Quality Assurance and Safety Conformity for the 4-metre Multi-Object Spectroscopic Telescope (4MOST) project

Domenico Giannone*[a], Gero Rupprecht[b], Wolfgang Ansorge[c], Roger Haynes[a], Olga Bellido[a], Steffen Frey[a], Joar Brynnel[a], Roelof de Jong[a], Arno van Kesteren[b], Jean-François Pirard[b].

[a]Leibniz-Institut für Astrophysik Potsdam, An der Sternwarte 16, 14482 Potsdam, Germany; [b]ESO Headquarters, Karl-Schwarzschild-Str. 2, 85748 Garching bei München, Germany; [c]RAMS-CON Management Consultants, Loitersdorf 15, 85617 Assling, Germany.

ABSTRACT

With more than 200 scientists and engineers involved, the design and manufacture of the 4MOST instrument, a second-generation spectroscopic instrument built for ESO's 4.1-metre VISTA telescope, is a challenge requiring the implementation of an efficient quality assurance strategy during each project phase (i.e., design, manufacture, test, installation, and operation), and including the maintenance. This paper introduces the 4MOST product assurance approach used by the project to make sure that 4MOST will comply with all necessary quality and safety requirements over the whole instrument's lifetime of 15 years. For quality assurance, the guiding principles are mainly given by the ISO 10007:2017 and ISO 9001:2015 quality management standards. Related to safety, 4MOST design and manufacture complies not only with the essential safety requirements from the European Union New Approach Directives (CE Marking Directives), but also with the additional requirements coming from the ESO Safety Policy, issued by the ESO Management for ESO-wide application. The implementation of the 4MOST project's Quality Assurance and Configuration Management is described in detail in the paper.

Keywords: quality, safety, configuration management, change control, 4MOST, AIP.

1. INTRODUCTION

This paper presents the quality and safety approach implemented in the 4MOST project, an international collaboration to develop a new integral field spectroscopy facility for VISTA (Visible and Infrared Survey Telescope for Astronomy), a 4-meters class telescope located at ESO's Paranal observatory site in Chile. By 2022 the 4MOST Consortium is expected to provide the European Southern Observatory (ESO) with a state-of-the-art fiber-fed spectroscopic survey facility that is able to acquire ~2400 simultaneous spectra of sky objects distributed over a hexagonal field-of-view of more than 4 square degrees, i.e. with big enough field-of-view to survey a significant fraction of the austral sky within a few years.

In order to comply with 4MOST's stringent technical and science requirements and to maintain the highest possible level of quality, the 4MOST Project Office at the Leibniz Institute for Astrophysics Potsdam (Germany) has created a specific work-package (WP) on "Product Assurance" (PA) and appointed a specific 4MOST Product Assurance Manager (PAM). It is the duty of the PA work-package to define and implement the strategy for monitoring the overall instrument's dependability and quality.

Moreover the 4MOST Consortium has to take into account all aspects related to the safety of the facility, which is partly done through compliance with all Essential Health and Safety Requirements (EHSRs) from the relevant European Union (EU) Product Safety Directives, and partly through compliance with the requirements contained in the ESO Safety Policy.

For implementation and constant monitoring of quality 4MOST relies on two complementary control disciplines: the 4MOST Configuration Management (CM) and the Quality Assurance (QA). In 4MOST, the scope of each of the two disciplines is defined within a general policy for Product Assurance Management, which is one of the competencies of the 4MOST Project Office.

*dgiannone@aip.de; phone +49 331 7499 655; fax +49 331 7499 436

In a way, CM can be understood as a tool to keep track of the 4MOST documentation and to implement changes in a disciplined and controlled manner throughout the entire project. CM is implemented at both 4MOST subsystem and system level, i.e. for subsystem design, manufacture, assembly, integration and test (MAIT); for system assembly, integration and test (AIT) in Germany; for system installation and commissioning at the VISTA telescope in Chile.

To provide visibility and control of the instrument's configuration status, a CM Plan is defined following the guidelines given in ISO 10007:2017[1] and implemented by the Consortium. For issues relevant for 4MOST QA we follow the ISO 9001:2015 quality management system approach.

