Evaluating aeronautical regulations using rigorous specifications

Safeguarding against unintended consequences

Eduardo Rafael López Ruiz
PhD Student
Long-term Design and Systems Integration Department
ONERA
Toulouse, France
eduardo.lopez-ruiz@onera.fr

***Abstract*—The purpose of this thesis project is to present an innovative methodology (consisting of methods, tools and procedures) which seeks to improve the rulemaking processes currently used to develop aeronautical safety and security regulations. The two main contributions of this methodology are: its use of rigorous methods and tools to help improve the regulation's validation process and its capacity to help identify the impact of proposed amendments on enacting regulation (while helping mitigate regressions).**

Keywords; Rigorous modeling, Very Light Jet, aeronautical regulations, safety, security.

I. INTRODUCTION

The chief objective of Civil Aviation Authorities (CAA) worldwide is to continuously guarantee the safety and security[1] of civil aviation. To ascertain this, they have implemented a set of complementing and hierarchical regulations at the international, national and local level.

These regulations impose standards and recommended practices specifically targeting the prevention[2] of either **accidental events** or **unlawful acts of interference** within a given domain. This "regulation enforcement" approach to safety and security imposes that the regulation's *innate quality* and its *homogenized* and *ubiquitous implementation* become effectual factors to the achievement of their objective.

In what concerns a regulation's innate quality, [1] identified that aviation **security regulations** have three esteemed traits steering their effectiveness, which are: *consistency*, *robustness* and *unambiguousness*. Presently, rulemaking procedures include a consultation and validation phase. In it, proposed drafts are analyzed and discussed until they are considered mature for adoption and publication. For this, special attention is placed in: verifying their compatibility with existing rules, attesting the exhaustiveness of their scope and limiting their equivocalness (given the inherent ambiguity of natural languages). Nonetheless, operational feedback has proven that the current process can benefit from improvements. This is of great significance since -analogously with safety-critical software- these properties ensure that the benchmark regulation being enforced by the CAAs is intrinsically effective.

Moreover, over the past few decades, technological and ideological changes have prompted amendments within the industry's established *Regulatory Framework* (see Section 4). The purpose of such amendments has been the continual assurance of safe, secure and efficient[3] commercial operations under an enhanced state-of-affairs (through the exclusion, inclusion and/or evolution of affected regulations and/or procedures). The predicament is that, independently of their origin and dimension, regulatory and procedural amendments inevitably lead to the (unwilling) introduction of new errors [2] and the obsolescing of sanctioned workarounds. In other words, amendments lead the framework from an "error-cognizant" state, where (an indicative part of) its inherent errors have been identified (and possibly solved or circumvented), to an "error-incognizant" state.

Therefore, the aim of this thesis project is to present an innovative methodology (consisting of methods, tools and procedures) that will help improve the rulemaking processes currently used to develop aeronautical safety and security regulations.

To better recognize this situation, this thesis also seeks to appreciate the *Regulatory Framework* being implemented in aeronautics, by identifying how the prevailing ideas (principles, objectives and policies) within civil aviation are linked to the regulatory infrastructure (regulations and procedures) being implemented. This will help identify and bound the "impingement zone" of the regulatory amendments, opening the path for the subsequent development of the methodology that will help identify possible regressions arising from such type of amendments. Finally, the methodology that is proposed shall be appraised by implementing it in the study of the

[1] **Safety** relates to the prevention and mitigation of accidental events, which can affect material or people while **security** is the prevention and mitigation of intentional acts, which aim to affect planes or people.

[2] Regulations seek to prevent accidental events and unlawful acts, whereas reactive/emergency procedures dictate actions that help mitigate their consequences.

[3] A global efficiency attained through the prioritized optimization of various factor such as: environmental and economic costs, performance …

ISBN: 978-0-615-20720-9

discerning operational certification requirements for Very Light Jets (VLJs) in Europe and the United States of America.

