Can regulatory bodies expect efficient help from formal methods?

Eduardo R. López Ruiz
Onera
Toulouse, France
eduardo.lopez-ruiz@onera.fr

Michel Lemoine
Onera
Toulouse, France
michel.lemoine@onera.fr

Abstract

In the context of EDEMOI -a French national project that proposed the use of semiformal and formal methods to infer the consistency and robustness of aeronautical regulations through the analysis of faithfully representative models- a methodology had been suggested (and applied) to different (safety and security-related) aeronautical regulations. This paper summarizes the preliminary results of this experience by stating which were the methodology's expected benefits, from a scientific point of view, and which are its useful benefits, from a regulatory body's point of view.

1 Introduction

In order to safeguard civil aviation against accidental events (which is the concern of aviation safety) and against intentionally detrimental acts (which is the concern of aviation security), governments worldwide have imposed regulatory requirements upon the different aviation participants or, as they will be refer to in this paper, entity-classes[1].

Under the vigilant eyes of regulatory bodies, safety/security requirements are imposed on the entity-classes in order to (1) prevent the body of causes that may directly or indirectly lead these entity-classes into a hazardous operating/behavioral state, and/or (2) mitigate the consequences associated to such states.

However, in order to be effectual, the regulatory requirements need to be robust, consistent and pertinent. Indeed, their robustness ensures that the requirements exhaustively cover all the safety/security relevant scenarios within the regulation's domain of competence, or purview. Their consistency ensures that they will not be mutually contradictory or incompatible. And their pertinency ensures that they are relevant to enhancing aviation safety/security. Yet these three qualities can only be achieved through a complete understanding of the regulatory domain, and of the concerned (or participating) entity-classes, including their mutual interactions.

For this reason, regulatory bodies seek to fully identify all of the safety/security-concerned entity-classes that exist within their purview, including their relevant (universe of) states[2]. This information, along with their extensive practical and theoretical expertise, enables the regulatory bodies to adequately determine the preventative or mitigative measures that they should impose onto the entity-classes, in order to reduce their associated safety/security risks.

[1] This paper uses the term *entity-classes* to refer globally to the types of aviation participants upon which the regulatory requirement are imposed. The nature of these participants can range from the persons involved in civil aviation operations, to the objects that they use and the infrastructures that they employ. Some examples of an entity-class are: PASSENGER, FLIGHT CREW MEMBER, AIRCRAFT, AIRPORT, COCKPIT.

[2] An entity-class' *relevant universe of state* is the grouping of all of its pertinent possible states. In other words, the grouping of all the states with: *(a)* a direct or indirect effect on the overall safety and/or security level and *(b)* a possibility of occurrence greater than zero. An example of a pertinent and possible state for the FLIGHT CREW MEMBER entity-class is the incapacitated state. Indeed, safety regulations have identified that the in-flight pilot incapacitation scenario is a remote (4.5x10-7 per flight hour) but possible scenario with consequential impacts on safety. Therefore, regulators ensure that this scenario is taken into account by their regulations

This way, but rather unwittingly, regulatory bodies created a composite, abstract and subjective description of their purview, corresponding to their *Conceptual View of the Real World*. This conceptual view is in fact implicitly found within their regulations, and it affords them a manageable (although approximate) model of their regulated domain that helps them better grasp their regulatory domain's structure, correlations and interactions. It also serves them as an arbitrarily well-defined categorization that groups individual entities (*e.g.* passenger Alice and passenger Bob) into a uniquely defined sets of entities (*e.g.* the entity-class PASSENGER), upon which the regulatory requirements can then be affixed[3]. Indeed, through well-defined categorizations such as this one, the regulatory bodies can specifically denote the sets/subsets of entity-classes that are concerned with a specific regulatory requirement.

This means that the regulator's *Conceptual View of the Real World* is intimately tied to a regulation's innate quality because: *what can be expected of a regulation whose regulator has a distorted view of the Real World? Or, if this view is missing relevant elements and/or relations?*

Therefore, the regulator's *Conceptual View of the Real World* needs to be checked to ensure the validity of its assumptions and statements, but also the robustness (comprehensiveness) of their concern.

