Towards Modeling Civil Aviation Safety Legislations

Eduardo R. López Ruiz[1] and Michel Lemoine[1]

[1]ONERA. 2, avenue Edouard Belin,
Toulouse, France. 31400
{eduardo.lopez-ruiz, michel.lemoine}@onera.fr

Abstract. Building on the work of the EDEMOI methodology, this paper proposes a twofold expansion of this methodology consisting in: (1) broadening its scope to include aviation safety legislations and (2) extending its usability to detect regression originating from regulatory amendments. Accordingly, this paper analyses the differences between safety and security legislations in civil aviation, develops on their similarities and proposes a tailored graphical model apposite for safety legislations. Finally, this paper defines the case-study in which the proposed graphical model will be initially implemented.

Keywords: Graphical specification, legislations.

1 Introduction

Aeronautics is an industry that is highly aware of the need to incorporate human factors science and engineering into its different domains to further improve safety and security. This includes the domain of printed materials. Accordingly, international aviation organizations, research centers and some aviation authorities have conducted human factor studies aimed at characterizing and improving the semiotic (i.e. the semantics, syntactics and pragmatics), visual and structural quality of their different printed materials[1] [1]. However, until recently, these studies and standards have mostly targeted the clarity, readability and legibility of the printed materials but not their *embedded logic*.

Yet, operational feedbacks have hinted that the effectiveness of these printed texts also depends on logical traits such as: their *consistency* and their *robustness*. This is of great consequence since (analogously with safety-critical software) these traits ensure that the benchmark legislation being enforced is not inherently rendered ineffective due to contradictory policies (either by themselves or globally), and that it exhaustively covers all the possible scenarios within its domain of application.

Consequently (and within the backdrop of September 11th, 2001), a group of French universities and research laboratories sought to enhance the rulemaking process used by civil aviation organizations and authorities, to create and validate *security* legislations. Their proposal was to incorporate simulation and counterexample checking tools into the legislations' validation phase, to better ensure

[1] Support material, training material, procedure manuals and checklists, etc.

their embedded logic. To this end, they propounded the utilization of formal methods to specify and validate aeronautical security-related requirements.

In fact, conscious of the necessities of civil aviation authorities, they proposed a specially conceived specification methodology that took into account the intricacies of formal notations and the familiarity needed for their comprehension (See Figure 1).

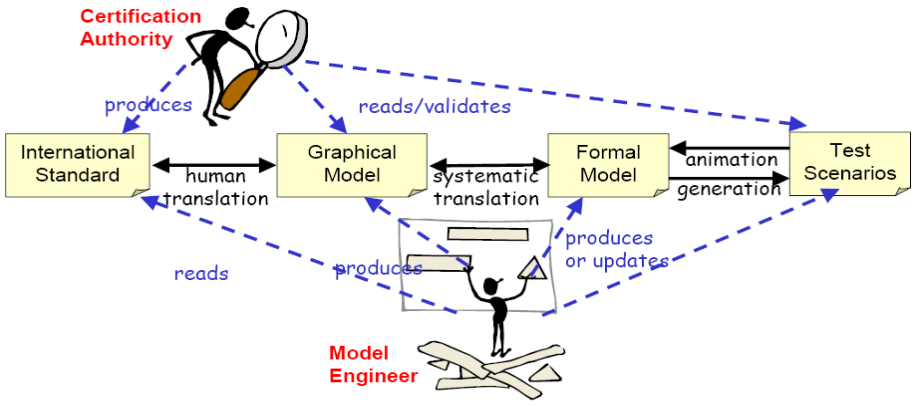

Fig. 1. In the first step of the EDEMOI approach, a *Model Engineer* extracts the security goals imposed by an *International Standard* and translates them into a *Graphical Model* that faithfully represents their structure and relations (while reducing the use of inherently ambiguous terms). Once this Graphical Model has been revised and validated by the *Certification Authority*, the *Model Engineer* performs a systematic translation of the Graphical Model to produce an implicitly valid *Formal Model*, which can be later analyzed using *Test Scenarios*.