II. The Chosen Approach

In 2003, a group of French universities and research laboratories proposed the implementation of rigorous methods to assist in the specification, design and validation of regulation documents [1]. They named their project EDEMOI.

Rigorous methods had already been used within other domains of aeronautics, "to enhance the current practice of procedures development" [3] and for the analysis and verification of aeronautical safety critical systems. However, the formal methodology developed by EDEMOI (see Figure 1) sought to enhance the rulemaking process by incorporating simulation and counterexample checking tools into the validation phase, to better ensure the regulation's innate quality. This methodology is centered on a two-step approach involving two stakeholders: the Certification Authorities, which establish International Standards concerning Civil Aviation Security, and the Model Engineers, who translate these natural language documents into formal models that can be tested.

In the first step of this approach, a *model engineer* extracts the security goals imposed in the *International Standard* and translates them into a semiformal model that faithfully represents their structure and relations (while reducing the use of inherently ambiguous terms). This *graphical model*, comprehensible to both stakeholders, is later revised and validated by the *certification authority*, giving way to the second step of the 'EDEMOI approach' in which the model engineer performs a systematic translation of the semiformal model to produce a *formal model* that can be analyzed through *test scenarios*.

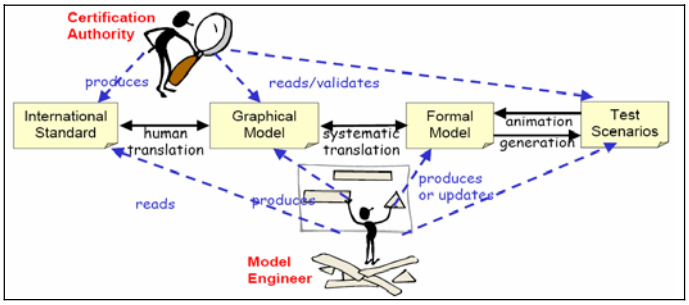

Figure 1. The EDEMOI methodology.

Having obtained positive results from these experiences, this thesis proposes a twofold expansion of the EDEMOI methodology by (1) broadening its scope to include aviation safety regulations and (2) by extending its usability throughout the regulation's "lifecycle".

More concisely, the extended methodology will devise methods and provide tools to help validate and enhance aviation regulations throughout their development, verification, validation and amending phases. This presents a large challenge as there are fundamental and operational differences between safety and security regulations. At the outset, safety regulations need to be more adaptive to the industry's constantly evolving state-of-affairs, helping steer developments instead of contriving their progress. Therefore, will their consistency and robustness still be driving traits? And can their adaptability be inferred through the models?

For example, given the current technological and economical trends in the aeronautical sector, the industry is preparing itself to the challenge of successfully extending single crew operations to jet aircraft. More concisely, the Very Light Jets (VLJs). The stakeholders to this undertaking -such as the aircraft manufacturers, service providers and safety regulators (which in the case of Europe would encompass EUROCONTROL and EASA)- are concerned with determining the regulatory enhancements (exclusions, inclusions and/or evolutions) that will be required to ensure safe operations under this new state-of-affairs.

The extended use of this methodology, in this case, would be focused in helping identify the impact of regulatory enhancements by modeling and comparing the regulations and procedures, before and after an amendment is enacted (see Figure 2).

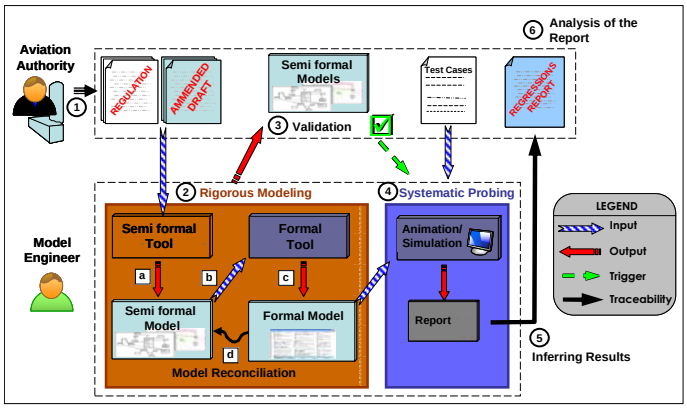

Figure 2. The extended methodology.

