Modelling Trust and Security Requirements: the Air Traffic Management Experience

Elda Paja[1], Fabiano Dalpiaz[1], Paolo Giorgini[1], Per Håkon Meland[2], Stéphane Paul[3]
[1]Università degli studi di Trento, Italy
[2]Sintef, Norway
[3]Thales Research and Technology, France

Presenter: Elda Paja

Industry involvement: Per Håkon Meland is research scientist at Sintef ICT; Stéphane Paul is Research Engineer at Thales Research and Technology. Both have modelled different scenarios in the context of Air Traffic Management (ATM) using secure SI*.

Setting and context: This industrial experience is within the scope of the Aniketos[1] project: "Ensuring Trustworthiness and Security in Service Composition". The Future Internet will provide an environment in which a diverse range of services are offered by a diverse range of suppliers, and users are likely to unknowingly invoke underlying services in a dynamic and ad hoc manner. Aniketos is about establishing and maintaining trustworthiness and secure behaviour in a constantly changing service environment.
One of the three case studies of Aniketos concerns ATM. As Aniketos is in its early phases, we used SI* to model different scenarios, in order to communicate with the industrial partners on what can be captured/represented using the modelling language.

Status: The project is at an early-stage.

Benefits: The ATM case study is characterized by the interaction among a large number of actors. The concepts of role and agent of SI* proved adequate to represent the different actors participating in the setting. The analysts found suitable the high-level of abstraction (with goals as first-class citizens), as this allowed them to represent the responsibilities of each actor. Goal delegations were extensively used to assign responsibilities from one actor to another. Also, the concept of resource has been widely used to identify the data manipulated in the scenarios (typically, flight data).

Lessons learned: Goal modelling requires a specific turn-of-mind, especially for system engineers used to model processes (e.g. BPMN), and consequently SI* requires some adaptation. Despite the benefits described above, SI* comes with some limitations and causes confusion, especially to the non-expert modeller, who tends to introduce ad-hoc solutions to overcome these limitations. For instance, our modellers added long labels to goals to describe the whole process of handover (cf. Figure 1) and the way resources are used by goals.
With service security engineering in mind, the major limitations we identified through the modelling were the following:

1. Though resources constitute valuable assets to protect, resources are a marginal concept in SI*. They are defined as supporting means for a goal, i.e. resource use, modification, production or destruction are not explicitly modelled. This is a limitation from a security standpoint, so extensions of the "means-end" relation will be assessed within Aniketos.
2. Complexity and appropriateness of some concepts. Two sets of concepts were emblematic of this issue for the industrial modellers.
   First, the Own-Request-Provide concepts: modellers found them confusing. For example, it was unclear to them what owning a goal could mean. The industrial engineers nearly exclusively used the resource ownership link.

[1] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant no 257930.

Second, the delegation of execution and of permission concepts. A typical question was about the meaning of permission for a goal when one has already delegated the execution of this goal.
Within Aniketos, we plan to simplify the concepts, so as to retain only the intuitive ones.

3. Trust semantics was not clear enough to be used in confidence by the industrial modellers. This was due to doubts between cognitive trust and trustworthiness, as well as to the use of the modelling of those relations beyond their simple elicitation and capture. When trust modelling was enforced, multiple questions were raised, related to whether and how trust is propagated to sub-goals, trust fusion and trust dilution.
   Within Aniketos, we intend to guide the modeller in its use of trust relations, and possibly integrate some reasoning based on them, as key enablers to federated identity and federated security policies.
4. Scalability, mainly due to the tooling, because different perspectives are mixed together in the same diagram. Large models in industry are in the order of thousands of elements at this abstraction level.
   Within Aniketos, scalability will be a veto during the evaluation of the language semantics and syntax.
5. Limited capability to express security needs: SI* captures and reasons about some security requirements, verifying if the overall model satisfies a set of built-in security properties. However, many security policies cannot be specified.
   In Aniketos, we plan to extend the scope of security needs that can be modelled.
6. Poor suitability for service-oriented architecting (SOA). Two main concerns were raised. The first relates to the autonomy of services. SI* makes the assumption that when a role requests a goal and delegates its execution to another role, then the latter cannot execute the goal if it doesn't have the permission to do that. In service-oriented settings, service providers are autonomous: the SI* concepts do not carry such semantics.
   The second concern relates to the "black-box" characteristic of services. While the security features provided by SI* are adequate for centralized settings, they do not adequately support service-oriented settings, in which each service does not reveal its internal construction (only its interface).
   Within Aniketos, we intend to propose a language that fits to the service paradigm.

