Modeling Airport Security Regulations in Focal

David Delahaye, Jean-Frédéric Étienne,
and Véronique Viguié Donzeau-Gouge

CEDRIC/CNAM, Paris, France,
David.Delahaye@cnam.fr, etien_je@auditeur.cnam.fr,
donzeau@cnam.fr

Abstract. We describe the formal models of two standards related to airport security: one at the international level and the other at the European level. These models are expressed using the Focal environment, which is an object-oriented specification and proof system. We show how Focal is appropriate for building a clean hierarchical specification for our case study using, in particular, object-oriented features to refine the international level into the European level and parameterization to modularize the development.

1 Introduction

The primary goal of the international standards and recommended practices regulating airport security is to safeguard civil aviation against acts of unlawful interference. These normative documents detail the roles and responsibilities of the various stake-holders and pinpoint a set of security measures (as well as the ways and means to implement them) that each airport serving civil aviation has to comply with. In addition, the entire regulatory system is organized in a hierarchical way, where each level has its own set of regulatory documents that are drafted and maintained by different bodies. All these documents are written in natural language and due to their voluminous size, it is difficult to manually assess the consistency of the entire regulatory system. Moreover, informal definitions tend to be inaccurate and may be interpreted in various inconsistent ways by different readers. However, these documents have the merit of being rigorously structured. Ensuring their consistency and completeness while eliminating any ambiguity or misunderstanding is a significant step towards the reinforcement of airport security.

In this paper, we describe the formal models of the two standards related to airport security as well as some results obtained from their analysis. The first standard is the international standard Annex 17 [4] (to the Doc 7300/8) produced by the International Civil Aviation Organization (ICAO) and the second one is the European Directive Doc 2320 [1], produced by the European Civil Aviation Conference (ECAC), which is supposed to refine the first one at European level. We took as a starting point the preventive security measures described in Chapter 4 of Annex 17 and focused on security measures 4.1, 4.2, 4.4, 4.5 and 4.7. The formalization was carried out within the framework of the

EDEMOI[1] project [5, 2], which aims to integrate and apply several requirements engineering and formal methods techniques to analyze regulation standards in the domain of airport security. The formal models have been designed using the Focal [6] environment and from their analysis, we have been able:

1. to clarify **ambiguities** and misunderstandings resulting from the use of informal definitions expressed in natural language;
2. to detect **inconsistencies** or to provide evidence of their absence;
3. to identify **hidden assumptions**, which may lead to shortcomings when additional explanations are required (for example, in airport security programs).

Another motivation of this work is to validate and assess the design features as well as the reasoning support mechanism offered by the Focal [6] specification and proof system. In Focal, it is possible to build applications step by step, going from abstract specifications, called *species*, to concrete implementations, called *collections*. These different structures are combined using inheritance and parameterization, inspired by object-oriented programming; moreover, each of these structures is equipped with a carrier set, a list of functions, properties and theorems. In collections, all functions are defined and all properties are proved.

In our case study, we intensively use the features of inheritance and parameterization. Inheritance allows us to naturally express the refinement of the international level by the European one. Parameterization provides us with a form of polymorphism so that we can factorize parts of our development and obtain a very modular specification. Finally, regarding the reasoning support, the first-order automated theorem-prover of Focal, called Zenon, bring us an effective help by automatically discharging most of the proofs required by the specification.

2 Formalization

2.1 Model domain

The first step of the modeling process is to identify the subjects necessary for the formalization of the preventive security measures, together with their respective properties/attributes and the relationships between them. It is also essential to determine the hierarchical organization of the identified subjects in order to effectively factorize functions and properties during the formalization process (through the use of inheritance and parameterization). This is done by determining the dependencies between the security measures w.r.t. the definitions of terms used in the corresponding normative document. For example, let us consider the following security measure described in Chapter 4 of Annex 17:

[1] The EDEMOI project is supported by the French National "Action Concertée Incitative Sécurité Informatique".

4.5.1 Each Contracting State shall establish measures to ensure that originating hold baggage is screened prior to being loaded into an aircraft engaged in commercial air transport operations departing from a security restricted area.

