

EDEMOI: a methodology for Security of Air Transport System

*M. Lemoine & E. Lopez Ruiz * , Y. Ledru & D. Bert ***

*R. Laleau *** , F. Peureux & F. Bouquet **** ,*

*V. Donzeau-Gouge , C. Dubois, J.-F. Etienne ***** , S. Vignes ******

**ONERA/CdT/SAE, 2 Avenue E. Belin – 31055 Toulouse CEDEX, France*

*** LSR/IMAG, Grenoble, France*

****LACL, Paris, France*

***** LIFC, Besançon, France*

******CEDDRIC/CNAM, Paris, France*

******GET/ENST, Paris, France*

Abstract

This paper focuses on the results obtained thru the employment of semi formal and formal specification methods to model security in the European Air Transport System. More specifically, this paper discusses the application and enhancement of the EDEMOI approach to the modeling of European Regulation 2320/2002, which sets the standards for aviation security at the airport level. The EDEMOI approach allows representing: the Air Transport domain and its security properties, with the goal of appraising their overall quality. For this, a semi formal **UML** model is used to capture the static and dynamic aspects of the system and the regulation. This allows aviation-security specialists validate/invalidate the conceptual layout that will subsequently be used to create a procedurally-abstract formal model (built using a dedicated logic) that will be used to test scenarios and thereby reinforce the checking of the security standards. This paper presents the EDEMOI methodology and its successful use in the context of airport security.

1. Introduction

In recent decades, the air transport sector has been hard-hit by a succession of attacks involving the introduction of prohibited articles onboard aircraft. Undoubtedly, the hijackings of September 11th, 2001 remain as the most dramatic of such attacks. Since this attack, both the International Civil Aviation Organization¹ (ICAO) and the European Commission (EC), by way of the European Civil Aviation Conference² (ECAC), have placed strenuous efforts and attention to improve ground based airport security.

Among the various measures taken to accomplish this goal was the drafting of Regulation 2320/2002, a natural language document that establishes the security standards regulating ground based airport security in Europe. This document came to be a refinement of the international standards set out in ICAO's Annex 17, establishing a common effort within Europe. Its final draft was validated in 2002 following a "peer review" process, where security specialist painstakingly analyzed and discussed its specific wording and nature, until a consensus was reached and all those involved considered the draft to be mature.

Today however, following operational feedbacks, Regulation 2320/2002 has undergone amendments to strengthen its innate quality, specifically concerning its overall **consistency** and **robustness**. Proving therefore, that the approach currently adopted to develop aviation regulations is very limited in terms of guaranteeing their innate quality.

This limitation is of great consequence since (analogously with safety-critical software) this quality is what ensures that the benchmark regulation, being enforced at airports, is not inherently rendered ineffective due to contradictory policies (either by themselves or globally). And that it exhaustively covers all the possible scenarios in its domain of application (from the airport entrance to the aircraft cabin).



¹ ICAO: <http://www.icao.org>

² ECAC: <http://www.ecac-ceac.org>

To illustrate the importance of these qualities, the paradigm of Article 4.3 (of Regulation 2320/2002) reveals the crippling effect that the slightest subtlety could have on the system's overall success.

The mind-set that led to the drafting of Article 4.3 was that most of the security measures imposed by Regulation 2320/2002 had been primarily conceived for "high traffic" commercial airports. It was therefore disproportionate to apply these same measures at "small airports". Article 4.3 would help alleviate such burdens by establishing the conditions (and limits) under which an airport could be labeled as "small" (and therefore be derogated from applying the same stringent security standards enforced at larger airports). But, as shown in Table 1, a very subtle phrasing error distorted its scope, alleviating only a fraction of the small airports it was supposed to exempt. Interestingly, this slip-up went unnoticed even during translations. However, when expressed **mathematically** the difference between the intended limit and the proposed limit are made apparent.

Table 1. Analysis of the revision of Article 4.3(a).

