subsequent applicability in the project suffered long delays which made them, once approved, basically not usable (at the time they had been approved they were already obsolete).
- Lack of knowledge of industrial processes. In the early stages of these *ad-hoc* LSI's, the consortium is led by the scientific committee. There is a lack of balance between the know-how in science tasks compared to engineering ones. As a result, the latters are under-estimated.
- Reluctance to adopt pre-existing standards. The change of paradigm that implies the construction of a LSI encompasses the need for a change of the way of working. Mainly in the design and implementation phases it is mandatory to adopt a series of rules that guarantee the quality of the final product. This is ensured in the industry through the usage of international standards. However, many scientists find them too demanding for the purpose of a LSI.

From the analysis of these elements it was conceived the idea of producing a tailored set of procedures to ensure the proper Product Assurance in an *ad-hoc* LSI. This solution came from the study of the international standards which are widely applied in the industry, and their subsequent adaptation of what is more suitable for a LSI.

The ideas behind this solution were exchanged [48] with experts in reliability from LSI's (ITER[5], LHC[6]) [24], [25], [26] and space projects. Their feedback was decisive in the final procedures presented.

This solution is presented in the form of standalone procedures for the main branches of Product Assurance, one defined inside a chapter, namely:

- Product Assurance Management, chapter 4.
- Quality Assurance, chapter 5.

[5] International Thermonuclear Experimental Reactor
[6] Large Hadron Collider

- Risks Management, chapter 6.
- Dependability and Safety, chapter 7.
- Rules for Software development, chapter 8.

Actually, the last chapter is not a discipline of Product Assurance by itself, but taking into account the importance of SW developments in any Large Scientific Installation (simulation, data acquisition & analysis, HW control, tasks scheduling, etc.), it was worth including a dedicated chapter for this specific aspect of the LSI's.

1.4 International Standards for Product Assurance

Among the large amount of standardization institutions and norms available, it was decided for the preparation of the procedures in the solution presented to stick mainly to the norms provided by two of the most important organizations: The International Organization for Standardization and the European Coordination for Space Standardization.

The reasons for selecting them are twofold:

- On the one hand, ISO is the most important organization in the world for standardization, with the most widely accepted set of norms.
- On the other hand, the standards provided by the ECSS are applicable to all the ESA projects, of which the most of the expertise used to develop the proposed solution come from.

Hereafter follows a brief description of both sets of standards.

1.4.1 ISO standards

The International Organization for Standardization (ISO) is a non-governmental organization based in Geneva, Switzerland, composed of national regulation institutions worldwide.

ISO produces a set of norms grouped by categories attending the subject to which they apply, labelled with a specific code (ISO 9001, ISO14000). It is important to remark that ISO norms are recommendations, since ISO being a non-governmental organization, cannot impose to a third party their rules. However, ISO allows the possibility to certify a given institution, industry or organization according to a specific norm. For instance, the ISO 9001 certification is widely used as the best indicator for the proper implementation of a Quality Management System.

The ISO standards referenced in this work are listed below:

- ISO 9000 [3], with the fundamentals for Quality Assurance.
- ISO 10006 [4], with the guidelines for Quality Assurance Management.
- ISO 17666 [8], with the recommendations for the proper Risks Management applied to space projects.

1.4.2 ECSS standards

The European Coordination for Space Standardization (ECSS) is an organization which works in the definition of a set of standards to be met by any company/institution involved in the Space sector in Europe. It was created in 1993 as an effort by ESA, national space agencies and industry for the harmonization the Product Assurance requirements.

The ECSS standards have been adopted by ESA so any contractor of this organization shall adhere to them.

ECSS rules are grouped into three branches attending the specific field to which they apply:

- ECSS-M-xx: Branch of rules applicable to Space Project Management.
- ECSS-Q-xx: Branch of rules applicable to Space Product Assurance.
- ECSS-E-xx: Branch of rules applicable to Space Engineering.

As in the case of ISO standards, inside a given branch there are many different documents, each labelled with a unique code, that group the set of rules applicable to a specific field (ECSS-E-ST-40, ECSS-Q-ST-20, ECSS-M-ST-80, etc.).

ECSS standards became the most important source of references for the procedures in the last chapters, namely the following:

- ECSS-P-001B [1], with the glossary of terms and definitions that serve to uniquely define the different concepts used.
- ECSS-S-ST-00C [2], which contains the overall description of the ECSS standards as well as the tailoring guidelines.
- ECSS-Q-ST-10C [5], with the general requirements for the Product Assurance Management.
- ECSS-Q-ST-20C [6], with the general requirements for Quality Assurance and ECSS-Q-ST-10-04C [7], with the Critical Items Control.
- ECSS-M-ST-80C [9], containing the rules for the proper Risk Assessment.
- ECSS-E-ST-40C [14] and ECSS-Q-ST-80C [15] with the engineering and quality assurance rules for software developments, respectively.

Chapter 2

Software Product Assurance in ESA's PLANCK mission: RaNA calibration software

2.1 Overview of PLANCK

2.1.1 High level description of PLANCK

PLANCK is the third medium-sized mission (M3) of ESA's Horizon 2000 programme, launched in May 2009, conceived to observe the entire sky to map the anisotropies of the Cosmic Microwave Background (CMB).

Figure 2–1: The PLANCK mission spacecraft

The CMB is the remnant radiation, almost homogeneous throughout the sky, with a black body-like thermal emission spectrum corresponding to a temperature of 2.73 K that fills the Universe. It is the most distant radiation that can be observed, as indeed it corresponds to the first photons able to propagate on a transparent medium right after the cosmological recombination. According to the Big Bang theory, when the Universe was 3.8 x 10^5 years old, the temperature descended below 3000 K approximately, allowing the protons and electrons to recombine producing the first hydrogen atoms, and the Universe became transparent to electromagnetic radiation (prior to this recombination, the scattering processes made it opaque). The study of the anisotropies of the CMB is the most valuable empirical test of cosmological models. The reason is straightforward: the anisotropies indicate the distribution of matter in the ancient Universe.

The CMB was theoretically postulated by R. Alpher and R. Herman in 1948, and observed for the first time in 1964 by A. Penzias and R. Wilson by change when mapping the radio interference spectrum.

The first anisotropies in the CMB were detected by the COBE satellite, led by G. Smoot, in 1992. PLANCK was at that time conceived as the second generation of CMB observers and was named COBRAS/SAMBA, but renamed to PLANCK in 1996 when the mission was approved by ESA.

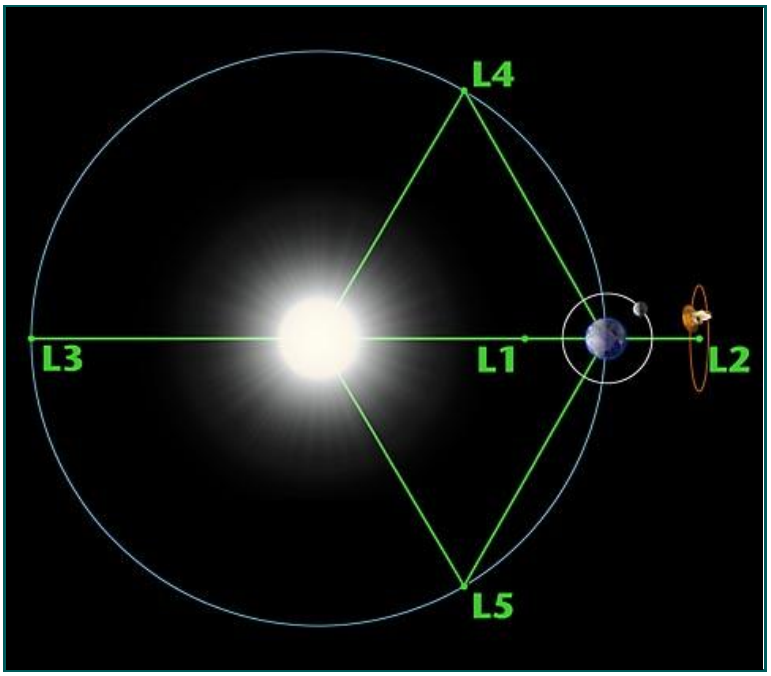


Figure 2–2: The five lagrangian equilibrium points of Sun-Earth system showing a spacecraft in a Lissajous orbit round L2

PLANCK is located in a stable orbit around the second lagrangian point of the Sun-Earth system, far enough from the interferences coming from our planet (Figure 2–2). The payload on board PLANCK consists of two instruments:

- The Low Frequency Instrument (LFI), with radiometers at 30, 44 and 70 GHz.
- The High Frequency Instrument (HFI), with bolometers at 100, 143, 217, 353, 545 and 857 GHz.

Both instruments have their front-end at extremely low temperatures, in order to reduce the noise by thermal radiation: HFI Front-End Module (FEM) operates at 4 K and LFI FEM at 20 K.

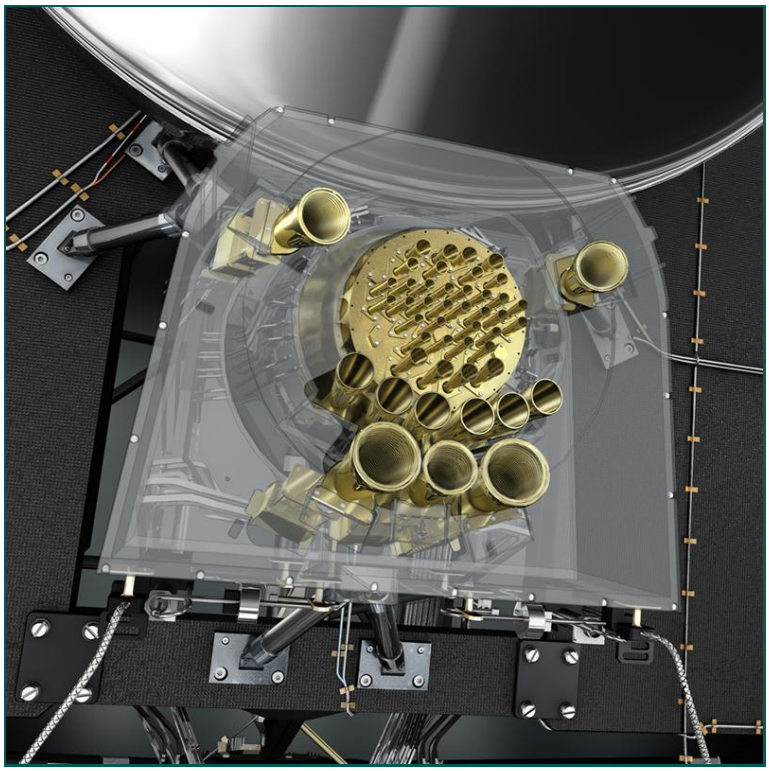


Figure 2–3: The PLANCK focal plane showing the feed-horns of the HFI bolometers (inside the circular plate) and the ones of the LFI radiometers (surrounding the plate)

2.1.2 The Low Frequency Instrument

The LFI instrument consists in:

- 2 radiometer chains at 30 GHz
- 3 radiometer chains at 44 GHz
- 6 radiometer chains at 70 GHz

All of them are **correlation differential radiometers**. In the signal acquired by any radiometer, as the frequency increases, the highest contribution to the noise is the white noise, with a plain spectrum (i.e. a noise amplitude which does not vary with the frequency). However, at the lowest frequencies, the 1/f noise dominates, as it varies its amplitude with the inverse of the frequency. The boundary between the spectrum region dominated by white noise and the region dominated by 1/f noise is the so-called **knee frequency**. Figure 2–4 shows the noise spectrums of two signals, with:

- The region where 1/f noise dominates (the smaller frequencies) on which the noise increases as the frequency decreases with a constant slope in the logarithmic plot.

- The region where the white noise dominates, with a constant amplitude
- The knee frequency, obtained as the intersection between the linear regression of 1/f noise and white noise (green vertical line)

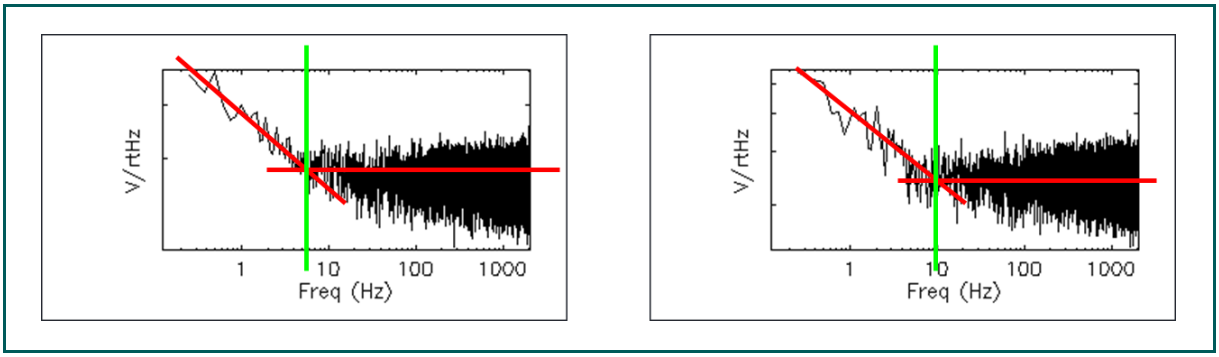


Figure 2–4: Noise spectrums of two signals showing the location of the knee frequency

A correlation differential radiometer uses the weighted difference between two correlated signals to reduce the knee frequency of the output signal obtained:

$$S = S_1 - r \cdot S_2 \qquad \text{[Eq.1]}$$

The result of the weighted difference for the optimal value of the adjustable parameter r in [Eq.1] is shown in Figure 2–5, where it is noticeable the displacement to the left of the new knee frequency obtained, and the reduction of the amplitude of the noise at lower frequencies.

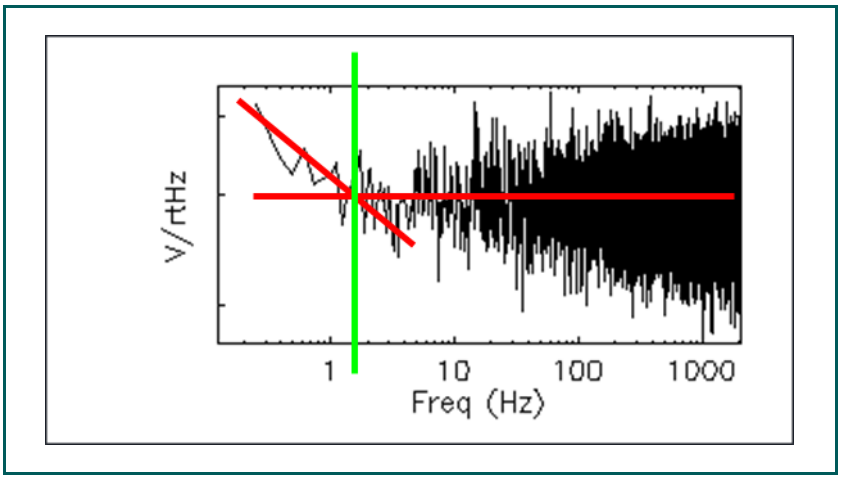


Figure 2–5: Knee frequency of the weighted difference of the previous signals

All of PLANCK LFI radiometers compute this weighted difference between two signals:

- The input signal from the feed horn coming from the sky.
- A reference signal, emulating a black body at 4 K, which is obtained through a reference horn that captures the signal of the cryogenic unit that cools the HFI at that temperature.

In order to obtain the best correlation between the sky and reference signals in the weighted difference, the radiometer splits each signal into two orthogonal components through the so called **Ortho-Mode Transducers (OMT)**. Thus, four different channels are obtained at this stage (2 sky signal components plus 2 reference signal components). Then, a **Hybrid Coupler ("magic T")** combines the sky and reference channels into four mixed signals. Afterwards, a series of **Low Noise Amplifiers (LNA)** augment these signals, but the key aspect is that, being the signals a combination of sky + reference signals in the four channels, the noise added to the sky and the reference signals is the same on each channel. These signals go through a series of **Phase Switches** which perform a relative phase shift of each signal with respect to the others, whereas each pair of signal and phase-shifted signal are combined in a second **Hybrid Coupler**, which due to the phase shift introduced between the signals, isolate again the sky and reference original signals in their output channels.

As a result, the noise added to both signals in the LNA's is highly correlated and the weighted difference between sky and reference signals has the 1/f noise contribution mitigated in a very efficient way.

The LFI has three main components:

- The **Front-End Module (FEM)**, located in the focal plane and connected to the feed-horn that acquires the sky signal and the reference horn that acquires the 4 K reference signal. This unit contains all the elements of the differential radiometer explained above (horns, OMT's, 1st Hybrid Couplers, LNA's, Phase Switches and 2nd Hybrid Couplers).
- The **Back-End Module (BEM)**, located beyond the thermal shields or **V-grooves** which isolate the cryogenic unit and the focal plane at 4 K and 20 K from the rest of the spacecraft, which operates at 300 K. The BEM amplifies again the microwave signals and converts them into output voltages to be sent to the **Data Acquisition Electronics** (DAE) module that will digitize them and prepare to be sent back to the ground stations.
- The **Waveguides (WG)**, which transport the output signals from the FEM to the BEM through the V-grooves, which operate with an extreme temperature gradient varying from 20 K to 300 K in 1-2 metres.

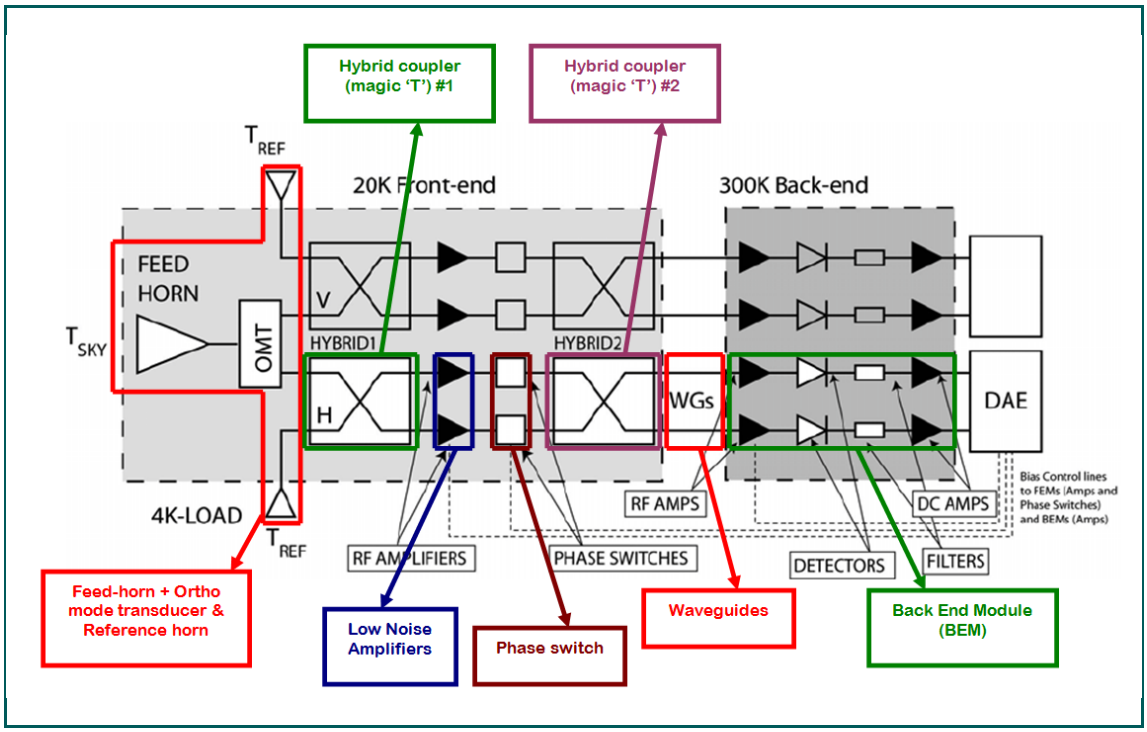


Figure 2–6: Schematic modular description of LFI radiometers

2.2 RaNA: The Radiometer aNAlyser SW

2.2.1 High level description of RaNA

RaNA (Radiometer aNAlyzer software) is a SW designed to analyse the PLANCK LFI Radiometer Chains Array (RCA) calibration data. RaNA consists in a Top level program, an interface to read the calibration FITS files created by RACHEL (RAdiometer CHains EvaLuator software) and several blocks, divided into RCA tuning, basic and advanced analysis modules.

Figure 2–7: RaNA software logo

The RaNA modules manager gave access to the different modules of the main program:

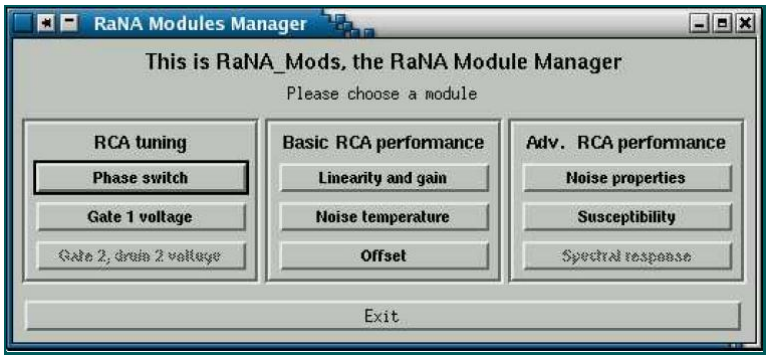


Figure 2–8: RaNA_Mods, the RaNA modules manager

The RCA tuning modules allowed changing the operation conditions of the radiometer to find the optimal configuration:

- Phase switch module was in charge of modifying the response of the Phase Switchers in the FEM prior to the second Hybrid Couplers to completely separate the sky and reference signals at the output channels of the FEM.
- Gate 1 voltage and Gate 2, drain 2 voltage were in charge of modifying the operational conditions of the HEMT transistors that comprised the LNA's to find the optimal signal to noise ratio.

The basic analysis modules allowed obtaining the elementary parameters of the RCA chain, namely:

- The Linearity and Gain module, in charge of characterising the linear response of the radiometer's response as a function of the input signal.
- The Noise Temperature module, in charge of computing the equivalent temperature of the noise added to the signals in the RCA chain.
- The Offset module, which was in charge of determining the zero-point values of the input signals and the output voltages, constituting the dark signal of the RCA.

Finally, the advanced modules were aimed at determining the advanced configuration parameters of the RCA chain:

- The Noise properties module was responsible for the computation of the knee frequency from the weighted difference of the sky and reference signals, returning the optimal value of the weight r (see [Eq.1]).
- The Susceptibility module was on charge of finding the parameters in the equations which characterised the radiometer's response to variations in the environmental conditions (temperatures of the different elements of the radiometers, voltages of the RCA amplifiers, etc.)

– Spectral response module was in charge of determining the fine parameters of the RCA response as a function of the frequency of the sky and reference signals.

2.2.2 RaNA_Susc and RaNA_Oft modules

RaNA_Susc and RaNA_Oft are the acronyms for **RaNA susceptibility to environmental variations** advanced analysis module and **RaNA offset** basic analysis module of RaNA software, respectively. As explained in 1.2.1, they are the modules entirely developed at Instituto de Física de Cantabria (IFCA), which provided the core of the background experience in the Product Assurance for software.

RaNA_Oft is a basic analysis module which computes the bias output values in absence of real input signal which the RCA chain provided. This constitutes the so called dark signal in an astronomical instrument, but the way to characterize it was somehow different from a typical camera at the focal plane of a telescope. In a radiometer, the thermal radiation from the instrument itself as well as the spurious output voltages from the electronics constitutes the dark signal, opposite to the thermal energy of the silicon in a CCD dark signal. The offsets in voltages and temperatures should then be characterized jointly.

The process of obtaining the temperature and voltage offsets was done by measuring the outputs of the RCA when both the sky horn and the reference signals were set to minimum by connecting them to the same source: a cooled (4K) black body-like source. In this scenario, sky and reference signals were (almost) equal, and the equivalent temperature and voltage of the output signals could then be characterized.

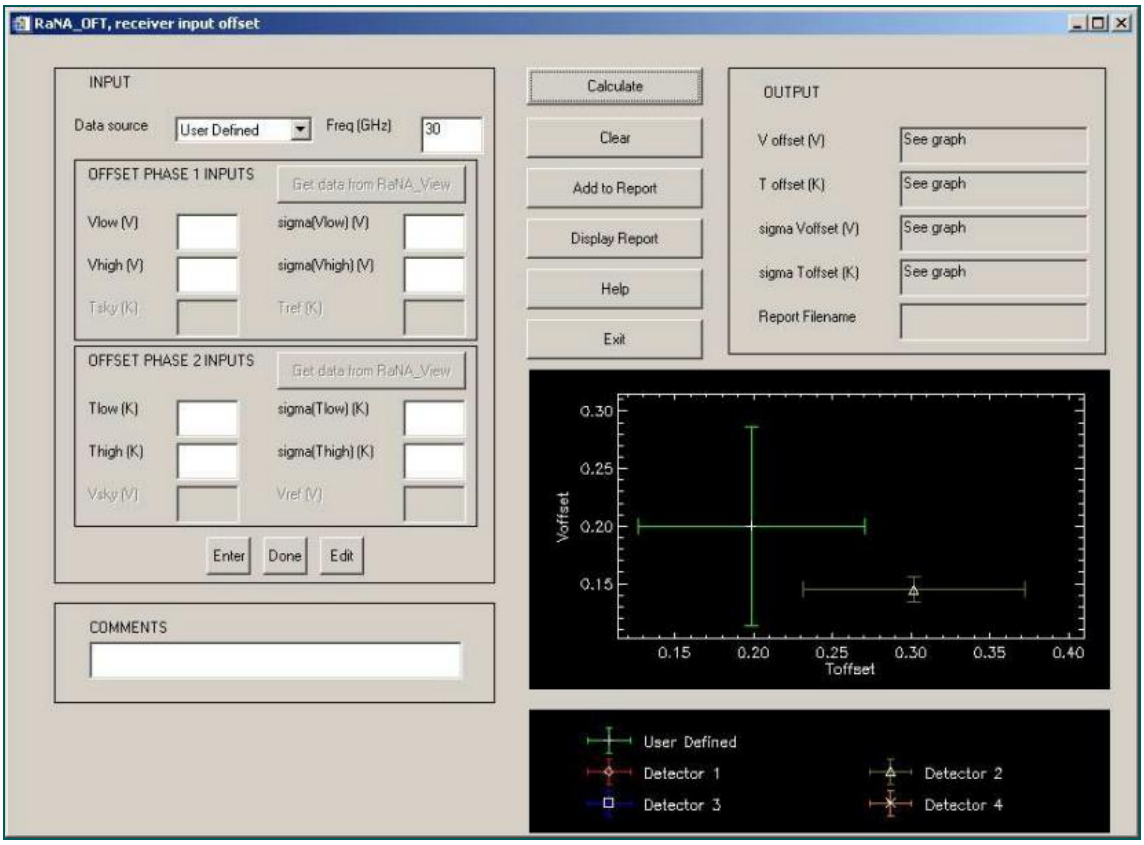


Figure 2–9: RaNA_Oft module

RaNA_Susc is an advanced analysis module in charge of computing the parameters of the model that characterise the variations in the outputs of the RCA chain due to variations in the environmental conditions. The output voltage of the RCA chain is determined by a general function f, which is the so called physical model of the radiometer:

$$V_{out} = f(T_{Sky}, T_{4K}, T_{FEM}, V_{bias}, T_{V-grooves}, T_{BEM}) \qquad \text{[Eq.2]}$$

This equation depends on the equivalent temperature of the sky and reference signals, plus many other physical magnitudes of the radiometer modules, namely:

- The physical temperatures of the Front and Back end modules, T_{FEM}, T_{BEM}
- The voltage bias of the Low Noise Amplifiers, V_{bias}
- The physical temperatures of the three thermal shields or V-grooves, $T_{V\text{-}grooves}$

These magnitudes in the ideal scenario remain constant with their values set for optimal performance of the system. However, this objective is not achievable in the real operational environment, reason why it is mandatory to characterize the variations in the output voltage due to small variations in these magnitudes. A first order perturbation method was used to obtain the coefficients of a linear equation that involved each variation in the magnitudes considered, and how they were related to the variations in the equivalent sky temperature which is the final

objective of the radiometers. The physical model of the radiometers is fully explained in next section (2.2.3), whereas the first order perturbation method to derive each of the variations is detailed in section 2.2.4.

2.2.3 Physical Model of the LFI radiometers

The different components of the LFI radiometers explained in section 2.1.2 are analysed to derive their physical model. Since all of them are connected sequentially, the output signal at each one acts as the input for the following stage.

2.2.3.1 Feed-horn + Ortho Mode Transducer & Reference horn Output Power

2.2.3.1.1 Power of the signals coming from the Sky and the Reference Load

The signals coming from the Sky and the Reference load can be expressed in terms of their **Equivalent Antenna temperatures** through the following expressions:

$$P_{Sky} = k \cdot \beta \cdot T_{Sky}^{ant} \qquad \text{[Eq.3]}$$

$$P_{4K} = k \cdot \beta \cdot T_{4K}^{ant} \qquad \text{[Eq.4]}$$

Where T_{Sky}^{ant} and T_{4K}^{ant} are the so called **Equivalent Antenna temperatures** for the Sky and the reference load signals, respectively; k is the Boltzmann constant; and β the bandwidth. In order to ease the nomenclature, from now on both equivalent antenna temperatures will be denoted T_{Sky} and T_{4K}. These antenna temperatures can be obtained from the thermodynamic temperatures using the following equations:

$$T_{Sky}^{ant} \equiv T_{Sky} = \frac{h \cdot \nu}{k} \cdot \frac{1}{e^{\frac{h \cdot \nu}{k \cdot T_{Sky}^{phys}}} - 1} \qquad \text{[Eq.5]}$$

$$T_{4K}^{ant} \equiv T_{4K} = \frac{h \cdot \nu}{k} \cdot \frac{1}{e^{\frac{h \cdot \nu}{k \cdot T_{4K}^{phys}}} - 1} \qquad \text{[Eq.6]}$$

2.2.3.1.2 Feed-horn + Ortho mode transducer & Reference horn Physical Model and Output Power.

Once the input signals have been expressed in terms of their equivalent antenna temperatures (i.e. the thermodynamic temperatures), a physical model of the Feed-horn + Ortho mode transducer & Reference horn is needed to obtain its output power. This model considers the Feed-horn, the Ortho mode transducer and the Reference horn separately as low lossy mediums. The general description of the output power of a signal that crosses a lossy medium is:

$$P_{out} = P_{in} \cdot e^{-\tau} + \left(1 - e^{-\tau}\right) \cdot P_{therm} \qquad \text{[Eq.7]}$$

The first part of the output power, $P_{in} \cdot e^{-\tau}$ is the power of the input signal, attenuated due to the optical depth of the medium, τ, and the other contribution, $\left(1 - e^{-\tau}\right) \cdot P_{therm}$, is the thermal reemission of the medium. We can now re-write the equation using the equivalent temperatures:

$$T_{out} = T_{in} \cdot e^{-\tau} + \left(1 - e^{-\tau}\right) \cdot T_{phys} \qquad \text{[Eq.8]}$$

In our case, both the Feed-horn + Ortho mode transducer and the Reference horn are low lossy mediums (i.e. $\tau << 1$), so the attenuation factor, $e^{-\tau}$, can be approximated as:

$$e^{-\tau} \cong 1 - \tau \equiv \frac{1}{L} \qquad \text{[Eq.9]}$$

Where L is the dimensionless attenuation factor of the low lossy medium and the previous equation can be written as:

$$T_{out} = T_{in} \cdot \frac{1}{L} + \left(1 - \frac{1}{L}\right) \cdot T_{phys} \qquad \text{[Eq.10]}$$

Finally, this result can be applied to obtain the output power for the Feed-horn + Ortho mode transducer:

$$P^{out}_{Feed-OMT} = k \cdot \beta \cdot \tilde{T}_{Sky} \qquad \text{[Eq.11]}$$

Where $\tilde{T}_{Sky} = \frac{T_{Sky}}{L_{Feed-OMT}} + \left(1 - \frac{1}{L_{Feed-OMT}}\right) \cdot T^{FE}_{phys}$ is the equivalent temperature of the output signal; $L_{Feed-OMT}$ is the attenuation factor, and T^{FE}_{phys} is the physical temperature of the system, equal to the physical temperature of the front end where it is placed.

Similarly:

$$P^{out}_{4K} = k \cdot \beta \cdot \tilde{T}_{4K} \qquad \text{[Eq.12]}$$

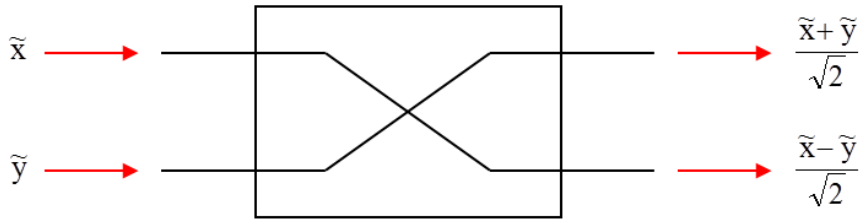
is the output power for the Reference horn system, where $\tilde{T}_{4K} = \frac{T_{4K}}{L_{4K}} + \left(1 - \frac{1}{L_{4K}}\right) \cdot T^{FE}_{phys}$ is the equivalent temperature of the output signal; and L_{4K} the Reference horn's attenuation factor.

2.2.3.2 Front End Module (FEM) Physical Model.

In this section, the physical models of the different elements in which the FEM can be divided are discussed. The input signals on each channel of the FEM are named $\tilde{x}$ and $\tilde{y}$, an correspond to the output signals of the Feed-horn + Ortho mode transducer and the Reference horn, respectively. In the next section the conversion from signals to powers to derive the FEM's output power will be discussed.

2.2.3.2.1 First Hybrid coupler

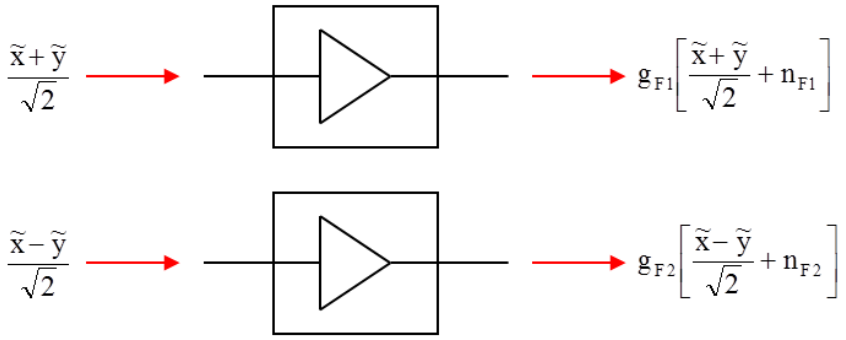
The physical model of the magic 'T' can be expressed as follows.



Where $\tilde{x}$ and $\tilde{y}$ are the signals coming from the Feed horn + Ortho Mode Transducer and the Reference horn, respectively. The average power of these signals can be expressed as $\langle \tilde{x}^2 \rangle = k \cdot \beta \cdot \tilde{T}_{Sky}$; $\langle \tilde{y}^2 \rangle = k \cdot \beta \cdot \tilde{T}_{4K}$, corresponding to the output power of the Feed-horn + OMT & Reference horn systems.

2.2.3.2.2 Low Noise Amplifiers

The output signals exiting the first hybrid coupler are amplified in the LNA's, according to the following expressions:

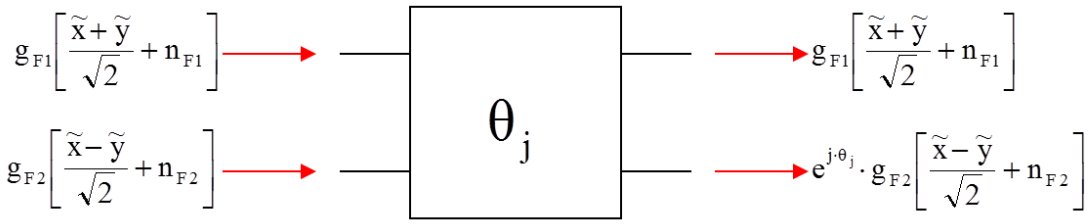


Where g_{F1}, g_{F2} are the signal gains for each amplifier, so the power gains are $G_{F1} = (g_{F1})^2$, $G_{F2} = (g_{F2})^2$; n_{F1}, n_{F2} are the noise added to the signals. Given the average noise power for

each LNA: $\langle n_{F1}^2 \rangle$ and $\langle n_{F2}^2 \rangle$, equivalent noise temperatures can be defined as: $T_{nF1} = \frac{\langle n_{F1}^2 \rangle}{k \cdot \beta}$, $T_{nF2} = \frac{\langle n_{F2}^2 \rangle}{k \cdot \beta}$.

2.2.3.2.3 Phase Switch

In order to alternately obtain a signal from the Sky or the Reference load on each channel, a phase switch is introduced. So, depending on the state of this element, the output signals will be different:



In this case, the output signal on channel 2 depends on the state of the phase switch. Assuming an ideal phase switch, there is no attenuation of the signals, and the phases for each state are: $\theta_1 = 0$, $\theta_2 = \pi$ radians. So, the output signals at this point are:

- Channel 1: $g_{F1}\left[\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right]$ (for both states of the phase switch)
- Channel 2 output depends on the state of the phase switch:
  - Phase Switch state 1: $g_{F2}\left[\frac{\tilde{x}-\tilde{y}}{\sqrt{2}}+n_{F2}\right]$
  - Phase Switch state 2: $g_{F2}\left[\frac{\tilde{y}-\tilde{x}}{\sqrt{2}}-n_{F2}\right]$

2.2.3.2.4 Second Hybrid Coupler:

The physical model of this second magic 'T' is the same as for the first one, but the input signals and hence the output ones are different.

The output signals of the second hybrid coupler depend on the state of the phase switch, so taking into account that the input signals for each channel are:

– Channel 1: $g_{F1}\left[\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right]$

– Channel 2: $e^{j\cdot\theta_j}\cdot g_{F2}\left[\frac{\tilde{x}-\tilde{y}}{\sqrt{2}}+n_{F2}\right]$

The output signals for the **state 1** of the phase switch are:

– Channel 1: $\frac{1}{\sqrt{2}}\cdot\left[g_{F1}\left(\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right)+g_{F2}\left(\frac{\tilde{x}-\tilde{y}}{\sqrt{2}}+n_{F2}\right)\right]$

– Channel 2: $\frac{1}{\sqrt{2}}\cdot\left[g_{F1}\left(\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right)+g_{F2}\left(\frac{\tilde{y}-\tilde{x}}{\sqrt{2}}-n_{F2}\right)\right]$

The output signals for the **state 2** of the phase switch are:

– Channel 1: $\frac{1}{\sqrt{2}}\cdot\left[g_{F1}\left(\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right)+g_{F2}\left(\frac{\tilde{y}-\tilde{x}}{\sqrt{2}}-n_{F2}\right)\right]$

– Channel 2: $\frac{1}{\sqrt{2}}\cdot\left[g_{F1}\left(\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right)+g_{F2}\left(\frac{\tilde{x}-\tilde{y}}{\sqrt{2}}+n_{F2}\right)\right]$

The output signals on each channel are equal on different states of the phase switch. So, the signal of the channel 1 on the state1 of the Ph. Sw. is the same as the output signal of the channel 2 on the state 2 of the Ph. Sw.; and the output signal of the channel 1 on the state 2 of the Ph. Sw. is the same as that of the channel 2 on the state 1 of the Ph. Sw.