The figure shown below (Figure 1) elucidates on the notion of the *Conceptual View of the Real World* (Figure 1, ACV) and on how it influences the pragmatic aspects of the regulatory framework.

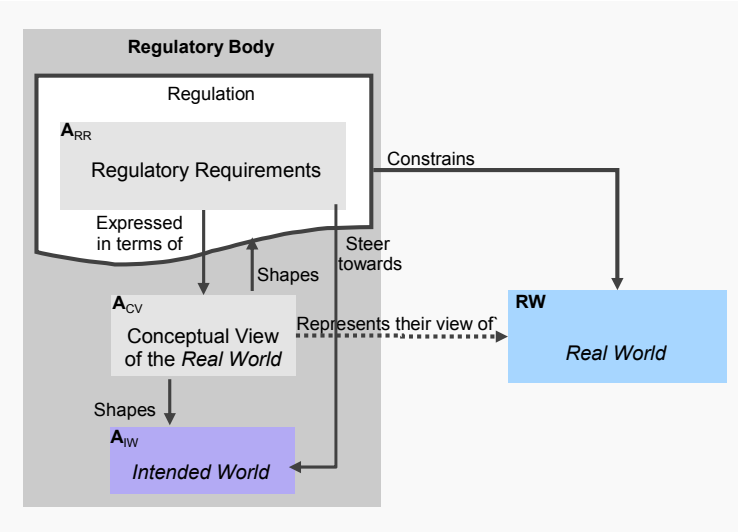

Figure 1: Conceptual Representation on the Operational description of the Regulatory Framework.

However, due to the (ever-growing) complexity of civil aviation and to its ever-changing state of affairs -brought on by *adjusting factors*[4]- regulators often find themselves overwhelmed by the challenge of continuously safeguarding such a dynamical and complexly interrelated industry.

Indeed, the process of 'developing/updating' the regulations undeniably entails the need to define and modify many of the fixed and context-dependent axioms and assumptions[5] that are the basis for the regulator's *Conceptual View*. This can result in the possible invalidation of some previously valid axioms and assumptions, as they change to reflect the new reality of the system.

[3] In accord with the principle that law must be general (*i.e.* impersonal).

[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.

[5] The axioms and assumptions are, respectively, the necessary truths and the generalized results that serve as the basis for the argumentation and/or inference of the regulatory requirements. They represent the *Domain Knowledge* shown in Figure 2

The *Conceptual View of the Real World* is therefore a crucial element in understanding the regulations, ensuring their pertinence and verifying their actuality. It is in this context that EDEMOI advocated the use of semiformal and formal methods and tools, to enhance the analysis (and consequently improve the inherent quality) of aeronautical safety and security regulations. In other words, EDEMOI sought to design an employable methodology[6] that would facilitate the assessment of regulatory requirements.

2 The Proposed Methodology

The underlying approach for the EDEMOI methodology was to determine the analogies that could be made between the domains where 'Requirements Analysis and Design in Systems and Software engineering'is successfully used, and 'civil aviation safety/security'. This was done with the objective of identifying the methods and tools used for these domains, to determine if they could be successfully implemented in the assessment of aviation safety/security requirements by way of a tailored methodology.

The EDEMOI methodology proposed enhancements to the rulemaking procedure currently used by civil aviation authorities. These enhancements included the incorporation of simulation and counterexample checking tools into the regulation's already established validation phase. This, with the objective of better ensuring the requirements' innate quality without any fundamental changes to the established rulemaking procedure.

The methodology is centered on a two-step approach (see Figure 2) involving two kinds of stakeholders: the *Aviation Authorities*, which establish regulations concerning civil aviation safety/security, and the *Model Engineers*, who translate these natural language documents into semiformal and formal models.

Given that regulations are rarely built from scratch, the methodology focused on studying/comparing the evolutions of existing regulations in search of possible regressions.

In the first step of this approach, a *Model Engineer* extracts the security goals and the imposed requirements from the original regulatory texts, and translates them into a semiformal (graphical) model that faithfully represents their structure and relations (while reducing the use of inherently ambiguous terms). Indeed, this model embodies the *Conceptual View of the Real World* that is partly implicit in the regulation (as discussed in Section 1). This *Graphical Model*, understandable by both kinds of stakeholders, is later revised and validated by the *Aviation Authority*, giving way to the methodology's second step, in which the *Model Engineer* performs a systematic translation of the semiformal model to produce a *Formal Model* that can be further analyzed.