4.3.(a) Criteria for Small Airports.		Version 30.12.2002
"airports with a yearly average of two commercial flights per day..."		 $\text{yearly_average} = 2 \frac{\text{flights}}{\text{day}}$
4.3.(a) Criteria for Small Airports.		– AMENDED*–
"airports with a yearly average of no more than two commercial flights per day..."		 $0 \leq \text{yearly_average} \leq 2 \frac{\text{flights}}{\text{day}}$
<p>* The original version of article 4.3.(a) was inconsistent with the stated hypothesis that "airports with a <i>lower frequency</i> of operations (usually) <i>present a lower level of threat</i>."</p>		

From this example, it can be intuitively seen that the security provisions contained in the regulation may be mathematically represented. And, in cases such as this one, the representation can even improve its comprehension. This goes to the basis of why the EDEMOI methodology [1] proposes the implementation of semi-formal and formal methods to assist in the specification and validation of regulation documents. Specifically those concerning the critical domains of civil aviation, such as ground based airport security.

This paper shall focus on the results obtained by the application of this methodology to the specification of the security-relevant parts of *Regulation (EC) 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security* [2].

2. The EDEMOI Approach

In 2003, this same group of French universities and research laboratories proposed the creation and adoption of a methodology - using requirement engineering and formal method techniques - that would assist in the specification, design and validation of regulation documents.

This proposed methodology, known as the 'EDEMOI approach', adopts the formal specification and design methods used in the computer-science community and adapts them in order to model, validate and check the legal framework influencing airport security.

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 for consistency, robustness and unequivocalness.

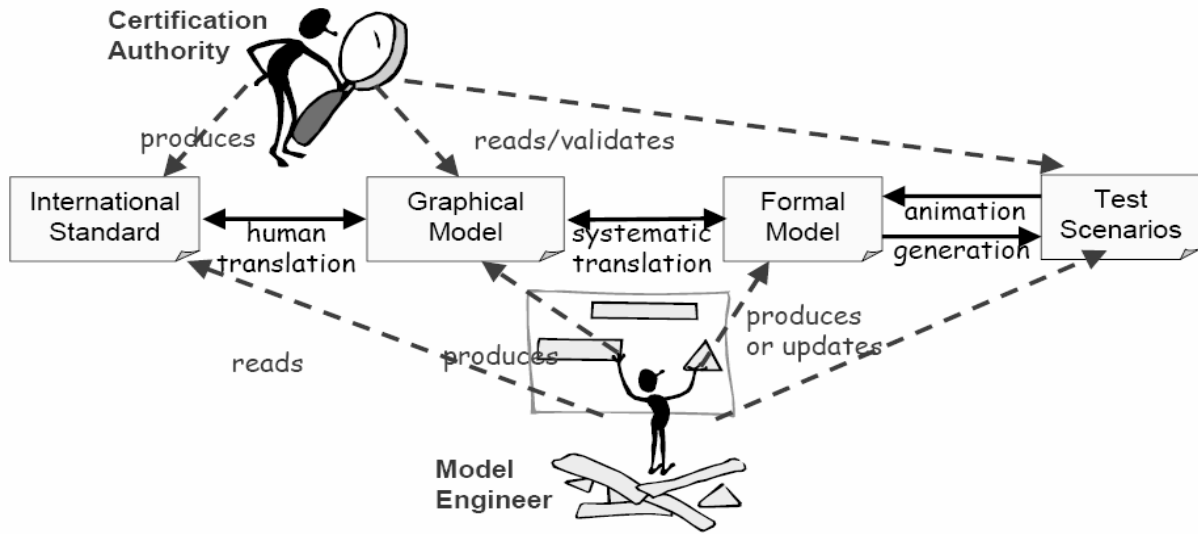


Figure 1. The EDEMOI stakeholders and methodology.

In the first step of this approach, a model engineer extracts the security goals imposed in the International Standard and translates them into a semi formal 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 semi formal model to produce a formal model that can be analyzed through test scenarios.

By employing this methodology, and with the encouragement of ICAO, EDEMOI project partners achieved positive results [3] in the modeling of the *Annex 17 to the Convention on International Civil Aviation*. In addition, a part of this methodology was applied in the New Aircraft Concept Research (NACRE) project, playing a leading role in the assessment of the security properties for a concept cabin [4].