This methodology, referred to as the EDEMOI methodology, has been implemented to the modeling of both international [2] and European security legislations [3]. In both cases, the analysis of passenger-related security standards was emphasized. These standards were translated into formal models using the B and Z notations and animated [4]. Thanks to this, its appropriateness (i.e. its aptitude to specify and assist in the design and validation of security requirements) has been established.

Still, as civil aviation authorities are concerned with ensuring both the security and the safety of civil aviation, and given that new legislations are evolutions of existing ones (prompting the study of their non-regression), an expansion of the EDEMOI methodology has been proposed. This expansion consists in: (1) broadening its scope to include aviation safety legislations and (2) extending its usability to detect regression originating from regulatory amendments.

Neither one of these two aspects can be considered as a simple, straightforward effort, given that there are fundamental differences between security and safety legislations. Therefore, their realization will entail a change in the techniques proposed within the EDEMOI methodology, to focus on the specificities of safety-related requirements. Additionally the study of the non-regressions is an endeavor on its own, based on the use of animation and proof techniques to compare successive versions and detect regressions.

In Section 2 of this paper, the differences between safety and security legislations will be discussed, emphasizing on how the EDEMOI methodology (its methods and tools) can contribute to improving safety legislations. Section 3 will highlight the new role that will be given to the legislations applicability criteria in the modeling of aviation safety legislations. Then, Section 4 shall propose a tailored graphical method apposite for safety requirements, and its use in a future case study to illustrate its benefits. Finally, Section 5 will draw the conclusions and perspectives of this work.

2 The Differences between Security and Safety Legislations

As mentioned previously, the expansion of the EDEMOI methodology has two objectives: firstly, to adapt it for a suitable implementation in the analysis of safety legislations and, secondly, to facilitate the analysis of regression between succeeding versions. In order to achieve the first objective, we need to have a very clear understanding of the differences between safety and security legislations. Furthermore, we need to correctly identify what civil aviation authorities seek in terms of improving safety legislations.

So, the first considerable difference between safety and security legislations is their purpose. That is to say, safety legislations focus on preventing accidental events (detrimental to civil aviation) while security legislations are focused on the prevention of intentional acts (detrimental to aircraft, airport infrastructures, persons, etc). For this reason, their legislative domains are markedly dissimilar in terms of coverage size and participating stakeholders.

Security legislations are implemented within a relatively small and contained domain, covering the airport areas (including off-site security zones), their perimeter and the aircraft's interiors. Conversely, for safety legislations, their corresponding domain is harder to limit, since civil aviation safety is a collaborative contribution of the aircraft's initial and continual airworthiness, its operation and also of navigation and control services. Moreover, the safety requirements for a specified element will vary in function of its geopolitical location and the type of operations it is performing. So, an aircraft that is entering European airspace will “automatically” be subjected to safety obligations that were not applicable the instant before.

Additionally, in terms of legislative evolution, it is primarily safety legislations that need to be more adaptive to the industry's constantly evolving state-of-affairs, helping steer developments instead of contriving their progress. This refers to the fact that, in aeronautics, advancements are the result of a fragile compromise between what is technologically achievable, what is economically profitable and what is cautiously acceptable. For this reason, civil aviation authorities must be careful not to impose unduly or unjustifiable safety requirements, as they might hinder future developments.

Nevertheless, safety and security legislations do have some commonalities. The most important is that they impose their requirements using 'directive statements'. Moreover, their requirements can be classified on the basis of their approach, and are said to be either *objective based* or *prescriptive* requirements. The difference between these approaches is that the first sets targets or goals to be met but provides flexibility

in terms of how they are met; while the second does not offer such flexibility and instead, details how these must be met. However, most requirements cannot be easily classified as either one or the other, but rather as a mix.

For example, a largely *objective based* safety requirement that has been central to the design of commercial aircraft is that (for the aircraft and its subsystems), there must be *an inverse relationship between the probability of a failure and the consequences of said failure*. In other words, the most dangerous failures should have the lowest probability of occurrence, yet it is up to the designer and manufacturers of aircraft (and their subsystems) to come up with ways to ensure this. In contrast, a largely *prescriptive* safety requirement could impose specific design constraints. For instance, authorities impose the number and types of emergency exits required for an airplane (given certain conditions), in order to maximize the probability of its safe evacuation.