Of particular interest for 4MOST PA is the list of so-called "critical items" that is produced starting from the information in the 4MOST Hazard Analysis and 4MOST Reliability, Availability and Maintainability (RAM) documentation (both at 4MOST subsystem and system level). 4MOST critical items are the items that are included in the design of the instrument that require special care – either for quality or for safety reasons. Their integrity must be carefully monitored during each phase of the project including operation and maintenance. As part of the 4MOST RAM Assessment procedure, the inventory of spare parts is produced to identify all the spare critical parts that need to be delivered together with the instrument in order to minimize the impact of potential failures that would lead to unacceptable instrument downtime.

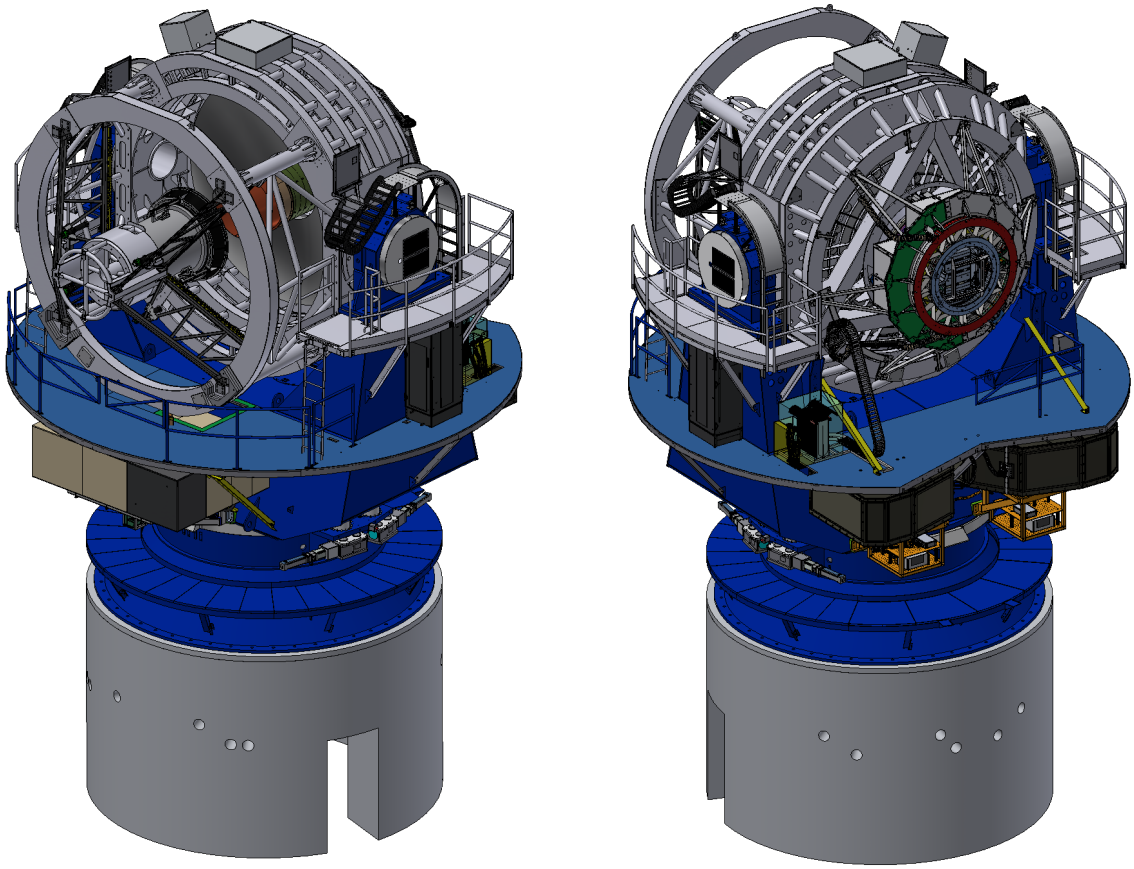

Figure 1. Integrated system level 4MOST facility drawings with a view of the Cassegrain components (courtesy of Allar Saviauk at the AIP).

2. QUALITY AND CONFIGURATION MANAGEMENT

2.1 4MOST Configuration Management (CM)

In adaptation of ISO 10007:2017 we define 4MOST CM as:

"*All activities for establishing and maintaining consistent records of the performance parameters of the 4MOST Instrument, as well as its functional and physical attributes, compared to the 4MOST Instrument and operational requirements*."

