Design according to liabilities: ACAS X and the treatment of ADS-B position data

Hanna Schebesta

Giuseppe Contissa

ALIAS project

EUI – European University Institute

Intro

- **We present a Test application of the Legal Case on ACAS X, the new generation airborne collision avoidance system.**

- Focus on potential liability implications of one specific design choice, namely different options for the treatment of ADS-B aircraft position data.

- liability considerations can affect design choices and the development process if opportunely taken into account.

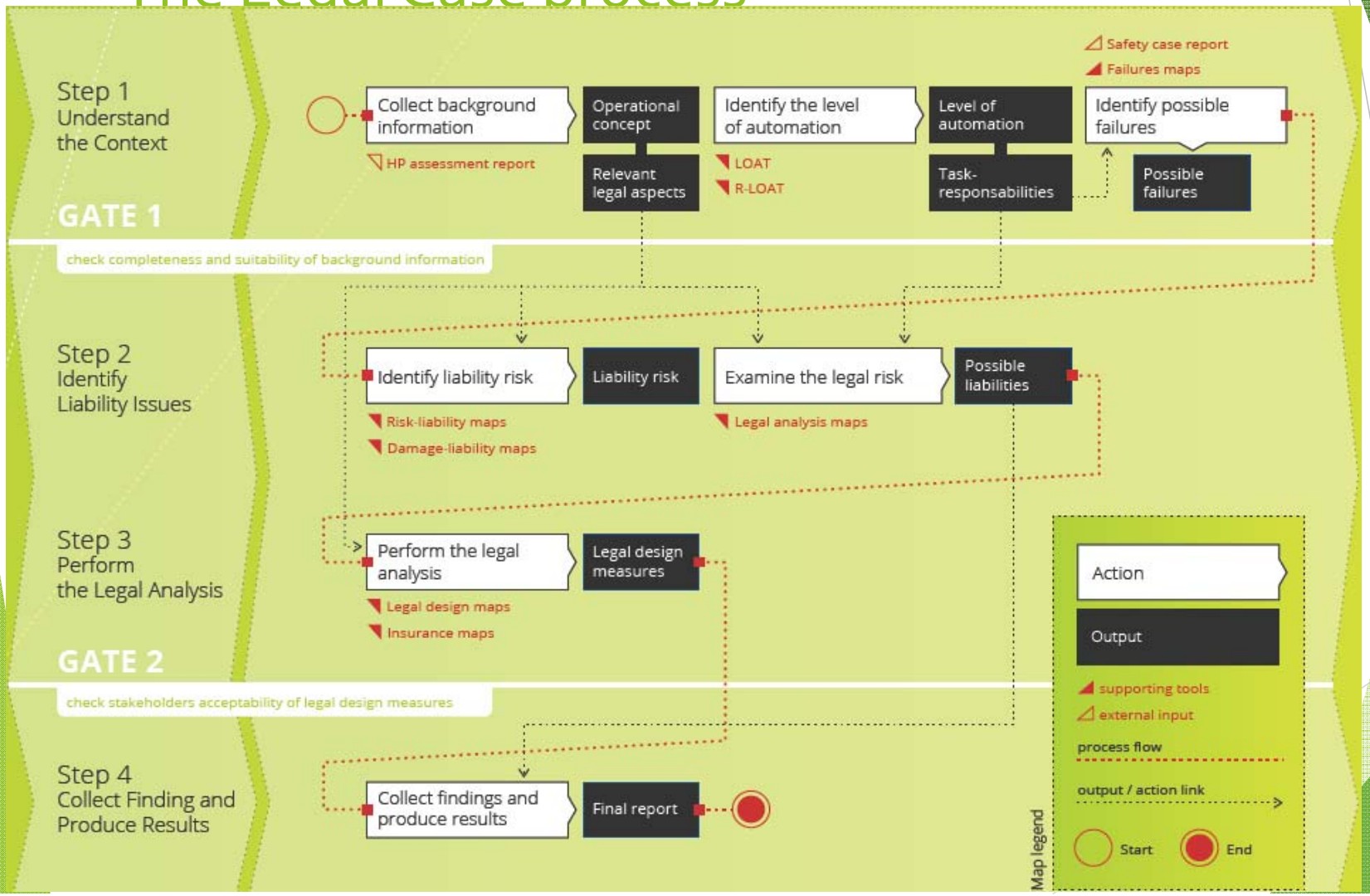
Alias

The Legal Case

- A **novel methodology** to address legal issues of automated technologies for ATM during their design process. It includes:
  - **A standard process** to identify legal liabilities at the design stage, in a structured way, so that problems are addressed before deployment, through convenient technological adaptations or legal arrangements.
  - A variety of **supporting tools** (such as tables to assess levels of automation and identify tasks and duties, flow diagrams to guide the assessment process, tables and reports which embed the produced results).

Alias

The Legal Case process



The Test Applications

- **Goal:** apply the Legal Case to a specific technology, collect feedback on results and methodology, validate the Legal Case
- **User group:** involving representatives of all stakeholders (for ACAS X : EUROCONTROL, IATA, aviation industries and air companies)
- **Focal point:** expert of the selected technology, supported in setting up the UG and mediated the cooperation btw the ALIAS team and the UG

Alias

ACAS X technology

- ACAS X is the new generation of Airborne Collision Avoidance Systems

- Challenge: different variants, different options
- Low maturity technology, a ‚moving target'
- Background information mainly based on Concept Of Operations
- Need to engage with experts to understand technological sides of the concept

Alias

4 ADS-B design options

1. No display of unvalidated ADS-B positions
2. Display unvalidated ADS-B positions visually distinct, no advisory
3. Display unvalidated ADS-B positions visually distinct, plus traffic advisory
4. Regular display and advice

A INFORMATION ACQUISITION	B INFORMATION ANALYSIS	C DECISION AND ACTION SELECTION	D ACTION IMPLEMENTATION
A0 Manual Information Acquisition	B0 king-memory based Information Analysis	C0 Human Decision Making	D0 Manual Action and Control