Now, this approach has been extended to examine European civil aviation security through the modeling of the security-relevant parts of *Regulation (EC) 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security*.

3. The Modelling of Regulation (EC) 2320/2002

The model of Regulation 2320/2002 was deliberately chosen to emphasize on the static and dynamic aspects of passenger and baggage screening. Consequently, it centers itself on the *annex* of Regulation 2320/2002. More particularly on the provisions concerning passenger and baggage screening, which are sections: 2. *Airport Security*, 4. *Passenger and Cabin Baggage*, and 5. *Hold Baggage*.

For this, the static aspect were considered to be all the innate properties and defining traits of the players (passenger, staff member and the different airport areas), while the dynamic aspects represent how these players evolve as a consequence of the operations they perform and of the conditions imposed upon them by the system (e.g. passenger’s transition from the check-in desk to the possible boarding of the aircraft).

The approach chosen for the study of Regulation 2320/2002 consists of mathematically expressing its security standards and then linking them together (using formal logic theories) into a formal model which can be tested to help identify contradictions between the security objectives (*Consistency check*) and/or to verify that it exhaustively covers all the possible states/scenarios in its domain of application (*Robustness check*).

3.1 Interpreting the Regulation

Natural language documents are inherently ambiguous text since the phrases and words which compose them take on different meanings, depending on the semantics. This immediately poses a problem for safety-critical texts such as aviation regulations, as no one can guarantee their homogenous interpretation. Regretfully, the situation is even bleaker for international conventions such as Regulation 2320/2002, which is translated and enforced in the 20 official languages of the European Union.

However, as our model requires that a standardized interpretation of the wording in Regulation 2320/2002 be used as the basis for the formal model, a deep study of its text (and that of its founding sources³ in their original

³ ICAO’s Annex 17 and Document 8973

language) was undertaken. This helped delineate the mind-set and purpose behind each of its security provisions, and led to the creation of an intuitive semiformal model (detailed in Part 4) that tackled its innate ambiguity.

3.2 Tools Used

For the construction of the semi formal Model of Regulation 2320/2003 the **Unified Modeling Language**⁴ (UML) profiled itself as the most appropriate tool, since it enables the creation of abstract, but graphically intuitive models that can be systematically translated to a more rigorous notation.

In this case, the semi formal model was composed of “*Class Diagrams*”, that captured the structural (static) aspects of the Regulation, and “*State-Transition Diagrams*” depicting its operational (dynamic) side.

The Formal model was itself created using the **Z notation**, which is a formal specification language that utilizes axiomatic semantics derived from pure mathematics –and specifically from: first order predicate calculus and set theory– to specify and model system’s behavior.

The specification was performed thru the statement of pre- and post-condition axioms describing the Regulation’s input and output limitations on the operations performed by the players.

So, in the case of nominal passenger screenings, the specification recognizes that the person being screened needs to be a passenger, and that he should not carry any prohibited articles. On the other hand, it is not concerned about details such as: the type of equipment that should be used or the number of persons implementing the security checks. This type of approach allowed the model to describe the system with complete *procedural abstraction*, allowing its **rationale** to be tested using formal verification techniques.

3.3 Traceability of Source Documents

Throughout the project, it was necessary to specify and reference all the security properties referred to in the models. Therefore, to assure traceability at every level, we implemented a referencing system using the Regulation’s own numbered structure. This eased the manual translation from the UML model to the Z model, and linked back model specifications to the specific requirements in the Regulation.

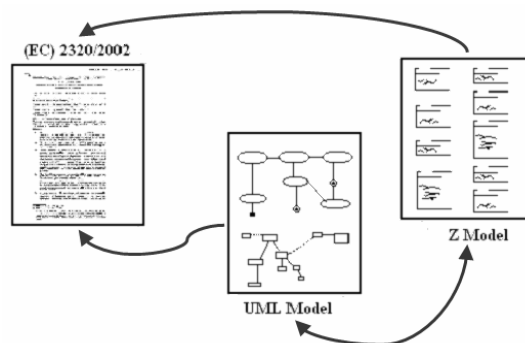


Figure 2. Traceability at every level.