Therefore, analogously with the work done in [4], rigorous formal models of the affected aeronautical regulations will be studied and animated to: (1) help identify the impacts of proposed technologies on the regulation (influencing the aircraft's operation and flight-cabin design), and (2) to infer possible solutions for such incompatibilities.

It is important to say that this methodology does not aim to provide the consequences of the "inaction" with respect to the *adjusting factors*[4], but rather to prevent the regression of the regulatory framework by assessing the impact that the amendments themselves have on the system (e.g. loss of consistency and/or robustness, introduction of ambiguous statements or ideas…).

III. Rigorous Specification

As was done in our appraisal of Regulation 2320/2002 [4], an interpretation of the regulation is captured using (part of) the UML language *(Figure 2, Step 2.a)*. The use of this graphical

[4] An adjusting factor is any operational, ideological and/or technological change whose introduction, into the civil aviation system, obliges a change in the contemporary regulations to preserve the appropriate overall functioning of the system.

ISBN: 978-0-615-20720-9

notation helps tackle the text's innate ambiguity, while proposing a conceptual layout that can be validated/invalidated by officials from the certification authority.

The validation of this conceptual layout *(Figure 2, Step 3)* helps establish the adhesion of the semiformal model to the convened international standard. For this, the appraisal and feedbacks provided by aviation authority officials are integrated into the model by way of amendments. Once validated, the semiformal model is translated *(Figure 2, Step 2.b)* to a rigorous formal model using translation rules between the semiformal and formal notations (in this case, UML → Z).

This ensures that our methodology benefits fully from the integration of both approaches: the intuitive structured notation of the semiformal approach and the precise semantics of the formal approach.

Finally, when the models have been deemed mature enough (both in their notation and their faithfulness to the regulation) an animation or verification tool *(Figure 2, Step 4)* is used to test the formal model's consistency (through simulation) and robustness (through counterexample checking). The results of the tests and simulation are stored to enable regression analysis after further evolutions of the regulation and the models *(Figure 2, Step 5)*. Currently, two formal method targets are being considered: RoZ + Jaza Animator [5] and Alloy Analyzer [6]. However, independently of the software option that will be ultimately chosen, it is important to fully apprehend the context of these regulations and of the approach privileged by the CAAs.

IV. THE REGULATORY FRAMEWORK

An important aspect of this thesis work is to correctly understand the regulatory framework being implemented today in the civil aviation domain. Therefore, the first part of this thesis sought to propose a model of the idealistic regulatory framework which is in place today.

As stated before, CAAs worldwide strive to continuously guarantee the safety, security and efficiency of the civil aviation system. For this purpose they define *policies* and administer *regulations* which are in line with globally embraced *objectives* and *principles.* In addition to this, concerned aviation stakeholders develop *procedures* that dictate safe and practical methods for the successful performance of aeronautical-related tasks[5].

Combined, these five elements make up what we will refer to as the *Regulatory Framework*. So, in broad terms, this framework is a mix of: (1) the underlying ideas/concepts (i.e. *principles*, *objectives* and *policies*) deemed essential for the development of civil aviation and (2) the regulatory infrastructure required for their implementation (i.e. *regulations* and *procedures*).

As shown in Figure 3, the Regulatory Framework is rooted from the *Principles* defined by the various concerned States. However, it is the task of the ICAO to translate these political goals into attainable *Objectives* and to define its *Policies*. The different CAAs then align their policies with those of the ICAO and define new policies for the domains outside of ICAO's competence.

