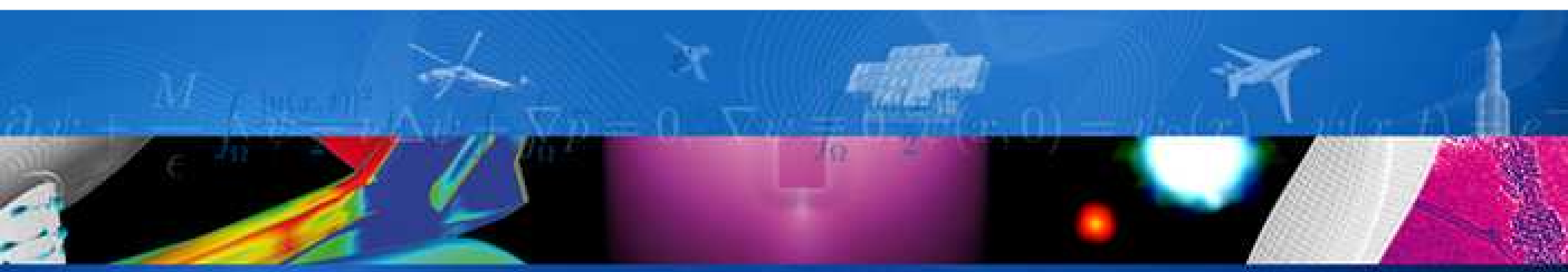


Can regulatory bodies expect efficient help from formal methods?

Second NASA Formal Methods Symposium

Eduardo R. López Ruiz and Michel Lemoine

ONERA

THE FRENCH AEROSPACE LAB

return on innovation

Our original question

Can we use formal methods to assess civil aviation regulations?

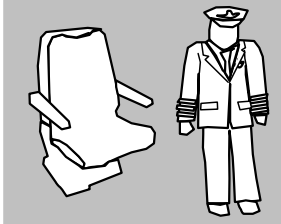
Example of aviation requirements

International Civil Aviation Organization

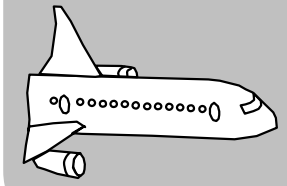
European Aviation Safety Agency

Federal Aviation Administration

Passengers **may not** carry prohibited articles into the security restricted area, nor the cabin of an aircraft



Flight crew members on flight deck duty **must** remain at the assigned duty station with seat belt fastened while the airplane is taking off or landing



When aircraft in flight are approaching each other head-on, or nearly so, each **must** alter its course to the right

Desiderata for the requirements?

Atomic	One provision, one requirement
Consistent	Free from contradiction
Robust	Exhaustive in its scope
Unambiguous	Having one meaning
Current	Not obsolete
Pertinent	Relevant to an identified need
Feasible	Implementable
Verifiable	Its implementation can be ascertained

Desiderata for the requirements

~~Atomic~~	~~One provision, one requirement~~
Consistent	Free from contradiction
Robust	Exhaustive in its scope
Unambiguous	Having one meaning
Current	Not obsolete
Pertinent	Relevant to an identified need
Feasible	Implementable
Verifiable	Its implementation can be ascertained