This methodology was used in the formalization of various international and supranational aeronautical regulations[7] [7], [3] with discerning purviews and objectives. This allowed us to test the methodology, and conclude that it provides some interesting benefits. However, not all of them can be fully exploited by the regulatory bodies. The following sections provides a brief overview of the useful advantages of the methodology (Section 3) and of its shortcomings (Section 4).

[6]The EDEMOI methodology was not designed as a substitute for the practices currently employed in the assessment of regulatory requirements. On the contrary, it was designed to complement existing safety/security managements tools. Indeed, the traditional assessment methods such as the regulation's preliminary impact assessments, as well as the open (or closed) consultation periods before their enactment, are sufficiently effective in identifying the more common errors. However, and this was the motivation behind the EDEMOI project, new assessment techniques can allow the detection of the more elusive shortcomings and errors.

[7]Parts of the following regulations were formalized : ICAO's Annex 17 *(International Airport security)*, ICAO's Annex II *(Rules of Air)*, Regulation (EC) No. 2320/2002 *(European Airport Security)*, Directive 2008/114/EC *(Security of European Critical Infrastructure)* and Regulation (EC) No. 2096/2005 *(regarding the provision of Air Navigation Services)*.

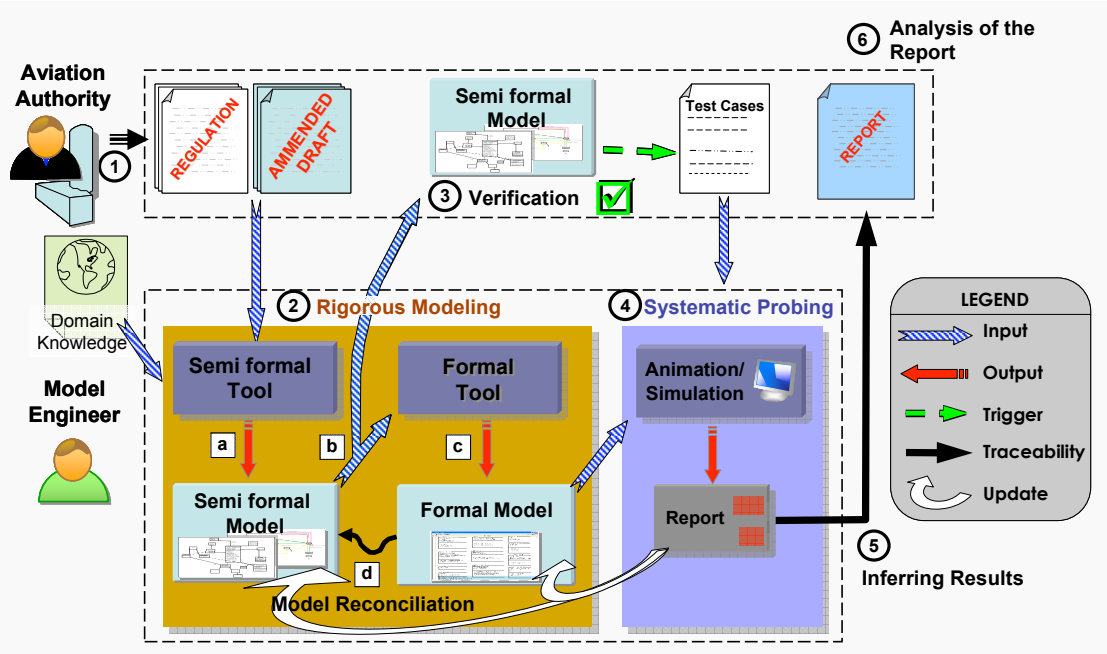

Figure 2: The Methodology proposed relies on the use of semiformal and formal tools to analyze regulatory requirements and enhance their innate quality.

3 The Methodology's useful benefits

3.1 Introduction

As was mentioned previously, aeronautical regulations are natural language documents that impose requirements onto real world entity-classes through a tacit abstract view of these entity-classes and of their environment. This was said to be the aviation authority's *Conceptual View of the Real World*. Formally specifying this *Conceptual View* yields a detailed documentation of its underlying assumptions and axiomatic base. Furthermore this formal specification can be accomplished while preserving a relatively high fidelity between the *Conceptual View* and the resulting models. Because, the *Conceptual View* is already an abstract and simplified model of the real world. This frees up the model engineer from the burden/responsibility of creating the models from zero.