A1 Artefact Supported Information Acquisition	B1 Artefact Supported Information Analysis	C1 Artefact Supported Decision Making	D1 Artefact Supported Action Implementation
A2 ow Level Automation Support of Info Acquisition	B2 ow Level Automation Support of Info Analysis	C2 Automated Decision Support	D2 Step by step Action Support
A3 ed. Level Automation Support of Info Acquisition	B3 ed. Level Automation Support of Info Analysis	C3 gid Automated Decision Support	D3 Low Level Support of Action Sequence Execut.
A4 igh Level Automation Support of Info Acquisition	B4 igh Level Automation Support of Info Analysis	C4 Low Level Automatic Decision Making	D4 High Level Support of Action Sequence Execut.
A5 Full Automation Support of Info Acquisition	B5 Full Automation Support of Info Analysis	C5 High Level Automatic Decision Making	D5 Low Level Automation of Action Sequence Exec
		C6 Full Automatic Decision Making	D6 Medium Level Automat. of Action Seq. Execut.
			D7 High Level Automation of Action Seq. Execut.
			D8 Full Automation of Action Sequence Exec

1. No display

A INFORMATION ACQUISITION	B INFORMATION ANALYSIS	C DECISION AND ACTION SELECTION	D ACTION IMPLEMENTATION
A0 Manual Information Acquisition	B0 king-memory based Information Analysis	C0 Human Decision Making	D0 Manual Action and Control
A1 Artefact Supported Information Acquisition	B1 Artefact Supported Information Analysis	C1 Artefact Supported Decision Making	D1 Artefact Supported Action Implementation
A2 ow Level Automation Support of Info Acquisition	B2 ow Level Automation Support of Info Analysis	C2 Automated Decision Support	D2 Step by step Action Support
A3 ed. Level Automation Support of Info Acquisition	B3 ed. Level Automation Support of Info Analysis	C3 gid Automated Decision Support	D3 Low Level Support of Action Sequence Execut.
A4 igh Level Automation Support of Info Acquisition	B4 igh Level Automation Support of Info Analysis	C4 Low Level Automatic Decision Making	D4 High Level Support of Action Sequence Execut.
A5 Full Automation Support of Info Acquisition	B5 Full Automation Support of Info Analysis	C5 High Level Automatic Decision Making	D5 Low Level Automation of Action Sequence Exec
		C6 Full Automatic Decision Making	D6 Medium Level Automat. of Action Seq. Execut.
			D7 High Level Automation of Action Seq. Execut.
			D8 Full Automation of Action Sequence Exec