Another use for this referencing system, already studied by the EDEMOI partners and ICAO, is to ease the implementation of modifications and corrections throughout the models. For example, due to its cascading effect it is possible to track the consequential effects of amendments proposed to the Regulation. Vice versa, any failure detected in the model is completely identified throughout the source document.

4. Semi formal Model

In order to exemplify the UML semi formal model obtained in the study of Regulation 2320/2002, this paper shall briefly go over an insightful part of the ‘UML class diagram’, where the static aspects of passengers are depicted.

To facilitate its comprehension, this will be done thru a sectional analysis of the diagram elements. The descriptions shall include analysis of both the ‘inter-box’ relationships, which describe the interactions and associations between the different boxes (classes) portrayed, and the ‘intra-box’ properties, which state the attributes and operations specific to the boxes.

With this in mind, one can notice that the diagram shown in Figure 3 is composed of 5 classes (one in each box): *Person*, *Passenger*, *Airline Ticket*, *Government Issued ID* and *Boarding Pass*.

⁴ UML: <http://www.uml.org>

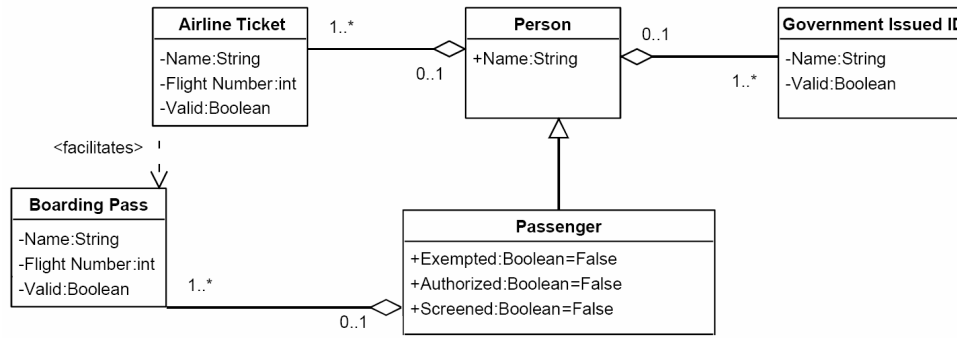


Figure 3. The Passenger-Person class diagram.

Focusing our analysis with respect to the *Passenger* element, the inter-box relationships graphically tell us that:

- A ‘*Passenger*’ is a type of (<—) traveling ‘*Person*’ which, in addition of having (<—) at least one (1..*) valid ‘*Airline Ticket*’ and ‘*Government Issued Identification*’, has at least one (1..*) ‘*Boarding Pass*’.
- This diagram also imposes that all three travel documents are of his/her exclusive property (0..1). And, it reminds us that it is the ‘*Airline Ticket*’ that facilitates the attainment of the ‘*Boarding Pass*’.

4.1 Person

Now, the intra-box analysis of a ‘*Person*’ (Figure 4) shows that each box (class) is composed of three sections. The first (from top to bottom) is used to identify the class, the second one shows the *attributes* (or properties) specific to this class, and the third one lists its *operations* (or allowed behaviors).

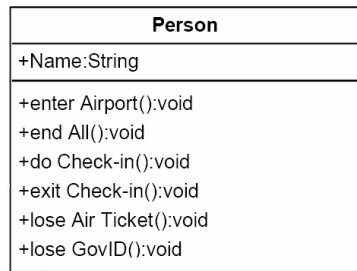


Figure 4. The Person class.

A more detailed analysis shows that this class has only one security-related attribute, ‘*Name*’, which in fact represents any individually unique feature that can be used to distinguish a person’s identity (i.e. a name, a national identification number, ...). More interestingly, its operations (shown in the lower box) reflect the fact that people, as such, cannot enter Security Restricted Areas (S.R.A.). This is imposed by limiting the domain of application of their operations, going from the airport’s exterior (*enter Airport()*) to just before the entrance to S.R.A.