Furthermore, formal tools can genuinely provide a sound basis for the comprehensive comparison of the abstract view and the real world it is supposed to embody. This, in order to detect diverging conceptions since a flawed view of the real world will suggest ineffectual or futile requirements. Also, using formal tools can facilitate the detailed understanding and analysis of the regulations' predicted implementation.

Figure 3 shows a side-by-side qualitative summary that synthesizes our experience and feedback with regards to the communicative aspects of semiformal and formal models for safety/security experts working within regulatory bodies. These results are part of the **A**ssessment of **L**egislative and **R**egulatory **R**equirements for **A**TM **S**ecurity (ALRRAS) project, a feasibility study into the use of computer science methods and tools to improve the assessment of pan-European aeronautical requirements. The eight criteria were selected based on the available literature [6], [4], [5], [2] and because practical knowledge of aviation safety/security identified them as facilitators of a regulation's quality.

With respect to these criteria, semiformal models (whose performance is shown in red diagonals)

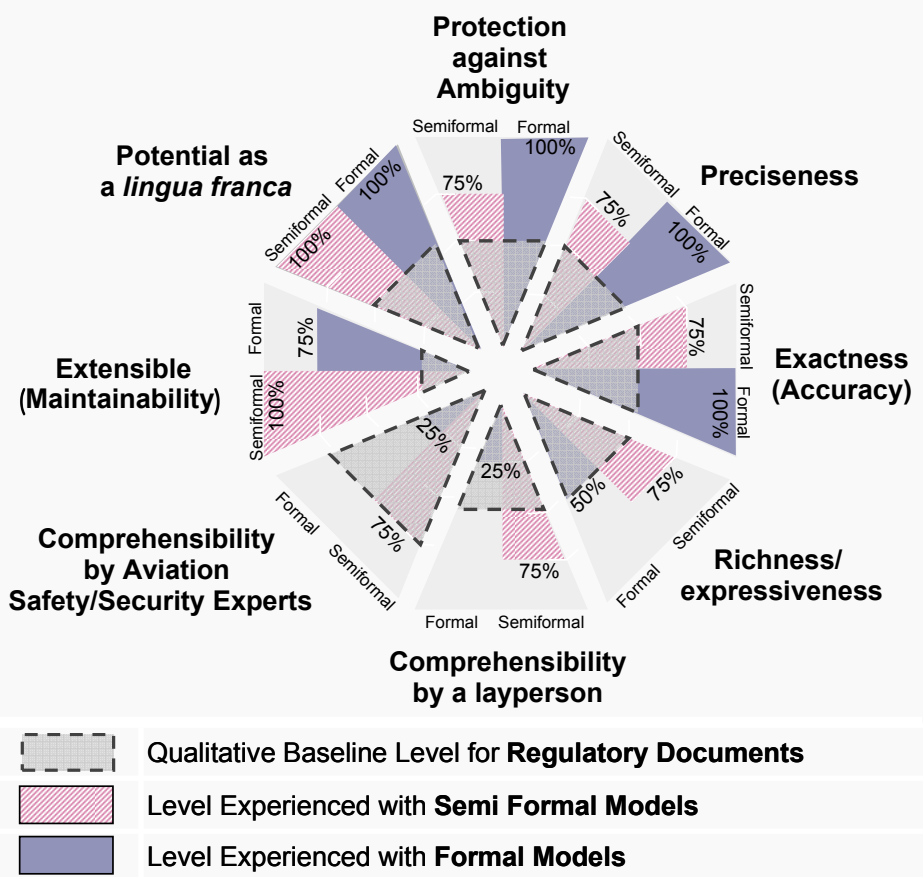

Figure 3: Graphical representation of a qualitative assessment of the communicative aspects of Aeronautical Regulatory Documents. Also shown, how these aspects are influenced by the complementary use of semiformal (in red diagonals) and formal models (in solid blue).

were found to be, overall, more consistent in their communicating capacities. Also, they have proven to be an enhancement for laypersons in terms of complementing their understanding of the aeronautical regulations.

