Contrasting STAMP and formal systemic approaches for incident analysis in aviation

Nataliya Mogles[1], Julian Padget[1], Tibor Bosse[2]

[1]*University of Bath, UK*

[2]*VU University Amsterdam, Netherlands*

{n.m.mogles, j.a.padget}@bath.ac.uk, t.bosse@vu.nl

The rapid development and increasing complexity of modern socio-technical systems suggest an urgent need for systemic safety analysis approaches because traditional linear models cannot cope with this complexity. In aviation safety literature, among systemic accident and incident analysis methods, STAMP and Agent-based modelling (ABM) are the most cited ones. STAMP is a qualitative analysis approach known for its thoroughness and comprehensiveness. Computational ABM approach is a formal quantitative method which proved to be suitable for modelling complex flexible systems. In addition, from a legal point of view, formal systemic institutional modelling potentially provides an interesting contribution to accidents and incidents analysis. The current work compares three systemic modelling approaches: STAMP, ABM and institutional modelling applied to a case study in an aviation domain.

CASE STUDY

The Airbus received a taxi clearance and started taxiing to its runway. Approximately at the same time, a military Hercules aircraft received a taxi clearance as well. The Hercules was supposed to take off from runway 36 that crossed with runway 03 that was designated for the Airbus. Some time later, when the Airbus was near the runway designated for taking off, it received a line up clearance on the assigned runway. The Hercules received a line up clearance as well, while at the same time a take off clearance was issued to the Airbus. However, due to unknown reasons, the Hercules pilot interpreted his line up clearance as a take off clearance and started taking off. As a result of this mistake of the pilot of the Hercules, two aircraft were taking off simultaneously on crossing runways, and none of the crews were aware of that. The air traffic controllers in the Tower observed the conflicting situation and communicated a 'STOP' signal to the pilot-in-command of the Airbus, while the Airbus was still on the ground (but at high speed). The pilot had to make a quick decision about the termination of the take-off. After having analysed the situation, the pilot-in-command of the Airbus gave a command to the co-pilot (who controlled the aircraft) to abort the take-off and start braking on the runway. The serious collision was prevented (Bosse and Mogles, 2014).

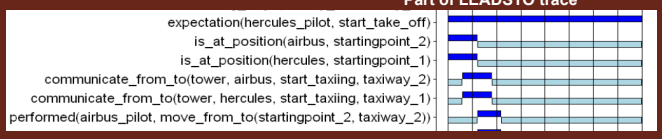
AGENT-BASED MODEL: LEADSTO/TTL

EP1 – Communication misinterpretation
incoming communication(A:Agent, I1:Action, R:Roadway) & belief(A:Agent, similarity(I1: Action, I2: Action))
& I1 ≅ I2
& expectation(A:Agent, I2:Action)
→ belief(A:Agent, I2:Action, R:Roadway)

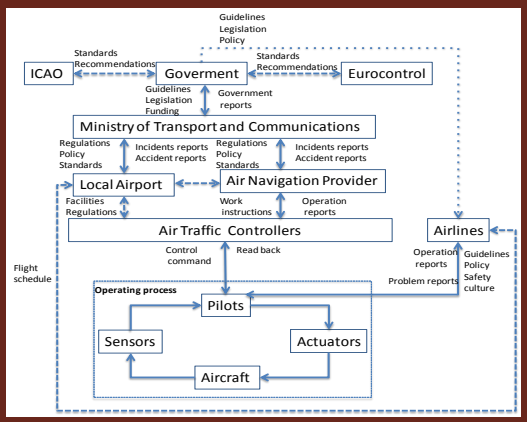
GP - No simultaneous take-off at crossing runways
There are no trace m, time points t1 and t2, agents a1 and a2, and runway r1 and r2 such that
agent a1 performs a take-off on runway r1 at time t1
and agent a2 performs a take-off on runway r2 at time t2
and runway r1 and r2 are crossing runways
and the difference between t1 and t2 is smaller than or equal to some constant d.

¬ [∃m:TRACE ∃t1,t2:TIME ∃a1,a2:AGENT ∃r1,r2:RUNWAY
state(m, t1) |= performed(a1, start_take_off(r1)) &
state(m, t2) |= performed(a2, start_take_off(r2)) &
state(m, t1) |= world_state(crossing_ways(r1, r2)) &
| t1 - t2 | ≤ d]

Part of LEADSTO trace



STAMP: CAST



Part of CAST analysis

Hercules Pilot

Safety requirements and constraints

- Understand and interpret data from instruments and controls
- Understand and interpret instructions of air traffic controllers
- Follow commands of air traffic controllers
- Make regular checks on the aircraft's technical performance and position, on weather conditions and air traffic during flight
- Complete a thorough pre-flight inspection of the aircraft…

…

INSTITUTIONAL MODEL: INST*AL*

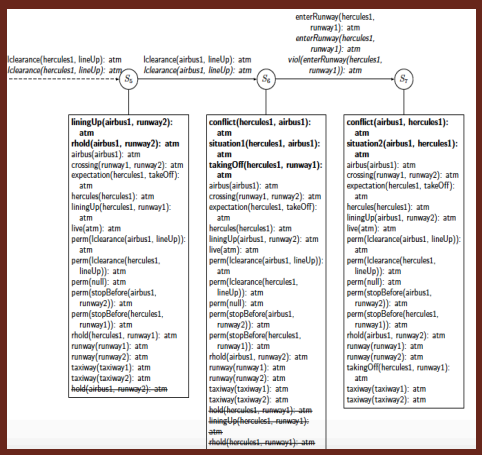
Conflict state definitions:
conflict(Agent1, Agent2)
when
situation1(Agent1,Agent2);

conflict(Agent1, Agent2)
when
situation2(Agent1,Agent2);

situation1(Agent1,Agent2)
when
crossing(Runway1, Runway2), liningUp(Agent1, Runway1) liningUp(Agent2, Runway2);

States initiation rule:
lclearance(A, Action) initiates liningUp(A, Roadway), rhold(A, Roadway)
if hold(A, Roadway), runway(Roadway), **not** conflict(A, A2);

Part of InstAL trace



MODELS COMPARISON

Criterion	STAMP: CAST	ABM: LEADSTO	Institution : InstAL
Levels of analysis	++ (all)	-(micro)	-(meso)
Taxonomy of failures	+	-	-
Quantitative representation	-	+	-
Qualitative representation	+	+	+
Events representation	-	+	++
Formalisation	-	+	+
Time dynamics	-	++	+
Emergent behaviour	-	++	+
Amount of training	+	-	-
Graphical representation	+	-	+
Data requirements	-/+	-	+
Time recourses	+	--	-
Additional resources (software, equipment etc)	++	-	--
Main vs complementary	main	compl	compl