2.2.3.3 Front End Module Output Power.

Depending on the state of the phase switch, different output signals for each channel of the FEM are produced:

FEM Channel 1 Output Power on the state 1 of the phase switch:

The output signal is:

$$s_{State1}^{Channel1}=\frac{1}{\sqrt{2}}\cdot\left[g_{F1}\left(\frac{\tilde{x}+\tilde{y}}{\sqrt{2}}+n_{F1}\right)+g_{F2}\left(\frac{\tilde{x}-\tilde{y}}{\sqrt{2}}+n_{F2}\right)\right] \qquad \text{[Eq.13]}$$

So the average output power can be obtained as $P_{State1}^{Channel1} = \left\langle s_{State1}^{Channel1} \cdot \left(s_{State1}^{Channel1}\right)^{*} \right\rangle$. Taking into account that the average of uncorrelated signals are null, $\left\langle \tilde{x} \cdot \tilde{y}^{*} \right\rangle = \left\langle \tilde{x} \cdot n_{F1}^{\ *} \right\rangle = \left\langle \tilde{x} \cdot n_{F2}^{\ *} \right\rangle = \left\langle \tilde{y} \cdot n_{F1}^{\ *} \right\rangle = \left\langle \tilde{y} \cdot n_{F2}^{\ *} \right\rangle = \left\langle n_{F2} \cdot n_{F1}^{\ *} \right\rangle = 0$, the output power is:

$$P_{State1}^{Channel1} = \frac{1}{2}\left[g_{F1}^{\ 2}\left(\frac{\left\langle \tilde{x}^2 \right\rangle + \left\langle \tilde{y}^2 \right\rangle}{2} + \left\langle n_{F1}^{\ 2} \right\rangle \right) + g_{F2}^{\ 2}\left(\frac{\left\langle \tilde{x}^2 \right\rangle + \left\langle \tilde{y}^2 \right\rangle}{2} + \left\langle n_{F2}^{\ 2} \right\rangle \right) + g_{F1} g_{F2}\left(\left\langle \tilde{x}^2 \right\rangle - \left\langle \tilde{y}^2 \right\rangle \right) \right] \quad \text{[Eq.14]}$$

Now, the average of the output signal powers can be expressed in terms of their equivalent temperatures, $\left\langle \tilde{x}^2 \right\rangle = k \cdot \beta \cdot \tilde{T}_{Sky}$, $\left\langle \tilde{y}^2 \right\rangle = k \cdot \beta \cdot \tilde{T}_{4K}$, $\left\langle n_{F1}^{\ 2} \right\rangle = k \cdot \beta \cdot T_{nF1}$ and $\left\langle n_{F2}^{\ 2} \right\rangle = k \cdot \beta \cdot T_{nF2}$; and the square of the signal gains of the LNAs can be expressed as power gains, $g_{F1}^{\ 2} = G_{F1}$, $g_{F2}^{\ 2} = G_{F2}$ and $g_{F1} \cdot g_{F2} = \sqrt{G_{F1} \cdot G_{F2}}$; so the FEM's Channel 1 output power on the state 1 of the phase switch is:

$$P_{State1}^{Channel1} = \frac{k \cdot \beta}{2} \cdot \left[G_{F1} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF1} \right) + G_{F2} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF2} \right) + \sqrt{G_{F1} \cdot G_{F2}} \cdot \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \right] \quad \text{[Eq.15]}$$

This output power can be expressed as:

$$P_{State1}^{Channel1} = k \cdot \beta \cdot T_{State1}^{Channel1} \quad \text{[Eq.16]}$$

Where $T_{State1}^{Channel1}$ is the equivalent temperature of the signal exiting the Channel 1 of the FEM on the state 1 of the phase switch, which is expressed as a function of the previous magnitudes as follows:

$$T_{State1}^{Channel1} = \frac{1}{2} \cdot \left[G_{F1} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF1} \right) + G_{F2} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF2} \right) + \sqrt{G_{F1} \cdot G_{F2}} \cdot \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \right] \quad \text{[Eq.17]}$$

FEM Channel 1 Output Power on the state 2 of the phase switch

Now, the output signal is:

$$s_{State2}^{Channel1} = \frac{1}{\sqrt{2}} \cdot \left[g_{F1}\left(\frac{\tilde{x} + \tilde{y}}{\sqrt{2}} + n_{F1} \right) + g_{F2}\left(\frac{\tilde{y} - \tilde{x}}{\sqrt{2}} - n_{F2} \right) \right] \quad \text{[Eq.18]}$$

And $P_{State2}^{Channel1} = \left\langle s_{State2}^{Channel1} \cdot \left(s_{State2}^{Channel1}\right)^{*} \right\rangle$ is its output power. Using the same hypothesis explained above, this output power is:

$$P_{State\,2}^{Channel1} = \frac{k\cdot\beta}{2}\cdot\left[G_{F1}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF1}\right)+G_{F2}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF2}\right)+\sqrt{G_{F1}\cdot G_{F2}}\cdot\left(\tilde{T}_{4K}-\tilde{T}_{Sky}\right)\right] \quad \text{[Eq.19]}$$

This output power can be expressed as:

$$P_{State\,2}^{Channel1} = k\cdot\beta\cdot T_{State\,2}^{Channel1} \quad \text{[Eq.20]}$$

Where $T_{State\,2}^{Channel1}$ is the equivalent temperature of the signal exiting the Channel 1 of the FEM on the state 1 of the phase switch.

$$T_{State\,2}^{Channel1} = \frac{1}{2}\cdot\left[G_{F1}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF1}\right)+G_{F2}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF2}\right)+\sqrt{G_{F1}\cdot G_{F2}}\cdot\left(\tilde{T}_{4K}-\tilde{T}_{Sky}\right)\right] \quad \text{[Eq.21]}$$

FEM Channel 2 Output Power on the state 1 of the phase switch

In this case, the output signal on the state 1 of the phase switch of FEM's Channel 2 is equal to that of the state 2 of FEM's Channel 1, so the output power is:

$$P_{State\,1}^{Channel2} = \frac{k\cdot\beta}{2}\cdot\left[G_{F1}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF1}\right)+G_{F2}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF2}\right)+\sqrt{G_{F1}\cdot G_{F2}}\cdot\left(\tilde{T}_{4K}-\tilde{T}_{Sky}\right)\right] \quad \text{[Eq.22]}$$

Or:

$$P_{State\,1}^{Channel2} = k\cdot\beta\cdot T_{State\,1}^{Channel2} \quad \text{[Eq.23]}$$

With:

$$T_{State\,1}^{Channel2} = \frac{1}{2}\cdot\left[G_{F1}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF1}\right)+G_{F2}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF2}\right)+\sqrt{G_{F1}\cdot G_{F2}}\cdot\left(\tilde{T}_{4K}-\tilde{T}_{Sky}\right)\right] \quad \text{[Eq.24]}$$

FEM Channel 2 Output Power on the state 2 of the phase switch

As explained before, the output signal is equal as the one of FEM's channel 1 on the state 1 of the phase switch, so the output power will be:

$$P_{State\,2}^{Channel2} = \frac{k\cdot\beta}{2}\cdot\left[G_{F1}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF1}\right)+G_{F2}\cdot\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{2}+T_{nF2}\right)+\sqrt{G_{F1}\cdot G_{F2}}\cdot\left(\tilde{T}_{Sky}-\tilde{T}_{4K}\right)\right] \quad \text{[Eq.25]}$$

Or:

$$P_{State\,2}^{Channel2} = k \cdot \beta \cdot T_{State\,2}^{Channel2} \qquad \text{[Eq.26]}$$

With:

$$T_{State\,2}^{Channel2} = \frac{1}{2} \cdot \left[G_{F1} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF1} \right) + G_{F2} \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{2} + T_{nF2} \right) + \sqrt{G_{F1} \cdot G_{F2}} \cdot \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \right] \qquad \text{[Eq.27]}$$

Brief analysis of the equivalent temperatures obtained

It is important to notice that the equivalent temperatures $T_{State\,1}^{Channel1}$ and $T_{State\,2}^{Channel2}$ are equal, and assuming a perfectly balanced radiometer, where both the power gains of the LNAs are equal, $G_{F1} = G_{F2}$, this equivalent temperature only contains information about the signal coming from the Sky, because the signal coming from the Reference Load is nulled. Although Planck's radiometers will never be perfectly balanced, the difference between the power gains will be as small as possible, so $T_{State\,1}^{Channel1}$ will contain basically information about the signal from the Sky. Similarly, $T_{State\,2}^{Channel1} = T_{State\,1}^{Channel2}$ and in the case of a perfectly balanced radiometer, the signal of the Sky is nulled and only the equivalent temperature from the Reference Load remains. Finally, the output on each channel of the FEM informs alternately about the Sky and the Reference Load, taking into account that when Channel 1 "carries" the Sky signal, Channel 2 will "carry" the Reference Load signal and vice-versa.

2.2.3.4 Waveguides Physical Model and Output Power

2.2.3.4.1 Waveguides Physical Model

The Waveguides do not transform the signals that propagate through them, so the scene is very similar to that described for the physical model of the Feed-horn + OMT & Reference load horn in 2.2.3.1.2. The only exception is that the physical temperature of the waveguides changes from one point to another, and there is to modify the equation described in 2.2.3.1.2 to include a temperature distribution along the system. As explained in 2.2.3.1.2, the equivalent temperature of a signal after crossing a low lossy medium was:

$$T_{out} = T_{in} \cdot \frac{1}{L} + \left(1 - \frac{1}{L} \right) \cdot T_{phys} \qquad \text{[Eq.28]}$$

Assuming that the attenuation factor does not change with small variations of the physical temperature of the system, the term $T_{in} \cdot \frac{1}{L}$ remains constant, while the reemission term, $\left(1 - \frac{1}{L} \right) \cdot T_{phys}$ varies with $T_{phys} = T_{phys}(\vec{r})$. The waveguide temperature distribution depends only on one dimension that corresponds to the direction of propagation of the microwaves along it, as will be explained later. So, the one-dimensional restricted problem consist in finding the

general reemission term for a given temperature distribution along the propagation direction, $T_{phys} = T_{phys}(z)$. On the general medium sketched in Figure 2–10, there is a direction along which the physical temperature varies from one point to another, so each interval $(z, z+\delta z)$ reemits a signal with an equivalent antenna temperature $T_{reem}(z)$ proportional to its physical temperature $T_{phys}(z)$.

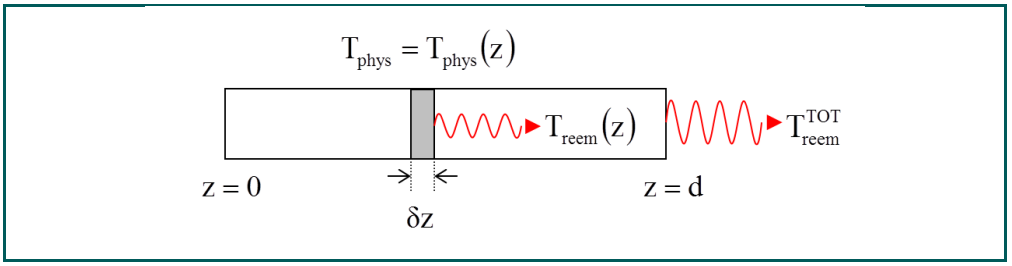


Figure 2–10: Schematic description of the thermal reemission through the waveguides

On each differential element δz, the reemission term values $T_{reem}(z) = \left(1 - \frac{1}{L}\right) \cdot T_{phys}(z)$, so the total reemission along the system is:

$$T_{reem}^{TOT} = \frac{1}{d} \cdot \int_0^d T_{reem}(z) \cdot dz \qquad \text{[Eq.29]}$$

The problem now is to find the temperature distribution along the waveguides. The waveguides are divided into several sections, each one made with different materials, so they have different attenuation factors and temperature distributions:

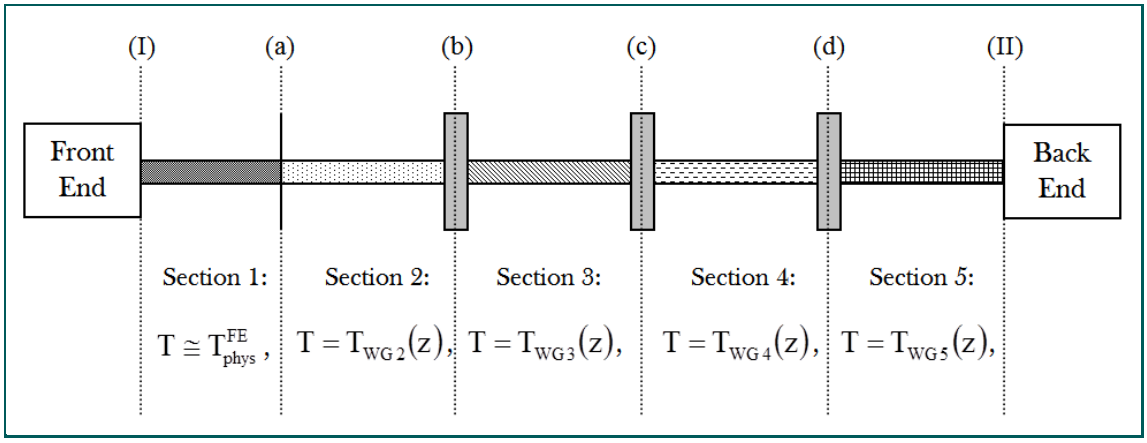


Figure 2–11: Schematic diagram of LFI radiometers waveguides

In Figure 2–11 above, the divisions between the different sections considered correspond to the following parts of the RCA:

(I) Beginning of the waveguides (junction between the front-end and the electroformed copper section)

(a) Junction between the Electroformed copper – Stainless steel sections of the waveguides
(b) V-groove #1 (coldest).
(c) V-groove #2.
(d) V-groove #3 (warmest).
(II) Ending of the waveguides (junction between the stainless steel section and the back-end)

Points (a) to (d) will have a fixed temperature equal to:

(a) $T_a \cong T_{phys}^{FE}$
(b) $T_b = T_{phys}^{V-groove1} \equiv T_{phys}^{V1}$
(c) $T_c = T_{phys}^{V-groove2} \equiv T_{phys}^{V2}$
(d) $T_d = T_{phys}^{V-groove3} \equiv T_{phys}^{V3}$

Besides, the waveguides extreme temperatures (I) and (II) are those of the Front End, T_{phys}^{FE}, and the Back End, T_{phys}^{BE}.

Considering the steady state, each section of the waveguides has its extreme points maintained at different temperatures, so there is a linear temperature distribution given by:

$$T_{phys}^{j}(z) = \left(\frac{T_{max}^{j} - T_{min}^{j}}{d^{j}} \right) \cdot z + T_{min}^{j} \qquad \text{[Eq.30]}$$

Where $T_{phys}^{j}(z)$ is the temperature distribution along the *j*-th waveguide section; z is the distance measured from the coldest to the warmest point (from left to right on the figure above); T_{min}^{j}, T_{max}^{j} are the "cold" and "warm" physical temperatures of its extreme points; and d^{j} its length.

Now, the reemission term can be calculated:

$$T_{reem}^{j} = \left(1 - \frac{1}{L^{j}}\right) \cdot \frac{1}{d^{j}} \cdot \int_{0}^{d^{j}} \left[\left(\frac{T_{max}^{j} - T_{min}^{j}}{d^{j}} \right) \cdot z + T_{min}^{j} \right] \cdot dz \qquad \text{[Eq.31]}$$

Solving the integral:

$$T_{reem}^{j} = \left(1 - \frac{1}{L^{j}}\right) \cdot \left(\frac{T_{max}^{j} + T_{min}^{j}}{2} \right) \qquad \text{[Eq.32]}$$

So, the reemission term of a system with a linear temperature distribution along a single dimension is equal to the reemission term of the same system with a constant temperature equal to the average of its extreme temperatures, which will be named from now on as **effective physical temperature of the *j*-th section of the waveguides**.

Now, the physical model of the waveguides can be obtained as a cascade of low lossy mediums that are the waveguide sections with their effective physical temperature, where the output of each section acts as the input for the next one. So, considering an input signal with an equivalent input temperature T_{in}, next subsections show how to obtain the equivalent output temperature, T_{out}.

Waveguide Section 1 output

$$T_{out}^{WG1} = \frac{T_{in}}{L_{WG1}} + \left(1 - \frac{1}{L_{WG1}}\right) \cdot T_{phys}^{FE} \qquad \text{[Eq.33]}$$

Waveguide Section 2 output

$$T_{out}^{WG2} = \frac{T_{out}^{WG1}}{L_{WG2}} + \left(1 - \frac{1}{L_{WG2}}\right) \cdot \left(\frac{T_{phys}^{FE} + T_{phys}^{V1}}{2}\right) \qquad \text{[Eq.34]}$$

It is now possible to replace the WG section 1 output, obtaining:

$$T_{out}^{WG2} = \frac{T_{in}}{L_{1,2}^{eff}} + \left(1 - \frac{1}{L_{1,2}^{eff}}\right) \cdot T_{1,2}^{eff} \qquad \text{[Eq.35]}$$

Where $L_{1,2}^{eff}$ is the **effective attenuation factor** and $T_{1,2}^{eff}$ the **effective physical temperature** for the combined waveguide sections 1 and 2. These two magnitudes are the attenuation factor and the physical temperature that a lossy medium must have to produce the same effect on the input signal as the waveguide sections 1 and 2 produce on the FEM's output signal. Finally, $L_{1,2}^{eff}$ and $T_{1,2}^{eff}$ can be obtained from the attenuation factors and the extreme temperatures of the waveguide sections 1 and 2 as:

$$L_{1,2}^{eff} = L_{WG1} \cdot L_{WG2} \qquad \text{[Eq.36]}$$

$$T_{1,2}^{eff} = \frac{L_{WG1} \cdot \left(T_{phys}^{FE} - T_{phys}^{V1} + L_{WG2} \cdot \left(T_{phys}^{FE} + T_{phys}^{V1}\right)\right) - 2\,T_{phys}^{FE}}{2 \cdot \left(L_{WG1} L_{WG2} - 1\right)} \qquad \text{[Eq.37]}$$

Waveguide Section 3 output

$$T_{out}^{WG3} = \frac{T_{out}^{WG2}}{L_{WG3}} + \left(1 - \frac{1}{L_{WG3}}\right) \cdot \left(\frac{T_{phys}^{V1} + T_{phys}^{V2}}{2}\right) \qquad \text{[Eq.38]}$$

Re-writing the equation in terms of the effective magnitudes:

$$T_{out}^{WG3} = \frac{T_{in}}{L_{1,2,3}^{eff}} + \left(1 - \frac{1}{L_{1,2,3}^{eff}}\right) \cdot T_{1,2,3}^{eff} \quad \text{[Eq.39]}$$

Now, $L_{1,2,3}^{eff}$ and $T_{1,2,3}^{eff}$ are the effective attenuation factor and physical temperature for the combined system Section 1 + Section 2 + Section 3 of the waveguides:

$$L_{1,2,3}^{eff} = L_{WG1} L_{WG2} L_{WG3} \quad \text{[Eq.40]}$$

$$T_{1,2,3}^{eff} = \frac{L_{WG1}\left(T_{phys}^{FE} - T_{phys}^{V1} + L_{WG2}\left(T_{phys}^{FE} - T_{phys}^{V2} + L_{WG3}\left(T_{phys}^{V1} + T_{phys}^{V2}\right)\right)\right) - 2\,T_{phys}^{FE}}{2\left(L_{WG1} L_{WG2} L_{WG3} - 1\right)} \quad \text{[Eq.41]}$$

Waveguide Section 4 output

$$T_{out}^{WG4} = \frac{T_{out}^{WG3}}{L_{WG4}} + \left(1 - \frac{1}{L_{WG4}}\right) \cdot \left(\frac{T_{phys}^{V2} + T_{phys}^{V3}}{2}\right) \quad \text{[Eq.42]}$$

Re-writing the equation in terms of the effective magnitudes:

$$T_{out}^{WG4} = \frac{T_{in}}{L_{1,2,3,4}^{eff}} + \left(1 - \frac{1}{L_{1,2,3,4}^{eff}}\right) \cdot T_{1,2,3,4}^{eff} \quad \text{[Eq.43]}$$

$L_{1,2,3,4}^{eff}$ and $T_{1,2,3,4}^{eff}$ are the effective attenuation factor and physical temperature for the combined system Section 1 + Section 2 + Section 3 + Section 4 of the waveguides:

$$L_{1,2,3,4}^{eff} = L_{WG1} L_{WG2} L_{WG3} L_{WG4} \quad \text{[Eq.44]}$$

$$T_{1,2,3,4}^{eff} = \frac{L_{WG1}\left(T_{phys}^{FE} - T_{phys}^{V1} + L_{WG2}\left(T_{phys}^{FE} - T_{phys}^{V2} + L_{WG3}\left(T_{phys}^{V1} - T_{phys}^{V3}\right) + L_{WG4}\left(T_{phys}^{V2} + T_{phys}^{V3}\right)\right)\right) - 2\,T_{phys}^{FE}}{2 \cdot \left(L_{WG1} L_{WG2} L_{WG3} L_{WG4} - 1\right)} \quad \text{[Eq.45]}$$

Waveguide Section 5 output

Finally, the output signal exiting the last section of the waveguide is the output signal of the whole system:

$$T_{out} \equiv T_{out}^{WG5} = \frac{T_{out}^{WG4}}{L_{WG5}} + \left(1 - \frac{1}{L_{WG5}}\right) \cdot \left(\frac{T_{phys}^{V3} + T_{phys}^{BE}}{2}\right) \quad \text{[Eq.46]}$$

As in the previous sections, this output equivalent temperature can be expressed in terms of an effective attenuation factor and an effective physical temperature. So, the physical model of the waveguides is that of a lossy medium as explained in 2.2.3.1.2:

$$T_{out} = \frac{T_{in}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}}\right) \cdot T_{WG}^{eff} \qquad \text{[Eq.47]}$$

Where L_{WG}^{eff} and T_{WG}^{eff} are the effective attenuation factor and the effective physical temperature of the waveguides, and can be obtained from the attenuation factors and the physical temperatures of each section through the following expressions:

$$L_{WG}^{eff} = L_{WG1} L_{WG2} L_{WG3} L_{WG4} L_{WG5} \qquad \text{[Eq.48]}$$

$$T_{WG}^{eff} = \frac{L_{WG1}\left(T_{phys}^{FE} - T_{phys}^{V1} + L_{WG2}\left(T_{phys}^{FE} - T_{phys}^{V2} + L_{WG3}\left(T_{phys}^{V1} - T_{phys}^{V3}\right) + L_{WG4}\left(T_{phys}^{V2} - T_{phys}^{BE} + L_{WG4}\left(T_{phys}^{V3} + T_{phys}^{BE}\right)\right)\right)\right) - 2T_{phys}^{FE}}{2 \cdot \left(L_{WG1} L_{WG2} L_{WG3} L_{WG4} L_{WG5} - 1\right)} \qquad \text{[Eq.49]}$$

2.2.3.4.2 Waveguides Output Power

Once the physical model of the waveguides is known, their output signals' power is, depending on the input signal coming from the front end:

$$P_{out}^{WG} = k \cdot \beta \cdot \left[\frac{T_{State\_j}^{Channel\_k}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}}\right) \cdot T_{WG}^{eff} \right] \qquad \text{[Eq.50]}$$

Where $T_{State\_j}^{Channel\_k}$ is the equivalent temperature of the front end output signal for the *k*-th Channel on the *j*-th state of the phase switch, as described in [Eq.17], [Eq.21], [Eq.24] and [Eq.27].

2.2.3.5 Back End Module (BEM) Physical Model and Output Power.

The Back End Module (BEM) is where the signal is transformed from a microwave signal to a DC voltage output. Once the input signal enters the module, it is first amplified and after transformed into a DC signal through square-law detectors. So, if the amplifiers of the *i*-th channel are modelled as described in 2.2.3.2.2 with a power gain G_{Bi} and a noise temperature T_{nBi}; and the square law detectors are considered to have a constant of proportionality named a, the output voltage V_{out} for an input signal which equivalent temperature is T_{in} is:

$$V_{out} = a \cdot k \cdot \beta \cdot G_{Bi} \cdot \left(T_{in} + T_{nBi}\right) \qquad \text{[Eq.51]}$$

So, the output voltages exiting each channel of the BEM are:

BEM Channel 1 Output Voltage on the state 1 of the phase switch

$$V_{State1}^{Channel1} = a \cdot k \cdot \beta \cdot G_{B1} \cdot \left[\frac{T_{State1}^{Channel1}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB1} \right] \quad \text{[Eq.52]}$$

Where $T_{State1}^{Channel1}$ is the equivalent temperature of the FEM described in [Eq.17].

BEM Channel 1 Output Voltage on the state 2 of the phase switch

$$V_{State2}^{Channel1} = a \cdot k \cdot \beta \cdot G_{B1} \cdot \left[\frac{T_{State2}^{Channel1}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB1} \right] \quad \text{[Eq.53]}$$

Where $T_{State2}^{Channel1}$ is the equivalent temperature of the FEM described in [Eq.21].

BEM Channel 2 Output Voltage on the state 1 of the phase switch

$$V_{State1}^{Channel2} = a \cdot k \cdot \beta \cdot G_{B2} \cdot \left[\frac{T_{State1}^{Channel2}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB2} \right] \quad \text{[Eq.54]}$$

Where $T_{State1}^{Channel2}$ is the equivalent temperature of the FEM described in [Eq.24].

BEM Channel 2 Output Voltage on the state 2 of the phase switch

$$V_{State2}^{Channel2} = a \cdot k \cdot \beta \cdot G_{B2} \cdot \left[\frac{T_{State2}^{Channel2}}{L_{WG}^{eff}} + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB2} \right] \quad \text{[Eq.55]}$$

Where $T_{State2}^{Channel2}$ is the equivalent temperature of the FEM described in [Eq.27].

Brief analysis of the voltages obtained

As explained at the end of 2.2.3.3, $T_{State1}^{Channel1} = T_{State2}^{Channel2}$ is the "Sky signal" because the contribution of Reference Load is almost nulled and $T_{State2}^{Channel1} = T_{State1}^{Channel2}$ is the "Reference Load signal". Therefore, the output voltages $V_{State1}^{Channel1} \cong V_{State2}^{Channel2}$ will be the "Sky voltages" and $V_{State2}^{Channel1} \cong V_{State1}^{Channel2}$ the "Reference Load voltages".

2.2.3.6 Radiometer Output

On each channel of the radiometer there will be two different outputs, carrying information about the Sky and the Reference Load signals, respectively. What is really important of these alternating outputs is that their main sources of noise, which are those produced by the FEM's LNAs, are correlated because of the two hybrid couplers that compose and decompose the input signals, and

therefore by subtracting both signals an effective reduction of the 1/f noise can be made, and the knee frequency shifts to lower values.

In order to optimise this 1/f reduction, the subtraction between both signals is weighted, so the "Reference Load voltage" (see considerations about the voltages obtained at the end of 2.2.3.5 for details) is multiplied by a **gain modulation factor**, r, and then subtracted from the "Sky voltage" on each channel:

- Channel 1: $\boxed{V_{State1}^{Channel1} - r \cdot V_{State2}^{Channel1}}$
- Channel 2: $\boxed{V_{State2}^{Channel2} - r \cdot V_{State1}^{Channel2}}$

Radiometer output on channel 1

$$V_1^{out} = a \cdot k \cdot \beta \cdot G_{B1} \left\{ \left[(G_{F1} + G_{F2}) \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{4 L_{WG}^{eff}} \right) + \left(\frac{G_{F1} T_{nF1} + G_{F2} T_{nF2}}{2 L_{WG}^{eff}} \right) + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB1} \right] \cdot (1 - r) + \frac{\sqrt{G_{F1} G_{F2}}}{2 L_{WG}^{eff}} \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \cdot (1 + r) \right\} \quad \text{[Eq.56]}$$

Radiometer output on channel 2

$$V_2^{out} = a \cdot k \cdot \beta \cdot G_{B2} \left\{ \left[(G_{F1} + G_{F2}) \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{4 L_{WG}^{eff}} \right) + \left(\frac{G_{F1} T_{nF1} + G_{F2} T_{nF2}}{2 L_{WG}^{eff}} \right) + \left(1 - \frac{1}{L_{WG}^{eff}} \right) \cdot T_{WG}^{eff} + T_{nB2} \right] \cdot (1 - r) + \frac{\sqrt{G_{F1} G_{F2}}}{2 L_{WG}^{eff}} \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \cdot (1 + r) \right\} \quad \text{[Eq.57]}$$

2.2.4 Susceptibility equations

2.2.4.1 Radiometer susceptibility to changes in the physical temperature of the Reference Load, RCA_THR

Through the following sections the procedure to explain the different variations induced on the radiometer output by changes on the environmental conditions will be the same. First of all, the physical magnitudes that are modified by the variation will be discussed. Then, the propagation of these variations in the radiometer output will be analysed.

Magnitudes that are modified by fluctuations in the physical temperature of the Reference Load

- **Equivalent antenna temperature of the Reference Load after the Reference horn**: In this case, the only magnitude that is modified is the signal entering the Reference horn, T_{4K}.

Variations induced in the equivalent Sky temperature

The variations induced in the equivalent Sky temperature are obtained using a first order perturbation method, so the Reference Load physical temperature can be written as a constant term plus a perturbation, $T_{4K} = (T_{4K})_0 + \delta T_{4K}$, and therefore the variations induced in the Sky temperature can be expressed as $T_{Sky} = (T_{Sky})_0 + \delta T_{Sky}$. Given the following identity:

$$\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)\cdot\delta T_{Sky}=\left(\frac{\partial V_i^{out}}{\partial T_{4K}}\right)\cdot\delta T_{4K} \qquad \text{[Eq.58]}$$

The fluctuations in the Sky temperature, δT_{Sky} can then be obtained:

$$\delta T_{Sky}=\frac{\left(\frac{\partial V_i^{out}}{\partial T_{4K}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)}\times\delta T_{4K}\equiv f_{therm}^{RL}\times\delta T_{4K} \qquad \text{[Eq.59]}$$

f_{therm}^{RL} is the **transfer function for variations in the physical temperature of the reference load**. Let us obtain its value:

The numerator value is:

$$\frac{\partial V_i^{out}}{\partial T_{4K}}=\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{4K}}\right)\cdot\left(\frac{\partial \tilde{T}_{4K}}{\partial T_{4K}}\right) \qquad \text{[Eq.60]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{4K}}\right)=\frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}+G_{F2}}{4}\right)\cdot(1-r)-\frac{\sqrt{G_{F1}G_{F2}}}{2}(1+r)\right\} \qquad \text{[Eq.61]}$$

$$\left(\frac{\partial \tilde{T}_{4K}}{\partial T_{4K}}\right)=\frac{1}{L_{4K}} \qquad \text{[Eq.62]}$$

The denominator value is:

$$\frac{\partial V_i^{out}}{\partial T_{Sky}}=\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{Sky}}\right)\cdot\left(\frac{\partial \tilde{T}_{Sky}}{\partial T_{Sky}}\right) \qquad \text{[Eq.63]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{Sky}}\right)=\frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}+G_{F2}}{4}\right)\cdot(1-r)+\frac{\sqrt{G_{F1}G_{F2}}}{2}(1+r)\right\} \qquad \text{[Eq.64]}$$

$$\left(\frac{\partial \tilde{T}_{Sky}}{\partial T_{Sky}}\right) = \frac{1}{L_{Feed-OMT}} \qquad \text{[Eq.65]}$$

So, finally:

$$f_{therm}^{RL} = \left(\frac{L_{Feed-OMT}}{L_{4K}}\right) \cdot \left\{\frac{(G_{F1}+G_{F2})\cdot(1-r) - 2\cdot\sqrt{G_{F1}G_{F2}}\cdot(1+r)}{(G_{F1}+G_{F2})\cdot(1-r) + 2\cdot\sqrt{G_{F1}G_{F2}}\cdot(1+r)}\right\} \qquad \text{[Eq.66]}$$

2.2.4.2 Radiometer susceptibility to changes in the physical temperature of the Front End, RCA_THF

Magnitudes that are modified by fluctuations in the physical temperature of the Front End

- **Power Gain of the Low Noise Amplifiers:** G_{F1} and G_{F2} are supposed to have a linear variation with T_{phys}^{FE}, so $\left(\frac{\partial G_{F1}}{\partial T_{phys}^{FE}}\right)$ and $\left(\frac{\partial G_{F2}}{\partial T_{phys}^{FE}}\right)$ are constant values.

- **Equivalent noise temperatures of the LNAs:** T_{nF1} and T_{nF2} are supposed to have a linear variation with T_{phys}^{FE}, so $\left(\frac{\partial T_{nF1}}{\partial T_{phys}^{FE}}\right)$ and $\left(\frac{\partial T_{nF2}}{\partial T_{phys}^{FE}}\right)$ are constant values.

- **Sky and Reference Load signals exiting the Feed horn + Ortho mode transducer & Reference horn system:** As the reemission term defined in 2.2.3.1.2 depends on the physical temperature of the system, $\tilde{T}_{Sky}$ and $\tilde{T}_{4K}$ will vary with T_{phys}^{FE}.

- **Effective temperature of the waveguides:** Although the effective temperature of the waveguides depends on T_{phys}^{FE}, its contribution to the fluctuation induced in the Sky temperature is negligible, compared with the rest of the terms, so its variation will not be included.

Variations induced in the equivalent Sky temperature

Using the identity given by the perturbation method:

$$\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)\cdot\delta T_{Sky} = \left(\frac{\partial V_i^{out}}{\partial T_{phys}^{FE}}\right)\cdot\delta T_{phys}^{FE} \qquad \text{[Eq.67]}$$

The fluctuations in the Sky temperature, δT_{Sky} are:

$$\delta T_{Sky} = \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{FE}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta T_{phys}^{FE} \equiv f_{therm}^{front\text{-}end} \times \delta T_{phys}^{FE} \quad \text{[Eq.68]}$$

$f_{therm}^{front\text{-}end}$ is the transfer function for variations in the physical temperature of the FEM, which value is:

$$f_{therm}^{front\text{-}end} = \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{FE}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \quad \text{[Eq.69]}$$

Let us replace the numerator and the denominator by their values. On the numerator:

$$\frac{\partial V_i^{out}}{\partial T_{phys}^{FE}} = \left(\frac{\partial V_i^{out}}{\partial G_{F1}}\right)\cdot\left(\frac{\partial G_{F1}}{\partial T_{phys}^{FE}}\right) + \left(\frac{\partial V_i^{out}}{\partial G_{F2}}\right)\cdot\left(\frac{\partial G_{F2}}{\partial T_{phys}^{FE}}\right) + \left(\frac{\partial V_i^{out}}{\partial T_{nF1}}\right)\cdot\left(\frac{\partial T_{nF1}}{\partial T_{phys}^{FE}}\right) + \left(\frac{\partial V_i^{out}}{\partial T_{nF2}}\right)\cdot\left(\frac{\partial T_{nF2}}{\partial T_{phys}^{FE}}\right) + \left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{Sky}}\right)\cdot\left(\frac{\partial \tilde{T}_{Sky}}{\partial T_{phys}^{FE}}\right) + \left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{4K}}\right)\cdot\left(\frac{\partial \tilde{T}_{4K}}{\partial T_{phys}^{FE}}\right) \quad \text{[Eq.70]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial G_{F1}}\right) = \frac{a\cdot k\cdot \beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{4}+\frac{T_{nF1}}{2}\right)\cdot(1-r)+\sqrt{\frac{G_{F2}}{G_{F1}}}\cdot\left(\frac{\tilde{T}_{Sky}-\tilde{T}_{4K}}{4}\right)\cdot(1+r)\right\} \quad \text{[Eq.71]}$$

$$\left(\frac{\partial V_i^{out}}{\partial G_{F2}}\right) = \frac{a\cdot k\cdot \beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{4}+\frac{T_{nF2}}{2}\right)\cdot(1-r)+\sqrt{\frac{G_{F1}}{G_{F2}}}\cdot\left(\frac{\tilde{T}_{Sky}-\tilde{T}_{4K}}{4}\right)\cdot(1+r)\right\} \quad \text{[Eq.72]}$$

$$\left(\frac{\partial V_i^{out}}{\partial T_{nF1}}\right) = \frac{a\cdot k\cdot \beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}}{2}\right)\cdot(1-r)\right\} \quad \text{[Eq.73]}$$

$$\left(\frac{\partial V_i^{out}}{\partial T_{nF2}}\right) = \frac{a\cdot k\cdot \beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F2}}{2}\right)\cdot(1-r)\right\} \quad \text{[Eq.74]}$$

$$\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{Sky}}\right)=\frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}+G_{F2}}{4}\right)\cdot(1-r)+\frac{\sqrt{G_{F1}G_{F2}}}{2}(1+r)\right\} \quad \text{[Eq.75]}$$

$$\left(\frac{\partial \tilde{T}_{Sky}}{\partial T_{phys}^{FE}}\right)=\left(1-\frac{1}{L_{Feed-OMT}}\right) \quad \text{[Eq.76]}$$

$$\left(\frac{\partial V_i^{out}}{\partial \tilde{T}_{4K}}\right)=\frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}+G_{F2}}{4}\right)\cdot(1-r)-\frac{\sqrt{G_{F1}G_{F2}}}{2}(1+r)\right\} \quad \text{[Eq.77]}$$

$$\left(\frac{\partial \tilde{T}_{4K}}{\partial T_{phys}^{FE}}\right)=\left(1-\frac{1}{L_{4K}}\right) \quad \text{[Eq.78]}$$

On the denominator the variations are the same as those in [Eq.63], with the partial derivatives as per [Eq.64] and [Eq.65].

So, finally, the transfer function is:

$$\begin{aligned}
f_{therm}^{front\text{-}end} = &\left(\frac{L_{Feed-OMT}}{(G_{F1}+G_{F2})\cdot(1-r)+2\cdot\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)}\right)\times\\
&\times\left[\left(\frac{\partial G_{F1}}{\partial T_{phys}^{FE}}\right)\cdot\left((\tilde{T}_{Sky}+\tilde{T}_{4K}+2\cdot T_{nF1})\cdot(1-r)+\sqrt{\frac{G_{F2}}{G_{F1}}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r)\right)+\right.\\
&+\left(\frac{\partial G_{F2}}{\partial T_{phys}^{FE}}\right)\cdot\left((\tilde{T}_{Sky}+\tilde{T}_{4K}+2\cdot T_{nF2})\cdot(1-r)+\sqrt{\frac{G_{F1}}{G_{F2}}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r)\right)+\\
&+\left(\frac{\partial T_{nF1}}{\partial T_{phys}^{FE}}\right)\cdot(2\cdot G_{F1}\cdot(1-r))+\left(\frac{\partial T_{nF2}}{\partial T_{phys}^{FE}}\right)\cdot(2\cdot G_{F2}\cdot(1-r))+\\
&+\left(1-\frac{1}{L_{Feed-OMT}}\right)\cdot\left((G_{F1}+G_{F2})\cdot(1-r)+2\cdot\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)\right)+\\
&\left.+\left(1-\frac{1}{L_{4K}}\right)\cdot\left((G_{F1}+G_{F2})\cdot(1-r)-2\cdot\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)\right)\right]
\end{aligned} \quad \text{[Eq.79]}$$

2.2.4.3 Radiometer susceptibility to changes in the voltage bias of the Front End, RCA_ELE

The LNAs of the FEM consist in two amplifying stages. Their point of operation, determined by the voltage biases of those stages, has a clear influence in the output signals.

Magnitudes that are modified by fluctuations in the voltage bias of the Front End

The voltage biases which variations are to be analysed are those of gate and drain for the two amplifying stages: (δV_{gate1}), (δV_{gate2}), (δV_{drain1}) and (δV_{drain2}). The fluctuations induced in the radiometer output are different, but the magnitudes that are affected are the same for all of them, so from now on all the analysis will be made over a general voltage bias called V_α that can represent any of the voltage bias defined above.

- **Power Gain of the Low Noise Amplifiers:** G_{F1} and G_{F2} are supposed to have a linear variation with the voltage biases, so $\left(\frac{\partial G_{F1}}{\partial V_\alpha}\right)$ and $\left(\frac{\partial G_{F2}}{\partial V_\alpha}\right)$ are constant values.

- **Equivalent noise temperatures of the LNAs:** T_{nF1} and T_{nF2} are supposed to have a linear variation with T_{phys}^{FE}, so $\left(\frac{\partial T_{nF1}}{\partial V_\alpha}\right)$ and $\left(\frac{\partial T_{nF2}}{\partial V_\alpha}\right)$ are constant values.

Variations induced in the equivalent Sky temperature.