Formal models, on the other hand (whose performance is shown in solid blue) stood out for their preciseness, exactness and their protection against ambiguity. However, as the qualitative values in the diagram need to be pondered for each modeling-type (to take into account the weight given to each criterion by regulatory bodies), the formal model's excellent protection against ambiguity was quickly overshadowed by its very poor comprehensibility by both laypersons and aviation safety/security experts.

Understandably, regulatory bodies, being less familiar with formal notations, need to be extremely cautious when validating/invalidating formal models, as they may be less able to detect specification errors[8]. This is especially true for regulators with a background in legal-studies, as they have been less exposed to such notations than their colleagues with an engineering background.

For this reason, the methodology foresaw the complementary use of semiformal and formal models (see Figure 2). Indeed, the process called for a semiformal model to be built directly from the regulatory text. This semiformal model was enriched with Object Constraint Language (OCL) expressions and -

[8]For the most part, regulators needed few instructions to be able to understand/interpret the semiformal notations

after having been analyzed and not invalidated[9] by the corresponding authority- used as the basis for a formal model.

A direct consequence of this methodology is that it provides a common semantic/understanding of the regulatory requirements that is (almost[10]) independent of any natural language. This is true for both the semiformal and formal models.

Also -and this is a byproduct of any specification process- the methodology can help identify imprecision, ambiguities and inconsistencies within the regulatory requirements.

More explicitly, we can say that formally specifying a regulation affords us:

- The ability to check where there are some holes in the regulations (a situation which is of a particular importance for security regulations!), and
- The ability to detect whether any regulatory amendments will introduce safety/security regressions.

3.2 Benefits of using Semiformal Models

The benefits provided by the semiformal models were, among others:

- Developing a common and understandable abstraction of the regulated domain and the participating entity-classes.
- Making the regulator's *Conceptual View of the Real World* explicit, enhancing the manipulation of their regulatory requirements.
- Providing a deeper linkage (traceability) between the different elements that comprise the regulatory framework.

The mixed semiformal/formal approach was indeed necessary, as was justified in figure 3. Through the use of UML-like notations, model engineers with a double competence in law and computer sciences can create semiformal models of the regulation's addressees. which convey their static (using class diagrams) and dynamic (using state-transition diagrams) properties. The utility of these models is that they can be used to represent, in a less ambiguous manner, how the regulatory requirements impact the entity-classes' structural and behavioral aspects. That is, the models can be used to show how the regulations reshape their static and dynamic properties.

Also, static models provide a deeper traceability between the different entity-classes and regulatory requirements. This allows a holistic view of normally separate (yet interrelated) regulations, and reconciles their *domain-oriented* structuring with their *class-entity oriented* implementation (*e.g.* all rules pertaining to the flight of an aircraft *vs.* all rules applicable to the FLIGHT CREW MEMBER entity-class). All of this helps facilitate the impact analysis of *adjusting factors*, as well as the regression analysis of the subsequent regulatory amendments.

Coupled with this, semiformal methods can help identify where the regulations are open for diverging interpretations. Moreover, these types of models can be used to create very rigorous specification of certain aspects of the entity-classes, particularly the dynamic diagrams (such as a state-transition diagram) where the use of guards can be very formal (more or less: IF ... THEN ... ELSE .. the presence of ELSE being mandatory for completeness reasons!). The advantage of this type of model is that the gain in formalism is not coupled with a loss in comprehensibility.

[9] When verifying the models, regulatory bodies are better positioned to detect errors within a specification -and therefore to 'invalidate' a model- rather than 'validating' them as being free of errors.

[10] The final models keep only remnants of the original regulatory text, preserving entity-class names, attribute and states descriptors.

3.3 Benefits of using Formal Models

Among the benefits provided by the use of formal models we can mention:

- It allows the regulation's meaning to be specified with more precision and exactness, helping the model engineer identify the more tricky areas (*i.e.* where the regulation can be interpreted differently).
- It affords the ability to automatically derive testing material.