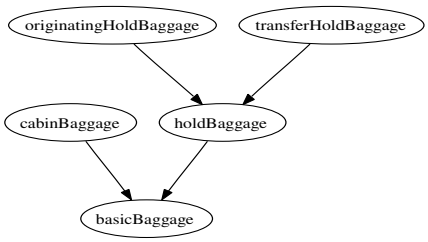

Fig. 1. Hierarchy for baggage in Annex 17.

To be able to formalize this security measure, we have to define the subjects *originating hold baggage*, *aircraft* and *security restricted area*, together with the relations between them. Moreover, we need to define appropriate attributes for the *originating hold baggage* subject to characterize the state of being *screened* and of being *on board*. Finally, to complete the formalization, we have to specify the integrity constraints induced by the regulation (e.g. weapons carried in hold baggage are considered to be inaccessible during flight time). The hierarchies of subjects obtained after analyzing all the preventive security measures of Annex 17 are represented by a Focal model, where each subject is a species. For instance, the Focal model for baggage is given in Figure 1[2] (where nodes are species and arrows inheritance relations s.t. $A \leftarrow B$ means species B inherits from A). For possible extensions during the refinement process, the carrier type of the species is left undefined (abstract) and their functions are only declared.

2.2 Annex 17: preventive security measures

An important aspect of regulation modeling is that the formal model needs to impose a certain structure that will facilitate the traceability and maintainability of the normative documents. To achieve this purpose, the model presented in this section follows the structural decomposition proposed by Chapter 4 of Annex 17, while taking into account the dependencies between the preventive security measures. Moreover, it is crucial for the model to make the distinction between the security measures and the ways and means to implement them. Most of the security measures are fairly general and correspond to objectives that each member state has to fulfill. As a result, in our model, they are defined as invariants and each airport security programme must provide procedures that satisfy these invariants. The consistency and completeness of the regulation are achieved by establishing that the fundamental security property, defined in paragraph 4.1 of Annex 17, is satisfied by all the security measures, while ensuring their homogeneity. The general structure of the Annex 17 model is represented in Figure 2.

[2] This figure (as well as the others in this paper) was automatically generated using the inhgraph tool of the Focal environment, which produce, from a Focal specification, a graph description in the DOT format.

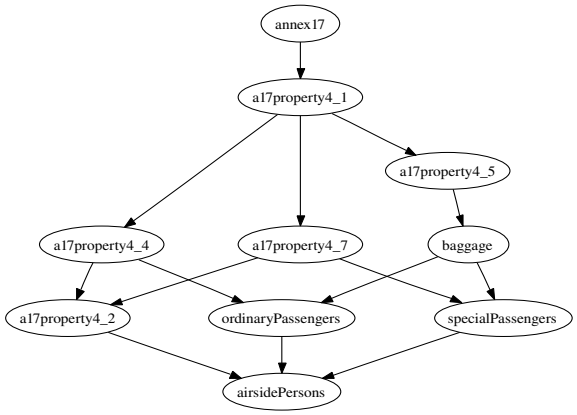

Fig. 2. Structure of Annex 17.

The species airsidePersons, ordinaryPassengers, specialPassengers and baggage introduce the set domain of the identified subjects as well as their relational constraints (e.g. two passengers cannot have the same luggage). The preventive security measures are formalized in species a17property4_2, a17property4_4, a17property4_5 and a17property4_7, and their dependencies are defined according to the hierarchical organization of the subjects they regulate. The fundamental security property is defined in a17property4_1. It is at this level that the set of on board objects is defined. Finally, the theorems establishing the consistency and completeness of the regulation are defined in the species annex17. The following is an example of such theorems:

```
theorem consistency : !property_4_2 -> !property_4_4 ->
  !property_4_5 -> !property_4_7 -> !property_4_1
proof : by do_set!union1, wp_set!union1 def !onboardDangerousObjects,
          !property_4_1, !property_4_2, !property_4_4, !property_4_5,
          !property_4_7;
```

where property_4_2, property_4_4, property_4_5 and property_4_7 correspond to the intermediate lemmas defined for each category of preventive security measures (for example, see Section 2.4). Property property_4_1 corresponds to the fundamental security property defined in Paragraph 4.1 of Annex 17.