The general expression for the variations induced in the equivalent Sky temperature is:

$$\delta T_{Sky} = (\delta T_{Sky})_{Vgate1} + (\delta T_{Sky})_{Vgate2} + (\delta T_{Sky})_{Vdrain1} + (\delta T_{Sky})_{Vdrain2} \equiv \sum_\alpha (\delta T_{Sky})_\alpha \quad \text{[Eq.80]}$$

Once again let us use the identity given by the perturbation method to find $(\delta T_{Sky})_\alpha$:

$$\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right) \cdot (\delta T_{Sky})_\alpha = \left(\frac{\partial V_i^{out}}{\partial V_\alpha}\right) \cdot \delta V_\alpha \quad \text{[Eq.81]}$$

So:

$$(\delta T_{Sky})_\alpha = \frac{\left(\frac{\partial V_i^{out}}{\partial V_\alpha}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta V_\alpha \equiv f_{bias-\alpha}^{front\text{-}end} \times \delta V_\alpha \quad \text{[Eq.82]}$$

$f_{\text{bias}-\alpha}^{\text{front-end}}$ is the transfer function for variations in the 'α' voltage bias of the FEM, where 'α' can be gate_1, gate_2, drain_1 or drain_2 and which general value is:

$$f_{\text{bias}-\alpha}^{\text{front-end}} = \frac{\left(\frac{\partial V_i^{out}}{\partial V_\alpha}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \qquad \text{[Eq.83]}$$

The values of the variations produced in the different magnitudes can now be replaced into this equation, on the numerator:

$$\frac{\partial V_i^{out}}{\partial V_\alpha} = \left(\frac{\partial V_i^{out}}{\partial G_{F1}}\right)\cdot\left(\frac{\partial G_{F1}}{\partial V_\alpha}\right) + \left(\frac{\partial V_i^{out}}{\partial G_{F2}}\right)\cdot\left(\frac{\partial G_{F2}}{\partial V_\alpha}\right) + \left(\frac{\partial V_i^{out}}{\partial T_{nF1}}\right)\cdot\left(\frac{\partial T_{nF1}}{\partial V_\alpha}\right) + \left(\frac{\partial V_i^{out}}{\partial T_{nF2}}\right)\cdot\left(\frac{\partial T_{nF2}}{\partial V_\alpha}\right) \qquad \text{[Eq.84]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial G_{F1}}\right) = \frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{4}+\frac{T_{nF1}}{2}\right)\cdot(1-r)+\sqrt{\frac{G_{F2}}{G_{F1}}}\cdot\left(\frac{\tilde{T}_{Sky}-\tilde{T}_{4K}}{4}\right)\cdot(1+r)\right\} \qquad \text{[Eq.85]}$$

$$\left(\frac{\partial V_i^{out}}{\partial G_{F2}}\right) = \frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{\tilde{T}_{Sky}+\tilde{T}_{4K}}{4}+\frac{T_{nF2}}{2}\right)\cdot(1-r)+\sqrt{\frac{G_{F1}}{G_{F2}}}\cdot\left(\frac{\tilde{T}_{Sky}-\tilde{T}_{4K}}{4}\right)\cdot(1+r)\right\} \qquad \text{[Eq.86]}$$

$$\left(\frac{\partial V_i^{out}}{\partial T_{nF1}}\right) = \frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F1}}{2}\right)\cdot(1-r)\right\} \qquad \text{[Eq.87]}$$

$$\left(\frac{\partial V_i^{out}}{\partial T_{nF2}}\right) = \frac{a\cdot k\cdot\beta\cdot G_{Bi}}{L_{WG}^{eff}}\cdot\left\{\left(\frac{G_{F2}}{2}\right)\cdot(1-r)\right\} \qquad \text{[Eq.88]}$$

On the denominator the variations are the same as those in [Eq.63], with the partial derivatives as per [Eq.64] and [Eq.65].

And finally, the transfer function is:

$$f_{\text{bias}-\alpha}^{\text{front-end}} = \left(\frac{L_{\text{Feed}-\text{OMT}}}{(G_{F1}+G_{F2})\cdot(1-r)+2\cdot\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)} \right) \times$$
$$\times \left[\left(\frac{\partial G_{F1}}{\partial V_\alpha} \right) \cdot \left((\tilde{T}_{Sky}+\tilde{T}_{4K}+2\cdot T_{nF1})\cdot(1-r)+\sqrt{\frac{G_{F2}}{G_{F1}}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r) \right) + \right.$$
$$+ \left(\frac{\partial G_{F2}}{\partial V_\alpha} \right) \cdot \left((\tilde{T}_{Sky}+\tilde{T}_{4K}+2\cdot T_{nF2})\cdot(1-r)+\sqrt{\frac{G_{F1}}{G_{F2}}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r) \right) +$$
$$\left. + \left(\frac{\partial T_{nF1}}{\partial V_\alpha} \right) \cdot (2\cdot G_{F1}\cdot(1-r)) + \left(\frac{\partial T_{nF2}}{\partial V_\alpha} \right) \cdot (2\cdot G_{F2}\cdot(1-r)) \right] \quad \text{[Eq.89]}$$

And the variations in the equivalent Sky temperature:

$$\delta T_{Sky} = \left(f_{\text{bias}-\text{gate1}}^{\text{front}-\text{end}} \times \delta V_{\text{gate1}} \right) + \left(f_{\text{bias}-\text{gate2}}^{\text{front}-\text{end}} \times \delta V_{\text{gate2}} \right) +$$
$$+ \left(f_{\text{bias}-\text{drain1}}^{\text{front}-\text{end}} \times \delta V_{\text{drain1}} \right) + \left(f_{\text{bias}-\text{drain2}}^{\text{front}-\text{end}} \times \delta V_{\text{drain2}} \right) \quad \text{[Eq.90]}$$

2.2.4.4 Radiometer susceptibility to changes in the physical temperature of the V-Grooves, RCA_THV

The three V-Grooves are thermal shields that allow the waveguides to change their temperature from that of the front-end (≈20 K) to the back-end's one (≈300 K). According to the convention established in 2.2.3.4.1, the coldest V-Groove is numbered as #1, the next one as #2 and the warmest one as #3.

Magnitudes that are modified by fluctuations in the physical temperature of the V-Grooves

– **Effective temperature of the waveguides:** The only magnitude of the physical model of the radiometer that varies with the temperature of the V-Grooves is the effective temperature of the waveguides, as described in [Eq.49].

Variations induced in the equivalent Sky temperature.

Now three different variations (one for each V-Groove) are to be taken into account in the identity:

$$\left(\frac{\partial V_i^{out}}{\partial T_{Sky}} \right) \cdot \delta T_{Sky} = \left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V1}} \right) \cdot \delta T_{phys}^{V1} + \left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V2}} \right) \cdot \delta T_{phys}^{V2} + \left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V3}} \right) \cdot \delta T_{phys}^{V3} \quad \text{[Eq.91]}$$

So there will be three different transfer functions:

$$\delta T_{Sky} = \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V1}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta T_{phys}^{V1} + \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V2}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta T_{phys}^{V2} + \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{V3}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta T_{phys}^{V3} \quad \text{[Eq.92]}$$

Or:

$$\delta T_{Sky} = f_{therm}^{V1} \times \delta T_{phys}^{V1} + f_{therm}^{V2} \times \delta T_{phys}^{V2} + f_{therm}^{V3} \times \delta T_{phys}^{V3} \quad \text{[Eq.93]}$$

f_{therm}^{V1} is the **transfer function for variations in the physical temperature of the V-Groove #1 (coldest)** and is computed as follows:

$$\frac{\partial V_i^{out}}{\partial T_{phys}^{V1}} = \left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) \cdot \left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V1}}\right) \quad \text{[Eq.94]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) = a \cdot k \cdot \beta \cdot G_{Bi} \cdot \left(1 - \frac{1}{L_{WG}^{eff}}\right) \cdot (1 - r) \quad \text{[Eq.95]}$$

$$\left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V1}}\right) = \left\{\frac{L_{WG1} \cdot (L_{WG2} L_{WG3} - 1)}{2 \cdot (L_{WG}^{eff} - 1)}\right\} \quad \text{[Eq.96]}$$

On the denominator the variations are the same as those in [Eq.63], with the partial derivatives as per [Eq.64] and [Eq.65].

So:

$$f_{therm}^{V1} = \left(\frac{L_{Feed-OMT} \cdot L_{WG1} \cdot (L_{WG2} \cdot L_{WG3} - 1) \cdot (1 - r)}{\frac{1}{2} \cdot (G_{F1} + G_{F2}) \cdot (1 - r) + \sqrt{G_{F1} \cdot G_{F2}} \cdot (1 + r)}\right) \quad \text{[Eq.97]}$$

f_{therm}^{V2} is the **transfer function for variations in the physical temperature of the V-Groove #2** and is obtained by:

$$\frac{\partial V_i^{out}}{\partial T_{phys}^{V2}} = \left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) \cdot \left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V2}}\right) \quad \text{[Eq.98]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) = a \cdot k \cdot \beta \cdot G_{Bi} \cdot \left(1 - \frac{1}{L_{WG}^{eff}}\right) \cdot (1 - r) \quad \text{[Eq.99]}$$

$$\left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V2}}\right) = \left\{\frac{L_{WG1} \cdot L_{WG2} \cdot (L_{WG3} L_{WG4} - 1)}{2 \cdot (L_{WG}^{eff} - 1)}\right\} \quad \text{[Eq.100]}$$

So:

$$f_{therm}^{V2} = \left(\frac{L_{Feed-OMT} \cdot L_{WG1} \cdot L_{WG2} \cdot (L_{WG3} \cdot L_{WG4} - 1) \cdot (1 - r)}{\frac{1}{2} \cdot (G_{F1} + G_{F2}) \cdot (1 - r) + \sqrt{G_{F1} \cdot G_{F2}} \cdot (1 + r)}\right) \quad \text{[Eq.101]}$$

Finally, f_{therm}^{V3} is the **transfer function for variations in the physical temperature of the V-Groove #3 (warmest)**, which value is given by:

$$\frac{\partial V_i^{out}}{\partial T_{phys}^{V3}} = \left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) \cdot \left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V3}}\right) \quad \text{[Eq.102]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial T_{WG}^{eff}}\right) = a \cdot k \cdot \beta \cdot G_{Bi} \cdot \left(1 - \frac{1}{L_{WG}^{eff}}\right) \cdot (1 - r) \quad \text{[Eq.103]}$$

$$\left(\frac{\partial T_{WG}^{eff}}{\partial T_{phys}^{V3}}\right) = \left\{\frac{L_{WG1} \cdot L_{WG2} \cdot L_{WG3} \cdot (L_{WG4} L_{WG5} - 1)}{2 \cdot (L_{WG}^{eff} - 1)}\right\} \quad \text{[Eq.104]}$$

For the derivatives in the denominator, refer to [Eq.63], [Eq.64] and [Eq.65]

So:

$$f_{therm}^{V3} = \left(\frac{L_{Feed-OMT} \cdot L_{WG1} \cdot L_{WG2} \cdot L_{WG3} \cdot (L_{WG4} \cdot L_{WG5} - 1) \cdot (1 - r)}{\frac{1}{2} \cdot (G_{F1} + G_{F2}) \cdot (1 - r) + \sqrt{G_{F1} \cdot G_{F2}} \cdot (1 + r)}\right) \quad \text{[Eq.105]}$$

2.2.4.5 Radiometer susceptibility to changes in the physical temperature of the Back End, RCA_THB

All the previous variations have been calculated considering a generic *i*-th output channel of the BEM, because this output channel did not affect the transfer functions obtained. In this latter case, as the physical magnitudes of the BEM are those to be affected by the variations of their physical temperature, the same generic *i*-th channel is to be used in the calculations, so finally two different transfer functions (depending on the BEM's output channel) will be obtained.

Magnitudes that are modified by fluctuations in the physical temperature of the Back End.

– **Power Gain of the BEM Amplifiers:** G_{B1} and G_{B2} are supposed to have a linear variation with T_{phys}^{BE}, so $\left(\frac{\partial G_{B1}}{\partial T_{phys}^{BE}}\right)$ and $\left(\frac{\partial G_{B2}}{\partial T_{phys}^{BE}}\right)$ are constant values, but will be expressed in units of *(dB·K^{-1})*, because the transfer functions are then simplified, using the following expression:

$$\left(\frac{\partial G_{Bi}}{\partial T_{phys}^{BE}}\right) = G_{Bi} \cdot \frac{\log(10)}{10} \cdot \left(\frac{\partial G_{Bi}^{dB}}{\partial T_{phys}^{BE}}\right) \qquad \text{[Eq.106]}$$

– **Constant of proportionality of the square-law detectors:** a is supposed to have a linear variation with T_{phys}^{BE}, so $\left(\frac{\partial a}{\partial T_{phys}^{BE}}\right)$ is a constant value, but will also be expressed in units of *(dB·K^{-1})*:

$$\left(\frac{\partial a}{\partial T_{phys}^{BE}}\right) = a \cdot \frac{\log(10)}{10} \cdot \left(\frac{\partial a^{dB}}{\partial T_{phys}^{BE}}\right) \qquad \text{[Eq.107]}$$

– **Effective temperature of the waveguides:** Although the effective temperature of the waveguides depends on T_{phys}^{BE}, its contribution to the fluctuation induced in the Sky temperature is negligible, compared with the rest of the terms, so neither its variation, nor the reemission term of the waveguides will be included in the following calculations.

Variations induced in the equivalent Sky temperature.

Using the identity given by the perturbation method:

$$\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right) \cdot \delta T_{Sky} = \left(\frac{\partial V_i^{out}}{\partial T_{phys}^{BE}}\right) \cdot \delta T_{phys}^{BE} \qquad \text{[Eq.108]}$$

The variations induced in the equivalent temperature of the Sky signal are:

$$\delta T_{Sky} = \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{BE}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \times \delta T_{phys}^{BE} \equiv f_{therm}^{back\text{-}end} \times \delta T_{phys}^{BE} \quad \text{[Eq.109]}$$

$f_{therm}^{back\text{-}end}$ is the **transfer function for variations in the physical temperature of the BEM**, which value is:

$$f_{therm}^{back\text{-}end} = \frac{\left(\frac{\partial V_i^{out}}{\partial T_{phys}^{BE}}\right)}{\left(\frac{\partial V_i^{out}}{\partial T_{Sky}}\right)} \quad \text{[Eq.110]}$$

Let us obtain the numerator:

$$\frac{\partial V_i^{out}}{\partial T_{phys}^{BE}} = \left(\frac{\partial V_i^{out}}{\partial G_{Bi}}\right) \cdot \left(\frac{\partial G_{Bi}}{\partial T_{phys}^{BE}}\right) + \left(\frac{\partial V_i^{out}}{\partial a}\right) \cdot \left(\frac{\partial a}{\partial T_{phys}^{BE}}\right) \quad \text{[Eq.111]}$$

where:

$$\left(\frac{\partial V_i^{out}}{\partial G_{Bi}}\right) = a \cdot k \cdot \beta \cdot \left\{ \left[(G_{F1} + G_{F2}) \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{4 L_{WG}^{eff}} \right) + \left(\frac{G_{F1} T_{nF1} + G_{F2} T_{nF2}}{2 L_{WG}^{eff}} \right) + T_{nBi} \right] \cdot (1 - r) + \right.$$
$$\left. + \frac{\sqrt{G_{F1} G_{F2}}}{2 L_{WG}^{eff}} \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \cdot (1 + r) \right\} \quad \text{[Eq.112]}$$

$$\left(\frac{\partial G_{Bi}}{\partial T_{phys}^{BE}}\right) = G_{Bi} \cdot \frac{\log(10)}{10} \cdot \left(\frac{\partial G_{Bi}^{dB}}{\partial T_{phys}^{BE}}\right) \quad \text{[Eq.113]}$$

$$\left(\frac{\partial V_i^{out}}{\partial a}\right) = k \cdot \beta \cdot G_{Bi} \cdot \left\{ \left[(G_{F1} + G_{F2}) \cdot \left(\frac{\tilde{T}_{Sky} + \tilde{T}_{4K}}{4 L_{WG}^{eff}} \right) + \left(\frac{G_{F1} T_{nF1} + G_{F2} T_{nF2}}{2 L_{WG}^{eff}} \right) + T_{nBi} \right] \cdot (1 - r) + \right.$$
$$\left. + \frac{\sqrt{G_{F1} G_{F2}}}{2 L_{WG}^{eff}} \left(\tilde{T}_{Sky} - \tilde{T}_{4K} \right) \cdot (1 + r) \right\} \quad \text{[Eq.114]}$$

$$\left(\frac{\partial a}{\partial T_{phys}^{BE}}\right) = a \cdot \frac{\log(10)}{10} \cdot \left(\frac{\partial a^{dB}}{\partial T_{phys}^{BE}}\right) \quad \text{[Eq.115]}$$

The derivatives in the denominator remain unchanged so the results in [Eq.63], [Eq.64] and [Eq.65] still apply.

So the transfer function for channel 1 of the BEM is:

$$f_{\text{therm}}^{\text{back-end}} = \left(\frac{L_{\text{Feed-OMT}}}{\frac{1}{2}\cdot(G_{F1}+G_{F2})\cdot(1-r)+\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)} \right) \cdot \left(\frac{\log(10)}{10} \right) \cdot \left(\frac{\partial a^{dB}}{\partial T_{phys}^{BE}} + \frac{\partial G_{B1}^{dB}}{\partial T_{phys}^{BE}} \right) \times$$
$$\times \left[\frac{1}{2}\cdot(G_{F1}+G_{F2})\cdot(\tilde{T}_{Sky}+\tilde{T}_{4K})\cdot(1-r)+(G_{F1}\cdot T_{nF1}+G_{F2}\cdot T_{nF2})\cdot(1-r)+ \right.$$
$$\left. \sqrt{G_{F1}\cdot G_{F2}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r)+2\cdot T_{nB1}\cdot(1-r) \right] \quad \text{[Eq.116]}$$

And for channel 2:

$$f_{\text{therm}}^{\text{back-end}} = \left(\frac{L_{\text{Feed-OMT}}}{\frac{1}{2}\cdot(G_{F1}+G_{F2})\cdot(1-r)+\sqrt{G_{F1}\cdot G_{F2}}\cdot(1+r)} \right) \cdot \left(\frac{\log(10)}{10} \right) \cdot \left(\frac{\partial a^{dB}}{\partial T_{phys}^{BE}} + \frac{\partial G_{B2}^{dB}}{\partial T_{phys}^{BE}} \right) \times$$
$$\times \left[\frac{1}{2}\cdot(G_{F1}+G_{F2})\cdot(\tilde{T}_{Sky}+\tilde{T}_{4K})\cdot(1-r)+(G_{F1}\cdot T_{nF1}+G_{F2}\cdot T_{nF2})\cdot(1-r)+ \right.$$
$$\left. \sqrt{G_{F1}\cdot G_{F2}}\cdot(\tilde{T}_{Sky}-\tilde{T}_{4K})\cdot(1+r)+2\cdot T_{nB2}\cdot(1-r) \right] \quad \text{[Eq.117]}$$

Depending on the channel considered, one of the two transfer functions above should be chosen.

2.3 Lessons learnt and ideas for the final solution proposed

The development of RaNA SW was a bottom up approach that involved several institutions from the PLANCK consortium, which each assumed the responsibility of one or more modules. Concerning the work devoted to this project, the Instituto de Física de Cantabria (IFCA-CSIC) led the development of RaNA_Susc and RaNA_Oft modules, as explained previously.

The initial stages of the design of these modules encompassed the development of the susceptibility equations explained in 2.2.4 from the physical model of the radiometers presented in 2.2.3, as well as prototypes of the derived equations which were developed in MATLAB. These preliminary SW packages were developed in a very similar approach to the "three P's problem" of ad-hoc simulation SW which will be detailed in section 8.1.2. Basically, they did neither contain a requirements specification document (apart from the on-going equations obtained), nor the minimum documentation available to the users; and they also were poorly validated, apart from source code inspections during the implementation.

Figure 2–12: PLACK RCA calibration equipment at LABEN. Vacuum chamber with the RCA cooled (left), and detail on the Data Acquisition Unit – RACHEL (right)

Once the final algorithms design was agreed [34], the final implementation of the modules in IDL 6.0 began. This implied a complete change of paradigm in the way of working for SW developments: From the "three P's scenario" on the prototypes for internal use only to a new development scenario where the management/coordination was carried out by an external institution (Istituto Nazionale di Astrofisica – INAF, Milano). The benefits of this coordination were evident from the very beginning of this phase, as it involved:

- The development of the modules RaNA_Susc and RaNA_Oft as a part of a higher level SW on which other institutions were developing other modules.
- The exchange of information about development status, procedures followed, relevant implementation details, etc. in weekly teleconferences.
- The centralized SW source code configuration management through a dedicated CVS server.
- The definition of the deliverables with the chapters to be filled in by each member of the RaNA coordination.
- The definition of a joint validation strategy with a common test data set which had to be used for the verification of each module and the validation of the entire SW.
- The organization of two collocations to review the status of the RaNA development:

- At Istituto di Astrofisica Spaziale e Fisica Cosmica – INAF-IASF in Bologna, Italy, from 07/06/2004 to 09/06/2004, to agree the design and validation strategy, in a very similar approach to what is meant by a Critical Design Review (CDR) in the procedure for SW developments, in chapter 8.
- At LABEN laboratories in Milano, Italy, from 06/03/2005 to 09/03/2005, to participate in the first tests of RaNA SW in the operational environment during the calibration campaign of the Qualified Models of the LFI radiometers at 30 and 44 GHz. This step constituted the transition from System Testing to Operations and Maintenance stages in a V-model life cycle (although RaNA was not formally developed with this specific life cycle, but on an incremental model basis), as depicted in Figure 8–2

The excellent results of the calibration campaign [27], [29], [30], [31] of which RaNA played a key role, led to the conclusions that the adoption of SW engineering rules had become a significant step ahead in the quality of the modules developed, and the motivation for including a dedicated chapter to the procedures for SW development in a Large Scientific Installation in the proposed solution (Chapter 8).

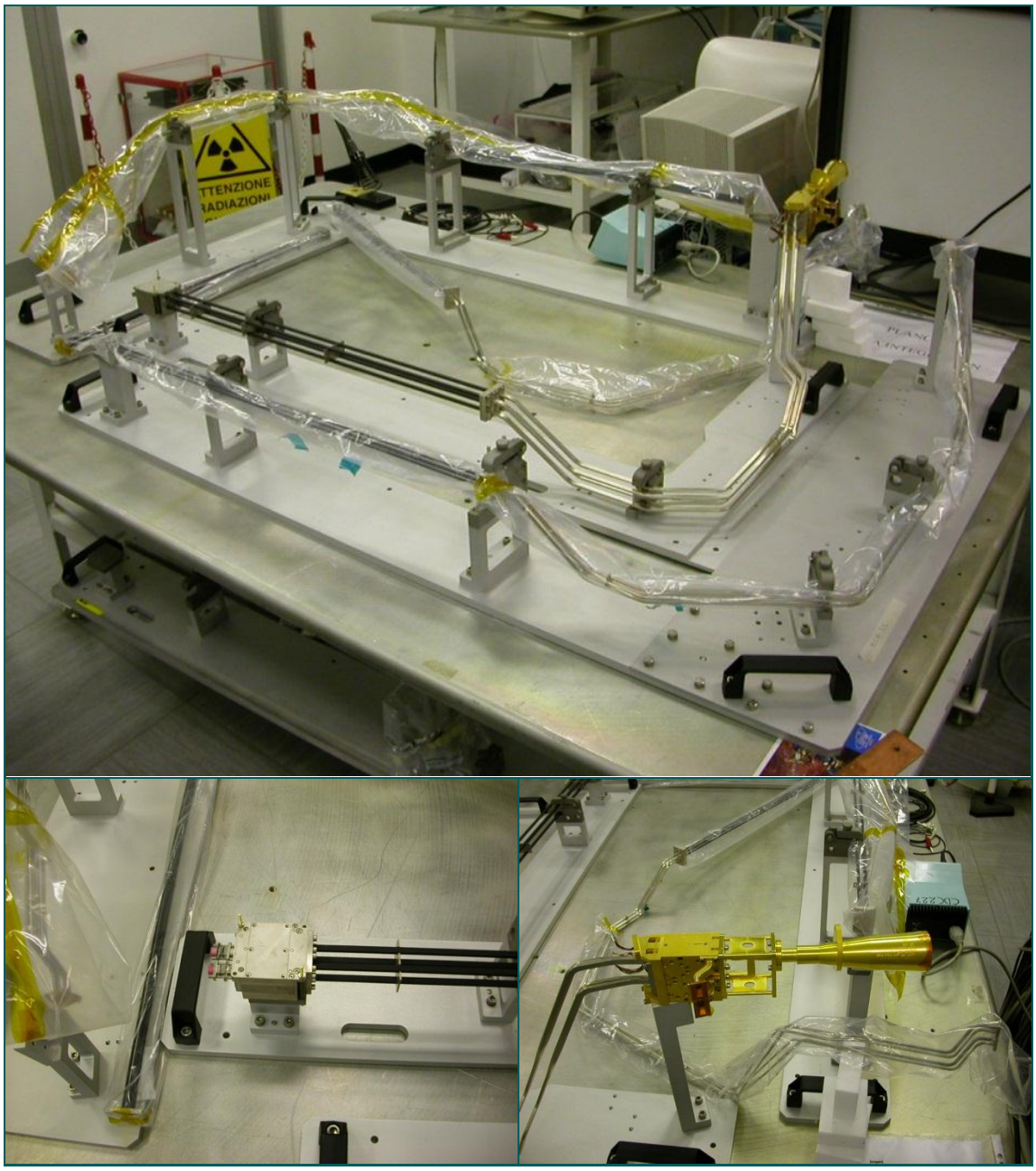


Figure 2–13: (Top) PLACK RCA in preparation on the test bench prior to be introduced in the vacuum chamber. (Bottom) Detail on the Back-End module and the stainless steel waveguides (left) and the Front-End module with the feed horn, the 4K reference connectors and the beginning of the electroformed copper waveguide (right)

Chapter 3

Product Assurance in the Cherenkov Telescope Array (CTA)

3.1 Overview of CTA

3.1.1 High level description of CTA

The Cherenkov Telescope Array is an ambitious international project aimed at the design & implementation of new generation of Imaging Air Cherenkov Telescopes (IACT's) at two observatories –in the northern and southern hemispheres– for the study of high/medium energy cosmic rays to cover the full sky.

The southern array will focus its activities in the study of high energy processes within our galaxy, provided that the Milky Way centre is located at southern latitudes (galactic centre activity, supernova remnants, pulsar wind nebulae, etc.), as well as extragalactic sources. The northern array will mainly devote its activities to the study of extra-galactic sources (AGN, quasars, blazars, etc.).

CTA concept emerged from the significant advances in the gamma-ray astronomy in the last years. The new generation of IACT's (MAGIC, HESS, VERITAS) have broadened the upper limits of the energies of the photons which can be detected with ground-based observatories. Contrarily to gamma-ray telescopes on board spacecraft's, several IACT's can combine their measurements to obtain an effective collection area much wider than the sum of the areas of their main mirrors. This allows the detection of very small radiation fluxes, typical of the higher energy photons. On the other hand, single IACT's with very large primary mirrors can increase the sensibility of lower energy photons.

Keeping both ideas in mind (many IACT's working together for the detection of the higher energy photons, and large single IACT's covering the range of the lower energies), CTA proposes to combine three types of telescopes to enlarge the sensitivity range in energies to the maximum extent.

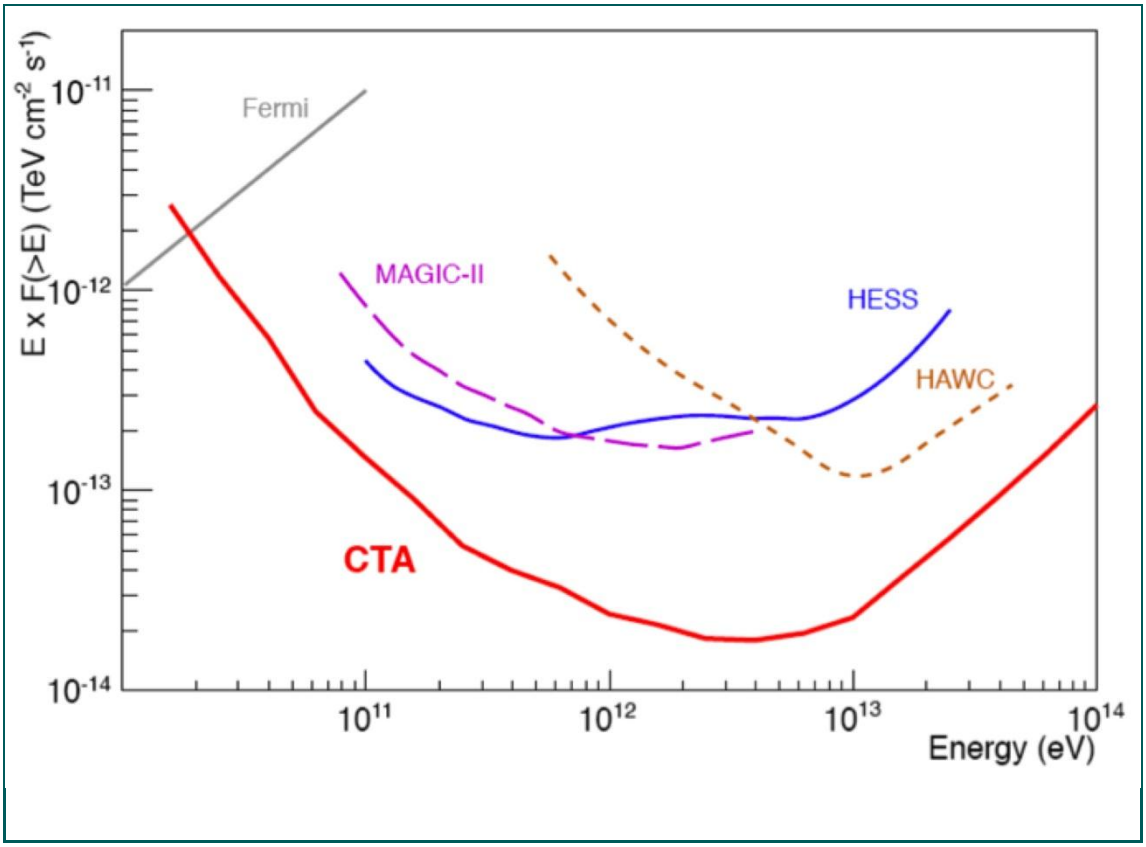


Figure 3–1: Expected ratio of the threshold flux detectable as a function of the input energy of the photons expected for CTA, compared with the real capabilities of existing observatories

Such a wide range of energies as that foreseen for CTA in Figure 3–1 can be achieved through the use of three types of telescopes, each one covering a smaller range which overlaps to produce the complete interval:

- **Large Size Telescopes (LST)**: With diameter of the primary mirror of about 24 metres, will cover the energy range up to tens of GeV.
- **Medium Size Telescopes (MST)**: Which primary mirror diameter is about 12 metres, will cover the range between hundreds of GeV and few TeV.
- **Small Size Telescopes (SST)**: Those with the smallest primary mirror (6 metres), but spread to a wider area to cover an effective collection surface which allows the detection of input photons of several TeV.

There are several alternatives for the distribution of the three types of telescopes above in the final observatories in the northern and southern hemispheres. Due to the different sources expected to be observed at each location, the southern array will be the largest and contain more telescopes than the northern one.

The final configuration of both arrays is one of the major drivers in the expected cost of CTA.

3.1.2 CTA organization

CTA is led by the so called CTA Consortium, the *ad hoc* institution defined for the concept, design and implementation of this project. The definition and organization of the CTA Consortium was established in the Memorandum of Understanding [16].

The CTA Consortium defined the organization which manages the project, which is presented in Figure 3–2.

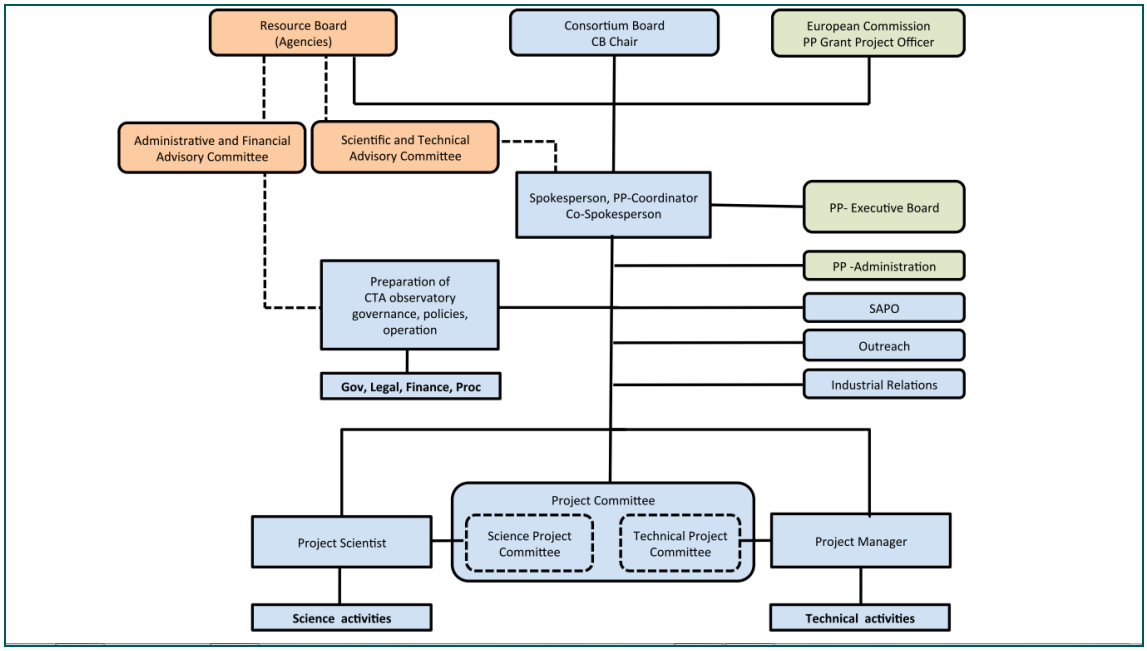


Figure 3–2: CTA Top level organization.

This top level organization defines the subsequent work packages for the different technical tasks of CTA, through the Product Breakdown Structure (PBS), as defined in the Project Management Plan [17]. This PBS has evolved with the project, as will be seen in the different phases of CTA in next section. Present paragraphs, on the contrary, will focus in the most remarkable elements of the CTA top level organization, as defined in [17].

Consortium Board

Concerning all scientific matters and organisational issues, the CTA Consortium is governed by the **Consortium Board (CB)**. The CB represents the ultimate internal authority in the CTA Consortium. It is the body through which all major decisions are endorsed.

The CB is composed of one representative from each institute representing a Regular Party, with voting right. CTA Management and Project / Work Package Leaders participate as ex-officio members, without voting right. The ex-officio members cannot at the same time represent a Party.

Each Associated Party may send one observer into the Board. The CB elects its chairperson (CB chairman) among its members, which is the representative of the CB in the remaining CTA governance entities.

Resource Board

The **Resource Board (RB)** of CTA oversees the work in the Pre-Construction Phase of CTA. The parties of the Resource Board are countries represented by ministries, governmental agencies, or other institutions suited for this purpose. The Resource Board consists of a maximum of two representatives for each country, representing all institutions of their respective country.

Spokesperson

The **Spokespersons (Spokesperson and Co-Spokesperson)** lead the CTA project in all scientific, technical, and administrative aspects of the design, construction and operation of the CTA observatory. The Spokesperson and Co-Spokesperson share tasks and responsibilities in mutual agreement. The Spokespersons report to the Resource Board and the Consortium Board.

The Spokesperson and Co-Spokesperson are part of the CTA Management and members of the Project Committee. The Spokesperson chairs the general part of the meetings of the Project Committee.

The election of the Spokesperson and Co-Spokesperson are organised by the CB chair. The terms of the Spokespersons are normally 3 years.

Project Manager

The **Project Manager** is the head of the **Central Project Management (CPM)**. As such he is responsible for the coordination of the overall design of the CTA Observatory, and controls the schedule, resources, and technical objectives of the project.

Project Committee

The **Project Committee (PC)** tracks progress and makes working decisions for all aspects within the responsibility of the CTA Management. The PC receives regular reports from the Project Team Leaders and Work Packages Leaders and returns advice to the teams. In particular, the schedule and topic of internal reviews and the composition of the review panels is decided by the PC.

The PC is composed of the members of the CTA Management, and the leaders of the Project Teams and of the Work Packages in the science branch. The members have the right to vote. The chairperson(s) may invite additional non-voting participants for specific topics. Members of the Central Project Management team can join regularly the PC meetings as observers.

The PC meets typically once per month.

3.1.3 CTA schedule

CTA began its activities in 2006 and it is foreseen that the two observatories start to operate around 2018. To cope with this objective, the following schedule has been proposed [20]:

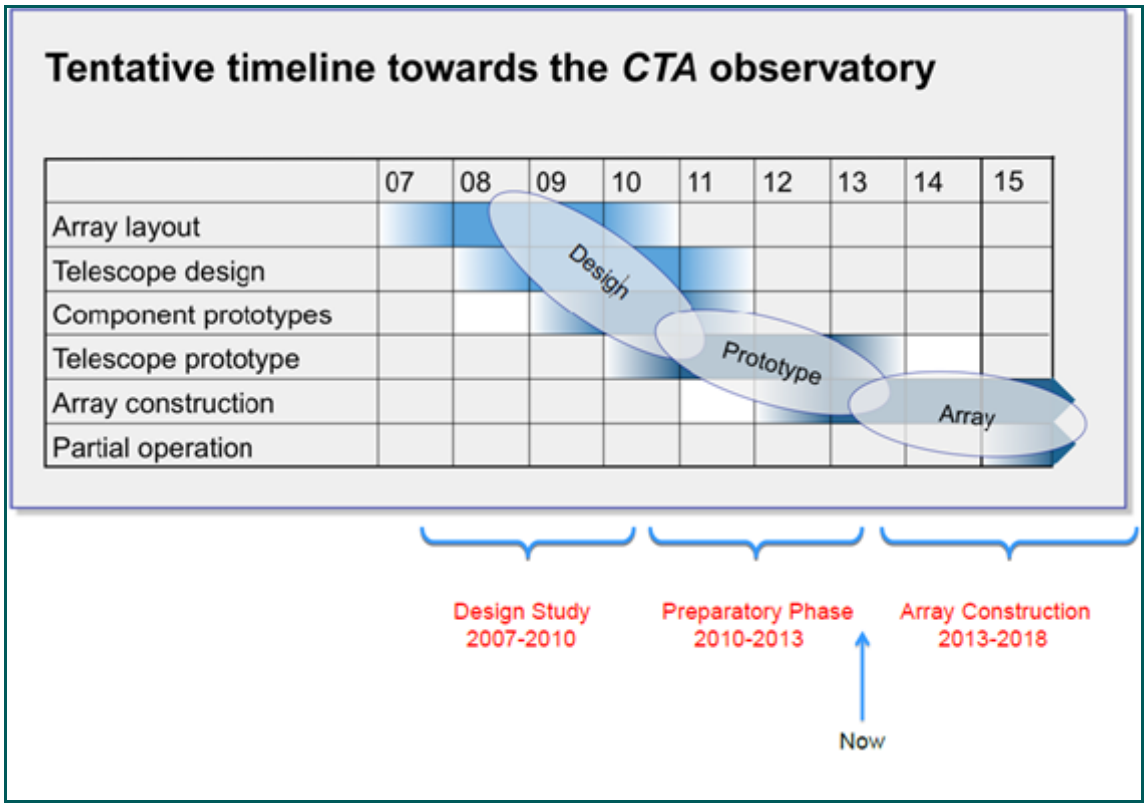


Figure 3–3: Schedule for CTA development

From the figure above, it can be identified three different phases in the CTA development [32]:

- **Design Study Phase** (2007-2010).
- **Prototyping & Preparatory Phase** (2010-2014).
- **Array Construction & Deployment** (2014-2018).

NOTE: The schedule in Figure 3–3 is outdated. At the time of preparing this document the Preparatory Phase had already been extended up to mid-2014.

3.1.3.1 Design Study Phase

This phase covered all the activities aimed at the mature design of the telescopes which will compose the CTA observatories, definition of the layouts of the observatories and small-scale prototyping. In order to properly focus on each of the critical parts and to effectively meet the goals proposed this Design Study was divided into different Work Packages.

Each Work Package in the Design Study Phase was linked to a specific area so that the members could collaborate in those WP's on which they have background experience sharing their knowledge for the sake of the efficiency.

Work Package Identifier	Name
PHYS	Astrophysics and astroparticle physics
MC	Optimisation of array layout, performance studies and analysis algorithms
SITE	Site evaluation and site infrastructure
MIR	Design of telescope optics and mirror
TEL	Design of telescope structure, drive and control systems
FPI	Focal Plane Instrumentation
ELEC	Readout electronics and trigger
ATAC	Atmospheric monitoring, associated science and instrument calibration
OBS	Observatory operation and access
DATA	Data handling, processing, management and data access
QA	Risk assessment and quality assurance

Table 3–1: Work Packages defined in the CTA Design Study Phase

The Design Study Phase concluded with the publication of an article that summarized the activities carried out to cope with the pre-defined objectives: The CTA Design Concepts [32].

3.1.3.2 Prototyping & Preparatory Phase

Once the Design Study phase was completed, the design choices underwent a campaign to test its capabilities and to pave the way for the final construction of the array in the so-called Prototyping & Preparatory phase. This phase, on which CTA development is currently immersed, is about to be completed, and has evolved from the way it was conceived when it began by the end of 2010.

This phase encompasses very different tasks:

- Prototyping of the elements identified in the final design of the CTA array.
- Establishment of a legal framework and governance structure for the future CTA observatories attending the requirements of the CTA consortium and the local authorities of the final places where they will be deployed.
- Management of the funding to ensure the financial coverage during the construction of the arrays.

The hierarchical structure of CTA has been modified throughout the Prototyping and Preparatory Phase to cope with these objectives. The responsibilities of the CTA Project Office increased, and new work packages were defined for the prototyping of the telescopes.