Formal methods can be used to perform a comparative analysis between the Real World (Figure 1, RW) and the legislator's *Conceptual View of the Real World* (Figure 1, ACV). Using a formal models and tools for this analysis entails two benefits. Firstly, the act of formally specifying both the Real World and the regulator's *Conceptual View of the Real World* can be a preliminary way of identifying their differences/incongruities. Secondly, the formal specifications can be put through a comprehensive comparative analysis that is not possible by other means.

Much like the semiformal models, formal models also help identify some areas where the regulation may be interpreted differently, but since they allow the regulation's meaning to be better specified, they undoubtedly help the model engineer identify more clearly those areas where the regulation can be interpreted differently but also help them make sense of these tricky parts. Indeed, revisiting the semiformal model after having developed the formal one allowed us to make significant improvements in the semi-formal model, particularly in terms of simplifying the model, but also by helping identify specification errors.

This was the case during the formal specification of a European airport security regulation, where a subtle language lapse in one of its articles[11] was discovered only after it had been formally specified. It had gone undetected in the original regulation, its eleven different language translations, and in its first semi-formal model. The article establishes the conditions (and limits) by which an airport can be labeled as 'small', and therefore be derogated from applying the stringent (and expensive) security standards enforced at larger airports. But, as shown in figure 4, the original text version alleviated only a fraction of the small airports it was supposed to exempt.

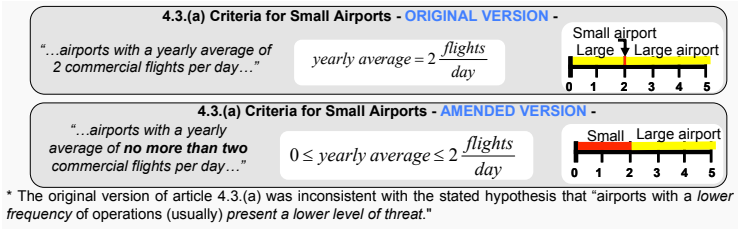

Figure 4: During the formal specification of Regulation (EC) 2320/2002, a subtle language lapse was identified. Although this wording error did not have a negative effect in terms of security -as it made the regulatory requirements more restrictive than originally intended-, it did have an economical impact on those small airports that where technically considered as large. The figure above transcribes the original regulatory requirement (on top) and its amended version (at the bottom). Also, the requirement is represented in two additional ways. In the center, as a mathematical expression. At the far right, as a one-dimensional graph.

[11] Regulation (EC) No. 2320/2002. Article 4.3.(a) Criteria for Small Airports

It is undoubtedly clear that formalization helps regulatory bodies to better understand and check their regulations from a technical point of view. But, what are the real uses and advantages that will result from this methodology?

4 The Methodology's shortcomings

As mentioned previously (Section 2), the methodology has both positive and negative aspects that need to be weighed, in order to define its utility as a tool to enhance the analysis of aeronautical safety and security regulations. This section will discuss its most consequential 'faults' or shortcomings.

From the previous section (Section 3), it is undoubtedly clear that formalizing regulatory requirements helps (from a technical point of view) regulatory bodies better understand their regulations by providing them with supplementary insight of their regulated domain and concerned entity-classes. However, it is not so clear from a practical standpoint.

Indeed lawyers are experts in law but they have a hard time understanding or, even more, developing such formal models [8]. Therefore, there will always be a need for a model engineer to develop the models. But, even when a model engineer develops a formal model of the regulations, the lawyers are unable to directly validate it, as they have a hard time understanding the notation. This leaves little use for such models. However there is a work-around to this problem. An alternative 'validation' solution is to animate/simulate the formal model in order to indirectly validate it. This indirect validation is done by comparing the results of the scenarios animatied/simulated, with the expected results of their actual implementation. The disparities between both results becoming the focus area for a detailed revision. However, this alternative solution also entails many difficulties, as regulations are very abstract texts, impossible to animate/simulate 'as is'. As shown in the following figure (Figure 5), regulatory texts need to be complemented by various other sources in order to have a model capable of being animated/simulated. Indeed, regulations need to be more or less stable through time -to ensure stakeholder's awareness of their obligations-, and the best way for ensuring this stability is for their regulatory requirements to be written using broad and general statements. Nevertheless other non-mandatory documents such as guidance material, industrial best practices, and standard procedures can help fill in the gaps between the regulation's abstract text and its detailed description, thereby enabling its animation/simulation.