Clearly it is important to guarantee the integrity of the 4MOST instrument over the time. The 4MOST configuration can be unambiguously described by the identified set of requirements, documents, drawings, compliance and acceptance tests, etc. at any time of the instrument design or manufacturing. The approach followed by implementing CM enables the traceability, which is a pre-condition to deliver an adequate level of support during the whole instrument's life cycle.

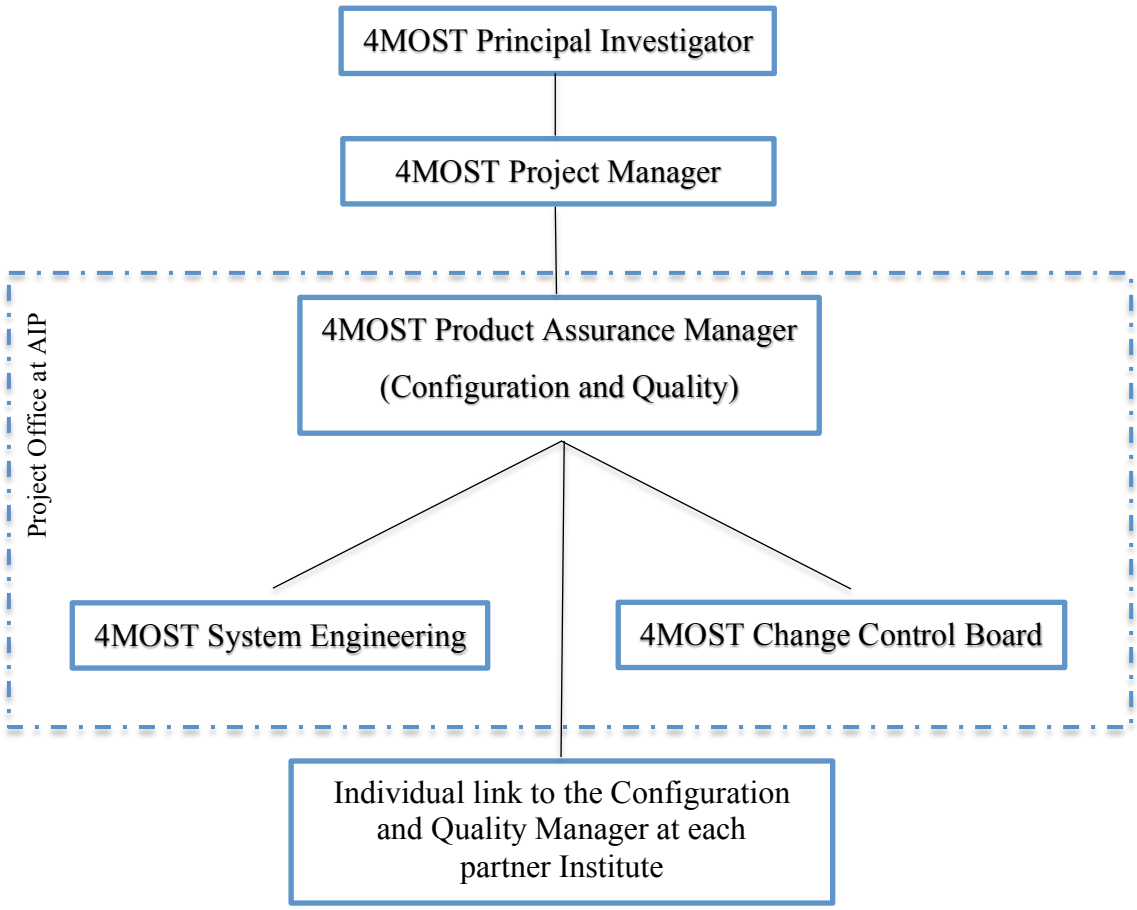

Figure 2. 4MOST Configuration and Quality Management organizational chart.