More precisely, and according to the information in [21], the new WP's defined for the Preparatory Phase were grouped into three major categories:

- **Preparing CTA organization**: This category –labelled as "A"– covers the legal, governance & logistical and financial work. This comprises the organization of the project, its management, identification of the potential funding sources from the different countries & institutions involved, etc. It is leaded by the Project Office as per WP A1 in Table 3–2.

- **Preparing CTA construction**: The work packages of this category (labelled "B") are those covering all the technical issues, such as telescope detailed design, quality assurance, risk assessment, site selection, etc. It is leaded by the Technical Project Coordination as per WP B1 in Table 3–2, which hierarchically depends on the Project Office.

- **Preparing CTA operation**: Finally, this group "C" comprises the strategic work to be performed. It is under the responsibility of this category the continuous revision of the project objectives w.r.t. the scientific advances achieved during the construction of the observatories to ensure that the scientific goals are preserved. The tasks to define the data handling, analysis tools, user interfaces, etc. will also be assumed by the WP's of this category.

The list of work packages inside each category was initially defined as follows:

Work Package Identifier	Acronym	Name
GROUP A	**PREPARING CTA ORGANIZATION**	
WP A1	MAN	Management
WP A2	LEGAL	Legal framework for constructing and operating CTA
WP A3	GOV	Governance scheme for CTA
WP A4	FINANCE	Financial model for funding construction, operation and decommissioning of CTA
GROUP B	**PREPARING CTA CONSTRUCTION**	
General Work Packages		
WP B1	TPC-INT	Technical Project Coordination
WP B2	SST-SYS	System engineering and integration of SST
WP B3	MST-SYS	System engineering and integration of MST
WP B4	LST-SYS	System engineering and integration of LST
WP B5	SITE	CTA site characterization
WP B6	SDEV	Planning site development and site infrastructure
WP B7	PROC	Procurement and industrial engagement in CTA
WP B8	IRD	Industrial R&D and pre-production
"Vertical" Work Packages		
WP B9	SST-STR	Design and prototyping of SST telescope structure and optics
WP B10	SST-CAM	Design and prototyping of SST camera
WP B11	MST-STR	Design and prototyping of MST telescope structure and optics
WP B12	MST-CAM	Design and prototyping of MST camera
WP B13	LST-STR	Design LST telescope structure and optics, and prototyping of components
WP B14	LST-CAM	Design and prototyping of LST camera
"Horizontal" Work Packages		
WP B15	MC	Simulation and optimization of instrument performance
WP B16	TEL	Telescope structures and drives – common aspects among Telescope types
WP B17	MIR	Mirror facets, facets support and alignment – common aspects among Telescope types

Work Package Identifier	Acronym	Name
WP B18	FPI	Focal plane instrumentation – common aspects among Telescope types
WP B19	ELEC	Electronics and triggering – common aspects among Telescope types
WP B20	ATAC	Atmospheric monitoring and calibration
WP B21	ACTL	Instrument control and data acquisition
GROUP C	PREPARING CTA OPERATION	
WP C1	LINK	Linking with science communities towards refining and preparing the science goals and utilization of CTA
WP C2	OUTR	Outreach activities
WP C3	CEIN	CTA e-infrastructure
WP C4	DAFA	Data formats, archiving and analysis

Table 3–2: Initial set of Work Packages defined in the CTA Prototyping & Preparatory Phase

The relationships between "A", "B" and "C" groups of work packages are shown in Figure 3–4.

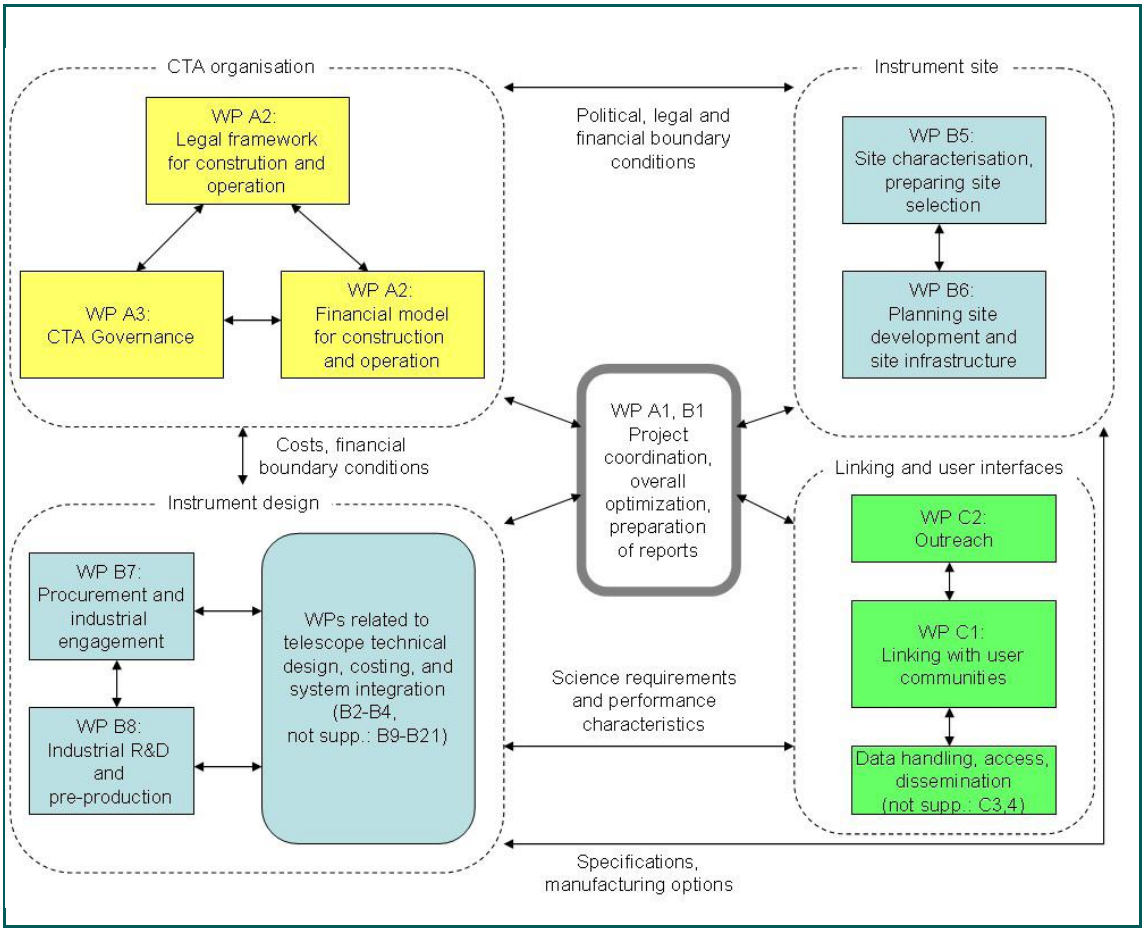


Figure 3–4: Links and connections among the WP's defined for the Preparatory Phase

It is important to remark that WP's **A1** (**MAN** – Management), and **B1** (**TPC-INT** – Technical Project Coordination) comprise all the tasks related to the management of the remaining work packages, whereas some WP's also depend hierarchically from other ones, being the Project Office the responsible for the correct management, coordination and integration among them.

Thus, the overall hierarchy for the WP's for CTA Preparatory Phase can be depicted as per Figure 3–5.

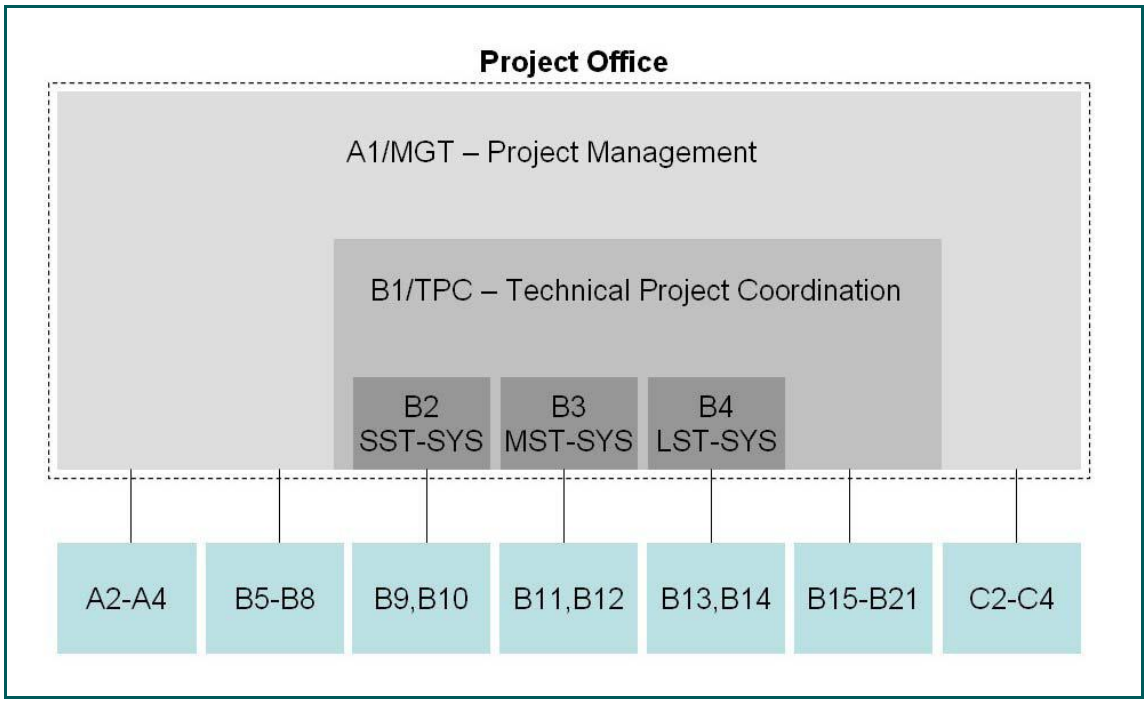


Figure 3–5: Hierarchy of WP's in the Preparatory Phase, being the Project Office on top of the management responsibilities

Group "B" of work packages related to the technical issues of the Preparatory Phase of CTA deserves a more detailed description, as its WP's are organized in a more complex structure than that of the management & dependence hierarchy introduced previously.

Table 3–2 divides the work packages of group B in three different sub-categories:

- **General work packages**: Includes WP's B1 to B8, of which B1 correspond to the overall management through the Technical Project Coordination, WP's B2, B3 and B4 are specific management and coordination work packages for the small, medium and large sized telescopes, and finally WP's B5 to B8 are work packages covering those activities not directly linked to the construction of the CTA observatories' telescopes but the associated infrastructures instead (site characterization, deployment, procurement, R&D, etc).

- **"Vertical" Work Packages**: The organization of the CTA observatories as composed by three types of telescopes spread in a different manner to cover a wide energy range (refer to section 3.1.1 for details) implies that there is a complete design chain per telescope type.

  "Vertical" work packages refer to those specific tasks of a given type of telescope.

– **"Horizontal" Work Packages**: Following the explanation above, "Horizontal" work packages refer to those specific tasks of a part of the design chain of a telescope which apply to the three types of telescopes.

Hereafter follows an example for a better understanding of the division above.

Example

Imagine that we want to produce uniforms for the students of a given school. There are three types of uniforms: One is designed for boys, another one for girls and the last one for practising sports, which fits to both boys and girls. All of these uniforms are composed of an upper cloth (polo shirt or T-shirt), a lower cloth (skirt, trousers or shorts) and socks (white for sports uniforms, coloured in the remaining cases).
Our textile enterprise is famous for its overall quality and outstanding prices, which is a result of the low internal costs due to optimal internal organization: we organized our staff in two categories: Uniform designers and Cloth manufacturers. The first group (uniform designers) is in charge of defining completely a given type of uniform according to the available cloths. Thus, part of the staff is specialized in the uniforms for boys, another part in uniforms for girls, and finally the staff which designs the sports uniform. They all care that on the uniforms produced the sizes of each cloth are coherent one another for each age, the colours of shirt and socks fit well, etc., though they do not care much about how each cloth is produced. The second group (cloth manufacturers) receive instructions from the uniform designers about the sizes, colours and other specific design tips of the uniforms and produce the different types of cloths. So, our staff of cloth manufacturers is divided into upper body manufacturers (producing polo shirts or T-shirts), lower body manufacturers (producing skirts, trousers and shorts), and finally, the socks manufacturers.

In the example above, the specialists of uniform designers in boys, girls and sports uniforms are equivalent to the vertical work packages defined within the group B above for Small, Medium and Large Sized Telescopes; whereas the cloth manufactures divided into upper & lower body cloths, and socks manufacturers are equivalent to the horizontal work packages defined previously (in charge of the mirrors, electronics, focal plane, structure, etc.).

On top of that, and following the example of our textile enterprise, we not also need uniform designers and cloth manufacturers, we need to procure the materials, manage our staff, provide the furniture and services needed for their work, organize out plant, etc. This is aligned with the general work packages of group B.

The naming convention for "vertical" and "horizontal" WP's comes from the fact that a very useful representation of them is through a matrix on which the columns are vertical WP's and the rows are horizontal WP's. In this matrix, the overlapping regions between a row and a column indicate common tasks to the corresponding horizontal and vertical WP's related. This matrix is presented in Figure 3–6:

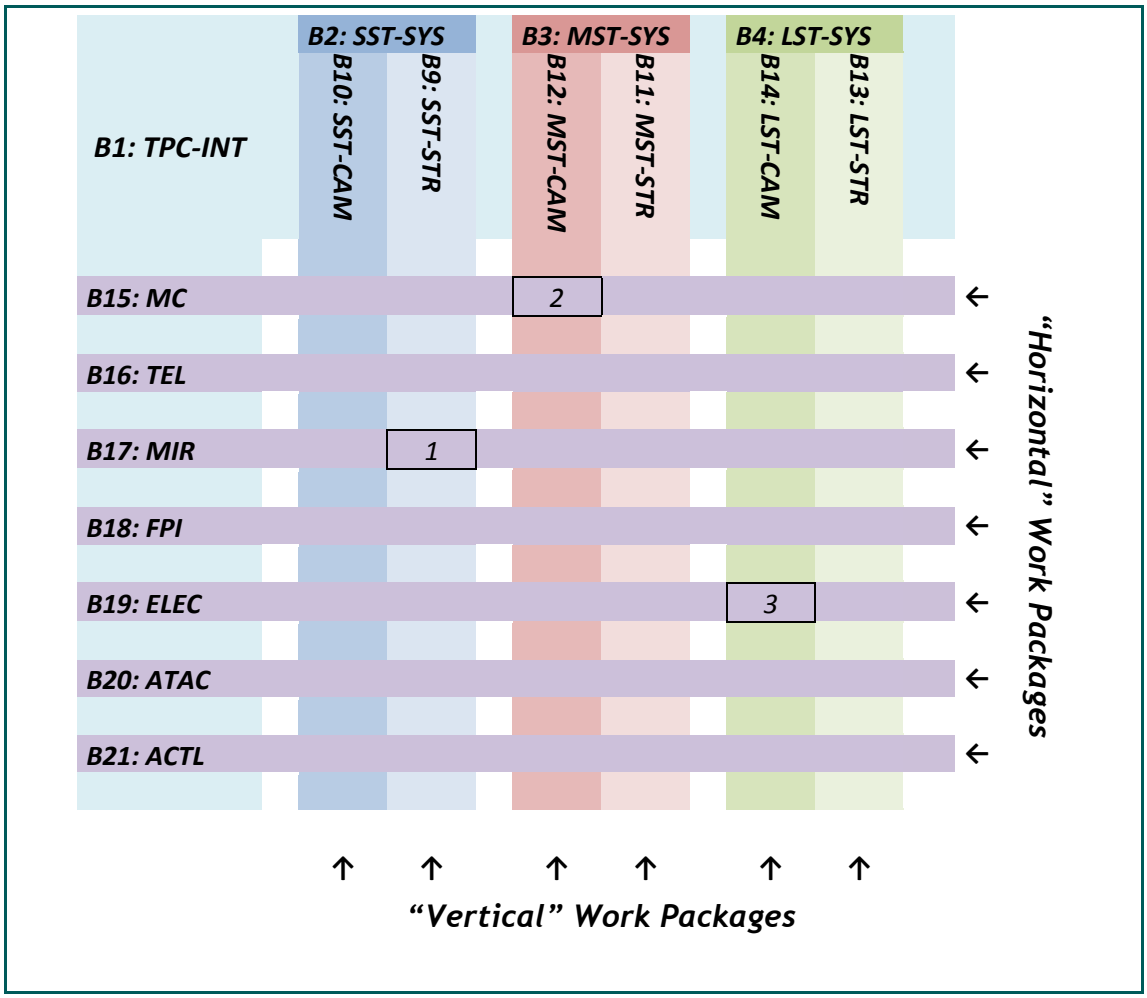


Figure 3–6: Matrix of Horizontal and Vertical WP's with three overlapping regions identified as examples: 1) Tasks related to the structure of the mirrors of SST's; 2) Tasks related to the Monte-Carlo simulations of the MST cameras; 3) Tasks related to the electronics of the LST cameras.

Soon after this structure had been established, it was refined to include some tasks not covered by the initial set of work packages presented in Table 3–2. As a result, the first Work Package structure consolidated for the Prototyping and Preparatory Phase was the one presented in Figure 3–7.

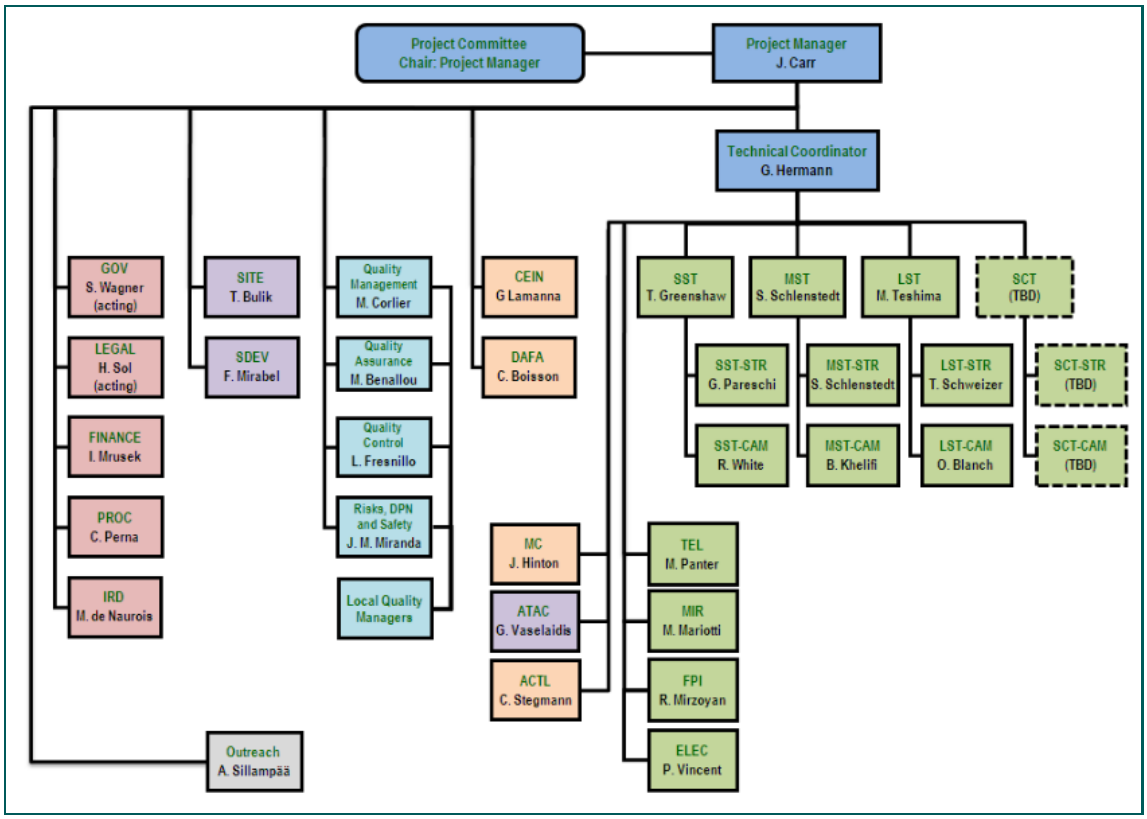


Figure 3–7: Initial Work Package structure for the Prototyping and Preparatory Phase

This initial Work Breakdown Structure for the Preparatory Phase has recently evolved in order to improve it with the lessons learnt in the on-going development. Currently, the "Vertical" work packages have turned into entire sub-projects within CTA. Besides, the three initial types of telescopes (LST, MST and SST) have evolved to consider up to five types: LST, MST, SCT, SST-1M and SST-2M. SCT are the medium sized Swarzschild-Couder Telescopes, whereas two different branches for the development of the small sized telescopes are considered: 1M and 2M, which indicates the absence or presence of a secondary mirror in their design.

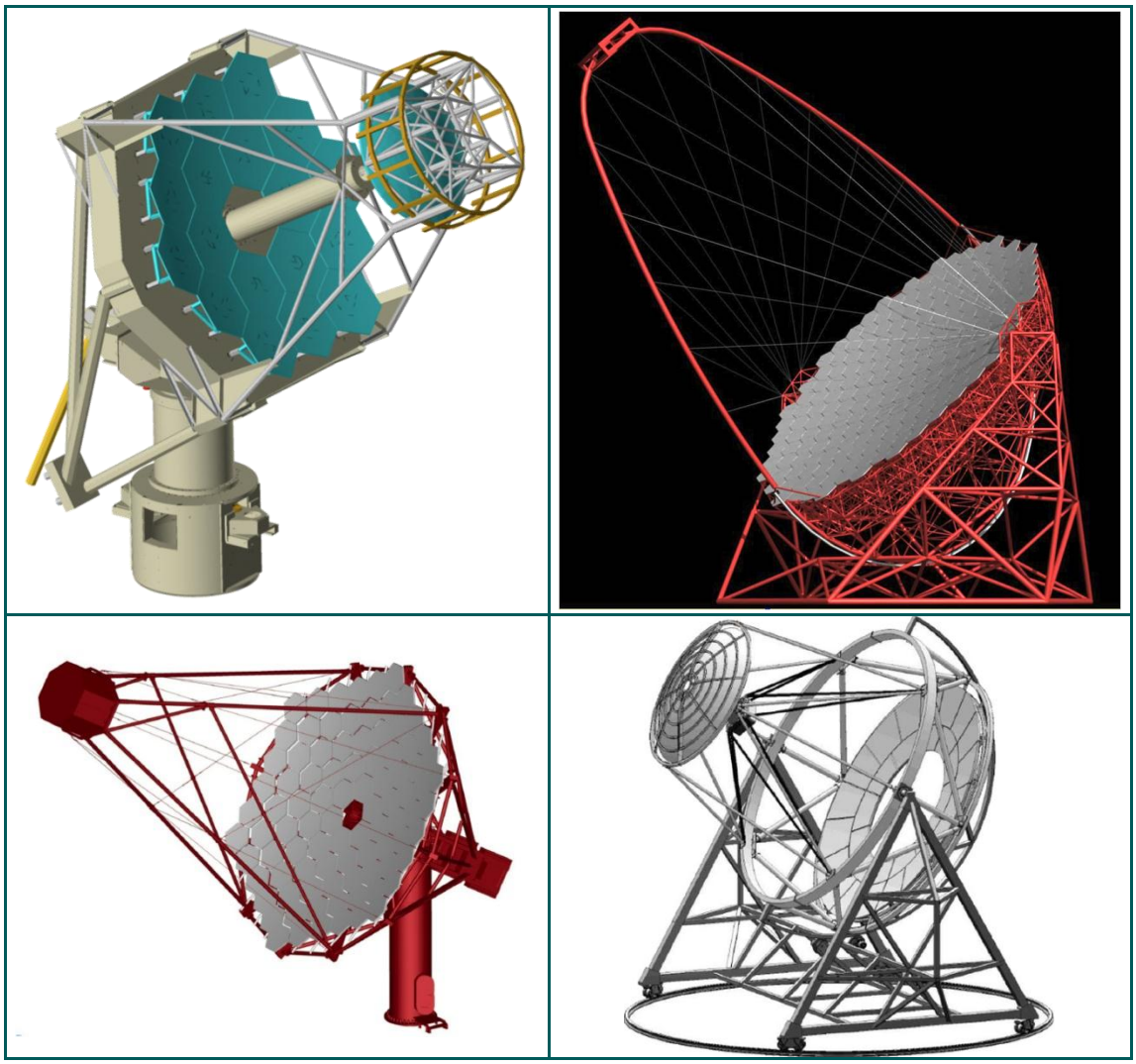


Figure 3–8: Representations of the different types of CTA telescopes, from left to right and then from top to bottom: SST-2M, LST, MST and SCT

The current hierarchy of Work Packages at the end of the Prototyping & Preparatory Phase is depicted in Figure 3–10.

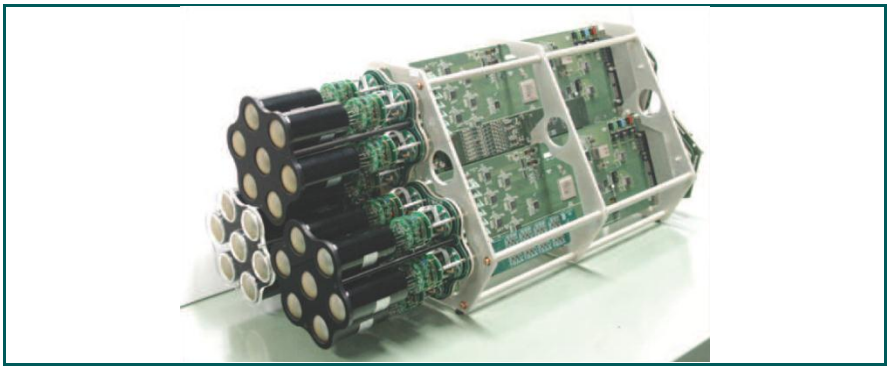


Figure 3–9: Array of three clusters of the DRAGON solution for LST cameras

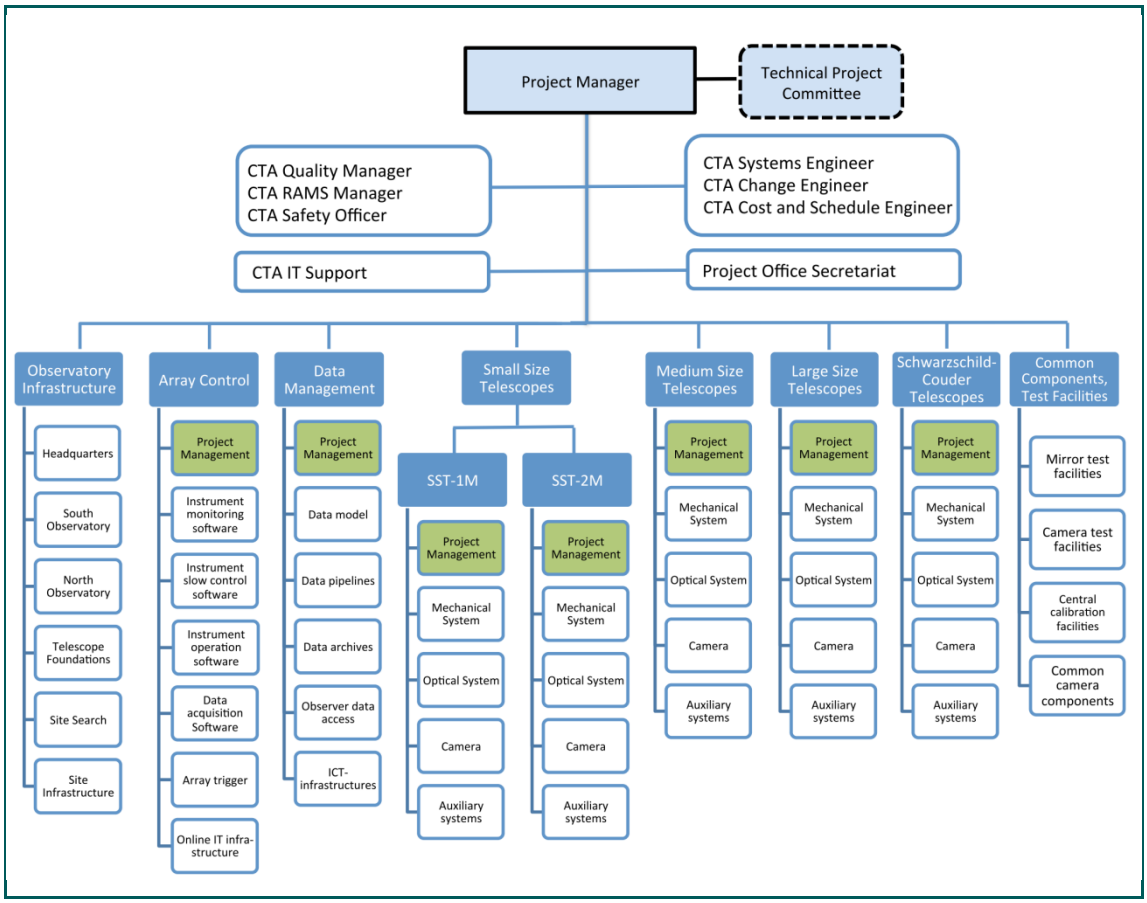


Figure 3–10: Current WP structure for CTA

It is noticeable that the "Horizontal" and "Vertical" work packages' approach remains, although not so explicitly as per the initial WP's in Figure 3-6. Figure 3-10 shows the subprojects (blue boxes) as drop boxes including the different work packages that compose them, in a similar way as the previous "Vertical WP's" did, being many of them identical from one subproject to another (the WP's names of each type of telescope are the same), hence constituting the former "Horizontal" WP's.

The Prototyping and Preparatory phase has been extended up to fall 2014, and its closure will be pronounced with the publication of the final design of the CTA which allows its construction: The CTA Technical Design Report. In the meanwhile, preliminary versions are being released with the results of the design reviews for the different technical work packages, the so called Preliminary Technical Design Reports, which latest version is [18].

3.1.3.3 Array construction and Roadmap to the operational stage

Once the preparatory phase is completed, the next stage will encompass in the construction of the two observatories, commissioning period for the assessment of its capabilities and transition to the operational life of the CTA arrays. It is foreseen that before the end of 2013 the sites for both the Northern and Southern observatories will be finally decided.

Currently, the site candidates for the construction of the Northern Observatory are:

- Teide Observatory at Tenerife (Spain).
- San Pedro Martir Observatory at Baja California (Mexico).
- Likr (India).
- Upshi (India).
- Arizona (USA) (potential candidate).
- Tibet (China) (potential candidate).

On the other hand, the site candidates to host the Southern Observatory are:

- Leoncito (Argentina)
- San Antonio de los Cobres (Argentina)
- HESS Observatory (Namibia)
- Aus (Namibia)

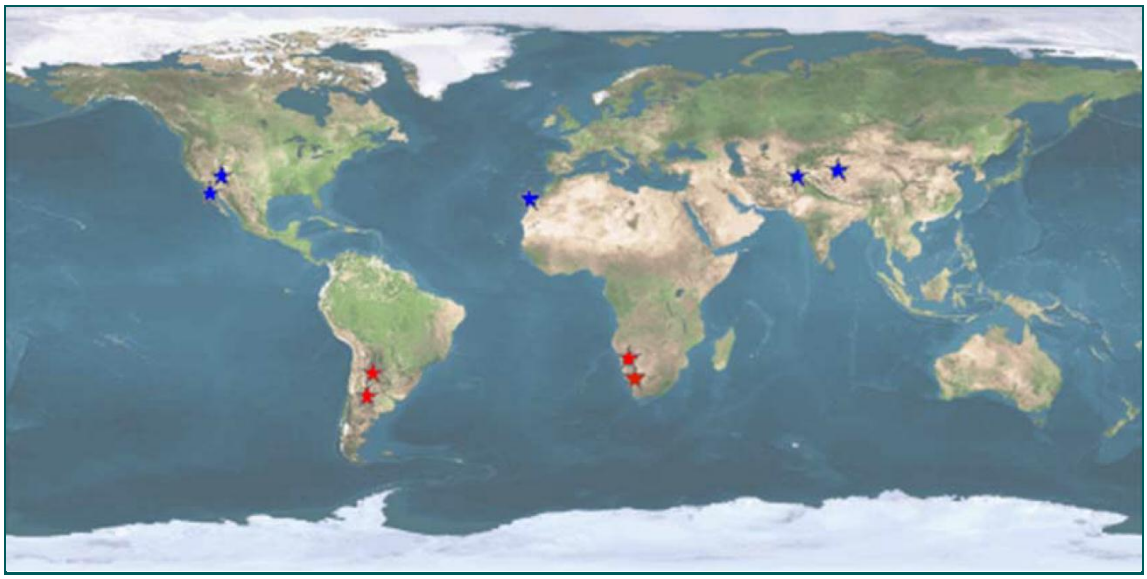


Figure 3–11: World Map with the location of the Northern (blue stars) and Southern (red stars) site candidates for CTA observatories.

The site candidates must be flat areas at high altitude, free of light pollution, stable from a seismological point of view, and allowing a relative easy access from the nearby towns. Obviously, from a meteorological point of view, the atmospheric conditions are a key aspect, imposing the most demanding requirements in terms of cloud coverage, average wind speed, snow load, etc.

CTA Site Requirements description	Target values
Topographic requirements	
Land flatness (maximum difference in height)	< 150m (< 50m is desirable in Northern site)
Area	>= 10 km^2 (Southern site) >= 1 km^2 (Northern site)
Altitude	1500 – 3800 m above Mean Sea Level
Seismic activity	< 5 $m \cdot s^{-2}$
Atmospheric requirements	
Cloud coverage percentage from satellite data	> 70% nights good for observation
Night Sky Background (light pollution)	U > 21.55 $mag \cdot arsec^{-2}$ B > 22.25 $mag \cdot arsec^{-2}$ V > 21.25 $mag \cdot arsec^{-2}$
Wind speed on observation conditions	< 50 $km \cdot h^{-1}$ for 80% of observable time
Maximum wind speed	< 200 $km \cdot h^{-1}$
Maximum snow load	< DIN 1055
Accessibility requirements	
Medical Rescue	< 2 hours or below (depending on local regulations)

Table 3–3: CTA Site requirements

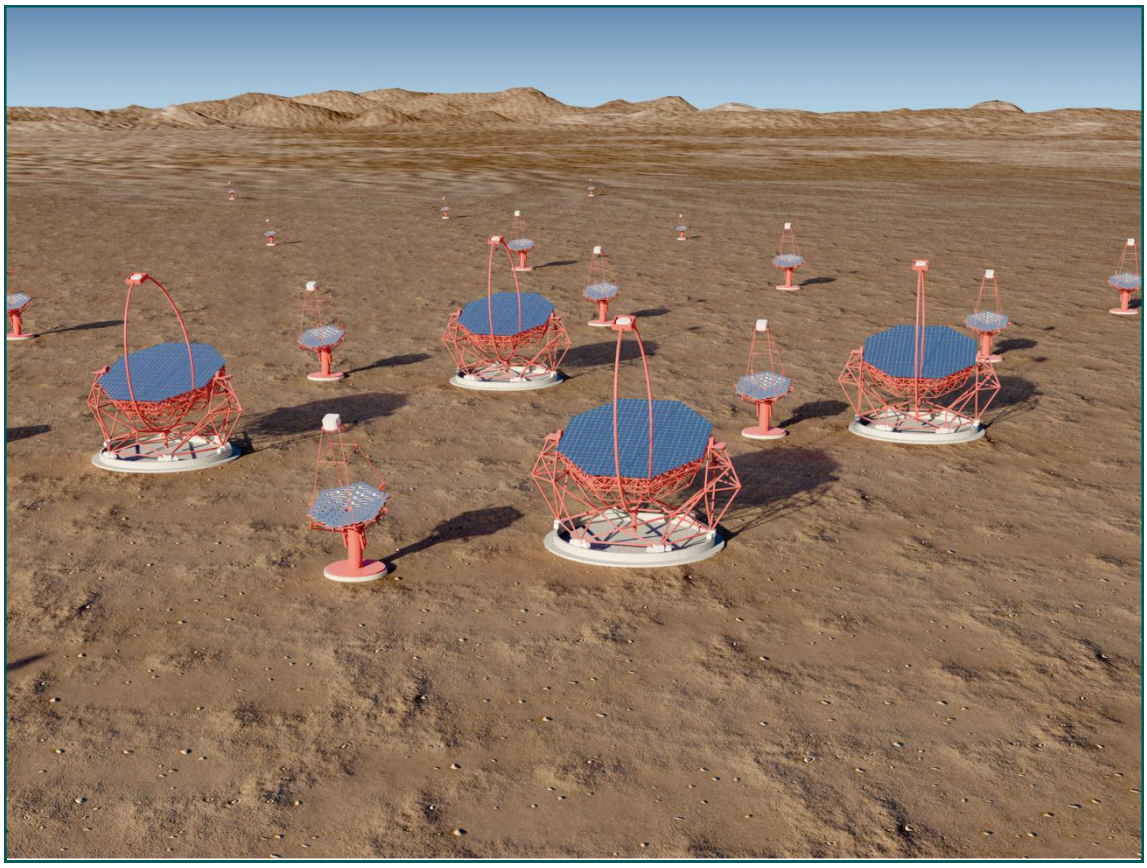


Figure 3–12: Computer simulation of the aspect of CTA observatory

3.2 Product Assurance in CTA

The management of the Product Assurance in CTA has evolved with the managerial structure of the project itself. This section presents a timeline of the different phases of the CTA schedule achieved to current date, with the relevant tasks carried out from the point of view of Product Assurance.

NOTE: It is important to remark that the concept *Product Assurance* is denoted *Quality* in CTA, being the remaining disciplines named as usual: Quality Assurance, Risks Management, Dependability and Safety. Therefore, the usage of *Quality* and *Quality Assurance* terms in CTA indicate two different concepts.

3.2.1 PA in the Design Study Phase

At the early stages of the CTA project, a dedicated work package was defined, the so called QA – Risk Assessment and Quality Assurance (refer to Table 3–1), aimed at preparing the Quality Plan for the project and the Product Assurance structure.

The Quality Plan for CTA suffered a long period of iterations and reviews up to the approval of the first agreed version [35], on 08/04/2011. At least seven previous draft versions were prepared and rejected since December 2009 up to March 2011.

Such a long period for the approval of the key document for the Product Assurance within CTA made it somehow useless, once approved, for the Design Study Phase at least. The reason is clear: The Design Study Phase had concluded at the end of 2010 leading to the Preparatory Phase.

The document has evolved since then, mainly to adapt to the various modifications of the managerial structure of CTA impacting the organization of the Product Assurance hierarchy. The problem of the long processes for the approval of the newer versions still remains, though somehow mitigated, as there is not yet a consolidated procedure for the revision and approval of documents within CTA. Instead of this, a list of reviewers is included in the document, but not so the deadlines for raising comments, nor the way to discuss them with the authors.