4.2 Passenger

As mentioned previously, the ‘*Passenger*’ (Figure 5) is a type of traveling ‘*Person*’. Therefore, due to this relation (<—) it inherits all of the attributes, operations, and relationships previously defined for such. Yet, in addition to these, the ‘*Passenger*’ has its own security-related attributes, such as: **exempted** from screening, **authorized** to carry prohibited articles, or **screened** (to the standard imposed by 2320/2002). These attributes have been declared as Boolean, so their values will be limited to the logical *True* or *False* value.

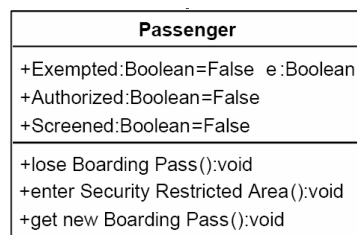


Figure 5. The Passenger class.

In a similar fashion to the class ‘*Person*’, the operations for the class ‘*Passenger*’ are also restricted in terms of their domain of operation. This is because entry into any S.R.A. requires a successful completion of the security controls carried out at its entry points. This led to the creation of a special category of passengers termed ‘*Secure Passenger*’, designating those whose attribute values comply with the requirements to enter S.R.A.

4.3 Secure Passenger

This class (Figure 6) inherits the properties and operations of both ‘*People*’ and ‘*Passenger*’ classes. It is exclusively composed of passengers that have been granted access into S.R.A. such as: *screened passengers* (where the attribute Screened is set equal to True), *diplomatic passengers* (Exempted=True) and *in-flight security officers* (Authorized=True and Screened=True).

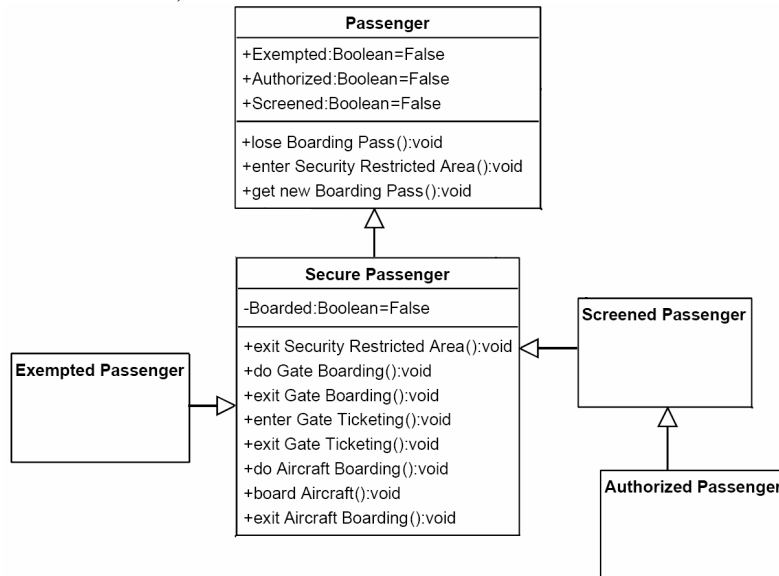


Figure 6. The different types of Passenger.

Correspondingly with the security objective (which entails that only secure passengers are allowed to board an aircraft), the list of operations available for ‘*Secure Passenger*’ is extended to include those required inside Security Restricted Areas. The attribute **Boarded** is also added.

It is important to notice that for all three of these aforementioned classes (‘*Person*’, ‘*Passenger*’ and ‘*Secure Passenger*’), an evolution seems to suggest itself, exposing the dynamic facet of a person’s transition through the airport.

Such transitions were depicted using a ‘State-transition Diagram’. In it, each distinct ‘State’ represents a unique combination of the class’ attribute values, with transitions leading to them (triggered by the different operations).

For example, the diagram shown in Figure 7 graphically represents how a nominal ‘*Secure Passenger*’ that performs the ‘*exit Security Restricted Area*’ operation, triggers a transition back to the ‘*Passenger*’ class, thereby reflecting that the logical value of his *Screened* attribute changed to *False*.