2. Distinct display; no advisory

A INFORMATION ACQUISITION	B INFORMATION ANALYSIS	C DECISION AND ACTION SELECTION	D ACTION IMPLEMENTATION
A0 Manual Information Acquisition	B0 king-memory based Information Analysis	C0 Human Decision Making	D0 Manual Action and Control
A1 Artefact Supported Information Acquisition	B1 Artefact Supported Information Analysis	C1 Artefact Supported Decision Making	D1 Artefact Supported Action Implementation
A2 ow Level Automation Support of Info Acquisition	B2 ow Level Automation Support of Info Analysis	C2 Automated Decision Support	D2 Step by step Action Support
A3 ed. Level Automation Support of Info Acquisition	B3 ed. Level Automation Support of Info Analysis	C3 gid Automated Decision Support	D3 Low Level Support of Action Sequence Execut.
A4 igh Level Automation Support of Info Acquisition	B4 igh Level Automation Support of Info Analysis	C4 Low Level Automatic Decision Making	D4 High Level Support of Action Sequence Execut.
A5 Full Automation Support of Info Acquisition	B5 Full Automation Support of Info Analysis	C5 High Level Automatic Decision Making	D5 Low Level Automation of Action Sequence Exec
		C6 Full Automatic Decision Making	D6 Medium Level Automat. of Action Seq. Execut.
			D7 High Level Automation of Action Seq. Execut.
			D8 Full Automation of Action Sequence Exec

3. Distinct display + advisory

A INFORMATION ACQUISITION	B INFORMATION ANALYSIS	C DECISION AND ACTION SELECTION	D ACTION IMPLEMENTATION
A0 Manual Information Acquisition	B0 king-memory based Information Analysis	C0 Human Decision Making	D0 Manual Action and Control
A1 Artefact Supported Information Acquisition	B1 Artefact Supported Information Analysis	C1 Artefact Supported Decision Making	D1 Artefact Supported Action Implementation
A2 ow Level Automation Support of Info Acquisition	B2 ow Level Automation Support of Info Analysis	C2 Automated Decision Support	D2 Step by step Action Support
A3 ed. Level Automation Support of Info Acquisition	B3 ed. Level Automation Support of Info Analysis	C3 gid Automated Decision Support	D3 Low Level Support of Action Sequence Execut.
A4 igh Level Automation Support of Info Acquisition	B4 igh Level Automation Support of Info Analysis	C4 Low Level Automatic Decision Making	D4 High Level Support of Action Sequence Execut.
A5 Full Automation Support of Info Acquisition	B5 Full Automation Support of Info Analysis	C5 High Level Automatic Decision Making	D5 Low Level Automation of Action Sequence Exec
		C6 Full Automatic Decision Making	D6 Medium Level Automat. of Action Seq. Execut.
			D7 High Level Automation of Action Seq. Execut.
			D8 Full Automation of Action Sequence Exec

4. Display + advisory

Level of automation analysis

- High level results:
- changes in automation on different cognitive categories shows difference between the different variants ACAS Xa, Xu, Xp, and Xu
- LOAT analysis shows difference between different ADS-B design options for ACAS Xa

Alias

ADS-B design options analysis

- …who should be responsible for taking the risk of implementing an action that is based on unvalidated ADS-B data: the technology (Option 4) or the pilot (Option 2-3)?
- …human-automation shifts in responsibility with respect to *automated decision-making* and *action selection* that deviate from the initial assessment of the ACAS Xa concept and the legacy of TCAS II.