Quality Plan version	Date	Status
v1.0	08/04/2011	First approved version with some comments to be implemented
v1.1	07/07/2011	Second approved version
v1.2.2	07/11/2012	Version submitted for review & approval. No more information provided to date

Table 3–4: CTA Quality Plan history (excluding draft versions prior to v1.0)

Among the contents of the Quality Plan it is worth remarking:

- The definition of a managerial structure for Quality within CTA composed of:
  - **Quality Manager** (Tasks: Coordination of the quality work packages, preparation and update of the Quality Plan, etc.). *Quality is understood as Product Assurance as per the NOTE in section 3.2.*

- **Quality Assurance Manager** (Tasks: Identification of the Quality Assurance requirements, preparation and update of the Documentation Plan, etc.)
- **Quality Control Manager** (Tasks: Audits)
- **Risk Assessment, Dependability and Safety (RADS) Manager** (Tasks: Management of the Risk Assessment, Dependability and Safety disciplines of Product Assurance; preparation and update of the Risks Management Plan and RAMS Plan)
- **Local Quality Managers** (Responsible for Quality tasks in the different Work Packages)

– A quality program that covers

- HW aspects
- SW aspects
- Documentation changes
- Non conformances
- Audits

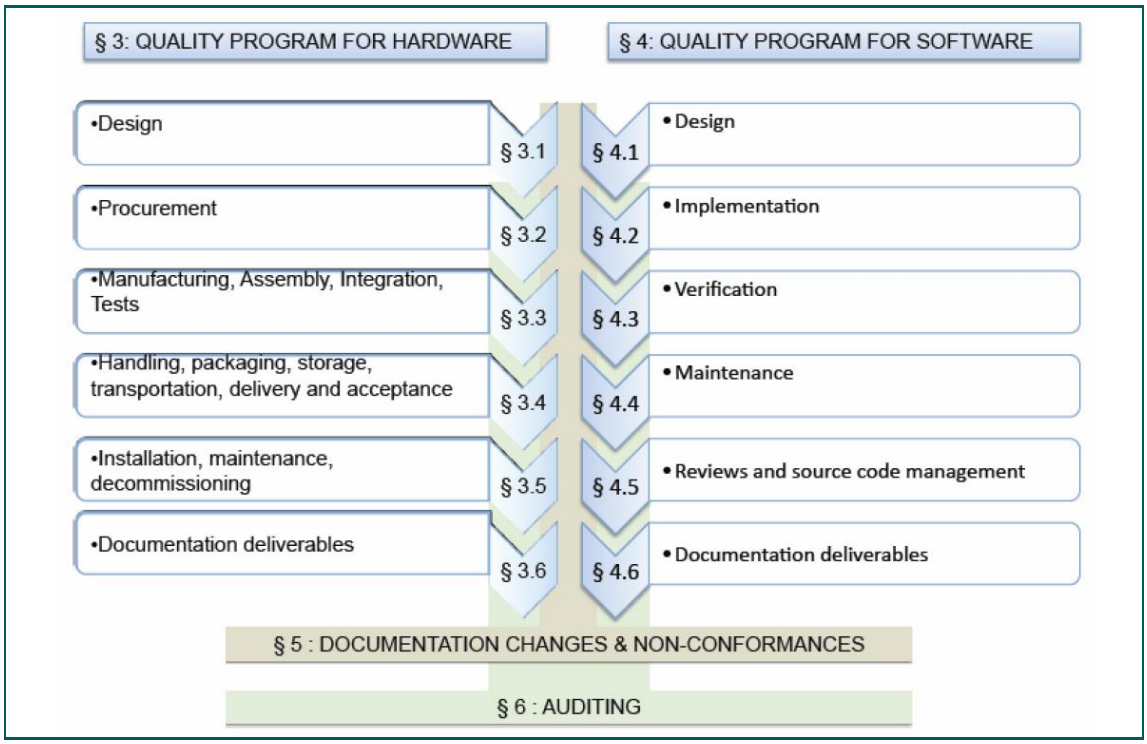


Figure 3–13: Quality Program defined for CTA

UCM_ELEC role played for the Product Assurance in the Design Study Phase

UCM_ELEC was involved in the preparation of the CTA Quality Plan from its very early stages: Initially as a part of the reviewers' team in charge of raising amendments to the different draft versions; afterwards as responsible for a specific section (Quality Program for Software). In

parallel, a separated document with Quality Assurance rules for SW developments [36] to extend the ideas in the Quality Program for SW was also delivered to the consortium.

3.2.2 PA in the Prototyping and Preparatory Phase

3.2.2.1 First part of Preparatory Phase (2010-2012)

When CTA development entered the Prototyping and Preparatory Phase, the work packages evolved from the list presented in Table 3–1 to the three levels (A, B and C) structure of Table 3–2 as per the hierarchy of Figure 3–7.

The first version of the Quality Plan was approved at the early stages of this Preparatory Phase once the iterations on their contents extended beyond the Design Study Phase. Therefore, although this plan was not available in the previous phase, as the new managerial structure for the so called **Quality Management Team** had been traced in the document, the drawback in its late approval become a benefit in this new one.

The Quality Management Team, as explained in previous section, was divided into four work packages.

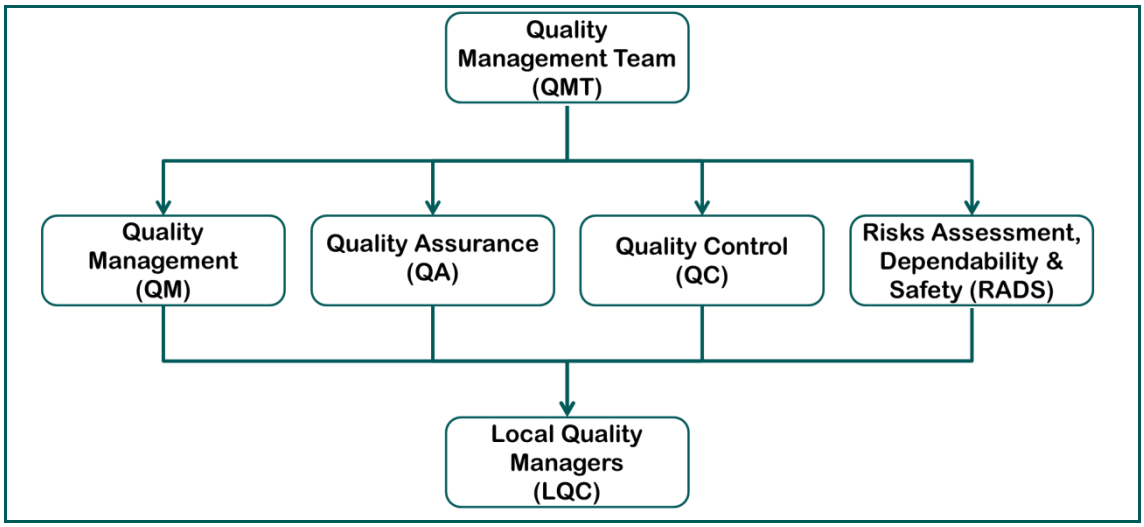


Figure 3–14: Organization of the Quality Management Team at the beginning of the Preparatory Phase

Quality Management (QM) work package

Quality Management work package was led by the Institut National de Physique Nucléaire et de Physique des Particules – IN2P3, and had the following responsibilities:

- Managing the QMT (quality activities planning and monitoring, LQMs and auditors list),
- Organizing periodic QMT meetings (progress status report: non-conformance status, report on identified risks and their management, summary of the audit reports),
- Developing and maintaining the Quality Plan, assisted by the QMT,

- Communicating and convincing the consortium on the necessity for quality management,
- Representing the QMT during Project Committee (PC) meetings (communicate PO decisions to quality team, collecting and reporting LQMs requests to PO),
- Providing support for quality activities to the collaboration,
- Coordinating the training of the LQMs on the quality manager's recommendations.

Quality Assurance (QA) work package

The responsibility of the Quality Assurance work package was assigned to the AstroParticule et Cosmologie – APC group of Université Paris Diderot – Paris 7. This work package encompassed the following tasks:

- Identifying quality requirements and developing quality tools (data base, future planning of the information management system tools),
- Developing and maintaining the Documentation Plan (documentation procedure, tool, identification procedure, and training),
- Checking the documents requiring quality control (management, quality or technical documentation and associated templates),
- Defining and implementing the traceability system (product identification, record, logbook),
- Developing and maintaining the product changes system (configuration management plan, traceability of versions, non-conformances, upgrades, maintenance).

Quality Control (QC) work package

This work package was initially assigned to Fidias Consulting, a privately owned Spanish company, with the following responsibilities:

- Assisting and providing support in the definition of product specifications.
- Providing support to LQMs as far as possible.
- Drawing up the auditing guides (prototypes, production launch, supplier audits).
- Holding on-site auditing when necessary.
- Collecting field-failure data for the development of the RADS documentation.
- Checking and auditing risk assessment for maintenance output.
- Checking the electronic components, materials, and processes used with RADS team support).
- Assisting in the identification of the product condition on delivery.

- Assisting in the identification of the product condition during its lifetime.
- Creating and organizing the auditing teams.

The lack of funding for QC, plus the long delay in the acceptance of the Product Assurance Plans and associated requirements postponed indefinitely the beginning of the activities of this work package.

Risk Assessment, Dependability and Safety (RADS) work package

The responsibility of this work package yielded in UCM_ELEC group, and therefore the activity devoted to the associated tasks in RADS comprise the most of the work that supports the procedures developed as well as the bulk of the experience gathered.

As per the definition in the Quality Plan [35], the tasks assigned to RADS work package are:

- Identifying and evaluating project risks.
- Developing and maintaining the Risk Assessment and Mitigation Plan.
- Developing and maintaining the Reliability, Availability, Maintainability, and Safety Document.
- Supporting the QC manager in the checking of the electronic components, materials, and processes used.
- Defining the RADS procedures and designing the corresponding templates.

Due to the relevance of the activity carried out for RADS in the final procedures proposed, a detailed summary is provided hereafter, unlike the previous work packages for which only an overall description is given.

3.2.2.1.1 RADS activities: The RADS management strategy

The first part of the work in RADS was the settlement of the managerial structure that allowed a proper implementation of the RADS procedures in the different technical groups of CTA.

This comprised two main procedures: The process for Dependability and Safety (RAMS) and the process for Risks Management.

RADS process for Dependability and Safety (RAMS)

The general RAMS process in CTA was structured through the establishment of an organization that allowed the down flow of RAMS guidance from the high project to the lower local level and the corresponding feedback, thus allowing the CTA RAMS assurance. With this aim, the technical working groups were requested to submit Dependability (Reliability, Availability and Maintainability) and Safety information about their components, operation and maintenance procedures. The Maintainability information would contain suggested Preventive Maintenance Schedules.

RADS working group would then gather all the RAMS information from lower local level and will

- incorporate it into the system level RAMS analysis and reports,
- flag problem areas and
- make the necessary modifications to ensure that the RAMS objectives are fulfilled.

Figure 3–15 summarizes the RADS work logic defined for RAMS in the context of the CTA project activities.

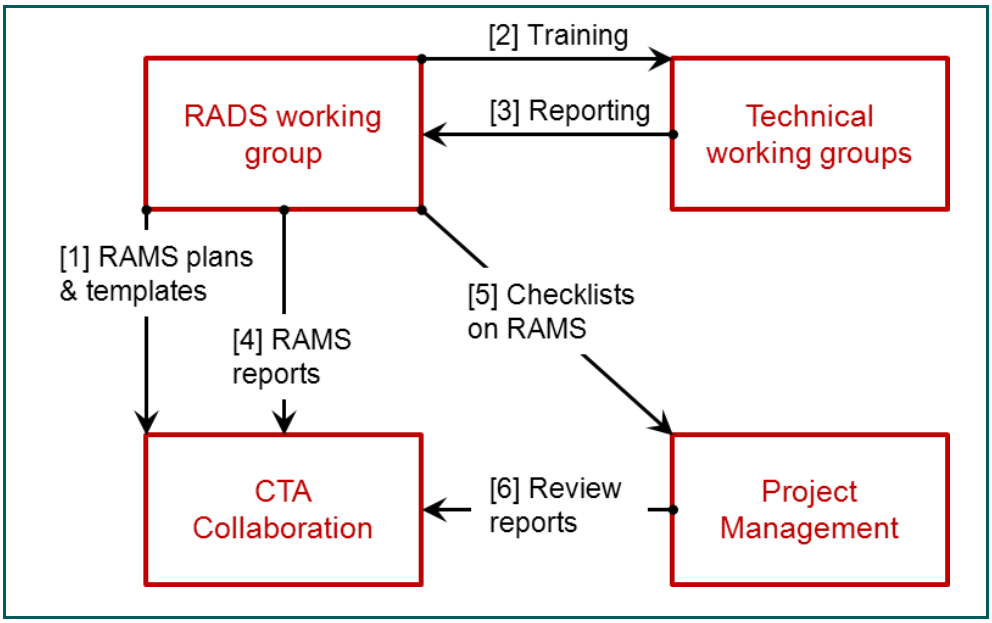


Figure 3–15: Overall of RADS process for Dependability and Safety (RAMS)

More precisely, the descriptions of the activities in RADS work logic for RAMS are summarized below:

1. RADS working group produces the RADS Plans (RAMS plan and Risks Management Plan) and submits them for review & acceptance, as well as the templates to fill in with the outputs from each procedure.
2. Once accepted, RADS working group conducts the training sessions for the technical group engineers in charge of the RAMS work.
3. The technical groups implement the RAMS procedures and deliver their reports
4. The RADS working group collects the reports from all the technical work packages, integrates them in a joint RADS report and makes it available to the CTA collaboration.
5. Based on the RADS plans, RADS working group prepares a set of checklists in RADS activities to be evaluated by the Project Management.

6. The Project Management carries out the reviews on RADS activities and makes the corresponding report available to the CTA collaboration.

RADS process for Risk Assessment

The Risks Management policy in CTA was defined so that the relevant information was properly exchanged between the local groups and the overall project management. This flow of information allowed identifying similar situations already tackled by other groups for which the previous experience could be an added value to solve them.

RADS working group would gather all the Risks management information from lower level and will

- incorporate it into the system level Risks management reports
- notify to the appropriate recipient the existence of Non-Acceptable Risks

The overall RADS work logic defined for RAMS in Figure 3–15 was adapted to the new discipline or Risks Management, as depicted in Figure 3–16.

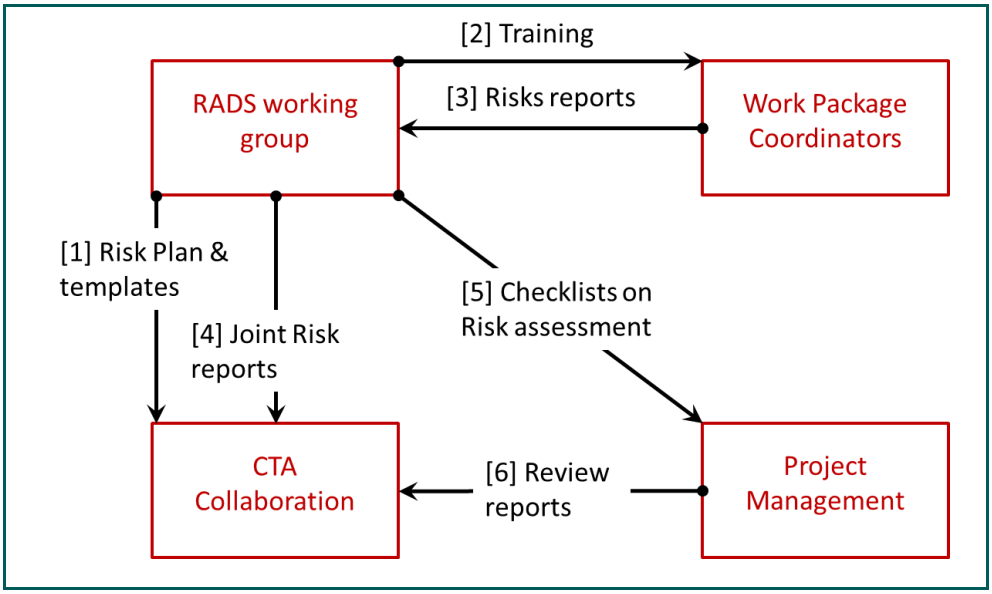


Figure 3–16: Overall of RADS process for Risks Management

The specific steps of the Risks Management policy deserving a detailed explanation are:

1. RADS Working Group produces the Risks Management Plan (present document) and distributes it for approval.
2. Once approved, RADS working group conducts specific training sessions for Risks Management. Such training is aimed at Work Package Coordinators and not at technical group engineers as it is done for the RAMS case.

3. The responsibility to conduct the Risks Management policy on each Work Package lies with its Work Package Coordinator. The risks identified will be assessed and reported to the RADS team by filling in the Risk register template, provided as a part of the Risks Management Plan [38].

Steps 4 to 6 remained unchanged from the overall work logic for RAMS, so once the complete information on risk assessment was collected by RADS team, the joint risk report would be distributed to the CTA collaboration.

Interaction with other technical groups

The processes defined for RAMS and Risks Management by the RADS team are essential parts of the RAMS Plan and Risks Management Plan under preparation. However, based on the experience with the Quality Plan, it was very likely that the approval of these plans became a long and difficult task.

Therefore, in order to mitigate the impact of this scenario in the remaining tasks of RADS work package and taking into account that the processes defined involved the technical groups as key actors, it was designed an information campaign to create awareness in CTA consortium about the foreseen strategy to implement RAMS and Risks Management procedures.

This strategy consisted of dedicated presentations with the proposed procedures at:

- CTA "Horizontal" (FPI, ELEC) and "Vertical" (LST) work package meetings [42], [45].
- CTA Project Office meetings [41].
- Parallel Sessions and Work Package Coordination Session of CTA Consortium General Meetings [43], [44].

3.2.2.1.2 RADS activities: The RAMS Plan

The RAMS Plan included all the procedures for the proper assessment of Dependability and Safety activities within CTA, alongside with their managerial aspects. Its preparation involved external collaborations other than the members of UCM_ELEC group, namely:

- RAMS experts from GMV Aerospace and Defence, a privately owned Spanish company.
- The Technical Coordinator of CTA.
- The Project Manager of CTA.
- The Systems Engineer of CTA at Project Office in Heidelberg, Germany.

First steps: Roadmap to version 1.0

The preparation of the RAMS Plan was planned so that the CTA technical and managerial representatives were involved from the very early stages. Two teleconferences were organized in summer and fall 2011 in order to:

- Agree a Table of Contents.
- Define the guidelines with the aspects to be covered by each section of the agreed Table of Contents.
- Assign the elaboration of each section to a different responsible, with the following repartition:
    - UCM_ELEC will write the managerial and organizational parts of the document
    - GMV RAMS experts will write the technical part of the document with the applicable RAMS procedures to each phase, templates, etc.
- Gather "on the fly" comments about the various intermediate draft versions by the Technical Coordinator, Project Manager and Systems Engineer of CTA to ease the formal review process once the document were completed.

As a result of this work plan, the first version of the RAMS Plan was ready for the CTA Consortium General Meeting in Madrid, on November 2011. This version already incorporated the comments received from the coordinators of the technical work packages, as it had been distributed two weeks in advance.

The RAMS Plan was then "officially" presented at that meeting [46] and was then released to the entire CTA collaboration for its last review, after it had been reviewed by the Project Manager, the Technical Coordinator and the Work Packages Coordinators.

Iterations with the Project Office

Finally, the RAMS Plan had incorporated all the comments received and was sent to the CTA Project Committee at the CTA Project Office for its approval, in February 2012.

At that time, the RAMS plan contained the process already explained in 3.2.2.1.1, plus a very detailed explanation of the RAMS techniques applicable to each phase of the project, along with their description and associated templates.

The meeting in Heidelberg on which this document was presented, [47], implied an inflection point in the RAMS Plan. The Project Committee in charge of approving the document rejected it with two main complaints about its contents:

- It was too complex and specific from the point of view of the techniques included.
- The CTA technical working groups were not prepared to implement it in their developments, as the ECSS standards on which it was based were perhaps too strict for CTA.

A major revision of the RAMS Plan was done on which all the templates and explanations about the techniques involved were removed. Two months later, the finally approved RAMS Plan [37] had significantly reduced its contents and concise description of the techniques involved, to turn into a generic summary of the procedures that should be applied at the different stages of a general development and no further information on the procedures themselves.

At the time of preparing this document, some of the templates in the original RAMS Plan rejected had been published as separated documents, along with guidelines for the elaboration of Failure Modes and Effects Analysis (FMEA) [23].

The RAMS Plan has been updated twice since the first version approved (1.0). The last version (1.2, dated 10/11/2012) is yet pending to be approved. The changes introduced are aimed at adapting the document to the last CTA organization of Figure 3-10.

3.2.2.1.3 RADS activities: The Risks Management Plan

The Risks Management Plan is the second major deliverable of RADS work package. Its preparation began in fall 2011, few after the first iterations on the RAMS Plan finished. The elaboration of this plan was entirely assumed by UCM_ELEC group, which released the first version for review by the end of February 2012.

Some iterations with people from the Project Office in Heidelberg, which were developing a similar procedure for Risks Management lead to a second version that integrated both contributions [38] in May 2012.

The CTA Project Manager let UCM_ELEC know that the review and subsequent approval of this plan was postponed until the RAMS Plan were consolidated, in order to take benefit of the agreed dispositions for this last document.

The Risks Management Plan has not yet been reviewed.

3.2.2.1.4 RADS activities: RAMS Requirements

As the design of the CTA progresses, three levels of requirements are being defined to be met by the final Observatory:

- Level A requirements: Requirements applicable to the entire CTA.
- Level B requirements: Requirements applicable to each Work Package of CTA.
- Level C requirements: Lower level Technical Specifications.

Figure 3-17 shows the three levels defined and the abstraction layer in the CTA blocks diagram to which they apply.

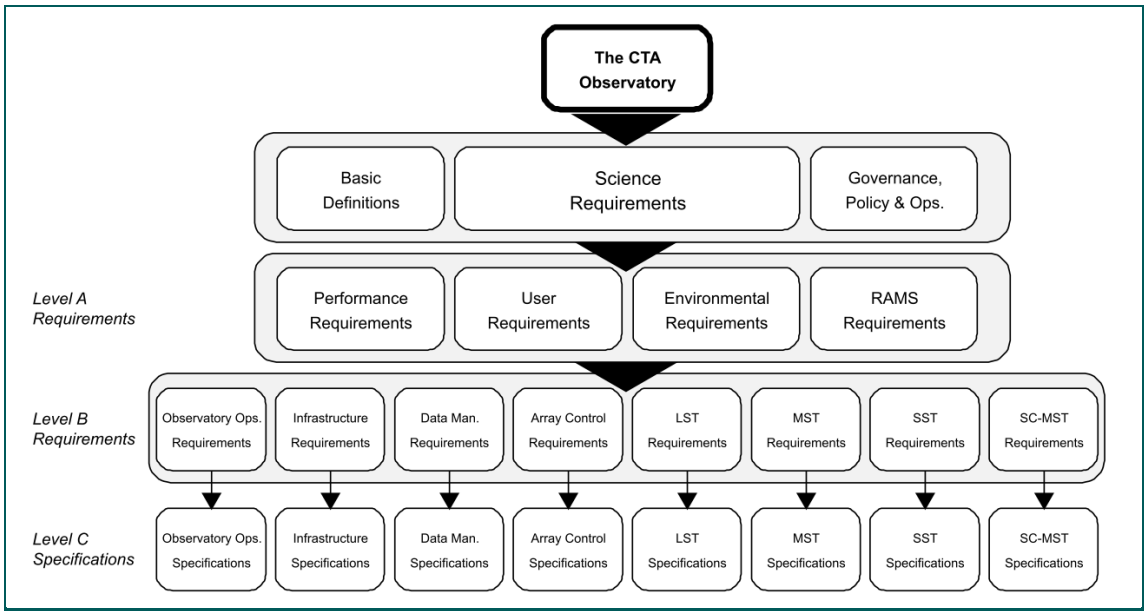


Figure 3–17: CTA Level A, B and C requirements and the elements to which they apply

UCM_ELEC has prepared the document with the RAMS level A requirements, which latest version [19] has been released for review & approval.

3.2.2.1.5 RADS activities: Support to technical groups

In parallel to the preparation of the RAMS Plan and Risks Management Plan, UCM_ELEC group attended support requests from other technical groups in RADS topics, namely:

- The preparation of the RAMS strategy for the Large Size Telescopes (LST) in the baseline design document for this work package of CTA at two different levels
  - [October 2011] In the first version of the LST baseline design document, [39], describing the overall RAMS organization and procedures in a very similar way as it was done for other technical groups in 3.2.2.1.1.
  - [March 2013] In the second version of the LST baseline design document, [40], detailing the RAMS life cycle and the applicable techniques to each phase once the RAMS
- The preparation of the Failure Modes and Effects Analysis (FMEA) for the cameras of the LST.
- Support to the definition of the RAMS strategy for the ACTL work package for their contribution to the Preliminary Technical Design Report [18].
- Support to the Spanish site candidate group in the assessment of the seismological risks for the report on the CTA northern candidate proposal at Teide Observatory [22].

3.2.2.2 Second part of Preparatory Phase [2013-]

The QMT structure disappeared with the new organization of the work packages of CTA (Figure 3–10). The main changes introduced in the new organization are:

- The transformation of the previous "Vertical" Work Packages of Figure 3–7 into *real* projects within CTA with their own managerial structure.
- The centralization of all the managerial tasks, including Product Assurance, in the Project Office at Heidelberg and therefore the definition of new roles there:
    - CTA Quality Manager
    - CTA RAMS Manager
    - CTA Safety Officer

As a result of this structure, UCM_ELEC group transferred the management tasks of the former RADS work package to the Project Office, but kept the responsibility of the RAMS Plan, Risks Management Plan and RAMS requirements documents.

UCM_ELEC from that moment on has joined the former work package and now LST project as the responsible for RAMS assessment.

3.3 Lessons learnt and ideas for the final solution proposed

CTA is a Large Scientific Installation managed by an *ad hoc* Consortium. This fact considerably complicates the definition of common working practices, as compared to other LSIs managed by an existing Agency. The large amount of institutions, 172, and members, more than 1000, together with the scarce amount of financial resources under the control of the central project office severely complicates the decision making process, including the approval of high level documents.

The lack of a procedure to review and approve the baseline documents for the development can make this task an endless loop with a continuous iteration of comments. As a result, key documents as the project plans may become too generic and subject to interpretations, whereas they should be concise, specific and unambiguous. Furthermore, the documents once approved may be already obsolete, as the context for which they were developed has evolved in the time elapsed between they were created and they were approved. This problem has been identified by the CTA management but a solution has not emerged yet.

On the other hand, there is an unbalanced ratio between scientists and engineers at a critical phase of the development, with the associated unbalanced expertise in the related aspects of the development of CTA. This issue naturally emerges in any scientific installation and has also been recognised by the CTA project management, which has devoted a significant but not yet enough amount of time, efforts and resources to bring experts from industry, including the space sector,

and previous large scale installations, with the aim of exchanging know-how in training courses, workshops and meetings.

The author of this thesis participated in the organisation of an international workshop on reliability engineering in scientific installations[7] to mitigate this deficiency. This was the first initiative made in CTA to compare the methods carried out in the most relevant LSIs of the last years: ITER and CERN LHC with those of the Aerospace Industry (GMV, SENER).

The RAMS in Science workshop served as a seed for the organisation of a second one[8], held recently at CTA Project Office, with the participation of experts from CERN ATLAS, ICE Cube, MAGIC, VERITAS, HESS and Pierre Auger, as well as experts from the companies Thales Aerospace, which shared its knowledge in the Herschel-Planck missions, Fractal, which participated in GranTeCan observatory, and RAMS-CON, a pioneer company in the implementation of RAMS techniques in astronomical research infrastructures.

The discussions in this workshop fully confirm the conclusions indicated in this section. Furthermore it became evident that the lack of availability of the information on product assurance techniques for Large Scientific Installations continually forces the need of starting from the scratch. This lack of availability has also been a major handicap for the development of this thesis. Despite these difficulties, CTA is considered a pioneer project concerning product assurance techniques: it has already developed a number of high level product assurance documents such as a quality plan, a RAMS plan, a risk management plan, a level A RAMS requirements document, a project management plan and a full product breakdown structure. The author of this thesis has actively participated in the first four.

As a main conclusion, it must be pointed out that the international standards developed to define the Product Assurance processes for the Industry cannot be applied to CTA in a straightforward manner, it is necessary to develop something new. This has been one of the main motivations for the development of this thesis. An intermediate solution between the consolidated plans of Agencies-managed LSIs and the definition from scratch of the ad-hoc consortiums-managed LSIs is deemed necessary.

[7] RAMS in Science Workshop (http://www.ramsinscience.es/)
[8] https://www.cta-observatory.org/indico/conferenceDisplay.py?confId=438

Chapter 4

Product Assurance management

This chapter is the first one of the proposed solution for a generic set of procedures for Product Assurance in Large Scientific Installations. The structure of this chapter and the next ones has been set so that:

- The first part describes the objectives of the discipline inside Product Assurance being analysed.
- The second part describes the overall procedure to ensure its proper management and implementation in a given project/LSI.
- Finally, the third part details the existing standards on which the procedure presented is based, along with the traceability matrices between the steps of the procedure and the requirements of the aforementioned standards.

4.1 Objectives of Product Assurance

Product Assurance is the discipline within a Project aimed at ensuring that the predefined requirements and expected quality level are met, so that the system produced is able to operate in a safe, available and reliable way. In order to cope with the goals behind this definition, Product Assurance is divided into different areas, the so-called Product Assurance Disciplines, each one focused on a specific aspect or the overall definition.

These Product Assurance Disciplines, as defined in chapter 10, are shown in Figure 4–1:

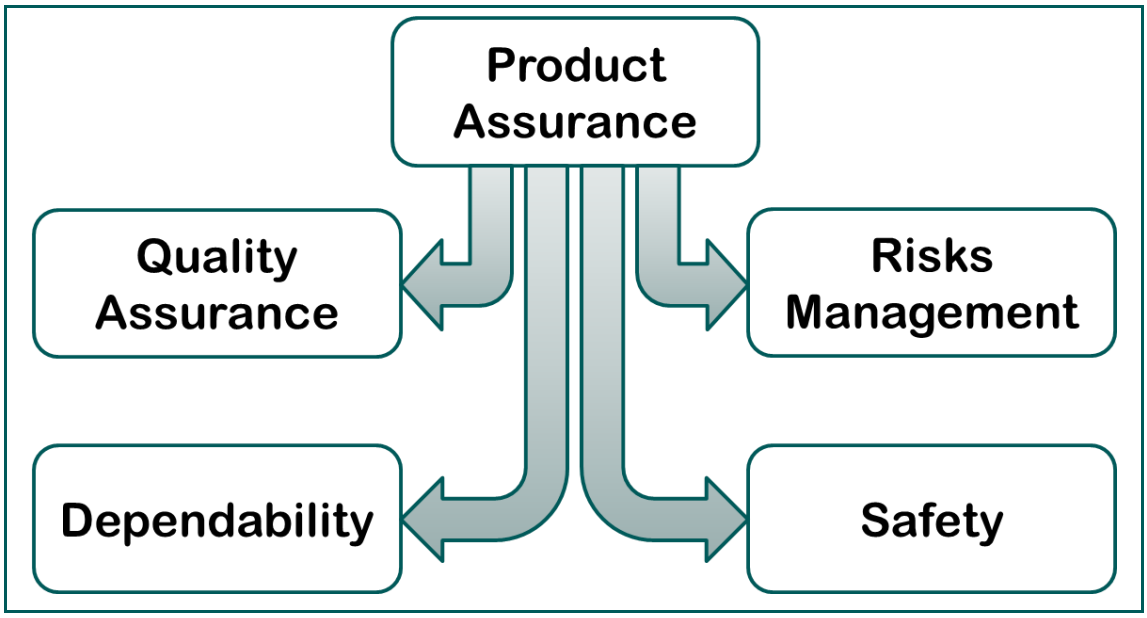


Figure 4–1: Product Assurance disciplines

In a Large Scientific Installation, where the magnitude of the project is so huge, the disciplines above are self-contained tasks involving their own staff. This is the reason for dividing the contents of the procedures presented into dedicated chapters for each of the Product Assurance Disciplines.

This chapter, on the contrary, has been conceived to define the Product Assurance structure from a managerial point of view, omitting any technical detail. Therefore, the procedure explained in next sections hence includes:

- The definition of the roles involved in Product Assurance Management and its organization.
- The definition of the Product Assurance Management deliverables.
- The definition of the monitoring and control entities within the project to check the correct implementation of the associated Product Assurance tasks (audits).

4.2 Product Assurance Management procedure

4.2.1 STEP 1: Define the Roles

For the complete understanding of present procedure, it is very important to remark the different actors involved, as defined in chapter 10, namely:

- The **Project Manager**, focal point of contact for all the managerial aspects of the project.
- The **Product Assurance Manager**, focal point of contact for all aspects of Product Assurance.

The first step of product assurance procedure is to properly assign the roles above with their responsibilities as defined in chapter 10.

Apart from the Project Manager and the Product Assurance Manager, an internal **Product Assurance Organization** shall be defined in order to properly account for the product assurance tasks within the project.

4.2.2 STEP 2: Define the Product Assurance organization

The Project Manager and Product Assurance Manager shall define the Product Assurance Organization able to cope with the objectives of Product Assurance. From the point of view of Large Scientific Installations, on which the different aspects of the entire project are assumed by different institutions, such organization shall be done in a way that allows the exchange of information in an efficient way. It is very likely that these organizations assume entire parts of a design and their subsequent development, so the Product Assurance Organization shall be done so that there is a fluent exchange of information with the Product Assurance Manager and that the applicable overall Product Assurance procedure is properly implemented.

The geographical distribution of the different institutions involved in the development of a Large Scientific Installation can be a significant drawback to this objective, or in other words, without a well consolidated product assurance procedure, the centralized product assurance vanishes.

The Product Assurance Organization shall be settled in a way that minimizes these boundary conditions. Therefore, here follows the proposed solution:

- Divide the Product Assurance management so that there is a **Product Assurance Delegate** on each of the institutions involved. Such delegates will have the same responsibilities within their institutions that the Product Assurance Manager has for the entire project.
- The Product Assurance Delegates report the activities carried out at their level in a regular basis through **Product Assurance reports**, delivered to the Product Assurance Manager.
- The Product Assurance reports shall contain:
  - The status with respect to the life cycle (current phase)
  - A justification of the applicable procedures of the different Product Assurance disciplines for the current phase within the life cycle.
  - A summary of the results obtained after these procedures are applied (in case of deliverables, the appropriate reference suffices).

The staff of the project dedicated to Product Assurance tasks is not limited to the Product Assurance Manager and the different Product Assurance Delegates. Based on the magnitude of the entire project (in the case of the Product Assurance Manager) or the part of the project assumed by a single institution (in the case of Product Assurance Delegates), there may be some additional people involved. It is responsibility of the Product Assurance Manager and Product Assurance Delegates to identify the needs of personnel to assist them in their tasks. The Project Manager –or the equivalent responsible in the institution involved in the case of Product Assurance Delegates– shall take the necessary means to attend these needs of personnel.

4.2.3 STEP 3: Prepare the Product Assurance Plan

The Product Assurance Manager shall prepare a **Product Assurance Plan** to contain all the Product Assurance activities foreseen.

This Plan has to be approved by the Project Manager at the beginning of the project, or even be provided as input before for the Project Manager to properly delegate the Product Assurance tasks.

The Product Assurance Plan shall contain:

- The Product Assurance Organization.
- The Product Assurance Procedures.
- The specific procedures for Quality Assurance.
- The specific procedures for Risks Management.
- The specific procedures for Dependability.

- The specific procedures for Safety.

Additionally, a chapter on specific procedures for Engineering rules and Quality Assurance in SW developments has also been added, although it formally it is not a discipline of Product Assurance, but a branch of Quality Assurance instead.

For the preparation of this Product Assurance Plan, the corresponding parts of this document that cover each of the contents listed above are provided in Table 4–1:

Product Assurance Plan contents	Related section in this document
Product Assurance Organization	**4.2.2**
Product Assurance Procedure	**4.2 and subsections**
Specific procedures for Quality Assurance	**5.2**
Specific procedures for Risks Management	**6.2**
Specific procedures for Dependability and Safety	**7.2**
Specific procedure for SW developments	***8.2***

Table 4–1: Product Assurance Plan contents and related sections in this document

4.2.4 STEP 4: Define the Audits policy

To verify the correct implementation of the Product Assurance procedure, the Product Assurance Manager shall conduct a series of **audits** to the project team on the different parts of the Product Assurance Plan. The audits shall be carried out on a regular basis and the results reported to the Project Manager.

The objectives of the Product Assurance audits are:

- To identify deviations to the procedures in the Product Assurance Plan and propose the appropriate corrective actions.
- To gather feedback from the technical groups about the procedures in the Product Assurance Plan and to propose improvements.
- To identify deficiencies in the project managerial structure and to propose the possible solutions.

It is responsibility of the Product Assurance Manager to propose a calendar to carry out the audits, and to collect the information from the internal audits performed by the Product Assurance delegates when applicable.

The results of the audits are the **audit reports**, containing the relevant information retrieved in a friendly format. The most efficient way to carry out the audits, should the Product Assurance Plan is prepared according to the guidelines provided in previous section 4.2.3, is to use a checklist template with the applicable procedures to be audited based on the steps of the different procedures involved. Such checklist is a table with a row for each step and four columns with different information:

- Column 1: The reference to the step of the procedure in the Product Assurance Plan,
- Column 2: The evidences presented to justify its proper implementation, and

- Column 3: The compliance status as a result of the evidences presented:
  - **Compliant**: If the step of the procedure is correctly applied.
  - **Not Compliant**: If the step of the procedure is not being applied.
  - **Partially Compliant**: If only a part of the step of the procedure is being applied
  - **Not Applicable**: If there is no need to apply this step of the procedure (on which case the appropriate justification shall be provided in Column 4)
- Column 4: Comments by the auditing team to justify the compliance status chosen in Column 3; suggestions to improve the procedure being audited, etc.

4.2.5 STEP 5: Procedure for the review & approval of relevant project documentation

One key aspect in the project development is the provision of the relevant documentation in due date. Each document elaborated in the frame of the project shall be duly reviewed and approved in order to be incorporated to the baseline and become applicable from that moment onwards.

This step of the Product Assurance procedure is aimed at defining an agile method for documentation review & acceptance processes that allows keeping track of all the comments discussed plus the dispositions agreed as a result of the discussions on these comments. Besides, the consolidated list of changes derived from the dispositions which are deemed necessary for the document to be approved is clearly defined and paves the way for its approval.

Therefore, the procedure to be followed comprises the steps below:

- The author submits the document for review to the Project Manager.
- The Project Manager designates a **review team**, composed of these personnel of the project (or even external collaborators) with deep knowledge and background experience in the subjects covered by the document, and a schedule containing:
  - The deadline for the provision of comments by the review team.
  - The deadline for the provision of answers by the author(s) of the document.
  - The date for the meeting to discuss and dispose the comments, and agree the related actions to update the document.
- A template of the so-called **Document Review Sheet** (DRS) is distributed to the review team.

  NOTE: A template of the DRS is provided in section 4.4 at the end of present chapter, which is used as the guideline for the fields referenced in the remaining steps.
- Each reviewer reports his/her comments/discrepancies to the document using a copy of the DRS template, filling in the "Part I" of the table.

- The authors of the document, once the deadline for sending comments is over, collect all the DRS received and answer them in the "Part II" of the table.

- The Project Manager, once the deadline for sending answers to the comments is over, collects all the answered DRS which are put together in a single document with a unique **DRS code** each. This document with all the DRS produced by the review team and answered by the authors (Part I and Part II completed) is distributed as input to the meeting to discuss all of them.

- The Project Manager chairs the aforementioned meeting, on which every DRS in the joint document is discussed until an agreement is reached for all of them. As a result of the discussion, a final disposition is written in the "Part III" of the DRS table with the agreements reached. The final status of each DRS can be any of the following ones:

  - **Closed by response (no action):** The response by the authors is enough to clarify the comment/discrepancy => this implies that the response is accepted and no further action is required.
  - **Closed by disposition (no action):** The response did not completely answer the comment/discrepancy, but the subsequent discussion during the meeting was enough to clarify the open points => this implies that no further action is required.
  - **Closed WITH ACTION according to response:** The response contains not only an answer but a proposal to include in the document the needed clarifications to close the comment/discrepancy which is agreed by the reviewers => this implies that the response is accepted and the document has to be updated accordingly.
  - **Closed WITH ACTION according to the disposition:** The response provided, although it proposes to update the document, is not enough to close the comment as it is, and the subsequent discussion includes additional amendments/clarifications to be included in the document => this implies that the disposition includes all the changes to be done to the document and the document has to be updated accordingly.

  The final Minutes of Meeting includes all the DRS with their final dispositions, as well as the deadline to provide the updated document with the modifications agreed as a consequence of the DRS which final status is *Closed WITH ACTION*.

- The Project Manager, upon reception of the updated document, checks the correct implementation of the dispositions and amends the Minutes of Meeting with the declaration of approval for the final document.

Once these steps are completed, the document is approved and can be incorporated to the project applicable baseline. Additionally, the Minutes of Meeting contains all the relevant information to track the history of the document until it was approved.

4.2.6 STEP 6: Contribution to Project & Configuration Management

Although neither Project Management nor Configuration Management is covered by this procedure, there are some contributions to these aspects of the general management of a project worth to be included as a part of the procedures for Product Assurance.

4.2.6.1 Baseline settlement

The Product Assurance Manager shall ensure that the applicable baseline documentation is properly identified. Besides, the Product Assurance Manager shall check that the documents in the baseline are available to the project's staff.

4.2.6.2 Availability of Product Assurance documentation

Apart from the baseline documents, the Product Assurance Manager shall check that the specific Product Assurance documentation is available to the project's staff: Product Assurance Plans, Product Assurance reports, Audit reports, Risk registers, etc.

4.2.6.3 Non Conformances control system

The Product Assurance Manager shall check that the non-conformances detected are properly stored for further monitoring and control.

4.3 Traceability to standards

The procedure presented is mainly based in ECSS-Q-ST-10C, [5]. Being ECSS the main reference, the tailoring process for ECSS standards in section 7 of [2] was followed. Thus, the correspondence is from the different sections of ECSS-Q-ST-10C, [5], to the corresponding sections of this procedure, and not the other way round. In the case of other procedures on which there are several baseline references not all of them being ECSS standards, like the Risks Management in chapter 6, the traceability matrix w.r.t. the standards is presented in the other way round, i.e., the traceability of each part of the procedure to the applicable standards is shown along with the appropriate justifications.