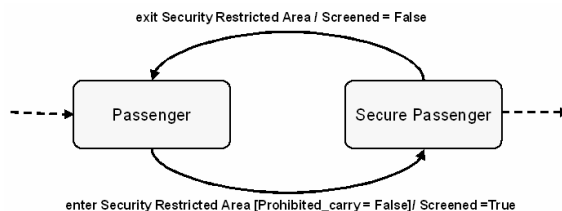


Figure 7. Abstract from the State-Transition Diagram.

Again, given the procedurally abstract approach used, the specificities behind each transition were irrelevant for the model. So, independently of the reason why the nominal passenger exited the S.R.A., the operation results in the losing of his/her screened status (Screened=True → Screened=False).

As a final point, the semi formal model proposed, (and discussed in this paper) was obtained after a heavy study of the Regulation text. And, while these diagrams are not the only possible representation of its security properties, they are the most compatible with the structure required by the Z notation to ensure a faithful duplication of its rationale.

5. Formal Model

As mentioned previously, the formal model of Regulation 2320/2002 is entirely composed of mathematical expressions. These describe its security objectives and are linked together under the premise of formal logic theory.

So, using the Z notation, the attributes declared within the semi formal model are fully described in the formal model by the system's properties, which represent the pre- and post-conditions influencing the security objectives. For example, the *Screened* attribute (initially declared in the semi formal model) only acquires relevance within the regulation when the implications surrounding its logical value are determined. That is to say, it is without sense until it is formally stated that “a passenger with a logical value of *True* in its *Screened* attribute, is not **illegally**⁵ carrying prohibited articles”. This is solely done in the formal model (Figure 8).

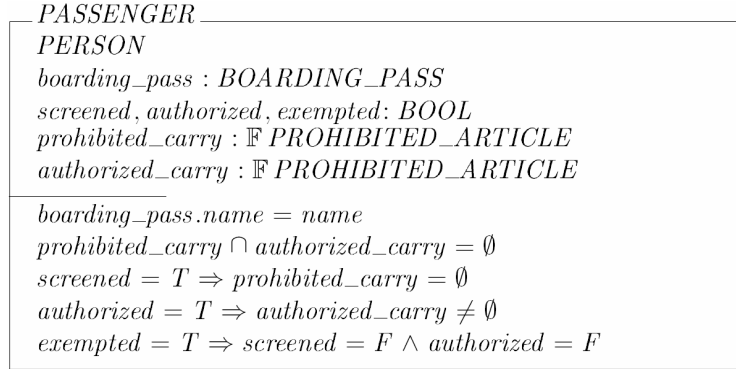


Figure 8. The Passenger schema.

So, without having to scrutinize the notation, one can immediately perceive that the formal specification in the *Passenger* schema not only restates the inheritance relation, attributes and associations that were present in the semiformal model, but actually goes a lot further by describing their interdependencies and implications.

The model also specifies the security provisions surrounding the operations performed by the different players, for instance, the screening of passengers, baggage and staff members, passenger boarding, baggage loading, etc.

Furthermore, the full model also includes mathematical specifications describing the different airport areas (e.g. the airside and landside areas, the airport perimeter, security restricted areas and their critical parts, the aircraft's cabin and baggage hold...). For example, Figure 10 describes the conditions and attributes associated to the ‘*Critical Parts of Security Restricted Areas*’ (i.e., the parts of an airport to which departing passengers, after screening, have access).

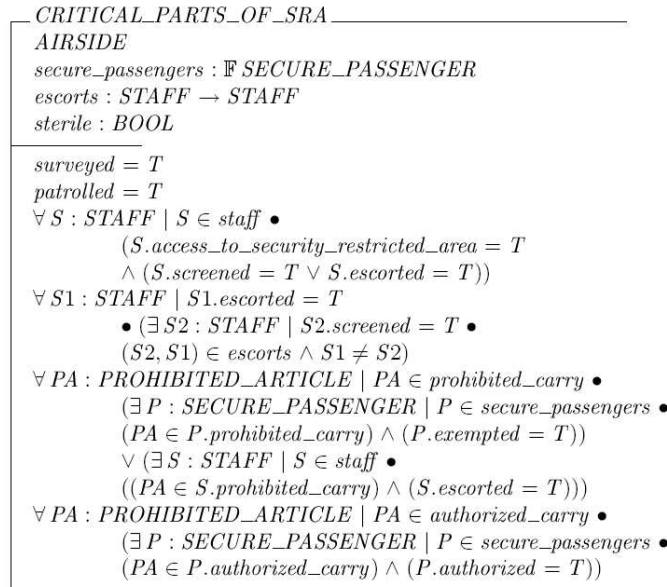


Figure 10. Formal specification of the airport's Critical parts of Security Restricted Areas.