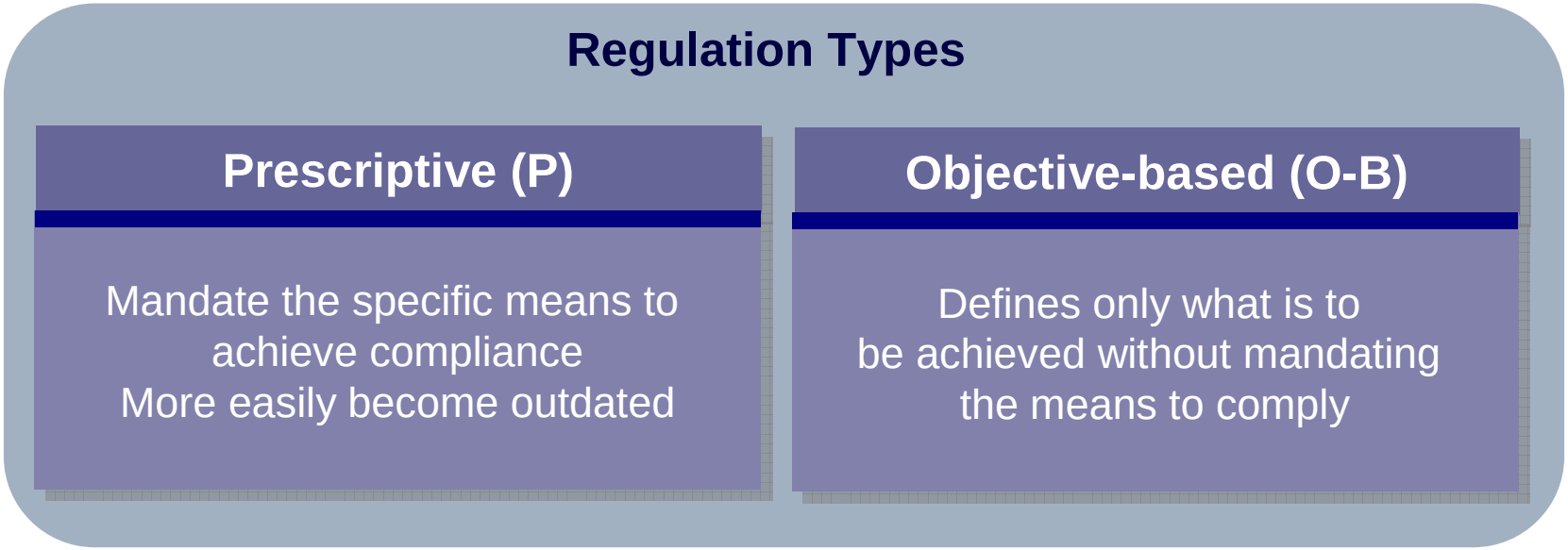
Require expertise in aviation safety/security

Our scope

Consistent	Free from contradiction (including with other regulations)
Robust	Exhaustively cover all the relevant scenarios (if only within a sub-domain)
Unambiguous	Having one meaning
Current	Not obsolete

Keeping regulations current

Promote objective-based requirements rather than prescriptive requirements



E.g.

When aircraft in flight are approaching each other head-on…

(P)…each must alter its course to the right

(O-B)...they must take the necessary actions so as to avert a collision

Making unambiguous, robust and consistent regulations

Regulations

Guidance Material

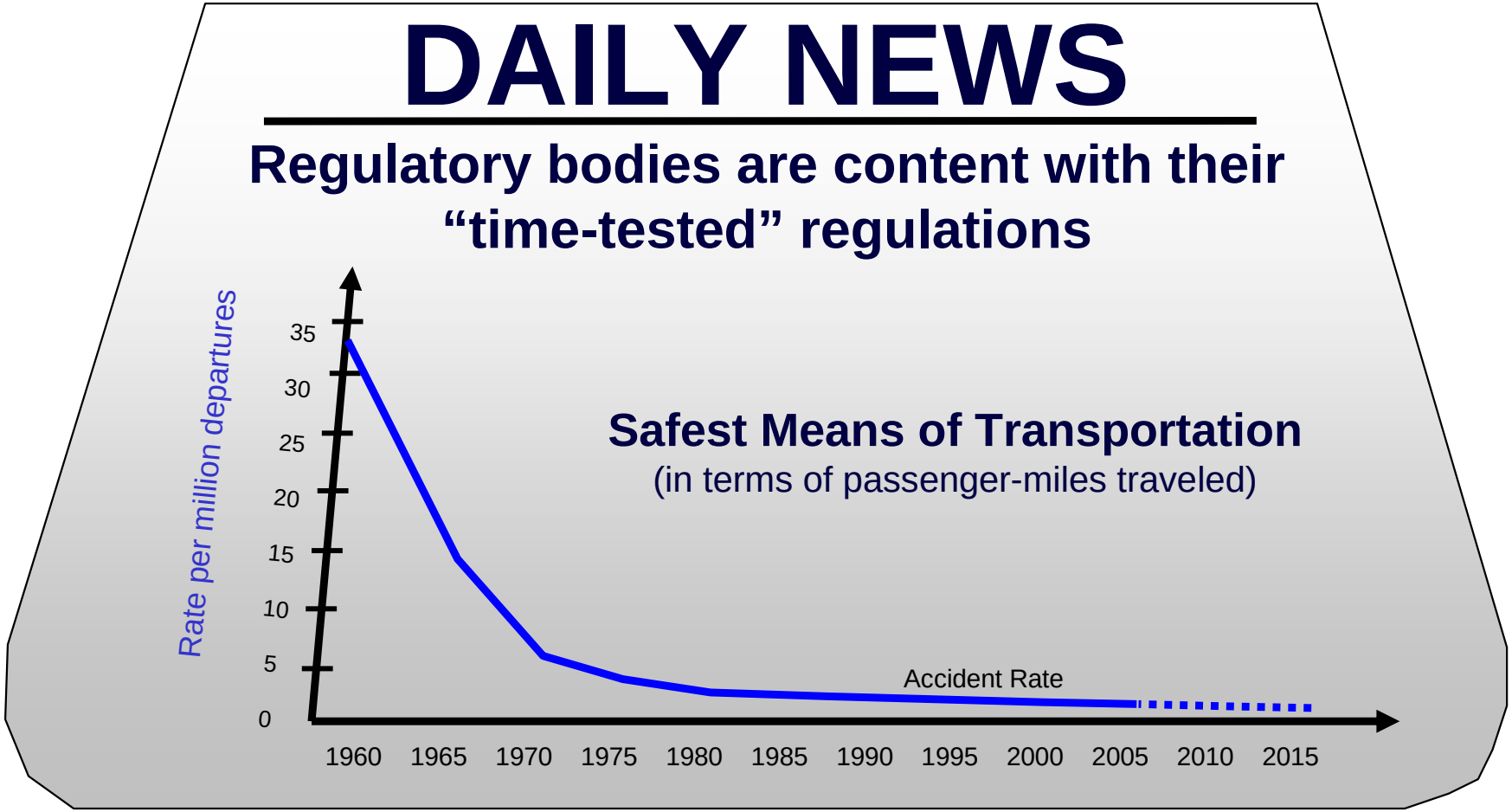
To fight ambiguity:

- Provide definitions for the terms employed
- Controlling the use of words
- Providing supplementary guidance material

To ensure robustness and consistency:

- Expertise
- Hindsight!

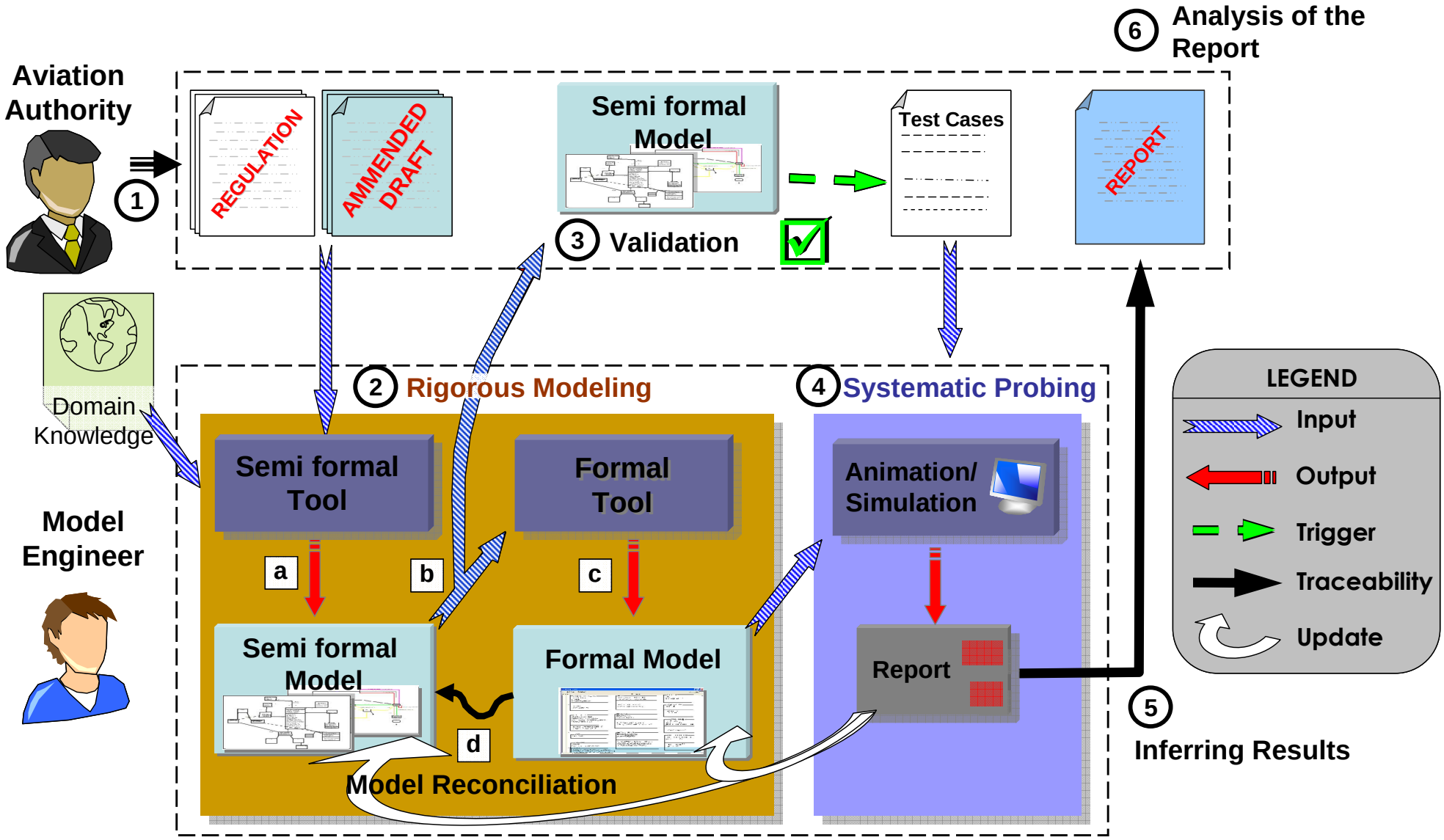
Too late?!