Yet, given the intrinsic nature of all **'directive statements',** we are confident that the underlying principle of the EDEMOI methodology (i.e. the use of formal methods to specify and validate their embedded logic) is still valid for civil aviation safety requirements. However, the usefulness of this expansion will be limited to certain domains of safety legislation. Tentatively, to the domains whose legislation is not highly objective based, such as: the operation of aircraft, the provision of air traffic services, aerodrome operation and aircraft airworthiness standards. As was the case in security legislations, a formal specification outside of these domains would be, either irrelevant or particularly ineffectual.

In what concerns regression analysis, we believe that the graphical modeling technique presented in [2] helps facilitate the detection of certain types of regressions independently of their safety or security nature, mainly thanks to the model's tree-like structuring which is rooted from a safety/security property and expands outwards (See Figure 2).

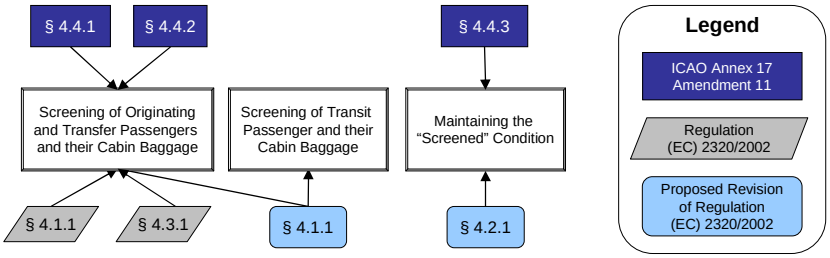

Fig. 2. The "security property" approach to modeling security legislations helps improve the management and traceability of such documents. Consequently, these types of model help detect certain forms of regressions. For instance, international standards such as ICAO's Annex 17 need to be further specified and adapted, before being enacted at a national level. In the case of Europe, this specification came in the form of Regulation (EC) 2320/2002. As illustrated above. The initial version of Regulation (EC) 2320/2002 (symbolized in a parallelogram) did not impose requirements concerning the prevention of unauthorized interference with screened passengers and baggage. However, both its founding text, *ICAO's Annex 17* and its *Proposed Revision* do contain such requirements (rectangle and a rounded-rectangle respectively).

Finally, having established the traits that are the most relevant (to civil aviation authorities) for safety legislations, we consider that a model around the requirements' *applicability criteria* will be an insightful tool for aviation authorities (as will be discussed in Sections 3 and 4).

3 The Applicability Criteria

Applicability criteria are used in legislations to explicitly define the set of elements upon which a set of requirements will be imposed. For example, the following statement (taken from ICAO's Annex VI) explicitly states a condition that is applicable to "All flight crew members…on flight deck duty".

> *ICAO - Annex VI §4.4.4.1 Take-off and landing. **All flight crew members** required to be **on flight deck duty** shall be at their stations.*

Moreover, this condition is only applicable during a particular moment, "[throughout the aircraft's] Take-off and landing [phases]".

Hence, in the case of civil aviation legislations, the applicability criteria will be a general element (e.g. “an aircraft”), an element in a specific state (e.g. "all flight crew members required to be on flight deck duty") or only a state (e.g. "during take-off and landing").

As these criterion and states are at the core of the legislative texts, their clear understanding is of high importance. This is why some legislations provide generic definitions of the elements and states invoked by their applicability criteria. For example, ICAO – Annex VI provides the following definition of a *Flight Crew Member*:

> “*A licensed crew member charged with duties essential to the operation of an aircraft during a flight duty period*”.

At any rate, applicability criteria are a rich source of information. They can be used to deduce the different elements affected by the legislation, their allowed operations and states.

For instance, by combining the definition given for a *flight crew member*, with the requirement §4.4.4.1 (referred to above), we can tentatively deduce that all *required Flight Crew Members* will be in one of the two following opposed states: “*not on flight deck duty*” and “*on flight deck duty*”.

Moreover, we suspect that there is a trigger operation that fires a transition of the flight crew member from the first to the second state (and that, from an implementation perspective, such trigger operation would occur only during the flight crew member's flight duty period. Hence the word *required* in §4.4.4.1).