⁵ For our model, in-flight security officers are considered to be *Screened Authorized passengers*, legally carrying a prohibited article.

However, given its intricacy, this type of description requires a strong familiarity with the Z notation to fully grasp its meaning. It is for this reason that (as shown in Figure 1) these schemas are only manipulated by model engineers, and why elaborating them further would be outside the scope of this paper. The formal model of Regulation 2320/2002 also integrates numerous ‘initialization operations’, which are used to generate the different players in the model and to define their attributes’ initial value. It is with the aid of these operations that the formal model can be animated, using the different test-case scenarios conceived by the authorities, to effectively analyze its behavior under relevant operational conditions.

6. Other Applications

Moreover, as a result of having adopted the methods commonly employed in the computer-science community, for the development of safety-critical software and hardware, our formal model comes to be the step previous to the creation of a source code. Therefore, being that our model has the regulation’s security requirements already specified in a machine-interpretable language, it can be used as the logical backbone of an automated airport-security system.

For example, the first invariant found in the *PASSENGER* schema (Figure 8) states that the name printed on the boarding pass must be reconciled with the passenger’s own identity. Our formal specification allows computers to know of this existing link, so, when fully electronic boarding passes are adopted; a computer component could be placed at the entrance to the screening checkpoints to reconcile the passenger’s identity (using Machine Readable Travel Documents or Radio Frequency Identity Card) to a known passenger manifest. The software required for such a task would be based on the logic proposed by our schemas, as these are the regulation standards imposed by the European Commission.

7. Conclusions

Current events in civil aviation have exposed the need to enhance the security of the Air Transportation System. These enhancements have been mainly put in place through two actions: the drafting of security standards and the establishment of audit and quality controls programs (to help states fight deficiencies and irregularities in the implementation of these standards).

However, a fundamental problem persists in the current approach. The same “peer review” process that failed to assess omissions in the previous regulations is again sought to validate the new versions.

This is why the EDEMOI consortium has taken to the task of implementing their approach on the key regulations influencing ground-based airport security in Europe: ICAO’s Annex 17 and Regulation 2320/2002. In both cases, the EDEMOI approach has proven its aptitude for modeling and analyzing the security standards. Currently, the proposed methodology is being broadened to include a systematic process that will ease the integration of new requirements into already established regulations. This is done with the idea of helping preserve the robustness and consistency of regulation documents, even while these evolve to incorporate the innovations in aeronautics.

References

- [1] R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge and F. Peureux.. Application of Requirements Analysis Techniques to the analysis of civil aviation security standards. In International Workshop on Situational Requirements Engineering Processes (SREP’05), Paris, France. 2005. Available at: <http://www-lsr.imag.fr/EDEMOI/PresentationsPubliques/SREP05LaleauVignes.pdf>
- [2] E. R. López-Ruiz, Formal Specification of Security Regulations: The Modeling of European Civil Aviation Security. M.Sc. Thesis. Ecole Nationale Supérieure de l’Aéronautique et de l’Espace (Supaero), Toulouse, FR. December 2006.
- [3] Y. Ledru, Elaboration d’une Démarche et d’outils pour la Modélisation Informatique, la validation et la restructuration de réglementations de « sûreté », et la détection des biais dans les aéroports. Rapport Final. October 2006, Available at: http://www-lsr.imag.fr/EDEMOI/LivrablesPublics/EDEMOI_RapportFinal.pdf
- [4] M. Lemoine, K. Yazdanian, A methodology for assessing security properties of a new cabin concept. Third Management Committee Meeting, NACRE Workshop. Munich, Germany. October 2006.



This page has been purposely left blank