Language and variants: We used SI* as proposed by Zannone et al., to communicate with our partners. In the Aniketos project, in order to overcome the SI* limitations, we will devise, use and evaluate a novel goal-oriented modelling language expressly thought for security in service-oriented settings. The language will build on the notion of *social commitments*, which formalize organizational interactions and high-level security needs (i.e. user requirements). The language and associated methodology will help identify security needs in a service-oriented setting, in particular when service composition is required.

Features used: SI* uses mixed diagrams, including both SR and SD elements. In our modelling, we used the concepts of role, agent, part-of, is-a, goal, task, resource, delegation of execution and permission, trust of execution and permission, and/or decomposition.

Tools and methodologies: SI* tool (http://sesa.dit.unitn.it/sistar_tool/home.php?7)

Model size: The largest model that was built by the industrial partners (part of it is shown in Figure 2) includes 13 actors, 30+ goals, a few tasks and resources. It is worth noting that the ATM setting consists of several settings (among which handover and arrival management).

Efforts: The University of Trento organized a training day open to all the Aniketos project partners (30+ people) to introduce the language (3 hours approximately) and let the partners play with the SI* tool (1.5 hours). Then two partners (the industrial co-authors of this proposal) worked for a couple of weeks on modelling the scenarios with SI*. We interacted several times to see difficulties and limitations.

