8 Systems engineering

Gie Han Tan

2000-12-07

8.1 Introduction

This chapter addresses the systems engineering efforts in the ALMA project. The accompanying tasks are under the responsibility of the ALMA Systems Engineering Group (ASEG).
Section 8.2 gives a concise summary of the concept of systems engineering and the areas which systems engineering will focus on in the ALMA project.
A major task for which the ASEG is responsible is the top-level system design of ALMA and this topic is summarized in section 8.3.
Sections 8.4 through 8.13 present more details on various important systems engineering management tasks and essential system wide requirements applicable to the ALMA project.

8.2 Survey of the systems engineering discipline

Complex systems like the Atacama Large Millimeter Array can only be created through the combined effort of many people. For this very reason, controlling the definition, design, production, integration, verification and validation of the instrument involves a major engineering effort as well as a technical managerial part. This is even strengthened by the fact that the people contributing to the project are geographically scattered among three, and when Japan joins four, different continents around the world.
Furthermore it is necessary that for all given life cycles of the instrument it be assured that the requirements of the astronomical users are also fulfilled. Given this situation the need for a separate, systems engineering, group who takes care of these issues is probably obvious on first sight.

However, this is different from past other radio astronomical projects and therefore details about the existence of this ALMA Systems Engineering Group (ASEG) are discussed in this section.
The process of interaction between the ALMA Systems Engineering Group and other groups within the project is also described since this is crucial for performing their tasks in an effective way.

8.2.1 Raison d'être of ASEG

In “The Engineering Design of Systems: Models and Methods” various definitions of what systems engineering is about are summarized [1]. Of these definitions, probably the most concrete one applicable with the ALMA project in mind was given in MIL-STD 499A:

> Systems engineering is the application of scientific and engineering efforts to:
> 1. Transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, analysis, design, test and evaluation.
> 2. Integrate related technical parameters and ensure compatibility of all related, functional and program interfaces in a manner that optimizes the total system definition and design.
> 3. Integrate reliability, maintainability, safety, survivability, human and other such factors into the total technical engineering effort to meet cost, schedule and technical performance objectives.

In previous radio astronomy projects so far, the tasks described by this definition were often distributed over the other participating disciplines. With the inherent risk that systems engineering issues would not be addressed properly resulting in less optimal technical solutions and/or the waste of resources.

Primary reasons to define a separate group responsible for systems engineering in the ALMA project are the following:

- The technical complexity of the ALMA instrument to be realized with limited resources and on a relatively short time scale need careful selection of the proper design technology for sub-systems:
  - A number of crucial technologies planned to be used in the design have never been demonstrated before at all or at least not at such a large scale. Trade-offs need to be made between science driven performance parameters like sensitivity and stability, and e.g. manufacturability and reliability.
  - Due to new technological capabilities sub-system functions can now be realized in more ways then in the past. Functions that were traditionally realized in hardware are now feasible in software and choices have to be made which approach is the most effective.
- ALMA will be a general-purpose instrument that should serve a versatile suite of different science requirements. A well-defined body must govern the flow-down of all these requirements to an appropriate system.
- The distributed nature of the project in terms of both geography as well as different, independent organizations needs a group that is responsible for achieving engineering commonality and interfacing in especially the design and construction phases of the project.

---

[1] Buede, D.M., “The Engineering Design of Systems: Models and Methods”, pp. 9. Wiley & Sons Inc., 2000.

- The extent and complexity of the instrument requires that its reliability and maintainability be addressed already during the design & development phase in a complete and objective way to obtain a system having high availability for reasonable operating costs.

From the definition of systems engineering it becomes obvious that its tasks are related to probably every other activity in the project. Project members at all levels should be aware of this fact, the interaction between them and the systems engineering group is essential for success.

Finally, from the given definition it is also clear that systems engineering is not equivalent to system design, an often made misconception. But system design, the creative process of conceiving a solution for a certain requirement, is part of system engineering.