At an early stage of the project, 4MOST PA defined the 4MOST CM Plan to clarify the rules for consistency (such as the verification and validation tools) of the instrument's performance and functions with the defined requirement specifications. The CM plan contributes to the identification of role and responsibility of each partner within the Consortium, but also defines the way the project will track, implement, and communicate the changes that may occur throughout the different project phases and that are related to any of the 4MOST Configuration Items (CIs), i.e. any

component that can be identified as a self-contained unit for purposes of change control and identification. The basis for the identification of the 4MOST CIs is the 4MOST Product Breakdown Structure. The list of 4MOST CIs may be reviewed as the design of the instrument evolves: the initial set of CIs includes all major 4MOST subsystems and several important lower-level components.

To record and control the configuration of each CI at any time during its evolution, 4MOST CM has established a Configuration Item Data List (CIDL). This is the list of all the 4MOST applicable documents, including the approved changes, that unambiguously and completely define and characterize a given 4MOST CI. The CIDL presents the approved and agreed configuration status of a CI at a given time in the life cycle of a CI. Different configurations of a given subsystem are recorded. At the end of the 4MOST final design phase, the 4MOST Project Office will release the so-called "As-Designed CIDL".

As part of the 4MOST PA work-package, the CM activities of the project are under the direct responsibility of the 4MOST PA Manager; for convenience, the practical day-by-day implementation of the configuration management for all subsystems is delegated to Local PA Managers (LPAMs) who are the single-point contacts for PA at the partner organisations. Amongst other tasks, LPAMs are responsible for reporting on PA matters and implementing all changes that are approved by the 4MOST Change Control Board (see Section 2.2).

At system level, 4MOST CM is a management function centralized at the 4MOST Project Office (PO) as part of the PA work package. The 4MOST PO defines the configuration requirements and processes for the entire project, which are applicable to all the actors of the project. As a set-up of interrelated management processes 4MOST CM's main objectives are:

- Supporting the project management (e.g., providing information for schedule and cost planning)
- Implementing various controlling activities:
    - Configuration identification and traceability,
    - Configuration and change control,
    - Configuration status accounting, and
    - Configuration verification and audit.

Under the supervision of the 4MOST PO, the Consortium is responsible for implementing and executing the documented procedures for inspection and test activities: amongst other tasks, this also includes to verify that all specified requirements are actually met. As a general rule, the Consortium shall keep manufacturing records in order to provide traceability, i.e. the capability of tracing backward in case of any problem. With this respect 4MOST adopts a decentralized approach, in which each partner organization is requested to implement quality and safety in agreement with the strategy defined by the 4MOST PO. However, the partners will retain the full responsibility for the design and MAIT of their subsystem, and for supporting 4MOST system AIT, AIV, and Integration and Commissioning.

2.2 4MOST Change Control Board (CCB)

Within CM, the 4MOST Consortium adopts a procedure for change control that aims to actively prevent unauthorized changes, either in the design phase or during manufacturing, which may compromise the instrument's performance. The objective is here to guarantee the integrity of the instrument at any time. The rules for making changes are defined in a dedicated CM Plan and these are applicable to all 4MOST instrument development, MAIT, AIT, AIV, and installation and commissioning activities and to all project phases until the installation on the VISTA telescope (Provisional Acceptance Chile, PAC).

A 4MOST Change Control Board (CCB) is established at AIP within the 4MOST PO. The CCB comprises the Project Manager, the PA Manager / Configuration Manager, at least one member of Systems Engineering, as well as the project's PI.

When required, the local PM, the local PA Manager or any other expert could be invited to participate in the CCB meetings in order to advise on the specific technical issues.

The main duties of the CCB are:

- To identify the 4MOST CIs,
- To review and approve the 4MOST Configuration Baseline Documentation,
- To review and approve or reject the Change Requests (CREs) and the Requests for Waivers (RfWs) and issuing dispositions on the Non-Conformance Reports (NCRs),
- To ensure that all approved changes are added to the CM data-base,
- To seek clarification on any CIs, as and when required.

Any change to the 4MOST Requirement Baseline has to be approved by the 4MOST CCB before it can be implemented.

The 4MOST CCB is the only authorized committee to take decisions regarding whether or not a proposed change to the instrument configuration can be implemented. Once they are approved, the changes are communicated for application to the concerned partners and more in general to the 4MOST Consortium.