ECSS-Q-ST-10C	Section (s)	Justification
5.1.1.1 (a) to (d)	4.2.1, 10	(a), (b), (c): The definition of the main roles involved is done in chapter 2. (d): Additional details in 4.2.1
5.1.1.2 (a) to (c)	4.2.2, 10	(a), (b), (c): 4.2.2 (b): Part of Product Assurance Manager definition in chapter 2.
5.1.1.3 (a) to (c)	4.2.2	(a), (b): 4.2.2 (c): Discarded (N/A)
5.1.2 (a) to (d)	4.2.2	(a), (b), (c), (d): 4.2.2
5.1.3 (a) to (c)	4.2.3	(a), (b), (c): 4.2.3
5.2.1 (a) to (l)	5, 10	(a), (b), (c), (d), (e), (f), (g), (k), (l): Included in the definition of Product Assurance Manager in chapter 2. (h), (i), (j): Qualification programme Covered by Quality Assurance procedure in chapter 5
5.2.2 (a) to (c)	4.2.2	(a), (b): 4.2.2 (c): Discarded (N/A)

ECSS-Q-ST-10C	Section (s)	Justification
5.2.3 (a) to (d)	4.2.4	(a), (c), (d): 4.2.4 (b): Discarded (N/A)
5.2.4 (a) to (c)	-	Discarded (N/A). There is a dedicated procedure for Risks Management, but critical items control is not covered by present work
5.2.5 (a) to (d)	4.2.6.1	(a): 4.2.6.1 (b), (c), (d): Discarded (N/A)
5.2.6 (a)	4.2.6.2	(a): 4.2.6.1
5.2.7 (a), (b)	-	Discarded (N/A)
5.2.8 (a)	4.2.6.3	(a): 4.2.6.3
5.2.9 (a) to (d)	-	Management of Alerts is excluded from PA management, the appropriate treatment of failures, not acceptable risks and hazards are addressed in their respective sections.

Table 4–2: Traceability of Risks management procedure to ISO and ECSS standards

4.4 Document Review Sheet template

Document Review Sheet	
DRS code	
Date	

Document information			
Title	Code	Version	Date

PART-I: Comment / Discrepancy *(to be filled in by the reviewer)*			
Originator (Name / Institution)			
Chapter / Section / Paragraph		Page(s)	
Description of the comment / discrepancy to the document			

PART-II: Response *(to be filled in by the author)*	
Responder (Name / Institution)	
Response	

PART-III: Disposition *(summary of the agreed conclusions and derived actions, if any)*
Disposition
Final status
☐ Closed by response (no action) ☐ Closed by discussion (no action) ☐ Closed WITH ACTION according to response ☐ Closed WITH ACTION according to disposition

Chapter 5

Quality Assurance

5.1 Objectives of Quality Assurance

Quality Assurance is, by far, the most extended discipline of Product Assurance. According to the definition provided in chapter 10, the main objective of Quality Assurance is to determine the level of fulfilment of the Quality requirements that a system has.

Quality requirements are defined in the form of a series of procedures and methods to be followed during a project implementation. Present chapter is aimed at defining the Quality Assurance procedure relevant to the development of a Large Scientific Installation.

5.2 Quality Assurance Procedure

5.2.1 STEP 1: General Quality Assurance requirements

5.2.1.1 Quality Assurance Plan

The Quality Assurance Plan is the document with the overall procedures that are defined for the proper implementation of the Quality Assurance within a project. This document is prepared by the Product Assurance Manager and submitted for approval to the Project Manager, as per the procedure described in STEP 5 of Product Assurance Management procedure in section 4.2.5.

The procedures presented in section 5.2 and related subsections covers all the elements for a Quality Assurance Plan.

5.2.1.2 Critical Items management

A Critical Item in a project, as defined in [7], is a potential threat to either the performance, quality, dependability or safety of the system under development which are controlled by a specific action plan aimed at mitigating the risks derived and the associated consequences.

Although formally the process of managing Critical Items is very similar but not equal to the one for Risks management, for the sake of the easiness of the procedures involved, they are treated in the same way as Risks.

Therefore, the procedure applicable for Critical Items management is the one described in steps 2 to 4 of Risks management chapter (sections 6.2.2, 6.2.3 and 6.2.4).

5.2.1.3 Non Conformances management

A Non Conformance is a deviation of an applicable requirement of a project. The Non Conformances control system was already introduced in step 6 of Product Assurance Management chapter (section4.2.6). As it was pointed out there, these elements are covered by the Configuration Management system which procedures are out of the scope of present work.

5.2.1.4 Stamp control

All the items produced in the frame of the project shall be properly stamped for inventory purposes. The stamp control system shall:

- Indicate uniquely the status of the element:
    - Under development
    - Under testing
    - Approved
- Define the roles within the project authorized to manage each item stamped, with the description of the operations allowed per each role, when necessary.
- Use unambiguous labels to clearly identify each item stamped, with an appropriate material.

5.2.1.5 Traceability

All the items produced or procured in the frame of the project shall be properly traced in an inventory document which contains the following information:

- A unique code to identify the item.
- The location of the item.
- In the case of items procured:
    - The vendor information.
    - The manufacturer information.
    - The manufacturer's Serial and Part numbers (S/N) (P/N).
    - The status (in stock, in use, for disposal, destroyed)
- In case of items produced:
    - The information contained in its associated stamp.

5.2.1.6 Handling, Transportation, Storage and Preservation

All the items procured in the frame of the project shall be handled and stored according to the manufacturer's information.

All the items produced in the frame of the project shall have documented the instructions for its secure handling, transportation, storage and preservation.

5.2.2 STEP 2: Quality Assurance requirements for design phase

5.2.2.1 Definition of a Design strategy

All the elements produced in the frame of the project shall have a documented design strategy approved before proceeding to the manufacturing phase.

Such design strategy shall ensure:

- The simplification of the modules involved.
- The standardization of the processes involved.
- The clear definition of the requirements to be met.
- The standardization of the interfaces.
- The repeatability of the characteristics among the different items of the same type produced.
- The inspectability and testability of the items produced with respect to the pre-defined requirements.

5.2.2.2 Definition of a Verification strategy

All the elements produced in the frame of the project shall have a documented verification strategy approved before proceeding to the manufacturing phase.

Such verification strategy shall include:

- The appropriate tests to cover all the requirements defined in the design strategy.
- The appropriate procedures to conduct these tests.
- The appropriate definition of the environment on which these tests shall be performed.
- The appropriate definition of the external elements (inputs, measurement equipment) needed to perform these tests.
- The conditions that shall be granted to declare the successful (PASSED) or not successful (FAILED) status of these tests once performed; the so called PASS/FAIL criteria.

5.2.2.3 Design reviews

Once the design and verification strategies are prepared, a Design Review milestone shall be organized to inspect their contents with respect to the expected elements defined in 5.2.2.1 and 5.2.2.2.

The design reviews are chaired by the Project Manager with the support of the Product Assurance Manager. The project's top level management institution (Agencies or and *ad-hoc* consortium) representatives will ultimately pronounce the status (approved / rejected) of the design review.

5.2.3 STEP 3: Quality Assurance requirements for implementation phase

5.2.3.1 Implementation Plan

Prior to the manufacturing phase, an implementation plan shall be defined for each item to be produced, containing all the elements needed for its proper construction, namely:

- Parts list, drawings, schematics.
- Equipment used for the manufacturing, assembly and integration.
- Environment constraints on the manufacturing laboratory (temperature, humidity, cleaningless levels, etc.)
- Identification of critical characteristics and/or especially complex steps in the production deserving specific clarifications or instructions.
- Provision of auditable breakpoints in the process that ensures its justification against and external witness (i.e., prepare the evidences for audits).
- Tolerance margins in the intermediate checks (inspections) to ensure that the item grants the design requirements.

5.2.3.2 Inspections

The manufacturing process shall define inspection points on which different aspect of the design can be verified.

The checks carried out at the inspection points shall constitute go / no-go decision points for the remaining manufacturing steps for the item being assessed on them.

5.2.4 STEP 4: Quality Assurance requirements for verification & acceptance phases

5.2.4.1 Test benches

The manufacturing process shall set up the environment on which the tests shall be executed according to the verification strategy defined in 5.2.2.2.

5.2.4.2 Test procedures

During the verification phase, the tests shall be executed according to the predefined test procedures defined in the verification strategy of 5.2.2.2.

5.2.4.3 Test reports

The execution of each test carried out in the verification process shall be properly documented in the Test Report, which shall contain:

- References to the applicable part of the verification strategy to the test performed:
  - Test case.
  - Test procedure.
  - Environment conditions.
  - External elements needed.

- Results of the evaluation of the PASS/FAIL criteria on the items tested.
- Final result of the test (PASSED/FAILED) based on the results of all the PASS/FAIL criteria evaluated.
- List of the foreseen corrective actions to be implemented in case of failures detected during the test execution.

5.2.4.4 Test reviews

The final approval of the items produced shall be pronounced on test reviews on which the evidences for the successful execution of all the tests are presented in the form of test reports.

The test reviews are chaired by the Project Manager with the support of the Product Assurance Manager. The project's top level management institution (Agencies or and *ad-hoc* consortium) representatives will ultimately pronounce the status (approved / rejected) of the test review.

5.2.5 STEP 5: Quality Assurance requirements for procurement

5.2.5.1 Procurement estimations

During the design phase, all the external elements which need to be procured from third party sources shall be properly identified, detailing:

- The description of the element to be procured (parts, equipment, fungible materials).
- The expected amount of items to be procured, including a spare provision.
- The list of sources from which the element can be procured (vendors, resellers).
- The expected future availability (whenever possible) and potential alternatives in case of discontinuation in their provision.

5.2.5.2 Selection of a provider

Based on the information collected for each element to be procured as per 5.2.5.1, and in the case that there are several providers identified, it shall be justified the final source from which it will be procured in terms of:

- Price.
- Delivery time upon procurement.
- Current and expected future stock available.

5.3 Traceability to standards

The standards on which the contents of this procedure are based are ECSS-Q-ST-20C [6] (mainly), and ECSS-Q-ST-10-04C [7] (for the identification of Critical Items Control and Risk

Assessment only). This section provides the traceability from the steps of the procedure proposed and the corresponding section of the main reference ECSS-Q-ST-20C [6], with the appropriate justifications to the adaptations made.

Section	ECSS-Q-ST-20C	Justification
5.2	5.1, 5.2	Refer to the justification for each requirement in the subsections
5.2.1	5.1, 5.2	Refer to the justification for each requirement in the subsections
5.2.1.1	5.1.1	
5.2.1.2	5.2.1	
5.2.1.3	5.2.2	
5.2.1.4	5.2.4	
5.2.1.5	5.2.1.5	
5.2.1.6	5.2.7.1, 5.2.7.2, 5.2.7.3	All the requirements in 5.2.7 for handling, storage and preservation have been joined in a single requirement in the procedure proposed
5.2.2	5.3	Refer to the justification for each requirement in the subsections
5.2.2.1	5.3.1.1, 5.3.1.2, 5.3.1.3	
5.2.2.2	5.6.3.1	The verification strategy documentation (test procedures) part only
5.2.2.3	5.3.2.2, 5.3.2.3	
5.2.3	5.5	Refer to the justification for each requirement in the subsections
5.2.3.1	5.5.1	
5.2.3.2	5.5.8	
5.2.4	5.6	Refer to the justification for each requirement in the subsections
5.2.4.1	5.6.1	
5.2.4.2	5.6.3.1	The test execution according to the test procedure part only
5.2.4.3	5.6.3.2	
5.2.4.4	5.6.5	
5.2.5, 5.2.5.1, 5.2.5.2	5.4	The procurement requirements have been deeply revised, not adhering to ECSS related requirements but only extracting general ideas to the final proposal

Table 5–1: Traceability of Quality Assurance procedure to ISO and ECSS standards

Chapter 6

Risks Management

6.1 Objectives of Risks Management

Risks, as per the definition in chapter 10, are potential events that may happen during the development of a Project, which in case they finally occur can affect either:

- The project's cost, or
- The project's schedule, or
- The expected technical performances.

The objective of defining and implementing a so called ***Risks Management*** policy is, according to [8] and [9]: *"to identify, assess, reduce, accept, and control project risks in a systematic, proactive, comprehensive and cost effective manner"*. Basically, the idea behind Risks Management is twofold: Identify risky situations affecting the normal development of the project and advance solutions before they occur.

An adequate Risks Management policy does not only avoid risky situations, it can also serve as a mean to improve some aspects of the project itself, on which case the risks become Opportunities.

The goal of implementing a Risks Management policy, following the strategy above, is to include this task as a part of the normal work so that Risks are assessed on a regular and systematic basis.

6.2 Risks Management procedure

The Risks Management is a continuous process which shall be performed in all the phases of the project. There are not specific procedures applicable to each of the development phases, but a single overall procedure instead which is suitable for all of them.

The Risks Management procedure is composed of four steps, three of which are repeated on a regular basis to account for the new risks that can arise and for the evolution of the existing ones previously identified; and they are listed below:

- Define Risks Management implementation requirements
- Identify and assess the Risks
- Decide and act
- Monitor, report and accept Risks

A schematic view of these steps and their repeatability during project evolution is depicted in Figure 6–1:

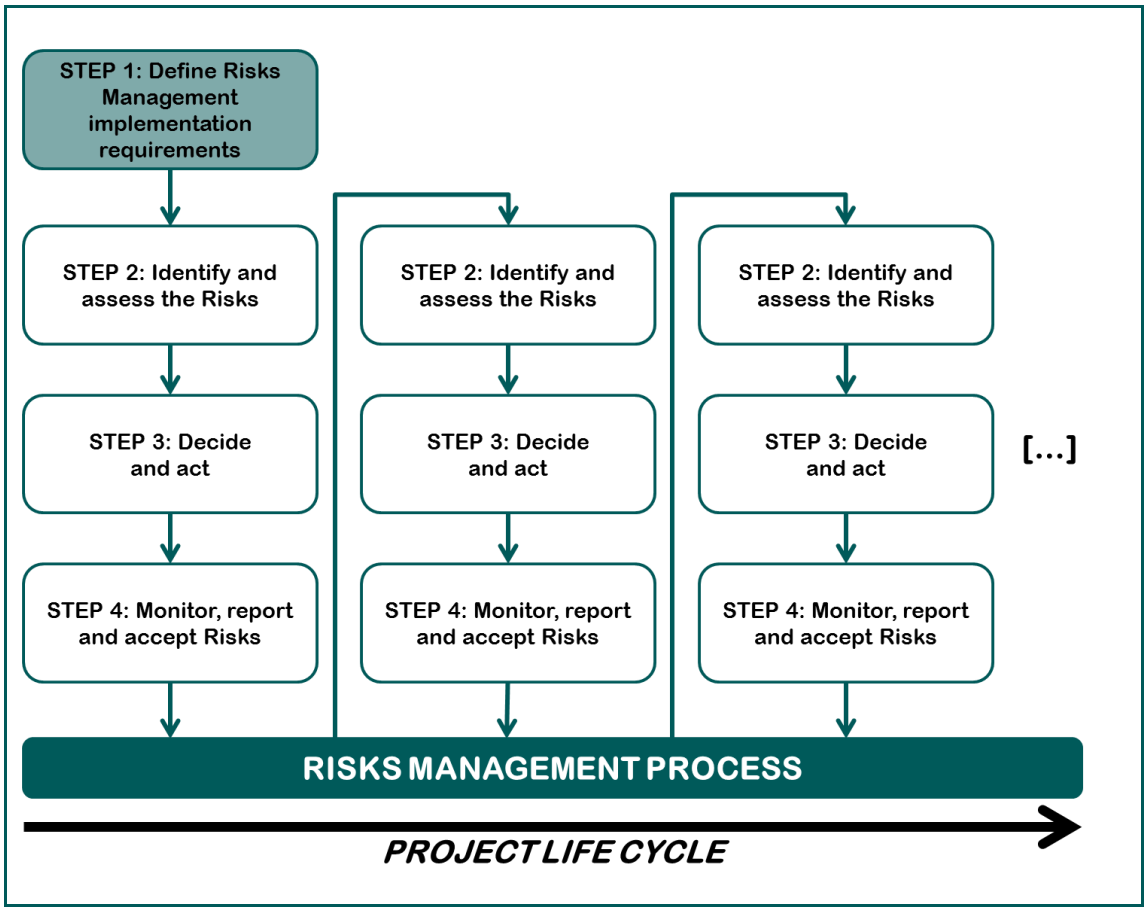


Figure 6–1: Steps of the Risks Management procedure during project's life cycle

It is important to remark the "asynchrony" of risks management and project's life cycle: The assessment of the risks is performed regularly regardless the phase of the development.

The vertical groups STEP 2 → STEP 3 → STEP 4 which are repeated in Figure 6–1 are the so called **Risks assessment cycles** and should be performed on a regular basis to properly detect new Risks and monitor the evolution of the existing Risks previously identified in former cycles.

6.2.1 STEP 1: Define Risks Management implementation requirements

This first step in the Risks Management procedure is different from the remaining ones for several reasons:

- It is not included in the Risks assessment cycles; this step is performed once at the beginning of the project.
- The implementation requirements defined are applicable to the entire project, unlike the risks identified in the Risks assessment cycles, which can vary and evolve with the project itself, reason why such cycles are repeated on a regular basis.

The tasks to be performed in this step are:

- Define the **Risks Management policy**.
- Prepare the **Risks Management Plan**.

6.2.1.1 Risks Management Policy

The **Risks Management policy** consists in establishing the responsibilities on the different aspects of Risks Management and the associated requirements. According to the roles defined in the procedure for Product Assurance Management in chapter 4, the following actors are involved:

- The responsibility for the Risks Management yields in the Project Manager. The related tasks which must encompass are:
  - Approve the Risks Management Plan prepared by the Product Assurance Manager.
  - Define the periodicity of the Risks assessment cycles.
  - Perform the tasks of the Risk assessment cycles (Identify and assess the Risks; Decide and act; Report, monitor and accept the Risks) or
  - Delegate the tasks of the Risks assessment cycles and collect the Risk reports to prepare the joint Risk report with the all the contributions. In this last case, the final magnitude of the Risks as well as their final acceptance shall be ultimately be decided by the Project Manager, based on the information in the reports provided by the **Risks delegates** (the persons which have been designated to carry out the Risks assessment cycles).
- The Product Assurance Manager, or the Product Assurance Delegate as defined in section 4.2.2 in the case of a distributed working group, have the following responsibilities in the Risks Management policy:
  - Prepare the Risks Management Plan and submit it to the Project Manager for approval.
  - Support the Project Manager or the Risks delegates in Risk assessment cycles.
  - Update the Risks Management Plan to adapt it to the specificities of the project as it evolves.

6.2.1.2 Risks Management Plan

The Risks Management Plan is the document which contains all the elements needed for the proper implementation of Risks Management within a project, namely:

- The Risks Management implementation requirements.
- The Risks assessment procedure requirements.
- The Risks reporting requirements.

The Risks Management Plan is prepared by the Product Assurance Manager and submitted for approval to the Project Manager, as per the procedure described in STEP 5 of Product Assurance Management procedure in section 4.2.5.

The Risks Management procedure presented in section 6.2 and its subsections covers all the elements defined above, and could be used directly as the Risks Management Plan.

6.2.2 STEP 2: Identify and assess the Risks

6.2.2.1 Risks identification

There is not a general recipe to identify Risks, provided the large amount of negative scenarios affecting a project and the different types of projects themselves. However, here follow some guidelines to proceed on a systematic approach intended to minimise the likelihood to miss-detecting them:

1. **Review project funding status**: Identify short and mid-term needs in terms of procurement and contracting, potential unexpected over costs that may occur due to new elements needed and not included in the project's initial budget, evolution of the prices of the materials not yet procured and needed for subsequent phases.
2. **Review technical status with the project's staff**: List short and mid-term needs of training, evaluate the probability to miss qualified members of the staff, check periodically the feasibility of those aspects of the project which are new technological challenges.
3. **Review project schedule**: Identify those elements in the project's critical path and assess their status w.r.t. the expected one.
4. **Check the boundary conditions on which the project is being developed**, i.e., those external elements which could ultimately affect the nominal development: legal issues, conflicts of interests with third parties, political constraints, etc.

The Risks identified by each of the steps above shall be annotated and categorized as Cost Risks, Technical Risks, Schedule Risks and Other Risks, respectively.

Many risks can be categorized on different ways, as they can impact, for instance, the project's cost and schedule simultaneously. In that case it shall be evaluated the first aspect being impacted to properly categorize the risk.

Example

The lack of funding to purchase a new generation of devices needed in the project could be categorized as cost risk and technical risk, simultaneously. It can indeed be categorized as a schedule risk also provided that the time needed to obtain additional investments will surely cause a delay. However, the first element of this chain of consequences derived by the unaffordable price of the needed devices is that the project's budget is not enough to purchase them, hence this risk should be categorized as a cost risk.

6.2.2.2 Risks assessment

This task consists of ranking each of the Risks identified attending two different conventions:

- Risk severity
- Probability of occurrence

The **Risk severity** defines five levels for Risks attending the impact that the potential events they represent could have in case they finally happened. The criterion to assign the severity of a Risk depends on its type (Cost, Technical, Schedule or Other Risks), and shall be reviewed and accepted by the Project Manager.

Level	Severity	Convention to assign severity levels for:			
		Cost Risks	Technical Risks	Schedule Risks	Other Risks
1	Catastrophic	Project cannot be funded	Project is not feasible	Project termination	Project termination
2	Critical	*Project cost increase up to TBD%*	Complete re-design of the project	*Project length enlarged up to TBD%*	*Project could continue in TBD% of the cases*
3	Major	*Project cost increase up to TBD%*	*Re-design of up to TBD% of the project*	*Project length enlarged up to TBD%*	*Project could continue in TBD% of the cases*
4	Significant	*Project cost increase up to TBD%*	*Re-design of up to % of the project*	*Project length enlarged up to TBD%*	*Project could continue in TBD% of the cases*
5	Negligible	Minimal or no impact	Minimal or no impact	Minimal or no impact	Minimal or no impact

Table 6–1: Definition of Risks severity levels for the different types of Risks

It is remarkable that Table 6–1 is not self-contained, i.e. there are some entries which depend on the final settlement of the TBD value to properly define the severity of a type of Risks. Such assignment of the values which determine the severity of each type of Risks is a task that must be done at the beginning of the project as a part of the Risk management policy defined in STEP 1 on section 6.2.1.

The **Probability of occurrence** defines five levels for Risks attending the likelihood they have to occur. Unlike the previous case, the criterion to define the probability of occurrence of a Risk is independent of its type.

Level	Probability of occurrence	Likelihood convention
E	Maximum	**Certain** to occur, will occur one or more times per project
D	High	*Will occur **frequently**, likelihood up to 0.1 (TBD)*
C	Medium	*Will occur **sometimes**, likelihood up to 10^{-2} (TBD)*
B	Low	*Will **seldom** occur, likelihood up to 10^{-3} (TBD)*
A	Minimum	*Will **almost never** occur, likelihood is 10^{-4} (TBD) or less*

Table 6–2: Definition of Risks Probability of occurrence levels

As per the Risks severity levels, the Probability of occurrence levels shall be reviewed and accepted as a part of the Risks management policy defined in STEP 1 on section 6.2.1.

6.2.3 STEP 3: Decide and Act

Once assessed, each of the Risks identified would have been ranked with a letter (A to E) plus a number (1 to 5) defining both its severity and probability of occurrence, e.g. E2, B4, C3, A1, etc. That combined severity and probability of occurrence is the so-called **Risk index**.

This step, based on the Risk indices obtained, has to:

- Determine the **Risk magnitude**, i.e. which Risks are **Acceptable** and which are **Not Acceptable**.
- Define **Mitigation Actions** for Not Acceptable Risks

The **Risk magnitude** defines two types of Risks: Acceptable and Not Acceptable. A Risk is **Acceptable** when it is considered that either the impact in the project in case it happened can be assumed or that the probability of occurrence is too small to be a real threat to the development. On the other hand a Risk is **Not Acceptable** when the project cannot assume the consequences in case it happened without altering significantly or even cancelling the development.

The convention to define Risk magnitudes is based on the Risk index defined previously. The Risk index can be plotted in a double entry table with their rows indicating the Probabilities of occurrence and their columns the Risks severities. The main diagonal of this table defines the boundary between the Acceptable and Not acceptable Risks:

		Risk Magnitude convention based on the Risk Index				
Probability of Occurrence	E	*TBD*	Not Acceptable	Not Acceptable	Not Acceptable	Not Acceptable
	D	Acceptable	*TBD*	Not Acceptable	Not Acceptable	Not Acceptable
	C	Acceptable	Acceptable	*TBD*	Not Acceptable	Not Acceptable
	B	Acceptable	Acceptable	Acceptable	*TBD*	Not Acceptable
	A	Acceptable	Acceptable	Acceptable	Acceptable	*TBD*
		1	2	3	4	5
		Risk Severity				

Table 6–3: Risk Magnitudes table: Definition of Acceptable and Not Acceptable Risks based on their Risk index

The Risks which Risk magnitude is *TBD –To Be Defined–* (those which Risk index is E1, D2, C3, B4 or A5; i.e. the yellow cells in the main diagonal of Table 6–3) shall be analysed on a case by case basis to determine whether they are considered Acceptable or Not Acceptable. Regardless the final choice taken, the Project Manager shall provide the appropriate justification to the final Risk magnitude set in all of the TBC cases identified.

Based on the Risk magnitude obtained for each of the Risks, the tasks to be done are:

- For Acceptable Risks: No additional tasks to be done → proceed to STEP 4.
- For Not Acceptable Risks: Reduce the Risk index or define a **Mitigation action**.

A **Mitigation action** is a backup solution taken in advance to reduce the consequences of a Not Acceptable Risk before it occurs. For example: The provision of a contingency budget to face the unexpected additional costs of the project.

Example
The provision of a contingency budget to face the unexpected additional costs of the project.

The other possibility is to reduce the Risk index of those Not Acceptable Risks to turn them into Acceptable ones. This can be done by either reducing their severity or their probability of occurrence, when possible.

Example

A Not Acceptable Technical Risk in a project can be the risk of missing an expert in a specific technical field of the project, who is the only person who knows about it in the entire project. The risk index could be reduced by planning training sessions to other people of the staff to spread the knowledge or to reduce the probability to miss that person by offering him/her a better position.

6.2.4 STEP 4: Monitor, report and accept Risks

This final step of each Risk assessment cycle deals more with the appropriate reporting of the activities carried out in the previous steps than with new tasks linked to Risk treatment.

The way to preserve and exchange information about the risks identified is to report all of them using a unified template that contains both the current information on each risk, and also their historic evolution.

The unified template to report that information is the so-called **Risk register**. It contains the complete information to assess the Risks. The elements of the Risk register are listed below:

- A ***Risk code*** to uniquely identify each of the risks, with a sequence number that allows identifying uniquely each Risk, on the form:

  RISK-<Risk_seq_num>

- The complete ***Risk description***, indicating the undesired event that this Risk represents, as detailed as possible.

- The ***Risk assessment***, as per the procedure described in sections 6.2.2 and 6.2.3, which comprises the following information:

  - The Risk type (cost, technical, schedule or other, as per the definition of Risks in chapter 2).
  - The ***Risk severity*** (level 1 to 5, as per Table 6-1).
  - The ***Probability of Occurrence*** (level A to E, as per Table 6-2).

  With this information it will be automatically obtained:

  - The ***Risk index*** associated to the combined severity and probability of occurrence.
  - The ***Risk magnitude***, to ultimately determine the subsequent actions to be taken. In case the risk magnitude is not properly defined (it is any of the *TBC* cases in Table 6-3), the register shall include the final magnitude selected, plus the appropriate justification to support that choice.

- ONLY for those Risks which magnitude is **Not Acceptable**, the register shall include the appropriate ***Mitigation action*** defined to minimise the consequences of the risk in case it happened.

– The **Risk trend** which consists in plotting the historic risk magnitudes that a risk has had when identified in several risk assessment cycles, to keep track of its evolution. To do so, a table with four levels is used:

		RISK-<*XXX*> trend					
Risk Magnitude	Not Acceptable		X				
	TBD – Not Acceptable						X
	TBD – Acceptable	X		X		X	
	Acceptable				X		
		#1	#2	#3	#4	#5	#6
		Risk Assessment Cycles					

Table 6–4: Risk trend obtained by plotting the magnitude in the different Risk assessment cycles

Actually, there are only two levels based on Risk magnitudes, Acceptable and Not Acceptable, but the "borderline cases" that lie on the main diagonal of Table 6–3 are actually the boundary between those categories. Explicitly distinguishing "TBD" cases that were finally assigned to each magnitude provides certain nuances to this binary division of Risks magnitudes.

6.3 Traceability to standards

The standards on which the contents of this procedure have been based are ISO-17666:2003, [8]; and ECSS-M-ST-80C, [9]. This section provides the traceability from the steps of the procedure proposed and the corresponding sections of these references, with the appropriate justifications to the adaptations made.

Section	ISO-17666:2003	ECSS-M-ST-80C	Justification
6.2	4.1	4.1	
6.2.1	4.2.1	5.2.1.3, 6.3, 6.5	The overall management scheme has been simplified, taking into account that the roles in a scientific team are not as well defined as they are in the industry.
6.2.2.1	4.2.1, 4.2.2.2	5.2.2.2	
6.2.2.2	4.2.1, 4.2.2.3	5.2.1.2, 5.2.2.3	The risk severities and probabilities of occurrence are defined in this section rather than in the risk requirements definition, to ease the references. In any case, the definition of the TBD values must be done as a part of STEP 1, in 6.2.1.
6.2.3	4.2.3	5.2.1.2,5.2.3	The risk magnitude table has been simplified with two categories, "Acceptable" and "Not Acceptable". Besides, the boundary between them has been defined as TBD for a further analysis on a case by case basis.
6.2.4	4.2.4.2	5.2.4	Risk trend has been simplified according to the simpler Risk magnitude definition. However, the borderline cases have been explicitly included to manage four different levels so that the risk evolution is more detailed.

Table 6–5: Traceability of Risks management procedure to ISO and ECSS standards

6.4 Risk register template

Risk register

Risk ID	
Date	

Risk Type *(select the appropriate checkbox)*			
	Cost Risk		Schedule Risk
	Technical Risk		Other Risk

Description

Risk Assessment			
Risk Severity		Probability of Occurrence	
	5 - Catastrophic		E - Maximum
	4 - Critical		D - High
	3 - Major		C - Medium
	2 - Significant		B - Low
	1 - Negligible		A - Minimum

Risk Magnitude	

Mitigation Action (only for Not Acceptable Risks)

Risk Trend						
Risk Magnitude	Not Acceptable					
	TBD – Not Acceptable					
	TBD – Acceptable					
	Acceptable					
		#1	#2	#3	#4	#5
		Risk Assessment Cycles				

Chapter 7

Dependability and Safety

Dependability and Safety, as defined in chapter 10, are two disciplines of Product Assurance that try to establish how robust a system is with respect to failures and accidents, respectively. Although they are different disciplines within a project, they are so interconnected one another that it is very often to explain their management jointly within a project.

More precisely, Dependability and Safety covers aspects of a system which overlaps in a common region: If Dependability deals with failures and Safety with accidents within a system, there is a common area with potential failures leading to accidents or vice-versa which is common to both disciplines, as Figure 7–1 illustrates.

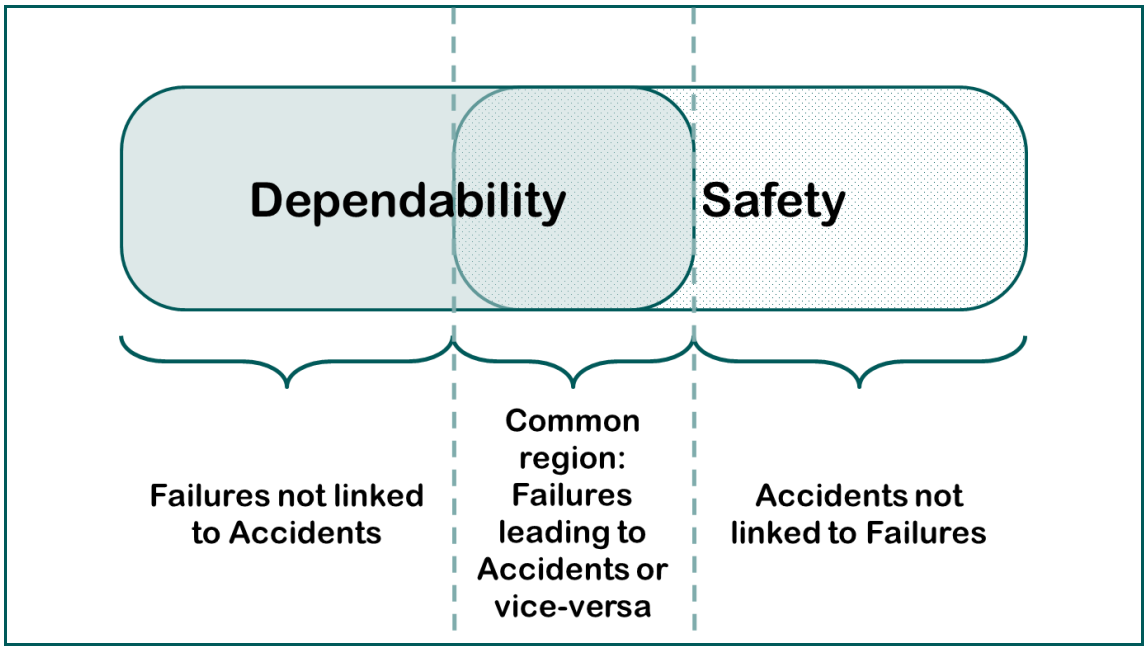


Figure 7–1: Graphical representation of Dependability and Safety and the common region to both disciplines of Product Assurance

This chapter is organized in a similar way as the previous procedures in chapters 4, 5 and 6, although the joint treatment of two disciplines (dependability and safety) deserves a general explanation of the structure followed.

- In section 7.1 the overall objectives of Dependability and Safety are presented, along with the managerial aspects.
- Section 7.2 explains the procedure for the proper implementation of Dependability and Safety analyses in a LSI.
- Finally, section 7.3 and 7.4 details the Dependability and Safety analyses introduced previously and how to conduct them in a given project.

7.1 Objectives of Dependability and Safety

Dependability involves three different elements to prevent the occurrence of failures in a system:

Reliability

Reliability is the capability of a system to operate with the expected performance margins under controlled conditions. Basically, a reliable system is that which is able to work without failures within a given time interval.

Availability

Availability is the capability of a system to be able to operate when requested to do so and maintain this operational state.

Maintainability

Maintainability is the capability of a system to return to the operational state from a previous non-operational state (due to a failure, for instance) through the application of predefined procedures for its restoration. Basically, the idea behind maintainability is the capability of a system to be repaired in an efficient way when it fails.

Dependability is often referred to as with an acronym that includes these three elements: **RAM** – Reliability, Availability and Maintainability.

Safety, on the other hand, is aimed at preventing the occurrence of accidents in a system.

The joint term used to denote both Dependability and Safety is **RAMS** – Reliability, Availability, Maintainability and Safety, and this will be the acronym used in this chapter from now on to refer to both disciplines jointly.

7.2 Dependability and Safety (RAMS) procedure

The procedure for RAMS implementation in a project is divided in several steps, each one covering a specific aspect from the organizational and managerial issues to the technical elements of RAMS.

7.2.1 STEP 1: Define RAMS implementation requirements

7.2.1.1 RAMS policy

The proper assessment of RAMS within a system shall begin with the project itself. A system which is free of failures and completely secure does not exist. However, the success in properly identifying the potential failures and accidents in a system, and the actions to prevent it occurrence or mitigate their effects in case they finally happened is strongly linked to the design of the project itself.

The Project Manager shall initiate the RAMS assessment within a project at the very early stages, through the designation of a RAMS Manager in charge of implementing the RAMS assessment in the project.

The responsibilities of the RAMS Manager are:

- Define the RAMS organization, by allocating the needed resources in the technical groups in charge of carrying out the RAMS analyses.
- Prepare and maintain the RAMS plan.
- Organize the training in RAMS aspects for the technical groups.
- Collect the information of the different RAMS analyses carried out from the different technical groups, and
- Elaborate the RAMS reports periodically with the relevant information about the RAMS activities.

The RAMS Manager shall have unimpeded access to the design documentation of the project, and iterate continuously with the technical groups in charge of designing and implementing the different elements of the system(s) developed in the project.

7.2.1.2 RAMS Plan

The RAMS Plan is the document which contains all the elements needed for the proper RAMS assessment within a project, namely:

- The RAMS implementation requirements.
- The RAMS assessment requirements.
- The RAMS reporting requirements.
- The description of the RAMS analyses involved and associated templates.

The RAMS Plan is prepared by the RAMS Manager and submitted for approval to the Project Manager, as per the procedure described in STEP 5 of Product Assurance Management procedure in section 4.2.5.

The RAMS procedure presented in section 7.2 and its subsections covers all the elements defined above, and could be used directly as the RAMS Plan.

RAMS Plan evolution

The RAMS Plan, unlike the other plans defined (Product Assurance Plan, Quality Assurance Plan and Risks Management Plan) which are expected to remain unchanged once approved, is expected to evolve with the project itself. The RAMS analyses proposed at the early stages of a project in the first version of the RAMS Plan, or even the RAMS policy itself, may be refined based on the conclusions of the RAMS reports.

It is responsibility of the RAMS Manager to propose and implement the changes in the RAMS Plan, and submit the updated document for approval as per the procedure described in STEP 5 of Product Assurance Management procedure in section 4.2.5.

7.2.2 STEP 2: Define the RAMS assessment requirements

7.2.2.1 RAMS requirements

The definition of the requirements of the system shall include the corresponding RAMS requirements to define:

- The tolerance margins that define the operational state of the system, or a failure state otherwise.
- The availability requirements (minimum % of time in operational state)
- The maintainability requirements (maximum time to repair, provision of spares, etc.)
- The classification with the different levels considered for the severity of the consequences of either failures or accidents inside the project.

7.2.2.2 Definition of Severity of consequences

Any potential failure or accident within a system shall be ranked according to a pre-defined scale of severities based on the consequences derived in case they occur.

For the purpose of this procedure, the following generic table of severities is provided, adapted from [10], [11]:

Severity	Level	Consequences from the point of view of			
		Dependability	Safety		
			On individuals	On the system	On the environment
Catastrophic	1	Failures propagation	Loss of life, life-threatening or permanently disabling injury or occupational illness	Loss of system	Severe detrimental effects
Critical	2	Loss of system	Temporarily disabling but not life-threatening injury, or temporary occupational illness	Major damage to the system and public or private properties	Major detrimental effects
Major	3	Major system degradation	Small injuries	Moderate damage to the system	Moderate detrimental effects
Minor or Negligible	4	Minor system degradation	Incident without damages	Incident without damages	Incident without damages

Table 7–1: Classification of Severity of consequences for Failures (dependability) and Accidents (Safety)

7.2.3 STEP 3: Define the RAMS life cycle

Once the RAMS policy and RAMS requirements have been established, the RAMS assessment can begin in the project. RAMS activities evolve with the project itself, so there is a strong link between the phases in the project life cycle and the associated RAMS activities to be carried out.

7.2.3.1 Phases of the project life cycle

For the definition of the RAMS analyses to be carried out at the different phases in the project, it is mandatory to establish a life cycle on which these phases are uniquely defined. For this purpose, an adaptation of the project phases defined in [12] is considered:

Phase 0 – System analysis / needs identification

This phase is aimed at assessing the main description of the system in terms of needs, expected performance, constraints, economic analysis, etc.

Phase A – Feasibility

This phase is intended to define the top level requirements of the system, analysis of the existing technologies to cope with the system objectives, preliminary project plans, managerial organization, identification of critical items, cost studies, etc.

Phase B – Preliminary Definition

This phase comprises the consolidation of the managerial structure of the project, project plans and project schedule. From a technical point of view, this phase encompasses the trade-off studies for the discrimination of the technologies to be used, define the operation concepts and the associated preliminary design, system requirements etc.

This phase usually ends with the Preliminary Design Review milestone.

Phase C – Detailed Design

This phase's objectives are the consolidation of the system design, including the lower level technical specifications, verification and validation strategies, HW manufacturing for assembly and testing, etc.

This phase usually ends with the Detailed Design Review and/or the Critical Design Review milestones.

Phase D – Qualification and Production

This phase comprises the construction, verification and validation of the system against the requirements and specifications and handover to the operational environment.

This phase often terminates with the Acceptance Review milestone.

Phase E – Operations

This phase comprises the system lifetime, on which it is used in the operational environment. This phase includes the maintenance activities aimed at keeping the qualification status of the system, as well as to bring it back to the operational state after interruptions of the service (failure, controlled stops, etc.)