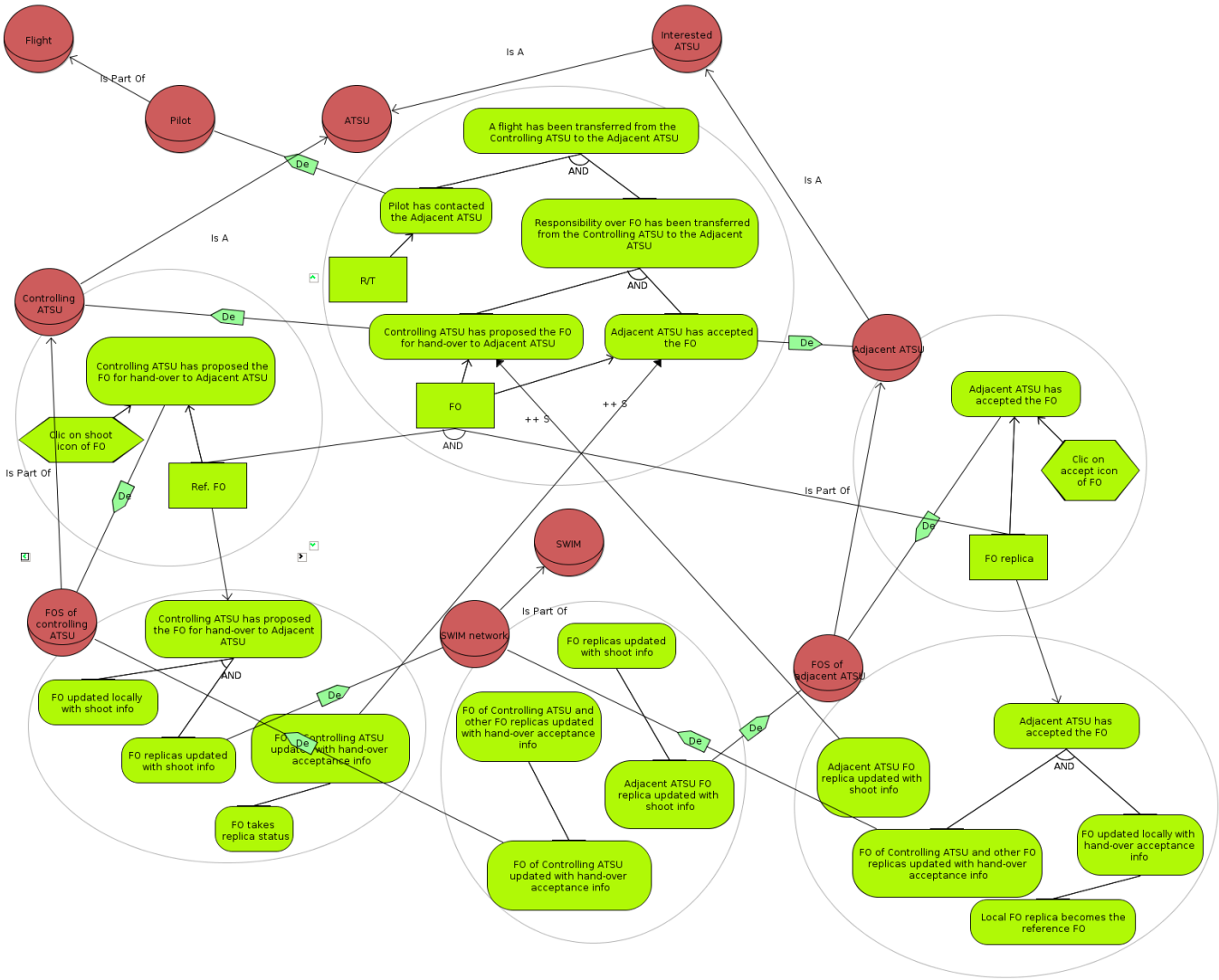

Figure 1: Handover scenario -- transferring a flight from one sector to another

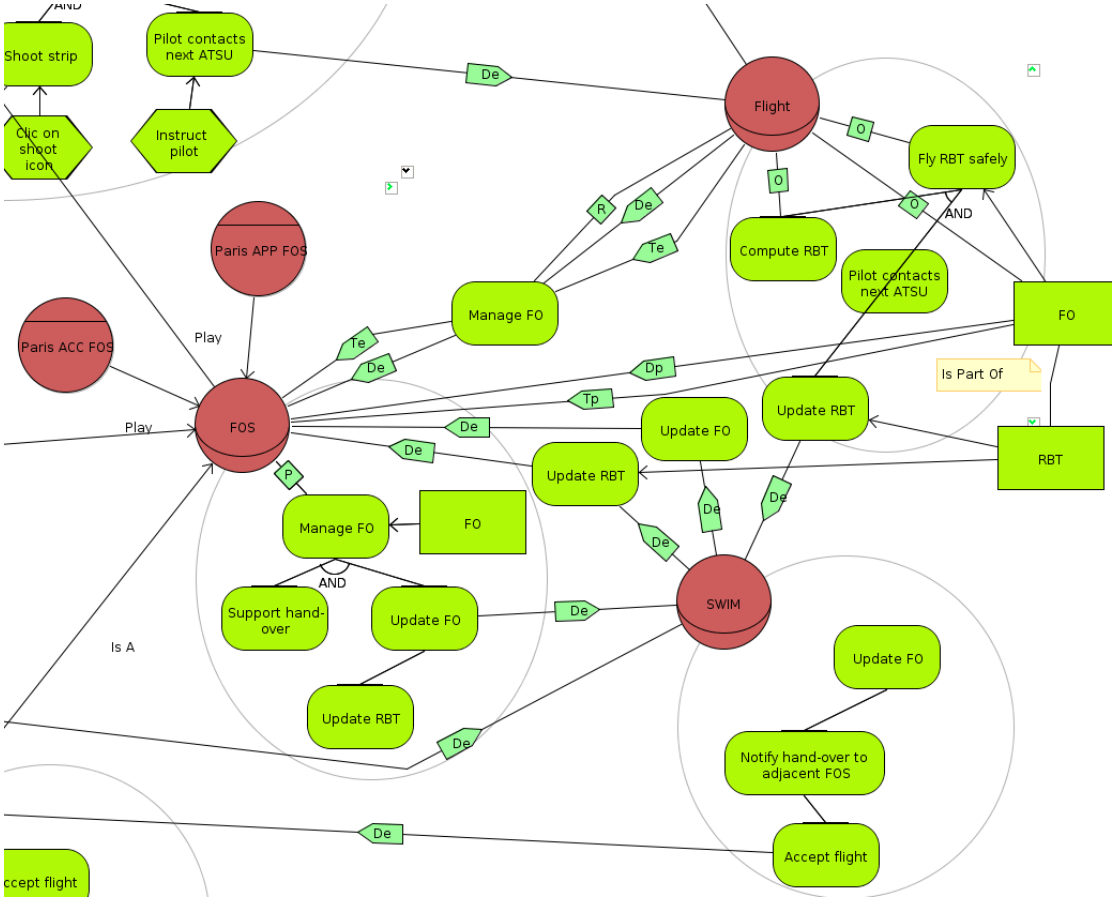

Figure 2: Part of the Arrival Manager (AMAN) scenario