Alias

ANALYSIS OF LIABILITY ALLOCATION

- Pilot/Air Carrier
- ATCO/ANSP
- **Manufacturer**
- Standard setter

Alias

	ACAS X: Legal risk of design defect for 4 design options for ADS-B data			
	Design defect risk	**State of the art defence strength** a) [if industry standard test, and manufacturers cannot choose options] b) [if industry standard test, and manufacturers can choose options, then depends on industry standard] c) [under the technical advancement test]	**Regulatory compliance defence strength** For all: Depends on how detailed the standards are written and whether manufacturers have discretion to opt for different ADS-B design options.	**Net liability risk for design defects (risk&defence)**
Option 1	Weak-medium	a) Strong b) indeterminate c)weak	Weak-medium	Medium
Option 2	Medium	a) Strong b) indeterminate c)medium-strong	Weak-medium	Medium
Option 3	Medium	a) Strong b) indeterminate c)medium-strong	Weak-medium	Medium
Option 4	Medium-high	a) Strong b) indeterminate c)medium-strong	Weak-medium	Medium

	ACAS X: Legal risk of warning defect for 4 design options for ADS-B data
	Liability
Option 1	Low
Option 2	High
Option 3	High
Option 4	Low-medium

Alias

measures mitigating design defect risk

- base the design on **scientific studies** (specific concerns are the reliability of ADS-B data in general, and the exposure of signals to spoofing)
- establish the **effects of certification** on safety
- explore **safety mechanism** designs to limit exposure to ADS-B risks.
- **State of the Art defence: l**obby for common industry standards in order to ensure that at the very least the customary practice of the industry defence can be met.
- **Regulatory compliance:** In order to limit liability of manufacturers, the ADS-B design options ought to be mandated for all manufacturers. With less discretion on manufacturers, their liability risk decreases.

Alias

measures mitigating warning defect risk

- manufacturers should provide **adequate warning information** for the technology. The documentation should be designed taking into account in particular the requirements on technology information of ACAS laid down in the Barcelona TCAS case following the Überlingen mid-air collision.

Alias

Liability design measures

- **Software components:** liability for failures of the prewritten ACAS X software component could be contractually severed from the liability of manufacturers.
- **Additional services:** responsibilities for maintenance, installation and resulting liabilities can be contractually addressed.
- **Insurance policies:** it ought to be ensured that 'spoofing' type of incidents are not excluded through specific exclusion clauses.

Alias

Other actors

- **Pilot/Air Carrier:** increased duty of care for the pilot under Options 2-3; can have an impact on Air Carrier liability risk.
- Suggested measure: task allocation should be enshrined in legally relevant documentation e.g. ACAS manual, PANS-OPS and training requirements
- **ATCO/ANSP:** same complexity risk as pilot under Options 2-3
- Suggested measure: Guidelines for controller actions and training must be enshrined in official documentation. ATCO training requirements regarding ACAS are currently much less well developed than for pilots.
- **Standard Setter:** it is strongly suggested that such bodies assess their respective level of duty of care critically when setting standards and certifications. This implies determining whether (i) ADS-B data is less reliable than other data streams, and (ii) whether the reliability issue can successfully be addressed through certification.

Alias

Systemic considerations

- Air carrier liability is partially strict, but capped.
- Manufacturer as defendant more attractive than air carrier due to no cap.
- Forum shopping: tendency to try to displace cases to the US.

- One has to distinguish two liability functions: a) compensation of victims, b) induce safety maximising behaviour

Alias

Options

- Capping the liability of manufacturers
- Introducing strict liability for manufacturers
- Compulsory insurance (and direct claim against insurer? CF Roger)

- Using the link between certification and manufacturer's liability to limit manufacturer's liability exposure
- Institutionalise the example of insurance practice and make common funds between air carriers/manufacturers (‚co-liability')

Alias