Older regulations may be consistent and robust, but when they are amended,

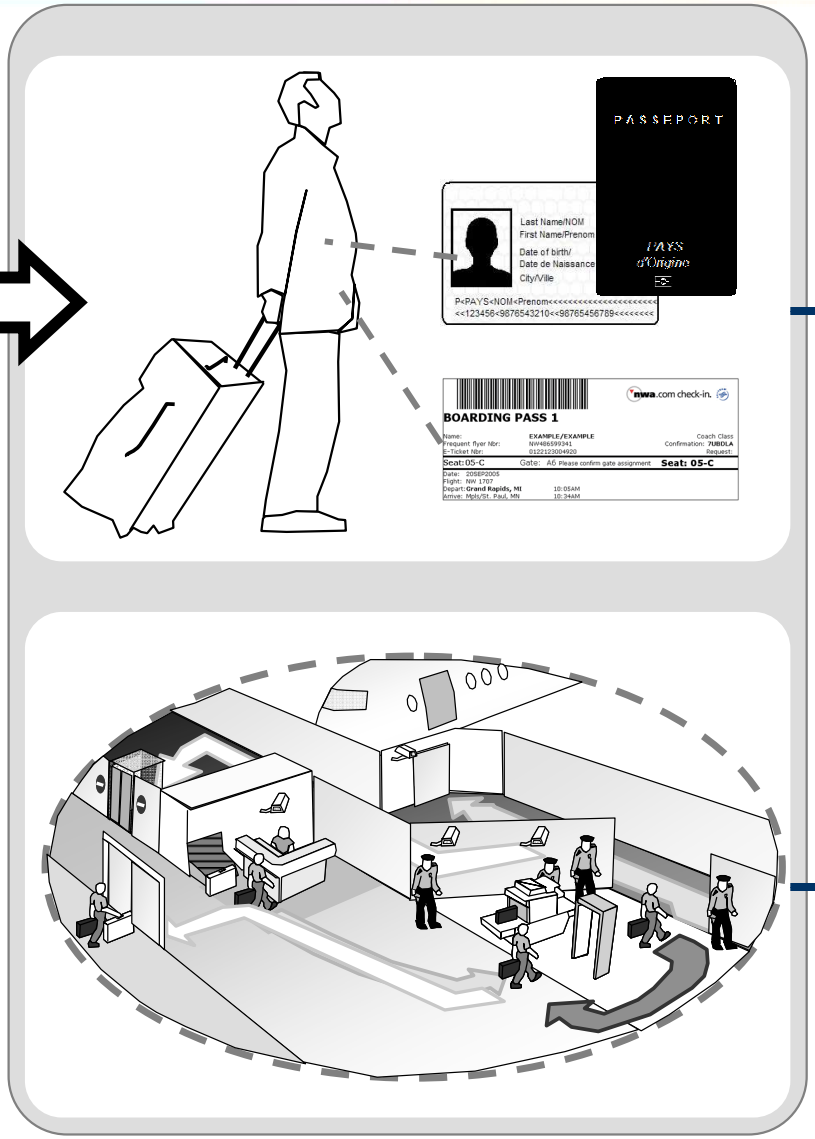
all bets are off!