8.2.2 Working methodology and interaction with other groups

As depicted in figure 8.1, there will be a strong interaction between the ALMA project management, the project scientists and the ASEG. Within this ALMA management entity these three groups are responsible for the following areas:

- ALMA project management: resources and planning
- Project scientists: representation of astronomical users, defining science requirements
- ALMA Systems Engineering Group: engineering discipline

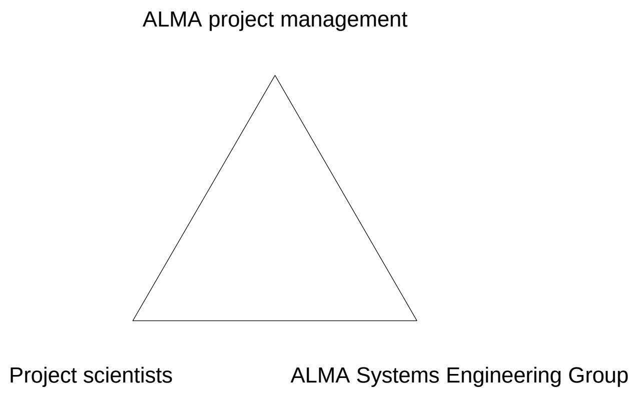

Figure 8.1, schematic representation of interaction within ALMA management team

The common main objective of the three groups is to optimally fulfill the scientific needs within the agreed constraints of budget and time.
The ALMA management is at the top of the triangle to represent its overall responsibility for the project.

The ASEG acts as the interface for engineering and technical issues between the project management and the technical groups contributing to the ALMA project.

Due to the relatively small size of the ASEG, involvement of specialist engineers from other disciplines is absolutely necessary to support the tasks of the ASEG. It is important that management and the specialist engineers are aware of this fact and that appropriate priority is given and time is allocated to these advisory tasks.

8.3 System design overview

Updated version of overview in MMA project book by Dick Thompson will be added here.

8.4 Product tree

The Product Tree (PT) is a top-down approach dividing the ALMA system systematically into successive levels of partial hardware and software based on the functions identified.

The products to be identified in the PT will as a minimum include:

- Items submitted to configuration control
- Items that are the subject of a project specification
- Items that are referred to in an interface control document

The primary aim of the product tree is to act as a tool in the systems engineering management of the project. It is a representation of which components the system consists off. Among others, it will improve the quality of keeping track of product specifications in a systematic way and the proper control of interfaces.

All items in the PT are partitioned on the basis of function, in some cases especially at the lower levels of the PT, an item might coincide with a physical assembly.

Since the PT is purely product oriented, activities that are not product oriented are not included in the PT and only appear in the Work Breakdown Structure. Typical examples are process-related tasks like project management and systems engineering.

