A Framework for Dependability and Completeness in Requirements Engineering

Marina M.N. Zenun  
Product Integrity Dept. - Embraer S.A.  
marina.zenun@embraer.com.br

Geilson Loureiro  
Aeronautics and Mechanical Dept. - ITA  
geilson@lit.inpe.br

Abstract

This paper aims to present a framework for Requirements Engineering (RE) in the development of civil aircraft, in order to achieve dependability and completeness, in the context of aircraft industry. In this industry, dependability and completeness are crucial to the success of product development. A missing requirement can mean a missing attribute in complex products, and a missing requirement can mean a major source of implementation defects in embedded software. The completeness of requirements is such a need, and at the same time it is a huge challenge. In order to improve the requirements elicitation processes, in a manner that all requirements receive the same level of attention, this paper proposes a framework which considers the entire system lifecycle, all processes, and people involved. The proposed framework shall be used to achieve dependability and completeness, starting at the early stages of product development.

1. Introduction

This paper presents a framework for Requirements Engineering (RE) to be used in the development of civil aircraft in order to achieve dependability and completeness, in the context of aircraft industry.

The completeness of requirements is such a need, both in sense of whether the requirements’ set contains all requirements and whether all requirements are completely specified [1]. A missing requirement results in a missing attribute in complex products [2], and a missing requirement can mean a major source of implementation defects in embedded software [3]. Accidents and major losses involving computers are usually the result of incompleteness or other flaws in the software, not coding errors [3]. Then, safety (one of the attributes of dependability) owns a straight correlation to completeness in RE. If the intent is to develop a system under safety perspective, the developers shall pursue completeness in RE.

Due to the relevance of this subject, this work applies an exploratory research involving a literature search to present the concepts of dependability, completeness, and completeness in development of civil aircraft. This paper also presents a framework to increase the likelihood of achieving dependability and completeness. The proposed framework shall be used starting at the early stages of product development. Following the framework, a complete set of requirements could be produced. However, a complete requirement in a sense whether the requirement is completely written is not covered by this study.

2. Background

Completeness is thought when it lacks nothing, or requires nothing more in order to be fit for use or serve its intended purpose [4]. All needs are covered by the set of requirements [5], this means that there are no other requirements necessary for the set of related requirements to fulfill their collective purpose or mission of defining what a given system must be and do, with respect to some specified context [4].

So, if completeness is defined in terms of fitness for purpose, and if who decides the needs, goals, and/or mission of the system are the stakeholders [4], then a complete set of stakeholders is the first condition to produce a complete set of requirements. A complete set of stakeholders is also required to validate a complete set of requirements. For a complete set of stakeholders, the system in its environment must be examined considering the entire lifecycle to determine who are the stakeholders [4].

While completeness is defined as a complete set of requirements, dependability is the system property that integrates such attributes as reliability, availability, safety, security, survivability, maintainability [6].
So, if the set of requirements is complete, requirements which represent reliability, availability, safety, security, survivability, maintainability should be produced within this complete set.

Considering that dependability is a subset of a complete set of requirements and based on the concepts presented in this section, this paper presents a framework in Section 3.

3. Framework for Dependability and Completeness in RE

The framework itself is under development and it was previously presented in the 19th ISPE International Conference on Concurrent Engineering – CE2012 [7]. The framework proposes a structured process to be followed in the development of complex products, more specifically in the context of aircraft industry. Following the framework, analysis shall be performed for stakeholders, system and architecture for product and organization. These analyses shall be made from layer i (higher level requirements) to layer n (lower level requirements). These analyses will result in elements, attributes and requirements of product and organization.

Framework steps and items to be identified are listed in the Table 1. In order to illustrate how the framework fits for addressing dependability and completeness in RE, this paper presents an example of the framework application. A development of Ground-Based Augmentation Systems – GBAS installed in a Transport Category Aircraft was elected as a complex product to be used as an example. Framework steps and example implementation are presented in the next paragraphs.

### Table 1 Framework steps and item to be identified

<table>
<thead>
<tr>
<th>Steps</th>
<th>Items to be identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Mission</td>
</tr>
<tr>
<td>Step 2</td>
<td>Product lifecycle process</td>
</tr>
<tr>
<td>Step 3</td>
<td>Product scenario</td>
</tr>
<tr>
<td></td>
<td>Organization scenario</td>
</tr>
<tr>
<td>Step 4</td>
<td>System</td>
</tr>
<tr>
<td>Step 5</td>
<td>Product scenario</td>
</tr>
<tr>
<td></td>
<td>Organization scenario</td>
</tr>
<tr>
<td>Step 6</td>
<td>Attributes for elements</td>
</tr>
<tr>
<td></td>
<td>Product scenario</td>
</tr>
<tr>
<td></td>
<td>Organization scenario</td>
</tr>
<tr>
<td>Step 7</td>
<td>Write requirements</td>
</tr>
</tbody>
</table>

**Step 1:** Identify the product mission. The mission of an Aircraft (A/C) with GBAS System is defined as: To provide capabilities to the A/C to make a landing in airports with GBAS Ground Subsystem, under coverage of GNSS Satellites.