The local PM is responsible for reviewing and accepting for execution those CREs that affect their work when originating from outside. Should the 4MOST CCB lack the authority to decide on the acceptance of a proposed change (e.g., when the change requested violates a contractual document, e.g. ESO Technical Specifications) the CRE is escalated to ESO and only released after the final decision from ESO is obtained.

2.3 4MOST Configuration Baselines

As described in the ISO 10007 a configuration baseline is the:

"*Approved product configuration information that establishes the characteristics of a product at a point in time that serves as reference for activities throughout the life cycle of the product.*"

The configuration baseline identified/defined at the beginning of each project phase consists of the product configuration information that represents the state of the product as approved in the terminating review of the previous project phase. Configuration baselines, plus the approved changes to those baselines, represent the current approved configuration. Any change of the established configuration baseline shall undergo the formal change process defined in 4MOST Change Control Procedure.

The documentation containing the configuration information and listed in the list of documents constituting the configuration baseline of the CI, is reviewed by the 4MOST Configuration Manager and approved by the 4MOST CCB before the release of the documents for the Final Design Review. Following this final release, the documentation is formally put under configuration control and listed in the corresponding CIDL by the Configuration Manager.

2.4 4MOST Non-Conformance Control

In line with the objectives for 4MOST QA the Project has established a control system for non-conformance that provides a disciplined approach to the identification, analysis, review, isolation, corrective action, re-verification and prevention of recurrence of confirmed or suspected non-conformances. In particular, such control system covers parts manufacturing, assembly and tests.

When a discrepancy (or failure) with respect to binding or non-binding requirements is detected, a Non-Conformance Report (NCR) shall be submitted by the WP Manager or the local PA Manager to the 4MOST CCB. Following the NCR, the 4MOST CCB issues a disposition with respect to using or not the defective part, and stopping or continuing the on-going activities.

2.5 4MOST Configuration Status Accounting

The 4MOST PO has established a configuration status accounting system to record, store and retrieve the following configuration data of their subsystems and system respectively:

- Design status of the CIs,
- As-built status of accepted products,
- Status of configuration documentation and configuration data sets,
- Status of approval of changes and deviations and their status of implementation, the status of waivers,
- Status of actions derived from technical reviews and configuration verification reviews.

Each 4MOST partner organization reviews the CIDL and provides notification to the Configuration Manager of any inconsistencies in the configuration status of their CIs. The implementation of the configuration status accounting system makes use of the project document repository. Links to the current documentation are provided with each entry in the CIDL. For the configuration verification the 4MOST Consortium make use of "Compliance Matrices" to document compliance of design and the as built system and subsystems to requirements. The configuration in terms of functional and performance characteristics for all CIs is verified at each stage of the project following the 4MOST final design (i.e., TRR, PAE, and PAC).

3. SAFETY CONFORMITY ASSESSMENT PROCEDURE

3.1 Safety Requirements from the EU law and ESO Safety Policy

The design and manufacturing of the 4MOST Instrument is done in conformity with Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety and with the safety requirements from the so-called EU New Approach Directives: a series of legislative requirements that are in place to ensure ultimate product safety. The New Approach Directives are also known as "CE marking" Directives and require that a) only safe products may be put into service or placed on the market and b) that the end-user shall be duly informed of any risk associated with the supplied product.

The 4MOST Consortium is also contractually bound to adopt the ESO Safety Policy that is issued by the ESO Management for ESO-wide application. While ESO acknowledges the need to invent and prototype specialised equipment to fulfil the ESO scientific objectives, they also require that only equipment and appliances that are demonstrated to be safe can be integrated, operated and maintained at ESO observing facilities.

ESO deems safe commercially available ("off the shelf") CE marked equipment, provided its intended use conforms to the conditions foreseen for affixing the CE Marking. Where equipment cannot be commercially procured with CE marking, ESO contractually requires the manufacturer (e.g., the 4MOST Consortium) to prove the conformity of that equipment or parts thereof (sub-systems, components) with the corresponding relevant provisions.

EU law and ESO Safety Policy are in line with each other given that for the assessment of conformity, the ESO Policy essentially relies on the EU New Approach, recognising the presumption of conformity for any equipment built, upgraded and/or substantially modified against European standards identified as "Harmonised Standards." The harmonised standards are prepared under mandate from the CEN (the European Committee for Standardisation) to support one or more Directives, which have been published in the Official Journal of the European Union (referenced on the New Approach website http://www.newapproach.org).