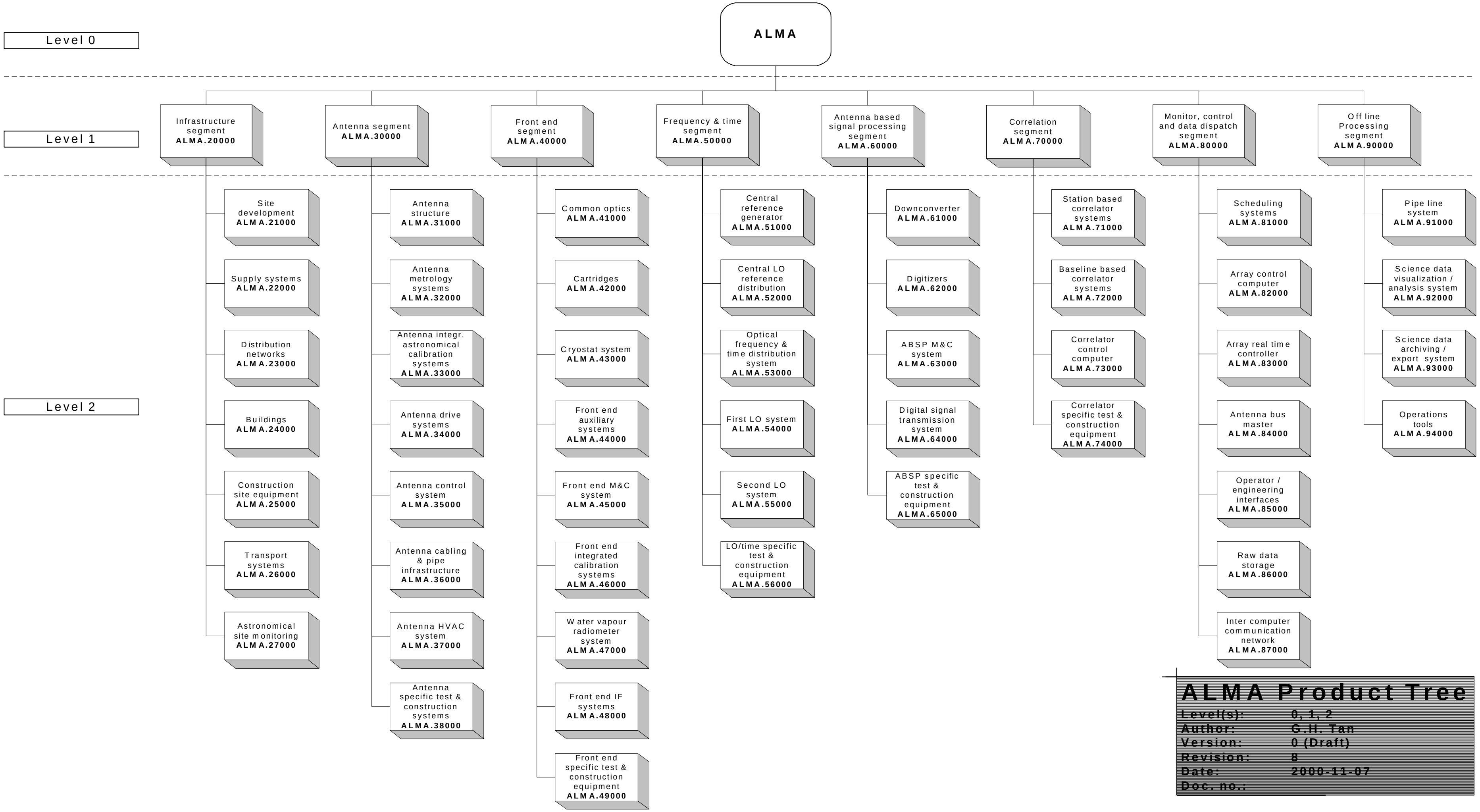

Figure 8.2, ALMA Product Tree / levels 0, 1 (approved by AEC) and 2 (preliminary)

Each Integrated Product Team will complete the PT at his level for the products under his responsibility. An exception is made for level 1 of the PT, which is the responsibility of the ALMA Systems Engineering Group.
The PT will be formally approved by the ALMA Executive Committee and will be under configuration control by the ALMA Configuration Control Board.

Figure 8.2 shows a preliminary version of the ALMA product tree. Level 1 of the PT is fixed and approved by the AEC, while level 2 needs to be completed in consultation with the responsible US Division Heads and European Team managers.

A full version of the ALMA product tree is available in a separate document "ALMA Product Tree" (in preparation).

8.5 Configuration control

What is under configuration and process description of configuration control to be included after consultation with AEC.

8.6 Quality management

Quality needs special care for a complex, hi-tech instrument like ALMA during its whole life cycle. Since this project book addresses phase 2 of the ALMA project, the quality management described in this chapter focuses on the development and production phases of the instrument.

It is anticipated that the required level of quality in the ALMA project must be obtained by using the following methods:

- Inspection of products
- Well described and controlled processes for, among others, Design & Development, construction and integration activities
- Use of standards
- Concurrent engineering

The traditional process of evaluation and inspection of products is definitely needed, but as the only measure not efficient to achieve the high level of quality as is needed in the ALMA project. Using this method only will for example result in the detection of defects, but does not identify the causes of these defects in an early stage. The repair of these defects will result in extra costs and delays in the project; a situation to be avoided by appropriate quality management measures.

A specific aspect of the ALMA project is the location where a major part of the instrument will be built, a site at more then 5000 m altitude having a hostile

environment for humans. Failures at this location can result in serious injuries or even death.
To avoid this problem, also here pro-active measures are necessary.

Based on industry experience, where it was also concluded that more inspection of products does not efficiently lead to better products, it is advocated to improve the definition and control of processes that play a role in the ALMA project. In industry this has been formalized under the well-known ISO 9000 standards.
According to the spirit of the ISO 9000 standards, a similar approach will be applied for the ALMA project. Several examples applicable to the ALMA project are:

- A well defined Design & Development process, including:
  - Clearly defined D&D phases
  - Proper review, based on well known terms, after every D&D phase
- Unambiguous and complete documentation, obtained through:
  - An ALMA document management plan
  - Use of templates and standard forms
  - The use of modern PDM tools to assure proper control of documentation

Improved process control will also be a major benefit to improve safety. Already in advance, when a process is analyzed and defined, possible risks are identified and solutions can be incorporated in the process to mitigate them to an acceptable, clearly defined level.

Where feasible the use of standards, either recognized general (e.g. ISO, IEEE) or project specific, should be used. The benefit of using standards is that these are well proven, widely known and accepted by a common group, thereby reducing the possibilities of making errors and minimizing the effort to get familiar with a certain topic.

Evaluation and inspection of products must already be addressed in the early design phase in the development of a product. Appropriate test plans must be established and the product design should be such that they can be easily and completely tested in the production phase.