The EDEMOI methodology used this type of reasoning to build the graphical models which comprised the legislation’s application domain. In this case a "class" *Flight Crew Member* would be proposed, with two Boolean attributes:

"*on_flight_deck_duty*" and *"on_flight_duty_period"*. Similarly, a number of representative operations would be generated to modify these attributes.

Simply, legislations can be regarded as a function which associates a set of applicability criteria to their corresponding set of safety and security requirements. As a result, the applicability criteria are an important constituent of legislative documents, central to their implementation. As such, they are a very familiar concept for civil aviation authorities; and it could be expected that, for this same reason, aviation authorities would be responsive to graphical models founded on these criteria.

In addition, applicability criterion can help understand the underlying justification of a given requirement. In particular in the context of safety requirements, applicability criteria are chosen on the basis that they are criterion relevant to the known (or likely) safety risks. Therefore it seems desirable that a graphical model of the legislation should be able to (implicitly or explicitly) show this relation, to substantiate that a given safety requirement is not unwarrantedly or wrongly imposed.

For example, in 1964 the U.S. Federal Aviation Agency (FAA) sought to amend the flight engineer requirements set fourth in three of its safety documents (CAR Sections 40.263, 41.263, and 42,263[2]). These requirements imposed a three person flight crew (the pilot, copilot and a flight engineer) on all civil airplanes[3] with a *maximum certificated takeoff weight (MCTOW) of more than 80,000 pounds* and *on all four-engine airplanes weighing more than 30,000 pounds MCTOW (when deemed necessary for the safe operation of the airplane)*[5].

The underlying reason behind this requirement was that, in the early days of aviation, the weight of the aircraft (and the number of engines it had) was representative of its size, which in turn was representative of it operational complexity. However, by 1964, this was no longer true, and the implementation of these requirements resulted in the employment of an additional flight-crew member without it contributing materially to the safety of the flight.

For this reason, an amendment was adopted prescribing broad standards to establish the minimum flight crew. This involved a shift in the requirement's applicability criteria, moving from the airplane's weight (which is a quantifiable but loosely representative criterion) to the workload involved in the airplane's operation (which is an unquantifiable but largely representative criterion).

This situation -where a set of requirements are no longer adequately enforced because their applicability criterion is no longer representative of the operational reality- is reasonably common within civil aviation, and it is mainly caused by the adoption of break-away technology.

Now, given that the capability to properly sustain the integrity of the legislative structure depends heavily in the timely anticipation and prevention of legislative incompatibilities, it is imperative that the EDEMOI extension takes into account such situations, and provides a tool to facilitate their detection and emendation.

Under these circumstances, a graphical model that is centered on the legislation’s applicability criteria is very informative, and might prove valuable for undertaking this type of comprehensive legislative enhancements.

---

[2] Now 14 CFR Part 121.

[3] Used in operations governed by these parts.

4 Proposing an Extension

Given the specificities of safety legislations, we consider that an enhancement in the EDEMOI methodology concerning the use of graphical models is warranted.

As was discussed in the previous section, safety legislations cover a very wide domain, with various domain-specific legislations governing a unique aspect. However, as each of these legislations may deal with a different aspect of a same element, there is a need for a tool that helps verify their inter-legislative coherence. This can be achieved by mapping the associations between the applicability criteria (i.e. the elements and/or states) and the safety requirements.

Yet, given that safety requirements may be pressed to evolve (in reaction to changes in civil aviation), the mapping of their association to the applicability criteria should be complemented with that of the safety risk that they are targeting (Refer to Figure 2), and the safety outcome they mean to provide.

Therefore we propose the creation of an interactive (adaptable) graphical model, centered on the legislation's applicability criteria, which will afford a pithy description of the safety requirements by:

- mapping out the association between the applicability criteria and the safety requirements,
- singling out the known or likely safety risk addressed by the different safety requirements (as well as the elements invoked), and
- highlighting the structure and hierarchy of the legislative texts and documents.