For instance, the following regulatory requirement[12] concisely imposes that each country shall screen their originating passengers: *4.4.1 Each Contracting State shall establish measures to ensure that originating passengers of commercial air transport operations and their cabin baggage are screened prior to boarding an aircraft departing from a security restricted area.*

This text could lead to a very simple binary animation/simulation of the passenger screening which would be interesting if this where the first time the regulation is being enacted, to test its basic logic. However, since this requirement has been around since 1975, the requirement has to be complemented by its associated guidance material and by integrating the domain knowledge and best practices, to produce a more complete animation/simulation of the same process, and try to find the more elusive errors.

The fact that lawyers cannot easily understand formal models entails another problem. Since the formal models cannot be directly validated by the regulatory bodies, there will never be a benchmark formal specification of the Real World! Any model-to-model comparison (such as the one between the Real World and the legislator's *Conceptual View of the Real World*) will only provide a **relative assertion** into their validity. In fact, since there is no single 'valid' model to which others can be compared, all that can be expected from a model-to-model comparison is a measure of compatibility among the compared models, without any clear reference into which one of the discerning models is preferable.

[12] ICAO - Annex 17. Eighth Edition, 11th Amendment. Measures relating to passengers and their cabin baggage.

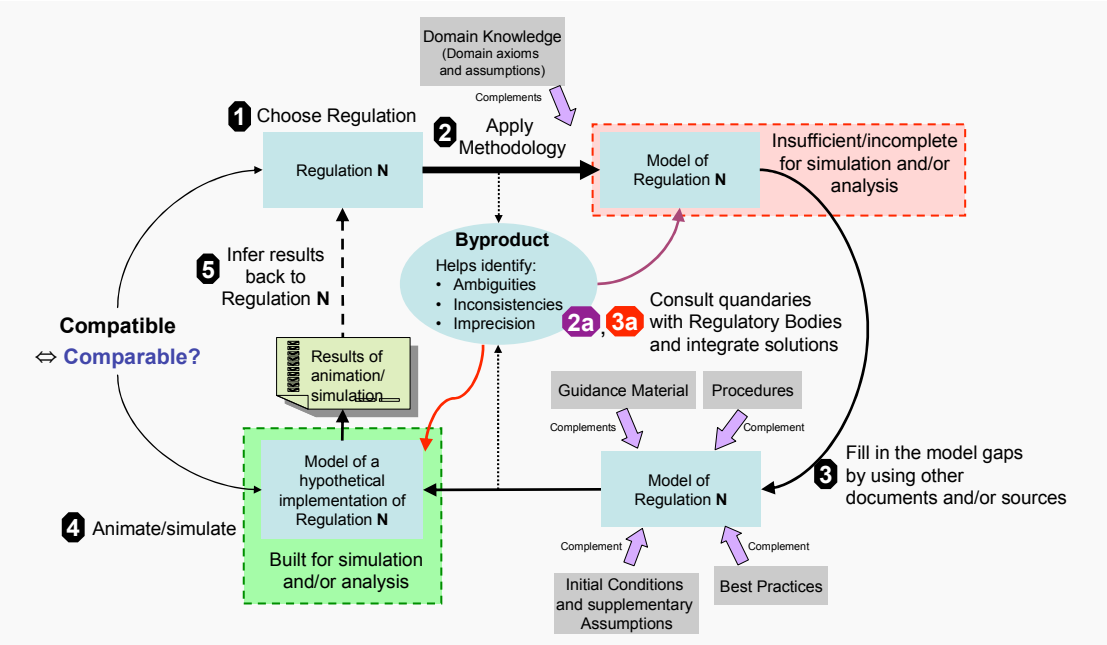

Figure 5: Regulations are not comprehensive sources of information so their modeling will not be able to produce an animatable/simulatable model. These models have to be completed through other sources in order to produce a 'runnable' model.

Nevertheless, one can look at the 'half-full' part of the glass and say that: even though the comparisons will only be relative, the disparities/incongruities between the compared models will help legislators by giving them a focus area or some starting points for their conventional validation process. And, in the end, this could lead to a more concrete and/or accelerated validation process (*i.e.* improve the assertiveness and reactiveness of the process).