From the description given above it will be clear that obtaining a proper level of quality is not only a systems engineering issue but can only be successful if there is commitment to it throughout the whole project organization.

8.7 Hardware design and production processes

A document providing a formal guideline for the hardware development and production process to be applied in the ALMA project is in preparation.
It has been prepared to standardize the hardware development and production process throughout the project and thereby assisting in:

- Creation of a common view on these processes
- Improvement of product quality
- Improvement of project control

Special attention is given to a methodology to track achieved performance during the development process against required product specifications.

It is recommended that this guideline is mandatory for the development and production of all hardware products that are under configuration control. Exceptions to this rule can be made after consultation with and approval by the ALMA Systems Engineering Group (ASEG).
It is encouraged to use this guideline also for the development and consequent production for other products that will be used in the ALMA system.

Due to the current status of the ALMA project a number of product development tasks have already reached the Preliminary Design Review milestone. In those situations the information given in the document with regard to objectives and deliverables at every phase can be used as a checklist if previous phases and milestones are completed according to this guideline.

Figure 8.3 shows a product development model, consisting of 7 phases with accompanying review milestones, which is applicable for hardware parts in the ALMA project. It is tailored to the needs of the project where high-tech products are developed and manufactured in large quantities.
Depending on the nature of the product, a/o technology maturity and production quantity, extra phases can be added or phases can be merged. For these specific situations where a different development model is proposed, the ASEG should be consulted and approval from this group is necessary to apply a modified product development model.
Note that the development model shown in figure 8.3 is represented as a classic linear model. The interaction between design, production and integration activities is not depicted explicitly, but should be taken into account.

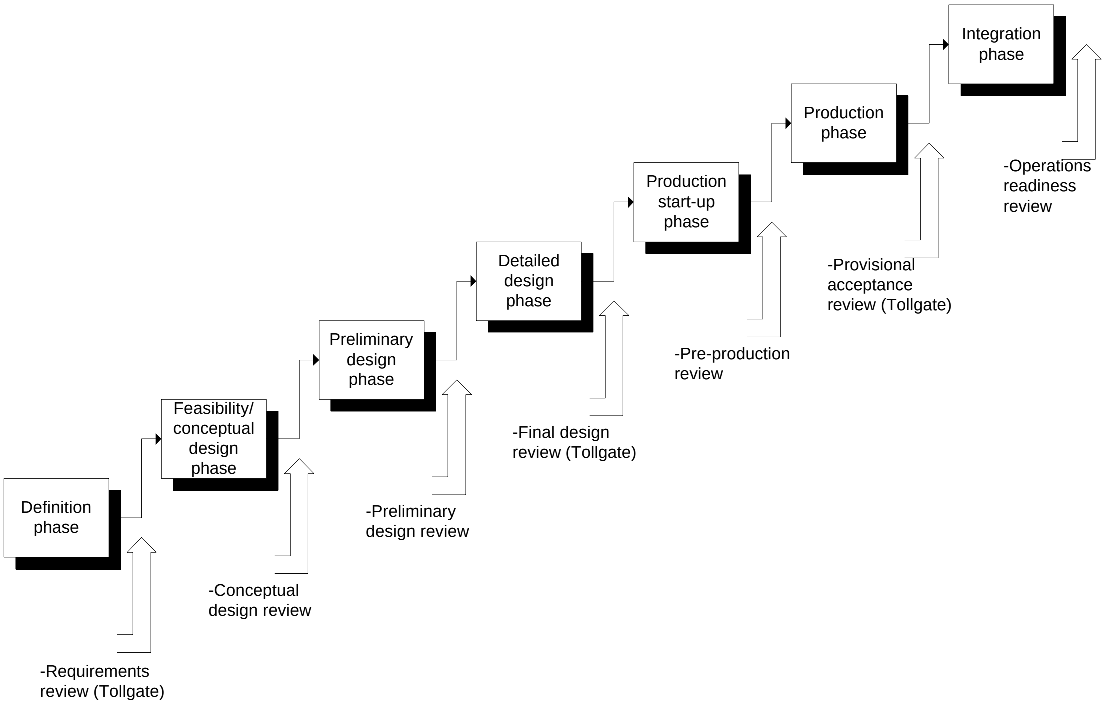

Figure 8.3, model of ALMA hardware development and production process

Note that some of the reviews in the ALMA development model have the status of tollgate. While a successful review milestone implies the formal completion of the previous phase, in addition at a tollgate explicit approval is given to commence with the next phase.