2.3 Doc 2320: some refinements

The document structure of Doc 2320 follows the decomposition presented in Chapter 4 of Annex 17. Refinement in Doc 2320 appears at two levels. At the subject level, the refinement consists in enriching the characteristics of the existing subjects or in adding new subjects. At the security property level, the security measures become more precise and sometimes more restrictive. The verification of the consistency and completeness of Doc 2320 is performed in the same way as in Section 2.2. However, since Doc 2320 refines Annex 17, an additional verification is required to show that the security measures that it describes do not invalidate (or are not less restrictive than) the ones defined in Annex 17. Thus, in addition to consistency proofs, another kind of proofs appears, that are refinement proofs. The model structure obtained for Doc 2320 is described in Figure 3 (where the existing species coming from Annex 17 are distinguished with dashed nodes).

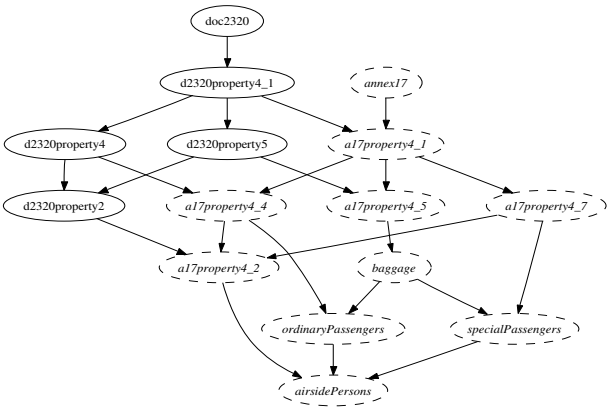

Fig. 3. Structure of Doc 2320.

As can be seen, the refinement is performed in such a way as to preserve the dependencies between the security measures. Moreover, it can be observed that species a17property4_7 does not have a Doc 2320 counterpart. This is because, in Doc 2320, no mention to special categories of passengers is made. We assume that in this case, the international standard still prevails. Species d2320property4_1 only extends the scope of property 4.1 to deal with newly identified subjects.

2.4 Certification: proving with Zenon

Basically, there are two ways of providing proofs to Zenon: the first one is to give all the properties and definitions necessary for Zenon to build a proof automatically; the second one is considered when Zenon needs some assistance (in the form of some reasoning steps or auxiliary lemmas) or when the user wants to present his/her proof in a more readable form (for this purpose, a proof language inspired by [3] is available).

As we are concerned with regulation modeling, the formal models produced are fairly abstract and have hardly any computational content. Consequently, most of the proof obligations could be derived by simple logical deductions from the formalized security properties. Therefore, knowing only the provided properties and definitions, Zenon managed to discharge them automatically. To give an insight of the complexity of such proof, let us consider the one derived for Property property_4_5 used in Theorem consistency (see Section 2.2):

```
theorem property4_5 : all s in self, all a in ac,
 ac_set!member (a, !departureAircraft (s)) -> all o in do,
  do_set!member (o, !dangerousObjectsInHold (a, s)) -> do!is_authorized (o)
proof: by ..., !property_4_5_1, ol!invariant_screened, tfl!invariant_screened,
       !property_4_5_4, !inv_secureTfLuggage def !dangerousObjectsInHold
```

where s is a particular instance of the regulation dedicated to hold baggage, a an aircraft, and o a dangerous object. With this theorem, we show that the prescribed security measures related to hold baggage (e.g. Paragraph 4.5.1 in Section 2.1) are sufficient to guarantee that hold baggage (whether originating or transfer) loaded into an aircraft do not contain any unauthorized dangerous objects. Here, we only provide the main properties and definitions necessary to understand the proof construction process. Moreover, to simplify the presentation, we slightly modify the specification to only consider dangerous objects in

general and ignore the special treatment required for weapons. To be able to visualize the automatically derived proof, we need to describe how the concerned security measures were formalized in species a17property4_5 (see Figure 2). The following concerns Paragraph 4.5.1 (see Section 2.1):

```
property property_4_5_1 : all s in self, all l in ol,
 ol_set!member (l, !originatingHoldLuggage (s)) ->
     ol!loaded (l) -> ol!screened (l);
```