This graphical model would build on the strengths of the previously proposed EDEMOI models. Especially in terms of: (1) highlighting the structure and hierarchy of the legislative documents, and (2) enabling the analysis of regressions (mainly those arising from the suppression of previously enacted requirements). For this reason, our interactive graphical model will be a complementary tool within the EDEMOI methodology, specially designed for safety legislations.

4.1 The Graphical Model Proposed

The graphical model that we are proposing –in order to answer to the specific needs of safety legislations- would result from the aggregation of multiple nuclear diagrams (in theory, one diagram per requirement).

These nuclear diagrams are intended to (1) delineate the **applicability criteria** of each requirement (including intricate relationships amongst these criteria, such as: signs of aggregation, conjunction, disjunction, sequential and/or temporal conditions, etc), (2) identify the **elements summoned** (affected or addressed), (3) associate the requirements with the **known (or likely) safety risks** they address, and (4) state the

desired **safety outcome** due to compliance with the requirement (i.e. the desired condition/state).

We propose a form of "spray diagram" combined with a "cause-and-effect diagram" (See Figure 3), in which the **applicability criteria** and **partaking elements** are connected to the **legislative provision** in which they are referenced. In addition, the diagram can include additional information such as the **mitigating measures prescribed** (if any), the **safety risk** being targeted and the measure's expected **outcome**.

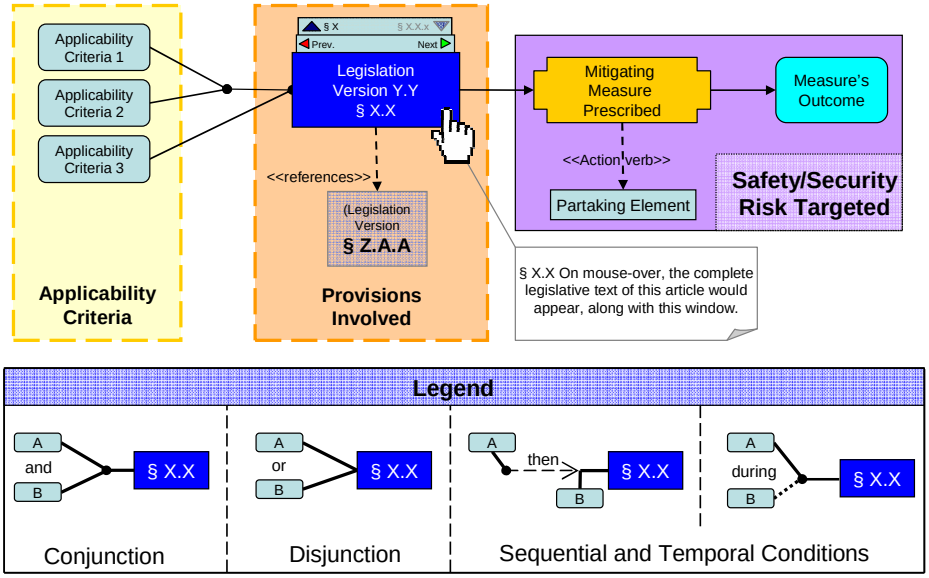

Fig. 3. The above figure is a representation of the nuclear structure of a safety requirement. An important characteristic of this diagram is the breakup of the requirement into three main particles: its *Applicability Criteria*, its *Provisions Involved* and the *Safety/Security Risk Targeted*. Indeed, this last particle encapsulates both the *Mitigating Measure Prescribed* and its expected *Outcome*. A partial caption is shown in the lower part. In the main diagram, the safety requirement is pertinent in either of two cases: (1) if Applicability Criteria 1 and 2 are both satisfied, or (2) if Applicability Criteria 3 is satisfied.

But, as we wish to continue conveying the structure (sections and sub-sections) of the legislative document, as the previously proposed EDEMOI model (See Figure 2), we are obliged to propose an interactive model whose visual structuring would be altered by the user, to facilitate specific browsing requirements. The extracted views of the model would resemble what is shown in Figure 4.