**Step 2:** Identify product entire lifecycle processes. The lifecycle processes of an A/C with GBAS System highlight the processes to be executed by the organizations. These processes are: Conception, Development, Production, Integration, Certification, Operation, Maintenance and Discard [7].

**Step 3:** Identify product stakeholders and organization stakeholders, and their concerns for each product life cycle process scenario. Figure 1 shows stakeholders and their concerns for A/C with GBAS in operation and Figure 2 highlights organization stakeholders and their concerns for A/C with GBAS Operation Organization analysis scenario. Concerns such safety, availability, and reliability (attributes of dependability) appear for stakeholders in the Fig. 1. The term safety also appears in the stakeholder organization scenario (Fig. 2).

**Step 4:** Identify system context for product at each life cycle process scenario and for organization at each lifecycle process scenario within the scope of the development effort.

![Fig. 1 Stakeholders and their concerns for Product in Operation analysis scenario](image1)

![Fig. 2 Stakeholders and their concerns for “Operation Organization” analysis scenario](image2)
Figure 3 shows system context for A/C with GBAS system in operation and Figure 4 shows system context for GBAS Operational Organization in operation. Fig. 3 identifies the elements in the environment of the system. The environment contains the elements outside the system function scope and that exchanges material, information and energy [8]. In this example, the elements identified are ATC, GNSS, and GBAS ground station. They exchange material and information with the system. Faults, errors, and/or failures of these elements prevent correct flows of material and information to the system. These elements represent threats to the system, they are sources of hazardous. Risk analysis shall be performed on each identified potential hazard and exception handling functions shall also be identified at this stage [8]. These analyses will provide subject to write safety requirements.

Step 6: Identify attributes for elements of product and organization. Table 2 lists, in first line, an attribute (parameter) derived from product stakeholders’ analysis for “Product in Operation”, and, in the second line, an attribute (parameter) derived from organization stakeholders’ analysis for “Organization in Operation”.

Table 2: Product stakeholders, their concerns and attributes for the “Product in Operation” analysis scenario

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Concerns</th>
<th>Attributes (Parameters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilots</td>
<td>Reliability</td>
<td>no lower than 99%</td>
</tr>
<tr>
<td>ATC</td>
<td>Safety</td>
<td>Extremely small rate of A/C accidents</td>
</tr>
</tbody>
</table>

Step 7: Write requirements. The final step of the framework is to write requirements. The requirements are derived from the Table 2, by adding, for this example, the three columns: <stakeholders>, <concerns>, and <attributes>. For example, a stakeholder requirement which states reliability could be derived from the pilots concerns (Table 2): The
pilots shall be able to land the A/C using GBAS at a minimum rate of 99 times per 100 flights.

At the end of those 7 steps, the first layer of the requirements set will be accomplished for the Operational scenario. It is necessary to repeat Step 3, 4, 5, 6 and 7 (which are highlighted in Table 1) to decompose requirements for the layers below.

Steps from 3 to 7 shall be applied for other lifecycle phases rather than operation.

8. Preliminary Results

The framework was applied for Operational scenario. The experience in its application was beneficial and provided a complete understanding of all elements of this phase, considering simultaneously product and organization. This assumption improves the probability of all kind of requirements for this phase will be elicited.

It was observed attributes of dependability, such as safety, availability, and reliability derived from stakeholders’ analysis. Threats to the system for operation were also identified through system and architecture analysis. Safety requirements may be derived from the risk analyses considering the identified threats. Other dependability attributes probably will be derived in other lifecycle processes analysis. For example, maintainability will be derived when maintenance scenario is analyzed.

9. Conclusions and Future Work

This paper has presented a framework for dependability and completeness in RE to be used in the development of civil aircraft, in the context of aircraft industry.

A complete pilot study is required to confirm the method validation. Then, future steps are: the framework will be populated for other phases rather than operation. A complete scenario will be derived from the higher level (layer i) to the lower level (layer n).

After a complete pilot study, the advantages and disadvantages will be evaluated to confirm the framework applicability. Nevertheless, the first results indicate that this work is on the right track. In the next future, the framework could be used as a method for requirements elicitation in order to increase the likelihood of achieving dependability and completeness, in the development of civil aircraft. It could also be very useful in the development of other complex products.

10. References


11. Acknowledgments

The authors acknowledge Embraer S.A. (www.embraer.com.br) and ITA (www.ita.br) by the opportunity for investing in technical researches and personal development. The authors also acknowledge the support granted by CAPES (www.capes.gov.br), CNPq (www.cnpq.br) and FAPESP (www.fapesp.br), Brazilian research funding agencies.