Our proposed process inherited from Computer Sciences



Example (1/3)

Passenger Bob



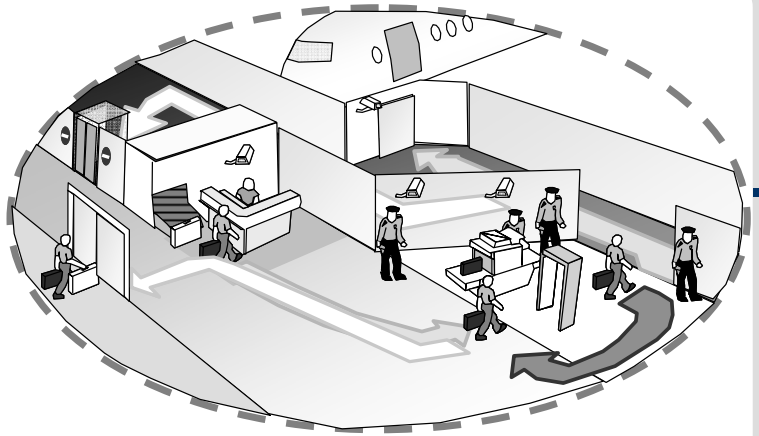
Conceptual View of a Passenger

Composition
(Static Aspects)

Behavior
(Dynamic Aspects)

ONERA

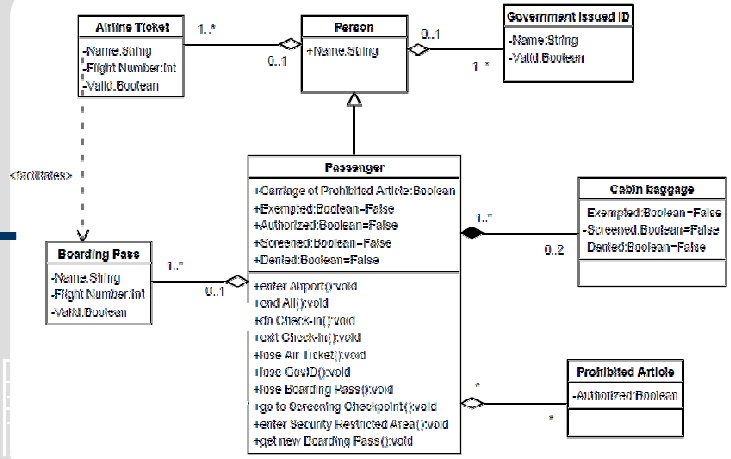
Example (2/3)

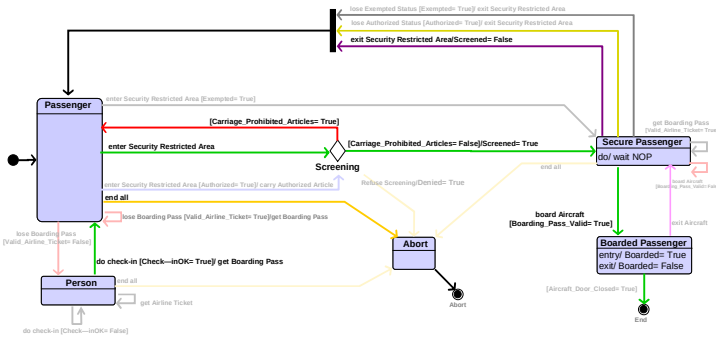


Conceptual View of a Passenger

Composition
(Static Aspects)

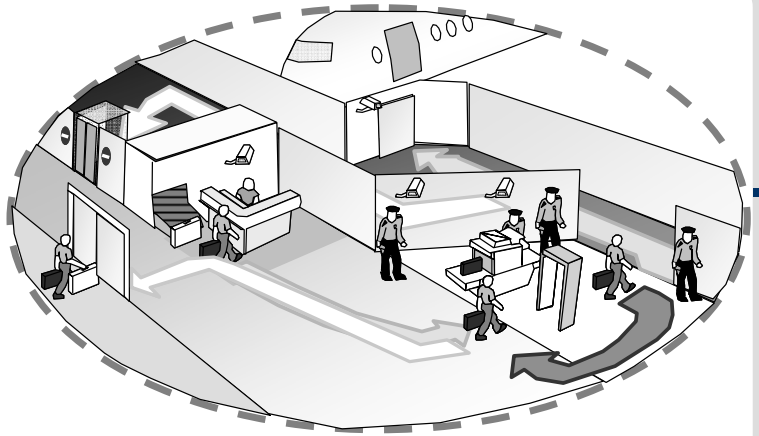
Behavior
(Dynamic Aspects)





