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.
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).
The Legal Case process

Step 1: Understand the Context
- Collect background information
  - HP assessment report
- Operational concept
- Relevant legal aspects
- Identify the level of automation
  - LOAT
  - R LOAT
- Level of automation
- Task responsibilities
- Identify possible failures
- Possible failures
- Safety case report
- Failures maps

GATE 1
check completeness and suitability of background information

Step 2: Identify Liability Issues
- Identify liability risk
  - Risk-liability maps
  - Damage-liability maps
- Liability risk
- Examine the legal risk
  - Legal analysis maps
- Possible liabilities

Step 3: Perform the Legal Analysis
- Perform the legal analysis
  - Legal design maps
  - Insurance maps
- Legal design measures

GATE 2
check stakeholders acceptability of legal design measures

Step 4: Collect Findings and Produce Results
- Collect findings and produce results
- Final report
- Action
- Output

Map legend
- Start
- End
- Output / action link
- Supporting tools
- External input
- Process flow
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
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
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
<table>
<thead>
<tr>
<th>A INFORMATION ACQUISITION</th>
<th>B INFORMATION ANALYSIS</th>
<th>C DECISION AND ACTION SELECTION</th>
<th>D ACTION IMPLEMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0 Manual Information Acquisition</td>
<td>B0 Working-memory based Information Analysis</td>
<td>C0 Human Decision Making</td>
<td>D0 Manual Action and Control</td>
</tr>
<tr>
<td>A1 Artefact Supported Information Acquisition</td>
<td>B1 Artefact Supported Information Analysis</td>
<td>C1 Artefact Supported Decision Making</td>
<td>D1 Artefact Supported Action Implementation</td>
</tr>
<tr>
<td>A5 Full Automation Support of Info Acquisition</td>
<td>B5 Full Automation Support of Info Analysis</td>
<td>C5 High Level Automatic Decision Making</td>
<td>D5 Low Level Automation of Action Sequence Exec</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D7 High Level Automation of Action Seq. Execut.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D8 Full Automation of Action Sequence Exec</td>
</tr>
</tbody>
</table>

1. No display
### 2. Distinct display; no advisory
### 3. Distinct display + advisory
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
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.
ANALYSIS OF LIABILITY ALLOCATION

- Pilot/Air Carrier
- ATCO/ANSP
- Manufacturer
- Standard setter
### ACAS X: Legal risk of design defect for 4 design options for ADS-B data

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