Phase F – Disposal

Once concluded the system lifetime, it shall be dismantled in a controlled manner with special care on the management of debris and minimizing the environmental impact.

7.2.3.2 RAMS activities at each project phase

Table 7–2 details the foreseen activities in RAMS for each project phase defined in 7.2.3.1. All of the analysis there will be detailed in sections 7.3 and 7.4, except the initial steps which deserve a special treatment in 7.2.3.3.

Project phase as per [12]	RAMS analyses applicable to each project phase								
	Dependability Analyses					Safety Analyses			
	List of undesired events	FTA	FMEA / FMECA	Reliability Prediction Analysis	Maintainability analysis	List of hazardous events	Hazard Analysis	Safety Risk Assessment	Human dependability analysis
A	X					X			
B		X	X				X	X	
C		X	X	X			X	X	
D			X	X	X		X	X	
E					X				X

Table 7–2: Applicable RAMS analysis on each project phase

7.2.3.3 Identification of modules subject to RAMS analysis

The first step for the RAMS assessment within a project starts with the identification of those potential events in the system on which either a failure or an accident occurs. In the first case (failures – dependability related) the annotated events comprise the so called **List of undesired events**, whereas for the second case (accidents – safety related) it becomes the **List of hazardous events**.

Both lists are prepared at the early stages of the project (phase A) once the concept of the system is nearly consolidated. The remaining RAMS analyses, based on the information in these lists, provide different information on each event that allows to determine if it needs to be mitigated or suppressed by modifying the on-going design.

Once the lists are collected, and based on the analysis of the potential failure / accident described, the associated event shall be ranked with a severity level as per the levels in Table 7–1.

A very important aspect of the lists of undesired and hazardous events is that they allow identifying the modules of the system which are RAMS-critical as those with the largest amount of events and / or the most severe ones, and focus the subsequent RAMS analysis on them.

Example

The need to identify the RAMS-critical parts of a system is sometimes so evident that there is no need to prepare the list of undesired and hazardous events. In a car, for instance, it is clear that the braking system is RAMS-critical whereas the radio-CD is not. This identification of RAMS-critical modules allows saving effort on the subsequent RAMS analyses of the system as they are done on an efficient basis focusing in them and discarding other non-RAMS-critical modules

7.2.4 STEP 4: RAMS reporting

Each technical group in charge of a RAMS-critical module shall carry out the RAMS analyses indicated for the phase of the project on which they are as per Table 7–2.

On a periodic basis, which interval shall be agreed between the Project Manager and the RAMS Manager during the preparation of the RAMS Plan, they must report the RAMS activities carried out, including:

- The project phase.
- The RAMS-critical modules included.
- The results of the application of the RAMS analyses applicable to that project phase for the identified modules, through the templates provided for each one.

The RAMS manager, once collected the activities reported by all the technical groups, shall emit the project RAMS report with the all information gathered, plus:

- A summary of the deficiencies identified (if any).
- The main lessons learnt and conclusions extracted from the results of the RAMS analyses reported.
- Suggestions to improve the RAMS assessment (if any) to be traced to the RAMS Plan.

7.3 Dependability analyses

7.3.1 Fault Tree Analysis – FTA

Description of the Fault Tree Analysis

The FTA method for reliability analysis is a formal deductive procedure for determining the various combinations of component-level failures that could result in the occurrence of specified undesirable events at higher level. FTA is performed to ensure that the design conforms to the failure tolerance requirements for combinations of failures.

The FTA provides valuable information such as:

- Identification of undesirable events (top events).
- Development of Fault Tree for each top event.
- Identification of basic failure events
- Evaluation of probabilities of basic failure events.
- Evaluation of probability of intermediate events and top event.

FTA template and guidelines

The Fault Tree Analysis, as explained before, is a top-down method to identify the **Basic Failure Events** of a system from the known failures at system level (list of undesired events), carried out by:

- Dividing the system into different abstraction levels, starting from the system as a whole downwards.
- For each of the known failures at system level:
    - Identify in the lower abstraction level those events that can provoke the failure by their own, or those that must occur simultaneously to provoke it
    - Connect all of these events from the lower level to the system level using logical gates so that the events that can cause the failure individually are connected one another with OR gates, whereas those that must occur jointly are connected through AND gates.
- Repeat the process above for each of the events in the lower level as if they were the final failures and how they are caused by the events in the next abstraction level.

Once this process reaches the lowest abstraction level, the different diagrams of each failure with the events and their connections though logical gates comprise the so-called Fault Tree Analysis for that failure. The events in the lowest abstraction level considered in the Fault Tree are the aforementioned Basic Failure Events.

The more amount of AND gates in a Fault Tree, the more reliable the system is, especially when they appear between the first level and the system as a whole, as it implies that the number of events which can cause a given failure by their own is small.

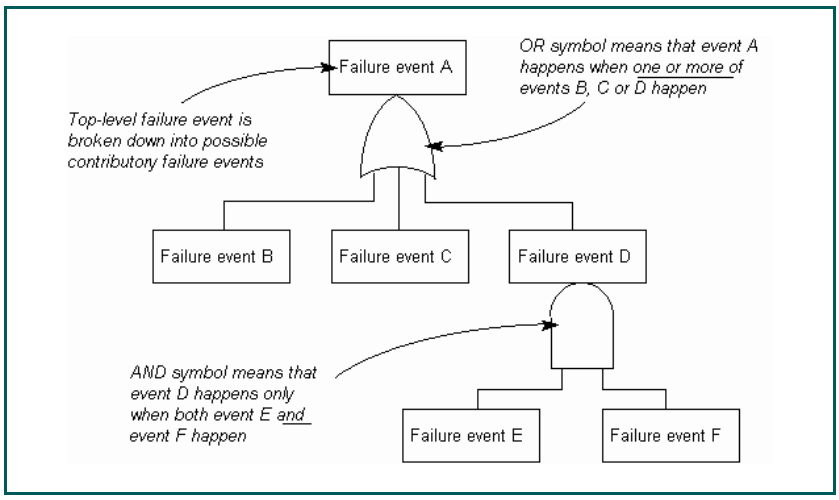


Figure 7–2: Example of a Fault Tree Analysis with two abstraction levels

The template for the FTA analysis along with the explanation of its different fields is provided below:

Fault Tree Analysis (FTA)									
Organisation:		System:			Subsystem:			Equipment:	
Date and issue:		Author:			Approved by:				
1 Id.	2 Top Level Event	3 HW/SW Fault	4 HW/SW Fault	5 HW/SW Fault	6 HW/SW Fault	7 HW/SW Fault	8 HW/SW Fault	9 ...	15 Remarks

Header information

The FTA worksheet contains the identity of the product (hardware or function) and the identity of corresponding equipment, subsystem, and system (as applicable).

1. Item number, Id

The identification number assigned for traceability purposes.

E.g. XXX-YYY-FT-nnn (TBC) where XXX is the system identification (TBD) and YYY the subsystem identification (TBD) and nnn a sequential number

2. Top level event

The identified top-level event to build each fault tree.

Each top-level event should be uniquely identified.

3. Hardware/Software fault(s)

Each column represents descending levels of the tree branches being faults causing the one on top. Each fault should be uniquely identified. The last column of the worksheet is the basic level event. The table can have a variable number of columns depending on the in-depth of the fault tree.

4. Recommendation

Column to describe the recommendation to eliminate the basic software fault identified.

E.g. S-XXX-YYY-FT-nnn (TBC) where XXX is the system identification, YYY the subsystem identification and nnn an identification number

In addition, each fault tree analysis can be supported with tables and lists of single events.

7.3.2 Failure Modes and Effects Analysis / Failure Modes, Effects and Criticality Analysis – FMEA/FMECA

Description of the Failure Modes and Effects Analysis – FMEA

The FMEA is a bottom-up reliability analysis which consists of studying how the failures of the most elementary blocks of a system are transmitted to the system as a whole. In a similar way as per the FTA, the system shall be divided into different levels of abstraction, but in this case the analysis starts at the lowest level, in this manner:

- Determine the failures modes of each of the elements of this lowest abstraction level
- For each of these failure modes identify the different events that each mode can provoke in the next abstraction level, and either the quantitative (when possible) of the qualitative estimated probability that it has to be transmitted in each of these ways.
- Process the next abstraction level with the events identified as if they were failure modes again, until the upper abstraction level is reached (i.e., the system as a whole)

The FMEA obtains the failures of a system from its basic failure events, whereas FTA determines the basic failure events from the system failures. Thus, it is possible to cross-check the results obtained by both analyses to determine if they are coherent one another.

Description of the Failure Mode, Effects and Criticality Analysis – FMECA

FMECA is an extension of FMEA that can be applied to the most critical subsystems. In the FMEA, the different events occurred by the transmission of the basic failure events to the higher abstraction levels can be assigned a pre-defined Severity Index, in which case the FMEA analysis turns into a FMECA – Failure Mode Effects and Criticality Analysis. As the original FMEA already contained an estimated probability of occurrence, the combined probability and severity allows assessing the criticality of the failures.

FMEA template and guidelines

The template for FMEA is extracted from [13] as follows:

Failure Modes Effects Analysis (FMEA)											
Organisation:			System:			Subsystem:			Equipment:		
Date and issue:			Author:			Approved by:					
1 Id.	2 Item / block	3 Function	4 Failure mode	5 Failure cause	6 Phase/Mode	7 Failure effects	8 Severity	9 Detection method	10 Compensating provisions	11 Recommendations	12 Remarks

Header information

The FMEA worksheet contains the identity of the product (hardware or function) and the identity of corresponding equipment, subsystem, and system (as applicable).

1. Identification number, Id.

Unique FMEA reference number for traceability purposes.

E.g. XXX-YYY-FM-nnn (TBC) where XXX is the system identification (TBD) and YYY the subsystem identification (TBD) and nnn a sequential number

2. Item/block

Name of the item or function being analysed, and the block of the reliability block diagram that is applicable to the analysis entry.

3. Function

A concise statement of the function performed by the item.

4. Failure mode

Identification and description of all potential failure modes of the item or function under analysis.

End effects of lower level FMEA are failure modes of the higher level FMEA.

5. Failure cause

When requested, identification and description of the most probable causes associated with the assumed failure mode.

- Failure modes of lower level FMEA are failure causes of the higher level FMEA.
- The failure causes are generally not identified when components are analysed (equipment level FMEA).

6. Mission phase/Operational mode

A concise statement of the mission phase and operational mode in which the failure is assumed to occur.

These elements can be addressed in the header of the worksheet. Although all of the different mission phases or operational modes are taken into account, the record of results is limited to the phase or mode in which the worst failure effects occur.

7. Failure effects

The FMEA worksheet shall contain the identification of the consequences of each assumed failure mode at local effects and end effects levels.

– Local effects: Local effects concentrate specifically on the impact of the failure mode on the operation, function, or status of the item identified in the second column of the worksheet. The local effects are recorded when different from the failure modes.

  The purpose of defining local effects is to provide a basis for evaluating compensating provisions and for recommending corrective actions.

– End effects: End effects define the effect that the analysed failure mode has on the operation, function, or status of the product under investigation and its interfaces, such that it allows integration into the next higher level FMEA.

8. Severity

The severity classification category assigned to each failure mode according to the worst potential end effect of the failure

9. Failure detection method

Expected failure detection method and the observable symptoms.

The failure detection means include telemetry, visual or audible warning devices, sensing instrumentation, other unique indications (e.g. the failure effect itself), or none.

10. Compensating provisions

Existing compensating provisions, such as design provisions or operator actions, which circumvent or mitigate the effect of the failure.

- Design provisions: Compensating provisions are considered design provisions when they feature a design that nullifies the effects of a malfunction or failure, control, or deactivate product items to halt generation or propagation of failure effects, or activate backup or standby items. Design compensating provisions include:
  - Redundant items or alternative modes of operation that allow continued and safe operation, and
  - Safety or relief devices which allow effective operation or limit the failure effects.
- Operator actions: Compensating provisions are considered operator actions when the operator circumvents or mitigates the effect of the postulated failure mode.

11. Recommendations

Recommendations for corrective actions need to be noted. Each recommendation shall have a non-ambiguous identifier for tracking purpose.

E.g. S-XXX-YYY-FM-nnn where XXX is the system identification, YYY the subsystem identification and nnn an identification number

12. Remarks

The FMEA worksheet also contains any pertinent remarks relevant to and clarifying any other column in the worksheet line.

7.3.3 Reliability Prediction Analysis

The reliability prediction analysis consists in the estimation of the rate of failures of a system during its design & implementation with the information available from other dependability analyses.

- At the very early stages of the development, (preliminary design), only coarse estimations based on the Dependability Risk Assessment can be done (from the pre-defined probability levels)
- The FTA provides the first refinement, as the basic failure events found can be assigned an estimated probability of occurrence and the connection among them through logical gates allows predicting a combined probability of occurrence from the fault tree of each of the system failures considered.
- Finally, as FMEA assigns estimated probabilities for the basic failure events and determines the connections with the next abstraction levels too, it is possible to obtain another estimation of the probability of occurrence of the failures at system level. In this case, being the basic failure events the inputs to the FMEA, it is very likely that their probabilities of occurrence are more accurate than those from FTA on which they are outputs.

As a result of the estimated probabilities of occurrence of the failures at system level it is possible to obtain two metrics:

- The **Estimated Mean Time Between Failures (EMTBF)**
- The **Estimated Mean Time To Repair (EMTTR)**

7.3.4 Maintainability Analysis

Once the system is constructed and becomes operational, the maintainability activities to be performed are the following ones:

- **Maintainability prediction**: Determination of maintainability parameters like MTBF (Mean Time Between Failures), MTTR (Mean Time To Restore) and MDT (Mean Down Time) for the components. MTTR includes failure detection and localisation times, removal and replacement or repair of default component, and preoperational testing time. MDT comprises the time between service interruption and service resumption.
- Isolation of critical items (like for instance products that cannot be checked and tested after integration, limited-life products or products that do not meet or cannot be validated as compliant to the maintainability requirements) and issue of recommendations.
- Support to design evaluation and trade-off studies.
- Identification of spares and sparing recommendations.

- Determination of maintenance strategy, considering preventive and corrective actions.
- Replacement strategy.

Every technical group shall provide an updated maintenance plan with suggested maintenance schedules. This document shall specify service procedures, diagnostics and checklists to aid both scheduled and unscheduled maintenance.

In order to define procedures for operations it is necessary to analyse, identify and assess the risks associated with operations, sequences and situations that can affect dependability performance. This analysis will take into account the technical and human environment. In addition, the operational procedures must:

- Include dispositions to face abnormal situations and supply the necessary safeguard measures.
- Not compromise equipment reliability.
- Be in accordance with established maintenance dispositions.
- Include dispositions to minimize failures due to human errors.

7.4 Safety analyses

7.4.1 Hazard Analysis

Description of the Hazard Analysis

Hazard analysis is performed in a systematic manner and allows estimating the main hazard' sources and their potential effects. More precisely, the target is:

- Identify hazards, potential risks, their occurrence conditions and the gravity of the induced effects.
- Plan and manage the way to search the safety elements in order to mitigate or eliminate the conditions which creates the risk (detection and recovery actions).
- Track the identified hazards up until inherent risk is acceptable for the intended use of the product.

This method is the most important one used for Safety analysis purposes and supports the hazard reduction process.

Safety verification is ensured by the fact that any accepted safety recommendation will be injected in the life cycle as requirement.

Hazard Analysis template and guidelines

CTA Hazard Analysis (CTA-HA)									
Product:		**System:**			**Subsystem:**			**Equipment:**	
Date and issue:		**Author:**			**Approved by:**				
1 Hazard ID	2 Hazard description	3 Cause	4 Consequence	5 PN	6 ISN	7 Recommendation	8 FSN	9 HRI	10 Trace to derived requirement

Header information

The HA worksheet contains the identity of the product (hardware or function) and the identity of corresponding equipment, subsystem, and system (as applicable).

1. Hazard Id.

Unique hazard reference number for traceability purposes.

E.g. XXX-YYY-HA-nnn (TBC) where XXX is the system identification (TBD) and YYY the subsystem identification (TBD) and nnn a sequential number

2. Hazards Description

Comprises identification of the hazard and the associated hazardous event.

E.g. Erroneous Input data in external interfaces.

3. Cause

Originating cause of the hazard. Note, in some cases the cause can be undetected hardware failures and/or software errors.

E.g. Input data is corrupted by the originator; communication problem.

4. Consequence

Output feared events that could result from the hazard.

E.g. Loss of control of the CTA components

5. Probability Number - PN

The likelihood of occurrence of the hazard is allocated as a probability following expert judgment. The approach used for the assessment can be either qualitative or quantitative. The qualitative approach based on engineering judgment shall be used if specific data are not available.

Probabilities of occurrence shall be grouped into defined levels which establish the qualitative probability level for entry into the worksheet column. The probability levels and limits shall be agreed between Project Manager and RAMS Manager and included in the RAMS Plan.

Each level is identified by a probability number (PN), as defined in Table 7–3.

PN	Occurrence Level	Description	Limits
4	Probable	It is likely to occur	$P > 10^{-2}$
3	Occasional	It is unlikely to occur but possible	$10^{-4} < P < 10^{-2}$
2	Remote	It is very unlikely to occur	$10^{-5} < P < 10^{-4}$
1	Extremely remote	It is assumed it will not occur	$P < 10^{-5}$

Table 7–3: Probability Numbers (PN) assignment for Hazard Analysis

Data sources, approved by the customer, will be listed and be the same as those used for the other dependability analyses performed for the programme.

The hazard probabilities shall be ranked as per Table 7–3 and relevant entry (the PN) listed in the HA worksheet column.

6. Initial Severity Number - ISN

Pre-mitigation severity of associated safety risk, as per the levels defined in Table 7–1. A severity number (SN) shall be given to each assumed Hazard, as per the values in Table 7–4. It is important to remark that severity numbers and severity levels are different.

SN	Severity
4	Catastrophic
3	Critical
2	Major
1	Minor or negligible

Table 7–4: Severity Numbers (SN) assignment for Hazard Analysis

7. Recommendation

Recommendations will be detailed and controlled in the RAMS report document. This field provides the link to the Recommendation ID (as stated in the RAMS report) proposed for each hazard.

E.g. S-XXX-YYY-HR-nnn (TBC) where XXX is the system identification, YYY the subsystem identification and nnn an identification number

8. Final Severity Number - FSN

Severity Number of the hazard once the Recommendation(s) is (are) implemented, as per the values in Table 7–4.

9. HRI

Hazard severity and hazard probability when integrated into a table format produces the **Hazard Risk Index (HRI)** matrix. The initial HRI is a risk categorization for hazards which is allocated prior to the establishment of control/mitigation requirements.

HRI are estimated, considering the final severity, that is, after the application of the identified mitigations using the matrix depicted in Table 7–5. The Hazard Risk Index (HRI) for a specific hazard is then derived from the severity of the failure effects and the probability of occurrence. The HRI is calculated as the product of the ranking assigned to each factor:

$$HRI = SN \times PN \qquad \text{[Eq.118]}$$

Hazards having a high HRI shall be given a higher priority in the implementation of the corrective actions than those having a lower HRI. An item shall be considered as **critical** (marked in red) item if:

- a hazard has consequences classified as catastrophic, or
- a hazard is classified as HRI greater than 6 in conformance with Table 7–5.

Yellow and green cell are non-critical with HRI equal or below 6. This difference is not essential

Severity category	SNs	Probability level PNs			
		1	2	3	4
catastrophic	4	4	8	12	16
critical	3	3	6	9	12
major	2	2	4	6	8
negligible	1	1	2	3	4

Table 7–5: Hazard Risk Index – HRI matrix

10. Trace to derived requirement

When a recommendation is accepted, the trace to the derived requirement(s) is provided.

7.4.2 Safety Risk Assessment

Safety Risk Assessment is the portion of Hazard Analysis similar to Risk Assessment in section 6.2.2.2, on which the severity and probability of occurrence are combined. However, the use of 4 levels allows distinguishing these type of risks to the general risks treated there. In general, the Safety Risk Assessment:

- comprises the identification, classification and ranking of safety risks and their contributors,
- is based on deterministic hazard analysis by combining the consequence severity and the likelihood of occurrence of the consequence,
- is used to facilitate effective and efficient safety risk reduction and control,
- supports project risk management,
- assesses compliance with probabilistic safety targets (if applicable).

7.4.3 Human Dependability Analysis

Given the human intervention in the system operation, the Human Dependability Analysis will support the safety analysis to take into consideration the human intervention during the operation and maintenance activities both preventive and corrective, as performed, in the operational phase.

Whenever safety analyses identify operator errors as a cause of catastrophic or critical hazards, this dedicated analysis will be carried out.

The human error analysis will be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human operator errors.

7.5 Traceability to standards

The ECSS standards on dependability [10], [13], and safety [11] were used as the main guidelines to elaborate this procedure However, this adaptation has been done on a case by case basis, hence not following the general structure of the aforementioned references unlike the previous ones on which there are clear references that were used and an explicit tailoring of existing standards.

Chapter 8

Procedure for Software developments

This last chapter includes a dedicated procedure for SW developments inside a Large Scientific Installation. Although it is not formally a Product Assurance discipline enumerated in 4.1

8.1 Objectives of SW development procedure

8.1.1 Context

Software is present in every aspect of a Large Scientific Installation. Starting from the simulations carried out at the very early stages of its conception (the "proof of concept" or "feasibility studies"), up to the complex modules for HW control, data acquisition, data archiving, data analysis, Monte-Carlo simulations, etc. SW development is one of the most important elements to be considered on a LSI.

Every scientist or engineer can be a SW developer at any time, but the way they encompass this task is crucial for the final product obtained. The effort needed to accomplish the development of SW products is very often under-estimated. The reason is straightforward: the SW programming allows designing and implementing complex systems rather more easily than any HW development. The outputs produced are so complex that the validation of all the potential states of the execution flow of the programs is basically impossible, reason why the proper adoption of a-priori design and validation strategies become key aspects for the successful accomplishment of the tasks assigned.

The scenario sketched above –SW programs so complex that it is impossible to properly verify their correct performance plus the difficulty to adapt them to the changing requirements of the users– is what was assessed in the first NATO Software Engineering Conference in 1968 and gave birth to the term *Software Crisis*. This conference was the starting point for the SW engineering, which from then on involved specialists in the definition of procedures, norms and rules to success in the development of complex SW.

At the time of writing this procedure, the work in SW engineering is basically done. It is clearly out of the scope of this chapter to address this problem from scratch. However, there are some typical scenarios in the SW developments for Large Scientific Installations worth to be analysed, and is for these specific contexts to which current procedure applies.

8.1.2 The "three-P's" problem of ad-hoc simulation SW

There is no doubt that the final assessment on the capabilities of a design is often based on the results of the simulation of its components and the system as a whole. In many cases, simulation by means of dedicated SW provides the most reliable reproduction of an element without the need to implement complex HW replicas, when the commercial SW cannot commit with the requirements of the simulations.

The SW elements in charge of simulating real systems are usually created as small packages with limited capabilities, which grow both in size and complexity as the requirements on more realistic performances become more and more demanding.

It is usual that the SW produced under these circumstances lay on a "metastable" existence during its lifetime, produced by the so-called three-P's problem:

- Poor SW requirements definition
- Poor SW documentation
- Poor SW validation

When this occurs the SW becomes not usable and "dies", even though this SW had been carefully implemented by talented programmers.

This scenario is very likely to occur at Universities and Research Institutions where the staff has very good knowledge on the target system under test and good skills in the programming language used for the simulation SW, but poor or inexistent experience on the production of qualified SW.

The programs produced become self-contained, i.e. the comments inside the source code are used to specify the functionalities of its modules, interfaces, even the operational user manual, to mitigate the lack of documentation. This is the reason why the usage of the SW is almost limited to the developers, which become the only ones able to operate it.

Although the scenario depicted in previous section seems a recipe for disaster, the continuous review of the SW by the programmers to implement/refine its capabilities leads to the aforementioned "metastable" phase which provides usability by the development team with good performances.

On the other hand, the effort to endow a SW with appropriate design documentation / operational manuals and validation evidences (test procedures, cases and results) is so high that it is neither feasible nor appropriate for small projects.

Needless to say that there is a wide greyscale in the ratio efficiency of the SW / applicable QA standards. Obviously the SW for the control system of an aircraft shall meet more demanding rules for its verification than that used to simulate a single diode in a laboratory.

In a Large Scientific Installation, mainly on those managed by an *ad-hoc* consortium created for that purpose, the delay in the provision of appropriate project plans also affects the SW developments. The typical unbalanced ratio between scientific and engineering background experience at the early stages of these projects usually leads to the occurrence of the "three P's problem" and is likely to be propagated to the development of real SW elements of the LSI as the project goes on.

8.1.3 Final considerations on the SW procedure

This procedure is aimed at providing a dedicated set of rules for SW developments in a Large Scientific Installation, without the need to adhere to any of the existing standards. Since the procedure proposed is a tailoring of ECSS rules [14], [15] (which was done respecting the ECSS tailoring requirements in [2]); and the peculiarities of a LSI has been the main driver for its

preparation, it could be directly applied and even serve as a dedicated SW Product Assurance Plan.

8.2 Procedure for SW developments

8.2.1 STEP 1: Rules for SW development

8.2.1.1 Naming convention for SW development rules

The rules have been assigned a code which allows to uniquely identifying one another. Therefore, each SW development rule has:

- a SW Rule ID, the aforementioned code.
- a SW Rule Title, which summarizes the contents of rule.
- a SW Rule Description, with the contents of the rule itself.

The naming convention for the SW Rule ID is defined hereafter:

[SW-PA-<Type of Applicability> <Identifier>.<Version>]

Where:

- **<Type of Applicability>** stands for the criticality of the rule and the situations where it applies, with the different categories:
  - M – Mandatory rules which shall be applied in all cases.
  - R – Recommended rules.
  - O – Optional rules.
- **<Identifier>** stands for a sequential number to be assigned to each rule which allows to uniquely identifying them. It is recommended to use multiples of 10 to allow the introduction of future rules between existing ones during reviews of the standards.
- **<Version>** is a number indicating the number of revisions made to the contents of rule with respect to the first version labelled as "0".

Example
The seventieth recommended SW rule defined, in a future revision 3 would be labelled as: [SW-PA-R 70.3] **The first version of mandatory SW rule number 10 is labelled as: [SW-PA-M 10.0]**

8.2.1.2 SW development rules

[SW-PA-M 10.0] Team organization

The Developer[9] shall set up a structure for software development with the roles clearly defined with tasks and responsibilities.

[SW-PA-M 20.0] SW PA designation

The Developer shall designate the responsible for software product assurance for the project (SW PA manager/engineer).

[SW-PA-R 10.0] SW PA manager functions

The software product assurance manager/engineer shall

- report to the project manager (through the project product assurance manager, if any);
- have organisational authority and independence to propose and maintain a software product assurance programme in accordance with the project software product assurance requirements;
- have unimpeded access to higher management as necessary to fulfil his/her duties.

[SW-PA-R 20.0] SW PA plan definition

- The Developer shall prepare a software product assurance plan in response to the software product assurance requirements.
- The software product assurance plan shall be either a standalone document or a section of the Developer overall product assurance plan.

[SW-PA-R 30.0] SW Problems reporting

The Developer shall set up a method for the logging, analysis and correction of all software problems encountered during software development.

[9] Refer to Developer definition in chapter 10

[SW-PA-R 40.0] SW Problems report contents

The software problem report shall contain the following information:

- identification of the software item;
- description of the problem;
- recommended solution;
- final disposition;
- modifications implemented (e.g. documents, code, and tools);
- tests re-executed.

[SW-PA-R 50.0] SW life cycle definition

- The software development life cycle shall be defined or referenced in the software product assurance plan.
- The following characteristics of the software life cycle shall be defined:
  - phases;
  - input and output of each phase;
  - status of completion of phase output;
  - milestones.

[SW-PA-R 60.0] Project plans documentation

The following activities shall be covered either in software-specific plans or in project general plans:

- development;
- specification and design documents to be produced;
- configuration and documentation management;
- verification, testing and validation activities;
- maintenance.

[SW-PA-M 30.0] Configuration Management

For every SW development a configuration management system shall be set up allowing secure backup and versioning

[SW-PA-M 40.0] Backup & Versioning

The software configuration management system shall allow any reference version to be re-generated from backups.

[SW-PA-R 70.0] Criteria for SW verification

- The outputs of each development activity shall be verified for conformance against pre-defined criteria.
- Only outputs which have been subjected to planned verifications shall be used as inputs for subsequent activities.

[SW-PA-R 80.0] SW metrics requirements

Based on the criticality of the software, test coverage goals for each testing level shall be agreed between the LSI project management or an authorised delegate and the Developer and their achievement monitored by metrics:

- for unit level testing;
- for integration level testing;
- for validation against the technical specification and validation against the requirements baseline.

[SW-PA-O 10.0] Tests coverage

- Test coverage shall be checked with respect to the stated goals.
- Feedback from the results of test coverage evaluation shall be continuously provided to the software developers

[SW-PA-R 90.0] SW Problems reporting during validation

The Developer shall ensure that non-conformances and software problem reports detected during testing are properly documented and reported to those concerned.

[SW-PA-O 20.0] Documentation update on re-qualification

In case of re-testing, all test related documentation (test procedures, data and reports) shall be updated accordingly.

NOTE: This activity should be carried out in case a major change in the SW is done thus implying a partial or complete re-qualification

[SW-PA-M 50.0] SW requirements definition

The LSI project management or an authorised delegate shall derive system requirements allocated to software from an analysis of the specific intended use of the system, and from the results of the safety and dependability analysis.

[SW-PA-M 60.0] Interfaces definition

The LSI project management or an authorised delegate shall specify the external interfaces of the software, including the static and dynamic aspects, for nominal and degraded modes.

[SW-PA-R 100.0] SW life cycle requirements - I

The software Developer shall define and follow a software life cycle including phases, their inputs and outputs, and joint reviews.

[SW-PA-O 30.0] SW life cycle requirements - II

- The life cycle shall be chosen, assessing the specifics of the project technical approaches and the relevant project risks.
- The software Developer shall define the development strategy, the software engineering standards and techniques, the software development and the software testing environment.
- The output of each phase and their status of completion, submitted as input to joint reviews, shall be specified in the software life cycle definition, including documents in complete or outline versions, and the results of verification of the outputs of the phase.

[SW-PA-O 40.0] SRR definition

After completion of the software requirements baseline specification, a system requirements review (SRR) shall take place.

AIM: Reach the approval of the software requirements baseline by all stakeholders.

[SW-PA-R 110.0] PDR definition - I

After completion of the software requirement analysis and architectural design, and the verification and validation processes implementation, a preliminary design review (PDR) shall take place.

AIM: To review compliance of the technical specification (TS) with the requirements baseline, to review the software architecture and interfaces, to review the development, verification and validation plans.

[SW-PA-O 50.0] PDR definition - II

In case the software requirements are baselined before the start of the architectural design, the part of the PDR addressing the software requirements specification and the interfaces specification shall be held in a separate joint review anticipating the PDR, in a software requirements review (SWRR).

AIM: e.g. in case of software intensive system or when an early baseline of the requirements is required.

[SW-PA-R 120.0] CDR definition - I

After completion of the design of software items, coding and testing, integration and validation with respect to the technical specification, a critical design review (CDR) shall take place.

AIM:

- To review the design definition file, including software architectural design, detailed design, code and user manual;
- To review the design justification file, including the completeness of the software unit testing, integration and validation with respect to the technical specification.

[SW-PA-O 60.0] CDR definition - II

In case the software detailed design is baselined before the start of the coding, the part of the CDR addressing the software detailed design, the interfaces design and the software budget shall be held in a separate joint review anticipating the CDR, in a detailed design review (DDR).

[SW-PA-O 70.0] QR definition

After completion of the software validation against the requirements baseline, and the verification activities, a qualification review (QR) shall take place.

[SW-PA-R 130.0] AR definition

After completion of the software delivery and installation, and software acceptance, an acceptance review (AR) shall take place.

AIM: To accept the software product in the intended operational environment.

[SW-PA-M 70.0] SW requirements documentation

The Developer shall establish and document software requirements, including the software quality requirements, as part of the technical specification.

[SW-PA-M 80.0] SW architecture definition - I

The Developer shall transform the requirements for the software item into an architecture that:

- describes its top–level structure;
- identifies the software components, ensuring that all the requirements for the software item are allocated to its software components and later refined to facilitate detailed design;
- describes the software behaviour.

[SW-PA-R 140.0] SW architecture definition - II

The Developer shall transform the requirements for the software item into an architecture that:

- covers as a minimum hierarchy, dependency, interfaces and operational usage for the software components;
- documents the process, data and control aspects of the product;

[SW-PA-O 80.0] SW architecture definition - III

The Developer shall transform the requirements for the software item into an architecture that:

- describes the architecture static decomposition into software elements such as packages, classes or units;
- describes the dynamic architecture, which involves the identification of active objects such as threads, tasks and processes;

[SW-PA-R 150.0] Detailed Design documentation

- The Developer shall develop a detailed design for each component of the software and document it.
- Each software component shall be refined into lower levels containing software units that can be coded, compiled, and tested.
- It shall be ensured that all the software requirements are allocated from the software components to software units.

[SW-PA-M 90.0] User manual

The Developer shall develop and document the software user manual.

[SW-PA-R 160.0] Unitary Testing - I

- The Developer shall develop and document the test procedures and data for testing each software unit.
- The Developer shall test each software unit ensuring that it satisfies its requirements and document the test results.

[SW-PA-O 90.0] Unitary Testing - II

The unit test shall exercise:

- code using boundaries at n-1, n, n+1 including looping instructions, while, for and tests that use comparisons;
- all the messages and error cases defined in the design document;
- the access of all global variables as specified in the design document;
- out of range values for input data, including values that can cause erroneous results in mathematical functions;
- the software at the limits of its requirements (stress testing).

[SW-PA-R 170.0] Integration Testing

The Developer shall integrate the software units and software components, and test them, as the aggregates are developed, in accordance with the integration plan, ensuring that each aggregate satisfies the requirements of the software item and that the software item is integrated at the conclusion of the integration activity.

[SW-PA-M 100.0] SW design validation definition

- The Developer shall develop and document, for each requirement of the software item in Technical Specifications, a set of tests, test cases (inputs, outputs, test criteria) and test procedures including:
  - testing with stress, boundary, and singular inputs;
  - testing the software product for its ability to isolate and reduce the effect of errors;

    NOTE For example: This reduction is done by graceful degradation upon failure, request for operator assistance upon stress, boundary and singular conditions.
  - testing that the software product can perform successfully in a representative operational environment;
  - external interface testing including boundaries, protocols and timing test;
  - testing Human-Machine Interface (HMI) applications.
- Validation shall be performed by test.
- If it can be justified that validation by test cannot be performed, validation shall be performed by either analysis, inspection or review of design.

[SW-PA-M 110.0] Traceability of design in User manual

- The Developer shall update the software user manual in accordance with the results of the validation activities with respect to the technical specification.

[SW-PA-M 120.0] SW requirements validation definition

- The Developer shall develop and document, for each requirement of the software item in the Requirements Baseline, a set of tests, test cases (inputs, outputs, test criteria) and test procedures including:
  - testing against the pre-defined validation data.
  - testing with stress, boundary, and singular inputs;
  - testing the software product for its ability to isolate and reduce the effect of errors;

    NOTE For example: This reduction is done by graceful degradation upon failure, request for operator assistance upon stress, boundary and singular conditions.
  - testing that the software product can perform successfully in a representative operational and non-intrusive environment.
  - external interface testing including boundaries, protocols and timing test;
  - testing Human-Machine Interface (HMI) applications.
- Validation shall be performed by test.
- If it can be justified that validation by test cannot be performed, validation shall be performed by either analysis, inspection or review of design.

[SW-PA-M 130.0] Traceability of requirements in User manual

The Developer shall update the software user manual in accordance with the results of the validation activities with respect to the requirements baseline.

[SW-PA-R 180.0] Acceptance Testing

The LSI project management or an authorised delegate shall perform the acceptance testing.

[SW-PA-R 190.0] Acceptance Testing environment

The acceptance shall include generation of the executable code from configuration managed source code components and its installation on the target environment.

[SW-PA-R 200.0] Acceptance Testing traceability

The acceptance tests shall be traced to the requirements baseline.

[SW-PA-R 210.0] Maintenance requirements

- The maintainer shall develop, document, and execute plans and procedures for conducting the activities and tasks of the maintenance process.
- Software maintenance shall be performed using the same procedures, methods, tools and standards as used for the development.
- The maintainer shall implement (or establish the organizational interface with) the configuration management process for managing modifications.
- The maintainer shall establish procedures for receiving, recording and tracking problem reports and modification requests, providing feedback to the requester.
- Whenever problems are encountered, they shall be recorded and entered in accordance with the change control established and maintained.

[SW-PA-R 220.0] Documentation update

All changes to the software product shall be documented in accordance with the procedures for document control and configuration management.

8.2.1.3 SW Rules classification

The rules in previous section have been organized attending different criteria for a faster reference.

The different criteria applied for SW rules classification are:

- Criticality: Whether they are
  - Mandatory
  - Recommended
  - Optional.
- Project Phase or Task to which they apply: Whether they apply to
  - Project Management
  - SW Design
  - SW Validation
  - SW Documentation
  - SW Maintenance

Classification by Criticality

SW Rule ID	Title
Mandatory Rules	
[SW-PA-M 10.0]	Team organization
[SW-PA-M 20.0]	PQC designation
[SW-PA-M 30.0]	Configuration Management
[SW-PA-M 40.0]	Backup & Versioning
[SW-PA-M 50.0]	SW requirements definition
[SW-PA-M 60.0]	Interfaces definition
[SW-PA-M 70.0]	SW requirements documentation
[SW-PA-M 80.0]	SW architecture definition - I
[SW-PA-M 90.0]	User manual
[SW-PA-M 100.0]	SW design validation definition
[SW-PA-M 110.0]	Traceability of design in User manual
[SW-PA-M 120.0]	SW requirements validation definition
[SW-PA-M 130.0]	Traceability of requirements in User manual
Recommended Rules	
[SW-PA-R 10.0]	SW PA manager functions
[SW-PA-R 20.0]	SW PA plan definition
[SW-PA-R 30.0]	SW Problems reporting
[SW-PA-R 40.0]	SW Problems report contents
[SW-PA-R 50.0]	SW life cycle definition
[SW-PA-R 60.0]	Project plans documentation
[SW-PA-R 70.0]	Criteria for SW verification
[SW-PA-R 80.0]	SW metrics requirements
[SW-PA-R 90.0]	SW Problems reporting during validation
[SW-PA-R 100.0]	SW life cycle requirements - I
[SW-PA-R 110.0]	PDR definition - I
[SW-PA-R 120.0]	CDR definition - I
[SW-PA-R 130.0]	AR definition
[SW-PA-R 140.0]	SW architecture definition - II
[SW-PA-R 150.0]	Detailed Design documentation
[SW-PA-R 160.0]	Unitary Testing - I
[SW-PA-R 170.0]	Integration Testing
[SW-PA-R 180.0]	Acceptance Testing
[SW-PA-R 190.0]	Acceptance Testing environment
[SW-PA-R 200.0]	Acceptance Testing traceability
[SW-PA-R 210.0]	Maintenance requirements
[SW-PA-R 220.0]	Documentation update
Optional Rules	
[SW-PA-O 10.0]	Tests coverage
[SW-PA-O 20.0]	Documentation update on re-qualification
[SW-PA-O 30.0]	SW life cycle requirements - II
[SW-PA-O 40.0]	SRR definition
[SW-PA-O 50.0]	PDR definition - II
[SW-PA-O 60.0]	CDR definition - II
[SW-PA-O 70.0]	QR definition
[SW-PA-O 80.0]	SW architecture definition - III

Table 8–1: SW Rules classification by criticality

Classification by Project Phase or Task

SW Rule ID	Title
Rules for SW Project Management	
[SW-PA-M 10.0]	Team organization
[SW-PA-M 20.0]	PQC designation
[SW-PA-M 30.0]	Configuration Management
[SW-PA-M 40.0]	Backup & Versioning
[SW-PA-R 10.0]	SW PA manager functions
[SW-PA-R 50.0]	SW life cycle definition
[SW-PA-R 80.0]	SW metrics requirements
[SW-PA-R 100.0]	SW life cycle requirements - I
[SW-PA-O 30.0]	SW life cycle requirements - II
[SW-PA-O 40.0]	SRR definition
[SW-PA-R 110.0]	PDR definition - I
[SW-PA-O 50.0]	PDR definition - II
[SW-PA-R 120.0]	CDR definition - I
[SW-PA-O 60.0]	CDR definition - II
[SW-PA-O 70.0]	QR definition
[SW-PA-R 130.0]	AR definition
Rules for SW Design Phase	
[SW-PA-M 50.0]	SW requirements definition
[SW-PA-M 60.0]	Interfaces definition
[SW-PA-M 80.0]	SW architecture definition – I
[SW-PA-R 140.0]	SW architecture definition - II
[SW-PA-O 80.0]	SW architecture definition - III
Rules for SW Validation Phase	
[SW-PA-M 100.0]	SW design validation definition
[SW-PA-M 120.0]	SW requirements validation definition
[SW-PA-R 70.0]	Criteria for SW verification
[SW-PA-O 10.0]	Tests coverage
[SW-PA-R 160.0]	Unitary Testing - I
[SW-PA-O 90.0]	Unitary Testing - II
[SW-PA-R 170.0]	Integration Testing
[SW-PA-R 180.0]	Acceptance Testing
[SW-PA-R 190.0]	Acceptance Testing environment
[SW-PA-R 200.0]	Acceptance Testing traceability
Rules for SW Maintenance Phase	
[SW-PA-R 210.0]	Maintenance requirements
Rules for SW Documentation	
[SW-PA-M 70.0]	SW requirements documentation
[SW-PA-M 90.0]	User manual
[SW-PA-M 110.0]	Traceability of design in User manual
[SW-PA-M 130.0]	Traceability of requirements in User manual
[SW-PA-R 20.0]	SW PA plan definition
[SW-PA-R 30.0]	SW Problems reporting
[SW-PA-R 40.0]	SW Problems report contents
[SW-PA-R 60.0]	Project plans documentation
[SW-PA-R 90.0]	SW Problems reporting during validation
[SW-PA-R 150.0]	Detailed Design documentation
[SW-PA-R 220.0]	Documentation update
[SW-PA-O 20.0]	Documentation update on re-qualification

Table 8–2: SW Rules classification by Project Phase or Task

8.2.2 STEP 2: Define the SW criticality levels

The rules in 8.2.1 were defined with three criticality levels:

- Mandatory
- Recommended
- Optional

The applicability of each criticality level shall be decided as a whole for the entire group of rules concerned, i.e., if the Recommended rules are considered applicable for a given development, then ALL the Recommended rules apply, and not on a case by case basis for each rule of this group. Only for those criticality levels which are considered not applicable for a given SW module can include exceptions to this policy, and single rules of the N/A category could be considered applicable.