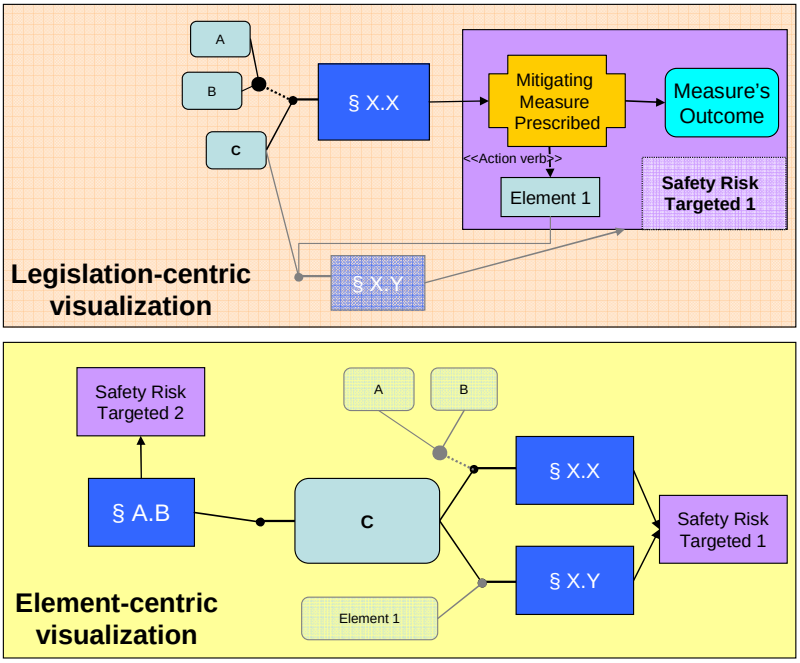

Fig. 4. Although the model's visualization will be centric (i.e. emanating from a single element), its root element will be changeable. The upper half of the figure illustrates the structuring characteristic to the 'Legislation-centric visualization', with requirement ***§X.X*** as its root element. The advantage of this visualization is that it allows a synthesized visual representation of the requirement. On the other hand, the 'Element-centric visualization' (shown in the bottom half of the figure) provides a holistic view of the safety requirements that bear on the ***C*** root element, along with the safety risk that they are meant to target.

Currently, the scope of this new graphic model is still being ascertained and its notation has not been finalized. Progress is being made through the implementation of this modeling technique in the assessment of the Very Light Jets (VLJ) [6] case study described in the following section. Furthermore, some security requirements have also been translated into this complementary notation in order to do an informal comparison of its "expressiveness" in this field.

4.2 A Future Case-study

The situation previously discussed in Section 3, where the safety requirements are no longer adequately enforced because their applicability criterion is no longer representative of the reality, is reappearing today. A case in point is that engine and material technologies have allowed the creation of high performance light jets. These jets, aptly named Very Light Jets, are capable of achieving the same flight performances (in terms of flight level and speed) as large commercial aircraft.

However, navigational equipments required for flights within controlled airspace are (until now) enforced based on the aircraft’s design and physical characteristics

(See Figure 5). Because of this, the VLJs will be able to find themselves within the same flight bands as large commercial aircraft, with incompatible and rudimentary navigational equipment.

Of course, ultimately safety will take precedence. For this, the applicability criterion of navigational requirements will need to be amended. A shift from the current criteria is required; the aircraft's weight, engine type and passenger seating capacity can no longer be regarded as the main parameters for determining its legislative requirements. New criteria must be adopted, to effectively highlight that it is the aircraft's operating environment which is determinant for such equipments. Under such circumstances, a graphical model that is centered on the legislation's applicability criteria is very informative, and might prove valuable for undertaking such a comprehensive legislative enhancement.