8.8 Software development process

Summary of "SE practices Software …." Document by Chiozzi et al. To be added

8.9 Design standards

A set of common engineering rules that are in principle mandatory for the whole ALMA system will be defined. The purpose of these system wide requirements is:

- To assure integrity of sub-systems and complete ALMA system
- Effective design, construction and operation of the ALMA system
- To improve quality of the ALMA system

These system wide requirements will be described in a separate document and will address at least the following items:

- EMC, the IEC CSIPR EMC standards will be taken as the basis and adapted to the needs of the project. For example, additional requirements for emitted EM interference based on ITU-R RA 769-1 are foreseen due to the outstanding sensitivity of ALMA
- Safety
- Packaging, a modular approach is advocated that makes it possible to have Line Replaceable Units (LRU) that enable a/o efficient operation of the instrument
- Power distribution
- Environmental
- Preferred component lists, e.g. for embedded processor families

The information in this document will be to a large extent based on international standards from organizations like IEC and IEEE. Considerable use is made of the experience gathered in MIL-STD-2036A, VLT Electronic Design Specification and this is tailored to the specific needs of the ALMA system.

8.10 System availability and reliability

ALMA system availability is defined as the ability of the instrument to perform the required function under given conditions over a given time interval, assuming that the required external resources are provided.

So far, no quantitative requirement for availability has been determined for ALMA. It is planned to establish a baseline figure for ALMA on the basis of experience with existing radio astronomical instruments with similar technical and operational properties. Examples are the Very Large Array (VLA), Very Long Baseline Array (VLBA) and the Westerbork Synthesis Radio Telescope (WSRT).
This baseline availability figure will be used as a target for the ALMA system to be designed.

Various efforts are planned to assure that the required availability will be achieved. At least, the following tasks are foreseen:

- A uniform and objective method of reliability prediction based on MIL-STD-217F for electronic components and The Handbook of Reliability Prediction Procedures for Mechanical Equipment (NSWC-94/L07) is selected. These standards will be used to predict the reliability in terms of MTBF for every product in the ALMA system
- Failure Mode and Effects and Criticality Analysis (FMEA) will be carried out
- Fault Tree Analysis (FTA) will be performed
- The results of all three mentioned analysis methods will be fed back interactively to the design process to optimize the availability of the instrument

8.11 Document management

It is recognized that documentation will play a vital role in the ALMA project. A/o documentation is the primary method to communicate information within the project organization and product design documentation is the only way, which defines the ALMA instrument and the sub-systems during all phases until final completion.

The ASEG will focus on and bear the responsibility for the management of engineering documents related to products that make up the ALMA instrument. However it is expected that the document management method will be general enough that other document types can be included without problem.

Important ingredients to the ALMA document management plan will be the following:

- Engineering document numbering system will be based on the ALMA Product Tree. This approach ensures a consistent and long lasting way of identifying product related documentation
- Archived documents, the originals, are only stored in electronic form. On paper, only copies of these original electronic documents are distributed when needed
- Submission, distribution and retrieval of documents is primarily done via Internet
- Different types of approval processes will be defined dependent on the type of document
- Mandatory standard file formats for general text documents will be introduced for the project. It is expected that for editable documents this will be Microsoft Office based file formats. For documents issued once only, storage in Adobe PDF format is advocated.
- For technical product documentation it is recognized that standardizing to a limited set of file formats is not feasible due to the large variety of CAD/CAE tools used across the project.
- Electronic distribution of document copies is primarily done in Adobe PDF format.
- The use of a modern Product Data Management (PDM) tool is essential in an efficient management of the project documentation. This tool must be able to handle the geographically distributed storage of documents into a single virtual database, assist in the approval and revision processes of documents, enable distribution and access of documents with proper security control

The complete ALMA document management plan will be described in a separate document.

8.12 Logistic and maintenance engineering

A maintenance philosophy for the operational phase of the instrument will be documented in a separate plan.
Already during the design of a product a maintenance requirements analysis must be carried out. This analysis will address at least:

- Mean Time Between Maintenance (MTBM) analysis
- Mean Time To Repair (MTTR) prediction
- Spare parts needs
- Necessary maintenance personnel skills and quantity
- Maintenance equipment

8.13 System safety

Based on international, as well as appropriate national standards, Chilean, European and U.S., a safety plan and system wide safety requirements will be established. Primary targets of the safety plan and system wide safety requirements is to preclude or limit hazards to personnel and equipment and to comply with applicable laws where needed during all life cycles of the instrument.
Safety plan and system wide safety requirements will be used as input for the design activity for all products.