Finally, the methodology is necessarily a collaborative modeling process, as it requires the regulatory body to validate the models produced by the model engineer. This can be done through a cross-reading of the semiformal models. Unfortunately, this does nothing to improve the quality of the validation process currently used[13]). This is because the validation process is still exposed to erroneous assessments -a false appreciation of the model that leads it to be validated as a faithful representation of the regulations. Nevertheless, an extensive traceability between the regulations and the produced models should strongly limit this situation.

5 Conclusion

The regulator's *Conceptual View of the Real World* is a crucial element for understanding the regulations, ensuring their pertinence and verifying their actuality. As such, it needs to be made explicit and checked to ensure the validity of its assumptions, of its statements and the robustness (comprehensiveness) of their concern.

Through the formalization of various international and supranational aeronautical regulations we have concluded that, in order to achieve this, it should be mandatory to integrate the use of semiformal methods into the current rulemaking process! Indeed, as mentioned in Section 3.2, semiformal methods

[13]For more information concerning the current rulemaking process see [1]

that have been enriched with OCL expressions allow regulatory bodies to 'master the complexity' of their regulations, by providing them with a comprehensible, structured and maintainable representation of their *Conceptual View of the Real World*, where the entity-classes and regulatory requirements are interlinked. This last point is very important as it promotes the holistic analysis/view of the regulations, and facilitates their regression analysis in case of amendments.

Granted, formal methods could also contribute to the accomplishment of these improvements, however their low comprehensibility by regulators (see Figure 3) means that they can only be used 'behind the scenes', to help disambiguate the most tricky elements/parts of the regulations before presenting them to the regulatory authorities via semiformal models. Otherwise, one must consider the costs associated to (and the time consumed in) training regulators in the use/utilization of formal notations. These costs, weighed against the foreseen benefits, have convinced us that, presently, this alternative is not a worthwhile enterprise.

Nevertheless, if one decides to undertake this course, and adopt formal methods as the primary tool for assessing civil aviation regulations, they should not undermine the importance of having the model validated by the aviation authority. For this, they should opt for a validation process involving a third trusted party. This party, external to the civil aviation authority and to the model engineers could be composed of engineers with a double-competency in civil aviation regulations and in formal methods. This double-competency would allow them to validate the formal models and help with the analysis of the regulations.

References

[1] European Aviation Safety Agency (EASA) Management Board. Decision of the Management Board Amending and Replacing Decision 7-03 Concerning the Procedure to be Applied by the Agency for the Issuing of Opinions, Certification Specifications and Guidance Material ('RULEMAKING PROCEDURE'), 2007. http://www.easa.europa.eu/ws_prod/g/doc/About_EASA/Manag_Board/2007/MBDecision08-2007amendingrulemakingprocedure.pdf.

[2] Asaf Degani. On the Design of Flight-Deck Procedures. Technical Report NASA Contract NCC2-327 and NCC2-581, Georgia Institute of Technology, 1994. http://ti.arc.nasa.gov/m/profile/adegani/Flight-Deck_Procedures.pdf.

[3] Regine 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 (S.P.I.P.)*, 11(5):487–503, July 2006. http://dx.doi.org/10.1002/spip.291.

[4] Federal Aviation Administration (FAA). *FAA Writing Standards. Order 1000.36*. Federal Aviation Administration (FAA), 2003. http://www.faa.gov/documentlibrary/media/order/branding_writing/order1000_36.pdf.

[5] United States Government Accountability Office (GAO). *System Safety Approach Needs Further Integration into FAAs Overisght of Airlines*. United States Government Accountability Office (GAO), 2005. http://www.gao.gov/cgi-bin/getrpt?GAO-05-726.

[6] Plain English Network (PEN). *Writing User-Friendly Documents: A Handbook for FAA Drafters*. Federal Aviation Administration (FAA), 2000.

[7] Eduardo Rafael López Ruiz. Formal Specification of Security Regulations: The Modeling of European Civil Aviation Security, 2006.

[8] Eduardo Rafael López Ruiz and Béatrice Trigeaud. La Modélisation Informatique des Règles de Droit Relatives à la Sûreté du Transport Aèrien International. *Annuaire Français de Droit International (A.F.D.I.)*, 53:672–696, 2007.