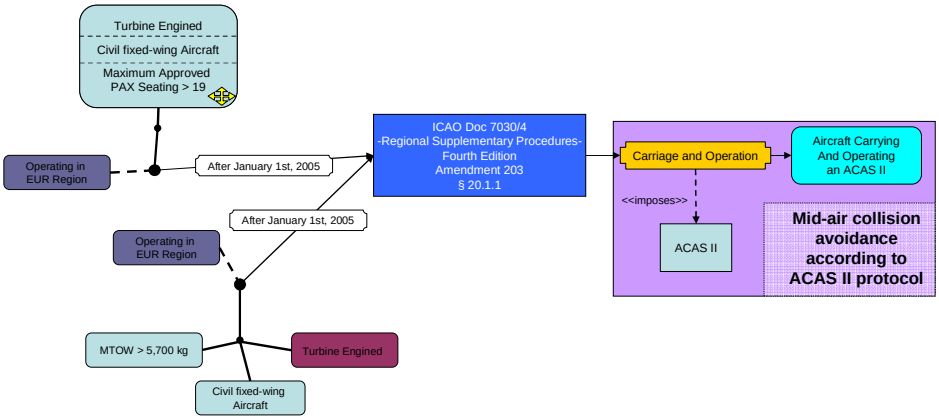

Fig. 5. ICAO's Regional Supplementary Procedures 7030/4 imposes requirements concerning the carriage and operation of the Airborne Collision Avoidance System (ACAS). The requirement (§20.1.1) states that *"[With effect from 1 January 2005] ACAS II shall be carried and operated in the EUR region by all…civil fixed-wing turbine-engined aircraft having a maximum take-off mass exceeding 5700 kg or a maximum approved passenger seating configuration of more than 19."* Given these applicability criteria, the new VLJ aircraft would not be required to carry and operate an ACAS II. The diagram presented above is a visualization of this safety requirement. In it, the two discerning cases that are concerned with this requirement are shown. The aircraft's weight discriminant is presented in its 'component-representation' (i.e. each of the criterions is placed as an independent element), whereas the other is presented in its constituted version (i.e. as an element with fixed attribute values).

5 Conclusions and Perspectives

In this paper we argue about the creation of an interactive graphical model based on the safety legislations applicability criteria. The purpose of this graphical model is to extend the application domain of the EDEMOI methodology to include safety legislations (taking into account the specificities of these legislations and the concerns of civil aviation authorities). By itself, the extension which we propose follows a

branch of the original EDEMOI methodology, in which graphical models were used as tools in the analysis of security requirements (in contrast to their use as a stepping stone to the formal specification of the requirements [7]). Nevertheless, given the intrinsic nature of all 'directive statements', it is foreseeable that this extension will be equally useful in the analysis of security requirements.

Furthermore, the underlying principle of the EDEMOI methodology (i.e. the use of formal methods to specify and validate their embedded logic) is still valid for civil aviation safety requirements. However, the usefulness of this methodology will be limited to certain domains of safety legislation. Tentatively, to the domains whose legislation is not highly objective based. The reason for this is that, as was the case for security regulations, the interest of the formal model lies in its ability to be animated. Yet, highly objective based requirements impose abstract and/or unquantifiable targets that are incompatible with an insightful analysis through test-case animation. Moreover, given this abstract and/or unquantifiable nature, less of their important aspects can be viably formalized.

Some perspectives of this work include the complete analysis of the case-study discussed in Section 4.2, finalizing the notation and defining the scope of the modeling technique proposed in Section 4.

References

1. Degani, A.,: On the Typography of Flight-Deck Documentation. NASA Technical Memorandum #177605. Moffett Field (1992)
2. Laleau, R. et al.: Adopting a situational requirements engineering approach for the analysis of civil aviation security standards. J. Soft. Proc. Vol. 11. Issue 5, 487-503 (2006)
3. Lopez Ruiz, E.R.: Formal Specification of Security Regulations: The Modeling of European Civil Aviation Security. Master Thesis. Toulouse (2006)
4. Ledru, Y.: Using Jaza to animate RoZ specifications of UML class diagrams. In: 16th IEEE International Z User Meeting, IEEE Press, Columbia (2006)
5. Moore, G.S.: Notice of Proposed Rulemaking. 14 CFR Parts 40, 41, 42. Federal Aviation Administration. Washington, D.C. (1964)
6. United States Government Accountability Office (GAO) Report to Congressional Requesters.: Very Light Jets, Several Factors Could Influence Their Effect on the National Airspace. Washington D.C. (2007)
7. Dupuy, S., Ledru, Y., Chabre-Peccoud, M.: An overview of RoZ: A Tool for Integrating UML and Z. In: 12th Conference on Advanced Information Systems Engineering. Springer Press, (2000)