where s represents a particular instance of the regulation and l an originating hold baggage. This property states that if originating hold baggage are loaded into an aircraft then they have been subjected to appropriate screening. The security property 4.5.4 regulating transfer hold baggage is formalized in a similar way, except that transfer hold baggage coming from secure destinations may not be subjected to screening. Finally, the fact of being a screened hold baggage is specified in species holdBaggage (see Figure 1) as follows:

```
property invariant_screened : all s in self, !screened (s) -> all o in do,
     do_set!member (o, !get_dangerousObjects (s)) -> do!is_authorized (o);
```

where s represents a hold baggage. This property states that screened hold baggage are considered to only contain dangerous objects that have been authorized. In species a17property_4_5, a similar property (inv_secureTfLuggage) is defined for transfer hold baggage coming from secure destinations.

2.5 Analyses and results

Ambiguity During the formalization process, various ambiguities could be clarified. For example, let us consider the following property:

> *4.1 Each Contracting State shall establish measures to prevent weapons, explosives or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, the carriage or bearing of which is not authorized, from being introduced, by any means whatsoever, on board an aircraft engaged in international civil aviation.*

This statement can be interpreted in two different ways: either dangerous objects are *never* authorized on board, or are admitted on board *only if* they are authorized. According to the ICAO, the second interpretation is the correct one, since Paragraph 4.1 cannot be interpreted without considering the general context of the regulation.

Consistency and completeness The purpose of Theorem consistency (see Section 2.2) is to verify whether the fundamental security property can be derived from the set of preventive security measures. However, this theorem does not guarantee the absence of contradictions in the regulation. A way to tackle this problem is to try to derive False from the set of security properties and to let Zenon work on it for a while (.e.g. one day or much more with a better knowledge of the strategies used by Zenon and with appropriate profiling methods). If the proof succeeds then we have a contradiction, otherwise we can only have a certain level of confidence.

Hidden assumptions The consistency theorems also allowed us to identify some hidden assumptions done during the drafting process, for instance:

1. since disruptive passengers who are obliged to travel are generally escorted by law enforcement officers, they are considered not to have any dangerous objects;
2. unlike other passengers, transit passengers are not subjected to any specific security control but should be protected from unauthorized interference at transit spots. This implies that they are considered to be secure and consequently do not carry any unauthorized dangerous objects.

Development The entire formalization takes about 10000 lines of Focal code, with in particular, 150 species and 200 proofs. It took about 2 years to be completed. The development is freely available and can be compiled with the latest version of Focal (0.3.1): `http://cedric.cnam.fr/~delahaye/edemoi.tar.gz`.

3 Conclusion

A way to improve security is to produce high quality standards. The formal models of Annex 17 and Doc 2320 regulations, partially described in this paper, tend to bring an effective solution in the specific framework of airport security. From these formalizations, some properties could be analyzed and in particular, the notions of consistency and completeness. This paper also aims to emphasize the use of the Focal language, which provides a strongly typed and object-oriented formal development environment. The notions of inheritance and parameterization allowed us to build the specifications in an incremental and modular way. Moreover, the Zenon automated theorem prover (provided with Focal) discharged most of the proof obligations automatically and appeared to be very appropriate when dealing with abstract specifications (i.e. with no concrete representation).

References

1. The European Civil Aviation Conference. *Regulation (EC) N° 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing Common Rules in the Field of Civil Aviation Security*, December 2002.
2. R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, and F. Peureux. Application of Requirements Engineering Techniques to the Analysis of Civil Aviation Security Standards. In *International Workshop on Situational Requirements Engineering Processes (SREP)*, Paris (France), August 2005.
3. L. Lamport. How to Write a Proof. *American Mathematical Monthly*, 102(7):600–608, August 1995.
4. The International Civil Aviation Organization. *Annex 17 to the Convention on International Civil Aviation, Security - Safeguarding International Civil Aviation against Acts of Unlawful Interference, Amendement 11*, November 2005.
5. The EDEMOI project, 2003. `http://www-lsr.imag.fr/EDEMOI/`.
6. The Focal Development Team. Focal, *version 0.3.1*. CNAM/INRIA/LIP6, May 2005. Available at: `http://focal.inria.fr/`.