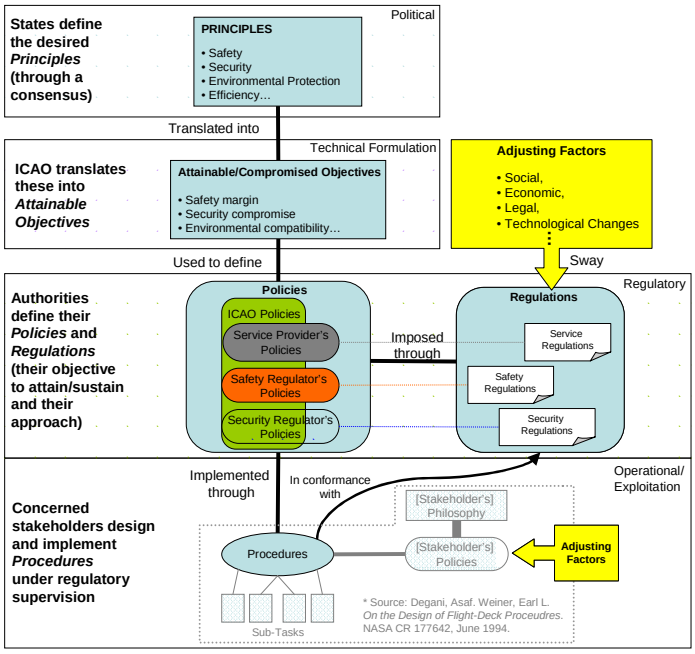

Figure 3. The Regulatory Framework.

The Policies defined by the CAAs are then imposed through local *Regulations*. These regulations must be consistent with the standards stated in the ICAO Annexes. This has led to a comprehensive base of compatible regulations. Concerned stakeholders then design and implement *Procedures* in conformance with these regulations.

However, these five elements cannot be considered as simple aggregates of the Regulatory Framework. As discussed in [7], the link between these elements is important and can be exploited to facilitate the detection of possible discrepancies and conflicts. Furthermore, a clear and structured representation of these links will provide: (1) an understanding of the Regulatory Framework and (2) insight on its interactions with the different adjusting factors (which impose a change in its state-of-affairs).

It should be noted that Figure 3, reflects the hierarchy of the different civil aviation organizations/agencies and their respective documents/rules by highlighting that CAA's derive their regulations from ICAO policies and adopt its standards. Furthermore, it identifies the regulations and the procedures, as the "impingement zone" for the *adjusting factors*. Because, given the industry's need for a flexible Regulatory Framework, its underlying principles, objectives and policies use abstract wording to convey what is deemed essential for the development of civil aviation. This makes them less susceptible to sways (owing to adjusting factors) than the regulations and procedures, which require detailed wording given the special need for unambiguousness at their level.

[5] Under the guidance and supervision of the Civil Aviation Authorities.

ISBN: 978-0-615-20720-9

V. APPRAISING THE METHODOLOGY

The methodology proposed will be appraised by implementing it on the study of the discerning operational certification requirements for Very Light Jets (VLJs) in Europe and the United States of America. These small but relatively high-performance airplanes are a potential adjusting factor to a large part of the regulatory infrastructure presently established within civil aviation. This is due, in part, to the considerable contrast between their small size/weight (seating between 5-8 passengers with an MTOW under 4,536 kg) and their relative high performance (Cruise speed: ~ 0.62 M). But more particularly, by the fact that they were designed to fly within the same flight band (and terminal airspace) as that of commercial-aviation airplanes (FL 330-350) with an "in-design" compatibility for both single and double flight-crew operations.

Concerned with this situation, both EUROCONTROL and the European Aviation Safety Agency (EASA) have taken steps to ensure the smooth entry of this new "technology" while seeking to alleviate the ripple effects that it will have on the civil aviation system. For example:

Under current mandates, VLJs are not required to be equipped with an Airborne Collision Avoidance System (ACASII) to operate within the EUR region.