Graphical Model

Example (3/3)



Conceptual View of a Passenger

Composition
(Static Aspects)

Behavior
(Dynamic Aspects)

$$
\begin{array}{|l}
\hline
PASSENGER \\
PERSON \\
boarding\_pass : BOARDING\_PASS \\
screened, authorized, exempted : BOOL \\
hold\_baggage : \mathbb{F}\, HOLD\_BAGGAGE \\
prohibited\_carry : \mathbb{F}\, PROHIBITED\_ARTICLE \\
authorized\_carry : \mathbb{F}\, PROHIBITED\_ARTICLE \\
\hline
boarding\_pass.name = name \\
prohibited\_carry \bigcap authorized\_carry = \emptyset \\
screened = T \Rightarrow prohibited\_carry = \emptyset \\
authorized = T \Rightarrow authorized\_carry \neq \emptyset \\
exempted = T \Rightarrow screened = F \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
ENTER\_SECURITY\_RESTRICTED\_AREA \\
\Delta PASSENGER \\
\hline
prohibited\_carry' = \emptyset \\
screened' = T \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
BOARD\_AIRCRAFT \\
\Delta SECURE\_PASSENGER \\
ac? : AIRCRAFT\_CABIN \\
\hline
boarding\_pass.flight\_number = ac?.flight\_number \\
\Rightarrow boarded' = T \\
\hline
\end{array}
$$

Formal Model

ONERA

Back to our original question

Can we use formal methods to assess civil aviation regulations?

Yes, we can !

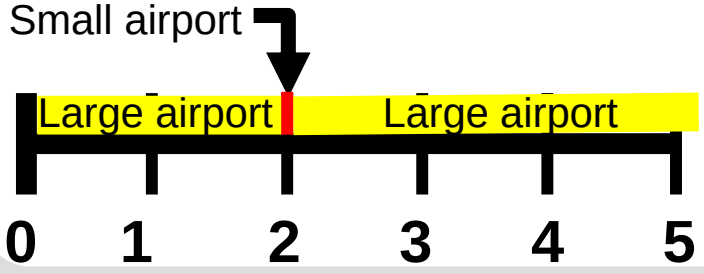
Best adapted for recently enacted or amended prescriptive requirements

We got results!

4.3.(a) Criteria for Small Airports
- ORIGINAL TEXT -

"…airports with a yearly average of 2 commercial flights per day…"

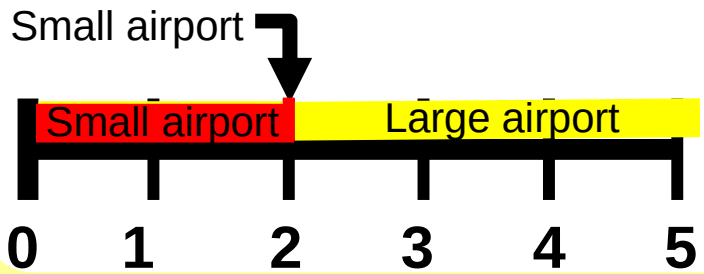
$$yearly\ average = 2\ \frac{flights}{day}$$



4.3.(a) Criteria for Small Airports
- AMENDED TEXT -

"…airports with a yearly average of ***no more than two*** *commercial flights per day…"*

$$0 \leq yearly\ average \leq 2\ \frac{flights}{day}$$



But…

Is it worth the candle?

No

Why not?

- Regulators are not particularly troubled by the state of their regulations' consistency and robustness
- Regulators have a hard time understanding formal notation
- Regulators cannot directly (in)validate the formal models
- An indirect (in)validation of the formal models is not straightforward

Conclusions

- Technically, formal methods can be used to assess regulations
  - Best adapted for recently enacted or amended prescriptive requirements
- Practically, their contributions fall outside the regulators' current needs
- Realistically, regulators show more interest for semi-formal methods
  - Easier to share knowledge between different end users
  - Better way of 'seeing' the impact of amendments

Conclusions

- A semi-formal specification of the regulations is a necessary first step that is yet to be achieved
- It is an intimidating task, considering the number of regulations that need to be taken into account
- But, thanks to harmonized regulations, agencies will be able to share the specification and validation efforts

Thank you for your attention!

Eduardo Rafael LOPEZ RUIZ
eduardo.lopez-ruiz@onera.fr
Michel LEMOINE
michel.lemoine@onera.fr