Therefore, this implies that there will be three different types of SW in a LSI:

- Critical SW: The SW elements inside this category shall met all the SW rules defined:
  - Mandatory rules
  - Recommended rules
  - Optional rules
- Relevant SW: The SW elements ranked with this category shall be compliant to:
  - Mandatory rules
  - Recommended rules

  NOTE: The applicability of the Optional rules can be decided on a case by case basis.
- Routine SW: The SW elements ranked with this category shall only stick to:
  - Mandatory rules

  The applicability of Recommended and Optional rules as a whole or in a case by case basis is left at the Developer's choice.

Examples
- **Critical SW examples: Control SW for HW elements, Data acquisition SW, Data archiving and restoration from archive SW, etc.** - **Relevant SW examples: Data analysis SW, Scheduling SW, Simulation SW of the main modules on which the LSI design relies, etc.** - **Simulation SW for secondary elements, Prototypes of algorithms, etc.**

8.2.3 STEP 3: Define the SW life cycle

The definition of a SW life cycle, covered by [SW-PA-R 50.0], [SW-PA-R 100.0] and [SW-PA-O 30.0] is a mandatory task for Critical and Relevant SW, not so for Routine SW, although even for this last case is a highly recommended practise.

The selection of the applicable life cycle is left at the Developer's choice. However a typical V-model is presented as a reference.

8.2.3.1 V-model description

The V-model is one of the most extended life cycles for SW development and can also be used for HW development. This model is an evolution of the waterfall model for SW development on which the design and verification phases are split into different levels of abstraction, which are connected one another.

It is very suitable for a LSI as it covers many of the SW rules defined. The V-model consists in the definition of several phases during the development of the project attending the level of abstraction of the phase itself. In this model the development is continuous and does not allow overlapping of phases unlike other life cycles, i.e., a new phase does not start until the previous one is finished. Figure 8–1 presents a schematic description of the model:

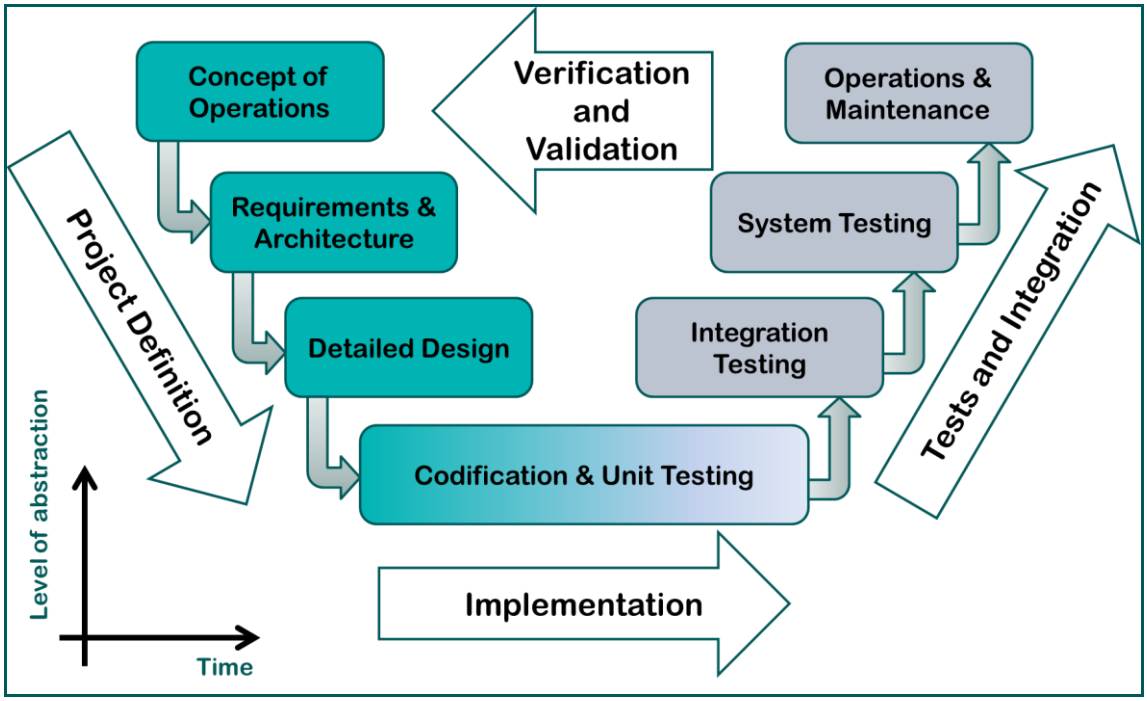


Figure 8–1: V-model life cycle schematic description

The different phases in the V-model can be grouped into three categories:

– **Project Definition**, which contains the following phases:

- Concept of operations
- Requirements Definition & Architecture Design
- Detailed Design

– **Implementation**, which comprises the activities:

- Codification
- Unitary Testing

– **Project Test & Integration**, which includes:

- Integration Testing
- System Testing
- Maintenance

8.2.3.1.1 Project Definition

Concept of Operations

This initial phase consists in the collection of the high level requirements of the system based on the needs expressed by the final user. The external interfaces which will be used as inputs or outputs of the system shall also be defined at this level.

Those high level requirements or User Requirements and interfaces identified in this phase shall be derived to the User Requirements Document and Interfaces Control Document, respectively.

Requirements Definition & Architecture Design

Once the high level requirements of the system are well known, this phase is in charge of defining a set of SW Requirements and a modular description of the system which shall meet them. This description shall contain the functional blocks or logical units, each of which implements some of the functionalities identified in the previous phase, whereas the SW requirements are the detailed set of fulfilments derived from the higher level User requirements.

The expected outputs of this phase are the Architecture Design and SW Requirements Documents.

Detailed Design

This phase is aimed at establishing the complete description of the modules which comprise each functional block in the architecture design. All SW requirements defined previously shall be traced to any of these modules to ensure that all the functionalities requested are correctly managed by our system.

As an output to this phase, the Detailed Design document shall be produced. Moreover, this phase completes the Project Definition branch of the V-model. So, the Verification Cases and

Procedures Document shall also be generated to ensure that the design proposed once implemented includes all the functionalities stated in the SW Requirements Document.

8.2.3.1.2 Implementation

Codification

This phase consist in the elaboration of the compilation units which implements the modules defined in the Detailed Design.

The expected output once this phase is completed is the preliminary source code ready to be tested.

Unitary Testing

Each compilation unit created shall be tested to ensure its correct performance within the system. To achieve this goal, a dedicated testing shall be done and each of the tests defined are named "Unitary Tests". This is the lower level of the verification and validation process.

The source code tested at unitary level shall be ready once this phase ends.

8.2.3.1.3 Project Test & Integration

The "ascending branch" of the V-model goes, level by level, checking that the outputs of the equivalent phase of the "descending branch" (Project Definition) is correctly implemented.

Integration Testing

This phase correspond to the same level of abstraction as the Detailed Design during the Project Definition. During this phase, the interconnection among the different modules comprising the functional blocks to ensure a proper operation is verified.

System Testing

The last step in the V-model corresponds to the validation of the system as a whole. All the requirements defined are checked to be correctly implemented.

The integration and/or the system tests are defined in the Validation Cases and Procedures, which establishes the different pass/fail criteria which shall be granted to considered a test passed, the environment description under which each test shall be run, etc.

The results of the Integration & System Testing campaigns shall be logged in the Verification and Validation Results Document once both phases are completed.

Maintenance

To ensure a proper operation of the system once validated after the system testing campaign, an active maintenance phase shall follow. This may allow the identification of these anomalies not covered by the system tests, as well as ensure its correction.

This phase can be extended during the operational lifetime of the SW produced. The management of the Non-Conformities and the re-qualification of the SW when needed shall be managed during this period.

8.2.3.1.4 Documentation Deliverables

Figure 8–2 presents a detailed overview of the V-model, as well as the expected documents to be produced as outputs once each phase is completed as per the SW rules defined.

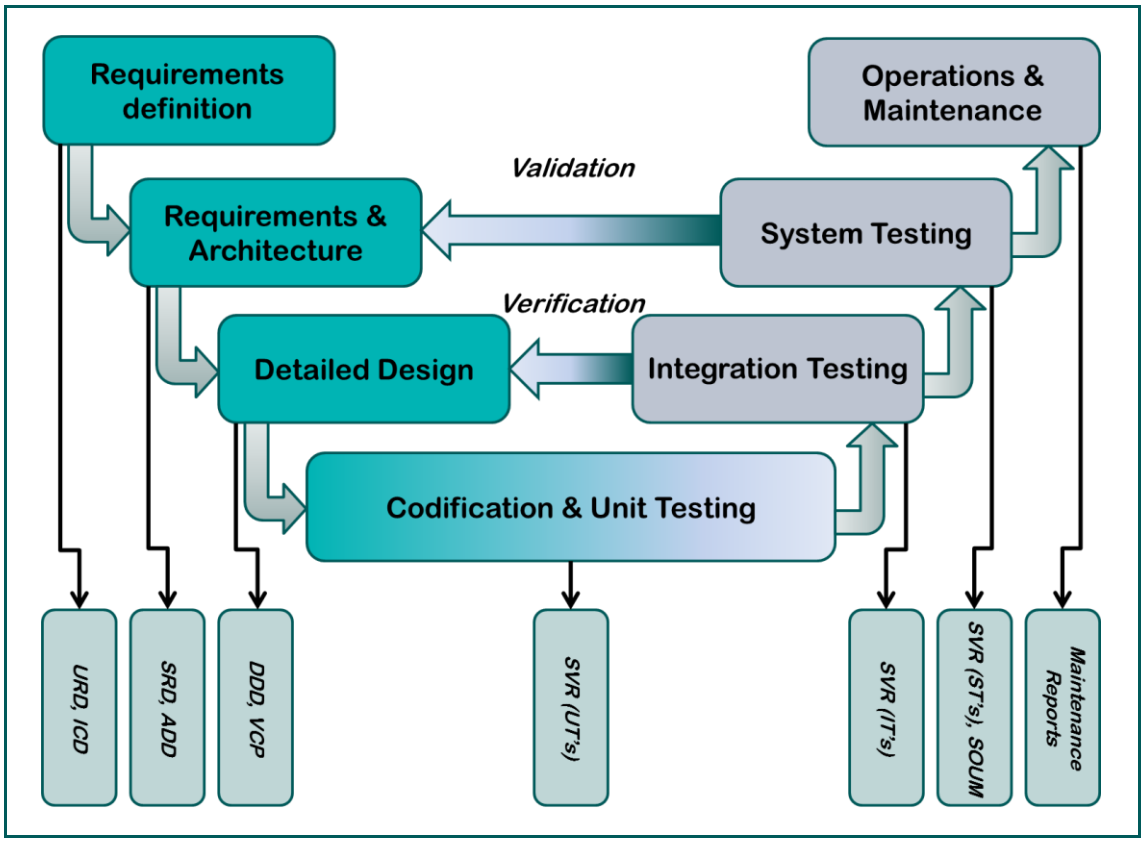


Figure 8–2: V-model life cycle including the expected documentation deliverables

A description of the documents referred above as outputs to each phase is provided below:

- URD - User Requirements Document: Summarizes the fulfilments of the system without regard to the technical details needed to implement them.
- ICD – Interfaces Control Document: Details the format of the inputs to & outputs from the system.
- SRD – SW Requirements Document: Traced to the user requirements, contains the specifications of the system taking into account the technical details needed to implement it.
- ADD – Architecture Design Document: It is a high level description of the system composed by functional blocks interconnected, so that each one is in charge of covering a part of the SW requirements.

- **DDD – Detailed Design Document**: Contains a complete description of each functional block defined in ADD, detailing their inputs/outputs, and the way to implement them.
- **VCP – Verification Cases and Procedures**: It is a collection of test cases to check the correct implementation of all the SW requirements of the system. Each test must have an overall description, a set of PASS/FAIL criteria, a procedure to be followed to execute it and the needed inputs and expected outputs.
- **SVR – SW Verification Results**: This document comprises the information about the testing campaigns to qualify the SW at three different levels: Unitary Testing (UT's), Integration Testing (IT's) and System Testing (ST's).
- **SOUM – SW Operations and User Manual**: This document contains a description of the system, version history, its functionalities and use cases for the most common operations.
- **Maintenance reports**: These documents shall be produced periodically highlighting the activities carried out in the period covered: Non Conformances detected, status of the known problems, version history and proposed schedule for the production of new releases.

8.3 Traceability to standards

The procedure presented is the result of a tailoring of the two main ECSS standards for SW, ECSS-E-ST-40C [14] and ECSS-Q-ST-80C [15]. The following table provides the traceability between the SW rules defined and its equivalent in the aforementioned standards.

SW Rule	ECSS standard	ECSS section	Amendment
[SW-PA-M 10.0]	ECSS-Q-ST-80C	5.1.1	**[general comment]** Supplier is replaced by developer **[general comment]** Customer is replaced by LSI project management or an authorised delegate
[SW-PA-M 20.0]	ECSS-Q-ST-80C	5.1.4.1	The role in the general Product Assurance Management procedure is the Product Assurance Delegate (see 4.2.2)
[SW-PA-R 10.0]	ECSS-Q-ST-80C	5.1.4.2	
[SW-PA-R 20.0]	ECSS-Q-ST-80C	5.2.1.1	The SW Product Assurance Plan expected as output to this rule can be either the overall Product Assurance Plan or a dedicated one.
[SW-PA-R 30.0]	ECSS-Q-ST-80C	5.2.5.1	
[SW-PA-R 40.0]	ECSS-Q-ST-80C	5.2.5.2	A template of the document for SW problem reporting/logging shall be defined.
[SW-PA-R 50.0]	ECSS-Q-ST-80C	6.1.1	The definition of a SW life cycle is mandatory, however, the characteristics of this cycle as specified in second bullet is optional and can be agreed between the development team and the PA Delegate.
[SW-PA-R 60.0]	ECSS-Q-ST-80C	6.2.1.1	
[SW-PA-M 30.0]	ECSS-Q-ST-80C	6.2.4.1	This rule shall be understood as follows: For every SW development a configuration management system shall be set up allowing secure backup and versioning
[SW-PA-M 40.0]	ECSS-Q-ST-80C	6.2.4.2	
[SW-PA-R 70.0]	ECSS-Q-ST-80C	6.2.6.2	
[SW-PA-R 80.0]	ECSS-Q-ST-80C	6.3.5.2	It shall be understood that the roles of supplier & customer refers to development team & PQC manager respectively.

SW Rule	ECSS standard	ECSS section	Amendment
[SW-PA-O 10.0]	ECSS-Q-ST-80C	6.3.5.5	
[SW-PA-R 90.0]	ECSS-Q-ST-80C	6.3.5.6	
[SW-PA-O 20.0]	ECSS-Q-ST-80C	6.3.5.16	Added note to refine the scope of the applicability
[SW-PA-M 50.0]	ECSS-E-ST-40C	5.2.2.1	
[SW-PA-M 60.0]	ECSS-E-ST-40C	5.2.4.3	
[SW-PA-R 100.0]	ECSS-E-ST-40C	5.3.2.1	Paragraph a is recommended, whereas paragraphs b, c and d are optional
[SW-PA-O 30.0]	ECSS-E-ST-40C	5.3.2.1	Paragraph a is recommended, whereas paragraphs b, c and d are optional
[SW-PA-O 40.0]	ECSS-E-ST-40C	5.3.4.1	
[SW-PA-R 110.0]	ECSS-E-ST-40C	5.3.4.2	Paragraph a is recommended, whereas paragraph b is optional
[SW-PA-O 50.0]	ECSS-E-ST-40C	5.3.4.2	Paragraph a is recommended, whereas paragraph b is optional
[SW-PA-R 120.0]	ECSS-E-ST-40C	5.3.4.3	Paragraph a is recommended, whereas paragraph b is optional
[SW-PA-O 60.0]	ECSS-E-ST-40C	5.3.4.3	Paragraph a is recommended, whereas paragraph b is optional
[SW-PA-O 70.0]	ECSS-E-ST-40C	5.3.4.4	
[SW-PA-R 130.0]	ECSS-E-ST-40C	5.3.4.5	
[SW-PA-M 70.0]	ECSS-E-ST-40C	5.4.2.1	The quality requirements can be references to the Product Assurance plan or this traceability matrix
[SW-PA-M 80.0]	ECSS-E-ST-40C	5.4.3.1	Bullets 1, 2 and 7 are mandatory, whereas bullets 3 and 4 are recommended. Finally, bullets 5 and 6 are optional
[SW-PA-R 140.0]	ECSS-E-ST-40C	5.4.3.1	Bullets 1, 2 and 7 are mandatory, whereas bullets 3 and 4 are recommended. Finally, bullets 5 and 6 are optional
[SW-PA-O 80.0]	ECSS-E-ST-40C	5.4.3.1	Bullets 1, 2 and 7 are mandatory, whereas bullets 3 and 4 are recommended. Finally, bullets 5 and 6 are optional
[SW-PA-R 150.0]	ECSS-E-ST-40C	5.5.2.1	
[SW-PA-M 90.0]	ECSS-E-ST-40C	5.5.2.8	
[SW-PA-R 160.0]	ECSS-E-ST-40C	5.5.3.2	Paragraphs a and b are recommended, whereas paragraph c is optional
[SW-PA-O 90.0]	ECSS-E-ST-40C	5.5.3.2	Paragraphs a and b are recommended, whereas paragraph c is optional
[SW-PA-R 170.0]	ECSS-E-ST-40C	5.5.4.2	
[SW-PA-M 100.0]	ECSS-E-ST-40C	5.6.3.1	
[SW-PA-M 110.0]	ECSS-E-ST-40C	5.6.3.3	
[SW-PA-M 120.0]	ECSS-E-ST-40C	5.6.4.1	
[SW-PA-M 130.0]	ECSS-E-ST-40C	5.6.4.3	
[SW-PA-R 180.0]	ECSS-E-ST-40C	5.7.3.2	
[SW-PA-R 190.0]	ECSS-E-ST-40C	5.7.3.3	
[SW-PA-R 200.0]	ECSS-E-ST-40C	5.7.3.5	
[SW-PA-R 210.0]	ECSS-E-ST-40C	5.10.2.1	

Table 8–3: Traceability between SW Rules and ECSS standards

Chapter 9

Conclusions

Review of the objectives of this work

The analysis of the different Large Scientific Installations presented in this work has shown how the industrial production and the scientific objectives are obliged to take along well in their joint effort to provide the new generation of instruments for the scientific research of XXI century.

This process is more or less consolidated in those LSI's managed by Agencies, whereas in those managed by *ad hoc* Consortiums there is an increasing awareness of the need to harmonize the procedures with the industrial production. However, the definition of procedures and plans from scratch is a huge task that demands a significant effort, which in this latter case turns into a handicap compared to agencies-managed LSI's.

The definition of intermediate procedures and plans –not so demanding as the existing standards– and focused in the idiosyncrasy of the LSI's can help mitigating this handicap.

The work devoted by UCM_ELEC in the CTA project has been an exceptional laboratory for the refinement of the procedures presented. The CTA project management has supported UCM_ELEC group and the best token is the provision of an Industrial Research & Development – IRD[10] project for the development of training material, templates and plans for Product Assurance within CTA, in 2012.

Besides, the co-authorship in the approved versions of the CTA Quality Plan and RAMS Plan, as well as the authorship of the Risks Management Plan under revision made UCM_ELEC become the reference in Product Assurance issues within CTA. This experience has served as the basis for the preparation of present thesis.

It is worth remarking that the different support actions taken as a result of the requests by CTA technical groups, as well as the comments and suggestions by UCM_ELEC to the managerial structures has improved the overall awareness on Product Assurance topics within the project, and ultimately driven the last corrective actions in the deficiencies identified.

The procedures proposed have been partially tested in the CTA environment, and the results become evident: The initial deficiencies identified are been addressed whereas the organization of two workshops in product assurance topics (Reliability Engineering Madrid 2012 and Risk Management Heidelberg 2013) has broadened the awareness on this issue by gathering the experience from other LSI's, both from the scientific aspects, as well as from the point of view of the industries involved.

[10] http://www.cta-industries.org/

Future work

The procedures presented are the starting point for the definition of global Product Assurance Standards for scientific research. Should the work presented is applied to new installations apart from CTA, new feedback could then improve them and spread their scope.

For the time being they have been conceived for a LSI with high demanding performance and availability requirements as well as technological challenges from the point of view of electronic devices, mainly. This is the typical scenario for a LSI devoted to physics. However, no procedures have been included yet for the management of chemical and biological installations, on which there are aspects not covered by present work.

There are currently two clear branches for the near future concerning the topics of present thesis:

- The next challenges in CTA project: Consolidation of a procedure for documentation approval, review and acceptance of Risks Management Plan, application of the more technical aspects of the procedures (RAMS techniques), and improvement of the templates proposed based on the experience from CTA reports on Product Assurance topics.
- The application to other LSIs (hopefully) on other topics different from physics (chemists, biology, medicine, etc.) to broaden its scope.

Chapter 10

Definitions

Accident

Undesired event occurred during the operation of a system that may lead to:

- Human death of injury.
- Loss or damage to the system elements (HW, SW, auxiliary materials, etc.).
- Loss or damage to public or private property.
- Detrimental effects on the environment.

Reference: [1].

Dependability

Dependability is the discipline within Product Assurance that is aimed at ensuring that a system is:

- **Reliable:** Reliability is the capability of a system to operate with the expected performance margins under controlled conditions. Basically, a reliable system is that which is able to work without failures within a given time interval.
- **Available:** Availability is the capability of a system to be able to operate when requested to do so and maintain this operational state.
- **Maintainable:** Maintainability is the capability of a system to return to the operational state from a previous non-operational state (due to a failure, for instance) through the application of predefined procedures for its restoration. Basically, the idea behind maintainability is the capability of a system to be repaired in an efficient way when it fails.

Developer

Developer is the organization / institution / team in charge of the development of a SW element.

Failure

The interruption of the capability of an element / system to perform a required function form which it was designed.

Reference: [1].

Hazard

Existing or potential condition of an element/system that may result in an accident.

Product Assurance

Product Assurance is the discipline within a **Project** which is intended to define the procedures, norms and controls to ensure that the development and the final product / system obtained:

- grants the predefined objectives,
- has appropriate the level of quality, and
- operates in a safe, available and reliable way.

References: [1], [5].

Product Assurance Disciplines

The different disciplines covered by **Product Assurance** are:

- **Quality Assurance**
- **Risks Management**
- **Dependability**
- **Safety**

For a complete description of the elements listed above, please refer to their corresponding definitions.

Product Assurance Manager

The **Product Assurance Manager** is the responsible for Product Assurance within a project and reports directly to the project manager, having unimpeded access to higher management.

The tasks which shall be assumed by the Product Assurance Manager are listed below:

- Ensure that the Product Assurance disciplines are well organized at the beginning of the project according to the project's requirements.
- Ensure that the inputs used to the Product Assurance disciplines are consistent and complete, and available in line with the project schedule.
- Ensure that the tasks described in the Product Assurance Management procedure for the different disciplines are performed in line with the project schedule.
- Ensure that the outputs produced as a result of the aforementioned tasks are consistent and complete, and in line with the project schedule.
- Ensure the application of the processes defined in the applicable project plans and documents.
- Control the quality of the elements provided by other project teams and/or external entities by:
    - Defining the product assurance requirements to be met, and
    - ensuring the implementation of these requirements by such project teams / external entities.
- Ensure that the Product Assurance contributions to verification are defined and provided.
- Ensure that a qualification programme is defined and maintained, and that the qualification results are recorded, evaluated and documented.

- Ensure that the results of the implementation of the qualification programme are kept in the form of a Qualification Status List for all the relevant components / subsystems.
- Review and approve the qualification status achieved as a result of the implementation of the qualification programme.
- Approve the final product / system during acceptance / delivery review.

References: [5].

Project

A **Project** is a standalone process encompassing several activities aimed at achieving a predefined objective, defined by a set of requirements. A project definition includes time, cost and resources constraints.

The term project is used in this document to identify:

- The process to design and implement a Scientific Installation.
- A sub-process inside a bigger project with enough entity to be considered as a project itself.
- The routine work of a scientific group which tries to align its internal procedures with the ones proposed here.

References: [1], [3], [4].

Project Manager

The **Project Manager** is the responsible for the fulfilment of the objectives of a project, namely: the planning, execution and closure tasks.

Quality

Quality is a concept used to denote the level of confidence of the inherent characteristics of a system with respect to a set of predefined requirements.

It is important to remark that Quality is a relative concept. It is not possible to determine the absolute quality of something, as it has to be compared against a set of requirements, often denoted as **quality requirements**.

References: [1], [3].

Quality Assurance

Quality Assurance is the discipline within Product Assurance that is aimed at checking that quality requirements are met.

References: [1], [3].

Risks

A **Risk** is a potential event which can jeopardize the nominal development of a project in case it finally occurred. Risks can be categorized by the type of impact they may cause to a project, as:

- **Cost Risks**: Events impacting project's cost: Situations that can either increase the estimated cost, or jeopardize the funding needed to cover the remaining activities.
- **Technical Risks**: Events impacting the expected project's performances, such as the availability of technology when necessary. The lack of expertise on a given technical aspect of the project by the project's staff is also covered by this type of risks.
- **Schedule Risks**: Events impacting the foreseen project's planning: Delays caused internally by, for instance, lack of available personnel when necessary (this type of schedule risk deals with the lack of personnel itself not with its expertise on a given technical subject as the previous case did); or externally by third parties (resellers not providing materials in time, etc.).
- **Other Risks**: Events which cannot be associated to any of the three previous categories but may have an impact in the project's development: Political or territorial constraints, managerial issues, etc.

It is very important to clarify the scope of the previous definition, i.e., what is a risk and what is not. There are many potential events that may affect a system itself rather than its development, which can be wrongly identified as Risks. The Risks definition above only deals with negative scenarios affecting project's development, not the final product/system. Whilst Risks are covered by Risks management, the negative events that may happen to / be caused by that final product / system are treated by the Dependability and Safety management, respectively.

Finally, there is a type of Risk which does not affect negatively the development of a project, but has benefits instead. Such potential events are called **Opportunities** and it is a must to exploit them once identified for the sake of the efficiency of the project.

Risks Management

Risks Management is the discipline within Product Assurance that is aimed at identifying Risks within a project and to rank them according to two criteria:

- The severity of their consequences in case they occur.
- Their probability of occurrence.

Aimed at the systematic and iterative optimization of the project resources and performed according to the established project risk management policy.

References: [1], [8].

Safety

Safety is the discipline within Product Assurance that tries to ensure that a system can operate with an acceptable level of risk with respect to the occurrence of accidents.

Chapter 11

Bibliography

11.1 References

[1] European Coordination for Space Standardization: **Glossary of Terms**. ECSS-P-001B. 14 July 2004. *This standard is the one applicable until ECSS-S-ST-00-01C is published.*

[2] European Coordination for Space Standardization: **ECSS System – Description, implementation and general requirements**. ECSS-S-ST-00C. 31 July 2008.

[3] International Standard ISO 9000: **Quality management systems – Fundamentals and Vocabulary**. ISO 9000:2005(E). Third Edition, 2005-09-29.

[4] International Standard ISO 10006: **Quality management systems – Guidelines for quality management in projects**. ISO 10006:2003(E). First Edition, 2003-06-20.

[5] European Coordination for Space Standardization: **Space product assurance – Product Assurance Management**. ECSS-Q-ST-10C. 15 November 2008.

[6] European Coordination for Space Standardization: **Space product assurance – Quality Assurance**. ECSS-Q-ST-20C. 15 November 2008.

[7] European Coordination for Space Standardization: **Space product assurance – Critical-item control**. ECSS-Q-ST-10-04C. 31 July 2008.

[8] International Standard ISO 17666: **Space systems – Risk Management**. ISO 17666:2003(E). First Edition, 2003-04-01.

[9] European Coordination for Space Standardization: **Space project management – Risk management**. ECSS-M-ST-80C. 31 July 2008.

[10] European Coordination for Space Standardization: **Space product assurance – Dependability**. ECSS-Q-ST-30C. 6 March 2009.

[11] European Coordination for Space Standardization: **Space product assurance – Safety**. ECSS-Q-ST-40C. 6 March 2009.

[12] European Coordination for Space Standardization: **Space project management – Project planning and implementation**. ECSS-M-ST-10C. 6 March 2009.

[13] European Coordination for Space Standardization: **Space product assurance – Failure modes, effects (and criticality) analysis (FMEA/FMECA)**. ECSS-Q-ST-30-02C. 6 March 2009.

[14] European Coordination for Space Standardization: **Space engineering – Software**. ECSS-E-ST-40C. 6 March 2009.

[15] European Coordination for Space Standardization: **Space product assurance – Software product assurance**. ECSS-Q-ST-80C. 6 March 2009.

[16] CTA Consortium. "**Memorandum of Understanding for the CTA design study**". CTA_MoU. 07/12/2009

[17] J. Carr, R. Ong and W. Hofmann. "Project Management Plan". CTA Managerial documentation. Ref. MAN-PO/121205 v5.2, 15 December 2012.

[18] J. Carr, T. Abegg, D. Torres, M. Doro, P. Vincent, O. Blanch, T. Bulik, G. Lamanna, C. Boisson et al. "**Preliminary Technical Design Report**". CTA Technical documentation. Ref. MAN-PO/120130 v4.2, 15 April 2013.

[19] J. M. Miranda. "**Reliability, Availability, Maintainability and Safety Requirements for CTA**". CTA Technical documentation. Ref. MAN-PO/121018 v2.1, May 31, 2013.

[20] M. Martinez. "**CTA: where do we stand and where do we go**". CTA General Meeting – Zeuthen 2010-05-10

[21] Proposal for the Preparatory Phase for the Cherenkov Telescope Array (CTA-PP). FP7-INFRASTRUCTURES-2010-1: INFRA-2010-2.2.10

[22] CTA-Spain Consortium. "**The Cherenkov Telescope Array at the 'Observatorio del Teide'. Tenerife as a candidate site for CTA-North**". Proposal document for CTA SITE Work Package. January 2012.

[23] B. Idzkowski. "**Dependability Risks Assessment for the Preliminary Design including FMEA and Safety Risk templates**". CTA Quality documentation. Ref. MAN-QA/120913 v3.0, 2013-04-23.

[24] J.M. Arroyo. "**RAMI analysis of IFMIF**". Proceedings of RAMS in Science Meeting. Madrid Sept. 2012.

[25] T. Pinna. "**ENEA experience in ITER RAMI**". Proceedings of RAMS in Science Meeting. Madrid Sept. 2012.

[26] M. Zerlauth. "**Reliability work in the LHC**". Proceedings of RAMS in Science Meeting. Madrid Sept. 2012.

11.2 Publications by the author

Brief notes about the author

The author of this thesis, Teodoro Bernardino Santos, received the degree of 'Licenciado' on Physics (Speciality of Astrophysics) in 1999 and the degree of Electronic Engineer in 2002, with the final project published in the Spanish URSI National Meeting 2002 [53]. He has been research assistant for the ESA "PLANCK" Mission at the CSIC (Instituto de Física de Cantabria, IFCA-CSIC), where he worked in the calibration and validation (thermal sensitivity studies and 'zero point' adjustment) of millimeter-wave radiometers, and the production of qualified calibration SW [27]-[31], [34]. In 2006, Mr. Bernardino received the Diploma of Advanced Studies and became Honorific Collaborator at Departamento de Física Aplicada III of Universidad Complutense de Madrid [50], [52]. Since 2005 he has worked at GMV Aerospace and Defence as manager of different projects related to the european navegation system EGNOS [49], and the ESA Global Monitoring for Environment and Security – GMES program [54]. He joined CTA project in 2010 as reliability engineer for the RADS work package lead by UCM_ELEC group [32], [33], [35], [37]-[45], [47].

11.2.1 PhD thesis related

PhD thesis related publications in journals indexed in ISI Web of Knowledge

[27] PLANCK LFI Calibration Team: A. Menella et al. (incl. T. Bernardino). "**PLANCK pre-launch status: Low Frequency Instrument calibration and expected scientific performance**". Astronomy & Astrophysics vol. 520, A4 (2010).

[28] PLANCK LFI Calibration Team: M. Bersanelli et al. (incl. T. Bernardino). "**PLANCK pre-launch status: Design and description of the Low Frequency Instrument**". Astronomy & Astrophysics vol. 520, A5 (2010).

[29] PLANCK LFI Calibration Team: F. Villa et al. (incl. T. Bernardino). "**PLANCK pre-launch status: Calibration of the Low Frequency Instrument Flight Model radiometers**". Astronomy & Astrophysics vol. 520, A6 (2010).

[30] PLANCK LFI Calibration Team: A. Menella et al. (incl. T. Bernardino). "**Calibration and testing of the PLANCK-LFI QM instrument**". Proceedings of SPIE meeting. Orlando (FL) June 2006.

[31] PLANCK LFI Calibration Team: M. Bersanelli et al. (incl. T. Bernardino). "**PLANCK-LFI: Instrument Design and Ground Calibration Strategy**". Proceedings of European Microwave Week 2005. Paris Sept. 2005

[32] CTA Consortium: M. Actis et al. (incl. T. Bernardino). "**Design Concepts for the Cherenkov Telescope Array CTA, An Advanced Facility for Ground-Based High-Energy Gamma-Ray Astronomy**". arXiv:1008.3703v3 [astro-ph.IM]

[33] CTA Consortium: B. Acharya et al. (incl. T. Bernardino). "**Introducing the CTA Concept**". Astroparticle Physics. Volume 43 Special Issue (SI) 2013.

Technical publications with referee

[34] T. Bernardino, E. Martínez-González and E. Artal. "**Description of the equations involved in the Radiometer Susceptibility to Environmental Fluctuations Module of PLANCK Radiometer aNAlyzer tool, RaNA**". PLANCK-LFI Technical documentation. Calibration campaign of 30 and 44 GHz LFI radiometers. Ref. PL-LFI-SAN-TN-129, issue 2.0, May 2005.

[35] C. Juffroy, M. Benallou, L. Fresnillo, J.M. Miranda and T. Bernardino. "**Quality Plan**". CTA Quality documentation. Ref. MAN-QA/110405 v1.1, 2011-07-07.

[36] T. Bernardino, L. Fresnillo and J.M. Miranda. "**Qualified software within CTA: Tailored Quality Assurance rules and SW Engineering Processes**". CTA Quality documentation. Ref. CTA-ELEC-UCM_ELEC-MEM-001/0001 v1.0, 2010-10-05.

[37] A. Atencia, S. Golmayo, T. Bernardino and J.M. Miranda. "**Reliability, Availability, Maintainability and Safety Plan**". CTA Quality documentation. Ref. MAN-QA/120424 v1.0, 2012-04-24.

[38] T. Bernardino, B. Idzkowski and J.M. Miranda. "**Risk Management Plan**". CTA QMT Work Package technical documentation. 2012-05-11. *Pending approval by CTA Project Committee.*

[39] M. Teshima et al. (incl. T. Bernardino). "**Baseline Design of 23m CTA Large Size Telescope**". CTA LST Work Package technical documentation. November 2011.

[40] G. Ambrosi et al. (incl. T. Bernardino). "**Baseline Design Document for Large Size Telescopes Rev. 2b**". CTA LST Work Package technical documentation. April 2013.

Presentations in International Congresses

[41] T. Bernardino, L. Fresnillo and J.M. Miranda. "**Quality Control and Risk Assessment for Preparatory Phase**". CTA Quality Meeting. Heidelberg 15/11/2010 (Oral presentation).

[42] T. Bernardino. "**Dependability procedures for CTA electronics**". CTA FPI/ELEC Work Packages Joint Meeting. Ciemat, Madrid 15/04/2011 (Oral presentation).

[43] A. Atencia and T. Bernardino. "**Dependability Procedures for CTA-ACTL**". CTA Consortium Meeting Toulouse 2011, ACTL Work Package session. 17/05/2011 (Oral presentation).

[44] T. Bernardino. "**Roadmap for CTA Quality working groups**". CTA Consortium Meeting Toulouse 2011, Work Packages Coordination session. 18/05/2011 (Oral presentation).

[45] T. Bernardino. "**Status of the RAMS plan for the LST's**". CTA LST Work Package Meeting. Munich 12/10/2011 (Oral presentation).

[46] C. Yoldi and T. Bernardino. "**The RAMS plan: Overview and a worked example**". CTA Consortium Meeting Madrid 2011, RADS Work Package session. 30/11/2011 (Oral presentation).

[47] T. Bernardino. "**The RAMS Plan for CTA**". CTA Project Committee Meeting. Heidelberg 06/02/2012 (Oral presentation).

[48] T. Bernardino. "**Product Assurance in Large Scientific Installations**". Proceedings of RAMS in Science Meeting. Madrid Sept. 2012 (Oral presentation).

11.2.2 Other Publications

[49] J. Caudepón, T. Bernardino and E. Sardón. "**Mitigation of the code-carrier divergence effect on single frequency user receivers for enhanced availability and accuracy under ionospheric degraded conditions**". Proceedings of ION Technical Meeting 2010. San Diego (CF) Jan. 2010 (Oral presentation).

[50] T. Bernardino, P. Antoranz, J.M. Miranda and J.L. Sebastián. "**Limitations of the transmission line theory in the simulation of ultra-thin wire conductivities with coaxial resonators**". Proceedings of the 37th European Microwave Conference – EuMC. Munich Oct. 2007 (Poster presentation).

[51] M. de la Cruz, T. Bernardino, J.M. Miranda, S. Muñoz and J.L. Sebastián. "**A switched four point cell for conductivity measurements of biological solutions**". Proceedings of 1st Seminario do Comite Portugues da URSI (International Union of Radio Science). Lisboa Nov. 2007 (Oral presentation)

[52] T. Bernardino, P. Antoranz, J.M. Miranda and J.L. Sebastián. "**DC to microwave conductivity spectroscopy of ultrathin wires using tapered coaxial lines**". Proceedings of the International Conference on Metrology, CAMET – JM. Casablanca April 2006 (Oral presentation).

[53] T. Bernardino, J.M. Miranda and J.L. Sebastián. "**Procedimiento para la mejora de las técnicas de reflectometría mediante redes neuronales**" *(Neural network driven improvements in reflectometry techniques)*. Proceedings of XVII Simposium Nacional de la Unión Científica Internacional de Radio – URSI. Alcalá de Henares Sept. 2002 (Oral presentation).

[54] E. de Miguel, R. Valenzuela, T. Bernardino, V. Rodríguez, A. Pizarro, D. de Miguel y C. Robles. "**Validación de algoritmos científicos para el GPP de SEOSAT/Ingenio**" *(Validation of scientific algorithms for the Ground Processing Prototype of SEOSAT/Ingenio satellite)*. Proceedings of the XIV Congreso de la Asociación Española de Teledetección (AET). Mieres Sept. 2011 (Oral presentation).