Related to safety, the 4MOST Consortium needs to demonstrate the conformity of the instrument (and of each of the constituting subsystems) with all the essential safety requirements from the relevant EU Directives and with the ESO Safety Policy. The safety assessment must be completed in advance, i.e. well before the transfer of instrument's responsibility to ESO site in Paranal.

Before commissioning the 4MOST Consortium has to collect all safety relevant information referring to installation, commissioning and operation and make this set of documents available to ESO as a single source called "Safety File". This is an ESO specific requirement to provide the operations staff at the observatory with quick access to all safety

relevant information.

The 4MOST Instrument must comply with the provisions of the applicable New Approach directives, as well as with the other national safety legislation at the moment it is "put into service" – and delivering an instrument to ESO qualifies as such (see Section 3.3).

The 4MOST Consortium shall be ready to deliver a "Technical Construction File". This set of documents contains the technical information describing the instrument as well as all information demonstrating how 4MOST meets the essential safety requirements of the relevant EU Directives, and the signed Declaration of Conformity, i.e. the final document listing the applicable EU Directives and declaring in what way the conformity with the essential safety requirements is achieved (e.g., by the use of Harmonised Standards).

Since each partner in the consortium is responsible for demonstrating the safety of the subsystem they are producing, 4MOST Project Office will also request partners to sign an individual Declaration of Conformity for each subsystem, before the subsystem is delivered to the AIP for the integration phase. A safety compliance report is used for any identified hazard and associated mitigation in order to describe and demonstrate the implementation and completion of the curative measures, and thereby to validate the residual risk declared in the final version of the hazard analysis.

All results from the conformity assessment (reports, tests, declarations, certificates, etc.) are collected in the Technical Construction File together with full as-built documentation to be able to demonstrate conformity with the declared requirements in accordance with all applicable EU Directives. Any change in the supporting documentation, which affects the validity of the Declaration of Conformity has to be duly documented.

The 4MOST Technical Construction File will be kept at the AIP for ten years after the transfer of ownership to ESO, as required by the EU legislation (notably by the Machinery Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006).

3.2 The 4MOST Safety Assessment Process

In order to demonstrate compliance of the 4MOST Instrument with all applicable safety requirements (from EU Safety Legislation, as well as from the ESO Safety Policy) the 4MOST Consortium must complete a number of tasks, the advancement of which is checked at each project review until full completion.

At an early stage each partner responsible for a given 4MOST subsystem (and AIP for 4MOST System) must identify all Essential Health and Safety Requirements (EHSRs) from the relevant EU Directives that apply to the specific 4MOST subsystem (or to the 4MOST System respectively).

In order to do so, the partner has to prepare a Preliminary Hazard List (PHL) for the specific subsystem (i.e. the list of identified hazards that are relevant for the subsystem and its interface to the system). The list also specifies at which phase of the project the hazard will be applicable. Once the PHL has been made, the partners will proceed to perform the Preliminary Hazard Analysis (PHA) for the 4MOST subsystem they are responsible for. The main objective of the PHA is to classify the relevance of the identified hazards for the subsystem in terms of their impact and likelihood. The process is iterated several times until the final document (Hazard Analysis, HA) is produced, which demonstrates that the subsystem design satisfies all contractual safety requirements, insofar as all identified hazards and risks associated with the design of the equipment are adequately mitigated.

For each hazard identified in the HA, the partner responsible for the design and manufacturing of the subsystem, is required to take steps to mitigate its risk, and whenever possible to completely eliminate the hazard by a convenient design (safe by design approach).

To properly document the adopted measures to mitigate the corresponding risks, the manager of a given subsystem has to provide the "List of Relevant Safety Provisions", which is based on the results of the PHL. This consists of all the applicable EU Directives and also contains the list of the Harmonised Standards adopted to meet the EHSRs set out in the EU Directives. The selection of Harmonized Standards depends on the product family used in the individual subsystems.