But, given their forecasted growth and their incompatible speed (with respect to large commercial airplanes), EUROCONTROL may seek to impose the mandatory equipping of VLJs with an ACASII system; to continue ensuring a high level of safety and efficiency in the pan-European Air Traffic Management (ATM) system.

EASA, on its part, has opted to limit the airplanes' operational envelope by restricting it to double-crew operations. This decision was based, in part, on the increased likelihood of: level busts, airspace incursions, runway incursions and fatigue in single pilot operations [8]. This is in clear contrast with the Federal Aviation Administration's (FAA) decision of certifying single flight-crew operations under a special scheme[6].

These concerns not only demonstrate some of the regulatory enhancements that will ensue the VLJ concept, they also hint the (possible) need for a larger and more comprehensive regulatory enhancement; namely the evolution of the regulations' applicability criteria. A shift from the current criteria is required; the aircraft's weight and passenger seating capacity can no longer be regarded as the main parameters for determining its regulatory requirements. New criteria must be adopted, to effectively highlight that it is the aircraft's operating environment and its performance which are determinant.

VI. CONCLUSIONS AND FUTURE WORK

Having already applied the methodology to the modeling of Regulation 2320/2002, we have tested the compatibility between the security guidelines imposed and the different notations used to represent them. Consequently we shall implement the extended methodology to the case of VLJ aircraft, in order to illustrate the main ideas and contributions of both the model and the methodology.

By our part we believe that the introduction of VLJs into the civil aviation system represents an excellent opportunity to appraise this methodology. For this, we shall benefit from the discerning operational certification requirements for VLJs in Europe and the United States of America. Since VLJs in Europe are not going to be certifiable for single crew operations (in contrast with the FAA's decision for Part 135 operations), this gives us a "Δ" (delta) between two state-of-affairs which can be used as a "before" and "after" state to compare (and tweak) the performance of our proposed tools. The systematic probing would focus on the regressions introduced by the amendments implemented in the USA, with regards to its VLJ stance in a bid to facilitate the detection of unintended consequences.

However, the work will not be a clear-cut translation of the requirements (into a graphical and formal model). There is a complexity in specifying all of their aspects; with a potential loss of connotation during the conversion. This problematic is inherent to the passage from a natural language to the semi-formal and formal notation. Nevertheless, the converse is also true; the translation to formal notation helps enrich the requirements by imposing precision in terms and relations.

Additionally, work is being pursued to determine the possibility (and the interest) of extending this same methodology onto other aspects of civil aviation, such as flight procedures and manuals.

[6] Limited to Part 135 operations. Requires an experienced professional-pilot licence holder that has undergone special training.

REFERENCES

[1] R. Laleau, et al. "Adopting a situational requirements engineering approach for the analysis of civil aviation security standards," The Journal of Software Process: Improvement and Practice (SPIP), Vol. 11, Issue 5, Pages 487-503. July 2006.

[2] S. Deutsch and R.W. Pew, "Single pilot commercial aircraft operation," BBN Report No. 8436, Cambridge, USA, November 2005.

[3] A. Degani, M. Heymann, and I. Barshi, "A formal methodology, tools and algorithm for the analysis, verification and design of emergency procedures and recovery sequences," NASA Internal white paper, 2005.

[4] E.R. López Ruiz, "Formal specification of security regulations: The modeling of European civil aviation security," Master Thesis, SUPAERO, Toulouse, France, December, 2006.

[5] Y. Ledru, "Using Jaza to animate RoZ specifications of UML class diagrams," IEEE Columbia, April, 2006, [The 16th International Z User Meeting, ZUM 2006].

[6] D. Jackson, "Dependable software by design," In Scientific American, June, 2006. Volume 294 Number 6. Page 68.

[7] A. Degani, and E.L. Weiner, "On the design of flight-deck procedures," NASA CR 177642. USA, June 1994.

[8] F. Woods, "Very Light Jets. The qualification challenge," EASA, Brussels, Belgium, May 2007, [Very Light Jet (VLJ) Workshop].

ISBN: 978-0-615-20720-9