Harmonised Standards can be used to demonstrate that the design of a given subsystem complies with all relevant EU safety legislation. As such, the use of the Harmonised Standards is not compulsory but it can be beneficial for the manufacturer who by using them can claim the "presumption of conformity". In case partners of the 4MOST Consortium choose not to make use of the Harmonised Standards, they still have the legal and contractual obligation to prove that the subsystem (or part of it) is safe and fulfills all safety requirements.

3.3 Applicable EU Directives and Standards

In addition to ESO technical and safety requirements, the design and manufacturing of the 4MOST System, as well as of each constituent subsystem (or, as required, part of a subsystem), shall comply with the EHSRs from the applicable EU Directives.[2] The applicability of a given EU Directive, either for the 4MOST System or for any of the subsystems, is decided by the partner responsible for the design of the unit by first assessing the scope of the Directive.

As an example, by using the generic definition of "machinery" that is given in the Article 2(a) of the Machinery Directive (2006/42/EC)[3], the 4MOST Instrument can indeed be considered as "*an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application.*" Therefore the Machinery Directive applies to the 4MOST instrument.

The list of the EHSRs is given in the Annex I of the Machinery Directive and in the commonly used approach the Harmonised Standards falling under the scope of the directive shall provide the means to assess the presumption of conformity with the EHSRs.

The Machinery Directive explicitly requires to perform a hazard analysis / risk assessment. In 4MOST this is done both at system level and for each subsystem: the responsible partner for each constituent unit is requested to perform an independent hazard analysis for the subsystem. This means that a 4MOST partner dealing with a given subsystem is also responsible for assessing its safety by fulfilling the EHSRs. The principle is true for the Machinery Directive but also applies to any other relevant EU Directive (such as the Low Voltage Directive 2014/35/EC or the EMC Directive 2014/30/EC).

The EMC Directive states the requirements to ensure that the electromagnetic disturbance generated by the equipment does not exceed a level allowing radio communication to operate and that the instrument has an adequate level of electromagnetic immunity for which 4MOST can operate as intended. ESO additional EMC requirements for the design of the electric and electronic equipment are contained in the ESO Electrical and Electronic Design document.[4]

At the system level, 4MOST electrical safety is checked by compliance with the EN 60204-1, "Safety of machinery – Electrical equipment of the machines – Part 1: General requirements" and by implementing the additional requirements and guidelines that are given in ESO Electrical and Electronic Design.[4] As a practical working tool, a check list based on EN 60204-1 is provided as basis for proof of compliance of the safety of all electrical equipment (including functions such as control) of the 4MOST instrument. This tool is used by ESO at the Preliminary Acceptance Europe (PAE) to draw-up the ESO requirement verification report.

3.4 Conclusions

The paper presents the quality and safety approach that are implemented in the 4MOST project.

Based on ISO 9001 Quality management system, the project has defined and progressively implemented a structured approach for product assurance in order to improve the quality of technical documentation and produced hardware, while taking care of the safety aspects at the same time. In the most general case, the safety aspects are dealt with by making the design of each subsystem compliant with all requirements from the EU Directives and ESO Safety Policy.

The consortium adopts a rigorous quality control mechanism based on guidelines for configuration management that are given in ISO 10007. The approach relies on a standard change control procedure for the traceability. This is complemented by inspection, review and test to ensure that the 4MOST facility will meet all requirements that are placed upon it.

The principles underlined at the beginning by 4MOST Product Assurance are now transposed into requirements for the manufacturing. This is a reactive process in which the consortium identifies failures at an early stage. As the cost of

detecting and removing a fault is inversely proportional to the stage at which it is detected this is clearly an issue of the outmost importance.

We gratefully acknowledge the financial support of the German Federal Ministry of Education and Research (BMBF) through the Verbundforschung (grant no. 05A14BA2 and 05A17BA3).

REFERENCES

[1] ISO 10007:2017 Quality management - Guidelines for configuration management
[2] Rupprecht, G., Muckle, C. and Geeraert, P., "Safety Conformity Assessment Procedure," ESO Document SAF-GEN-MAN-3444, Version 5 (2015).
[3] European Commission, "Guide to application of the Machinery Directive 2006/42/EC, " Edition 2.1 (July 2017)
[4] van Kesteren, A., Lucuix, C., and Hechenblaikner, G., “Electrical and Electronic Design Standards,” ESO Document ESO-044295, Version 4 (2016)