High-Level Modelling and Analysis of TCAS

Carolos Livadas, John Lygeros, Nancy Lynch

presented by

Daniel Karlsson
ESLAB, IDA, Linköpings universitet

Outline

- Introduction
- Hybrid IO Automata
- Modelling TCAS using HIOA
- Brief safety analysis
- Questions

What is TCAS?

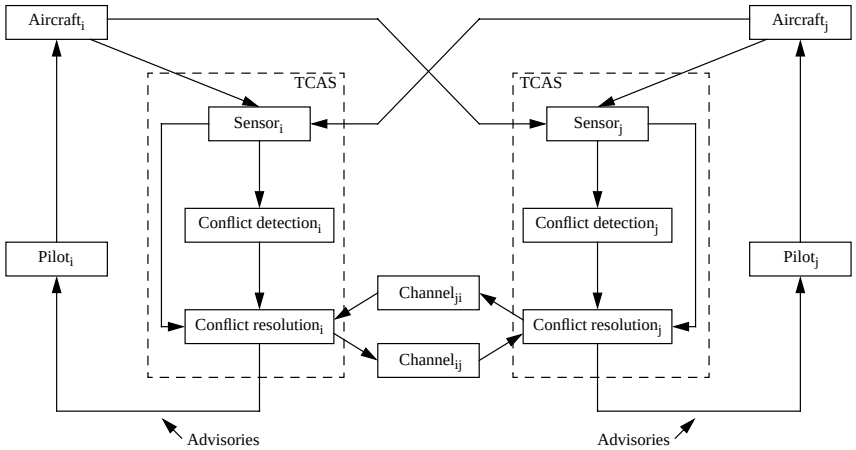
Traffic Alert and Collision Avoidance System

- Traffic Advisory (alert)
- Resolution Advisory (propose)
  - Reversal of previously issued RAs
- Hybrid:
  - Continuous: aircraft, sensors, pilot reaction
  - Discrete: Thresholds, discrete message passing

Hybrid IO Automata

- $A = \langle U, X, Y, \Sigma^{in}, \Sigma^{int}, \Sigma^{out}, \Theta, D, W \rangle$
  - U, X, Y - disjoint sets of variables (in, int, out)
  - $\Sigma^{in}, \Sigma^{int}, \Sigma^{out}$ - disjoint sets of actions
  - Θ - nonempty set of initial states
  - D - set of discrete transitions, $\langle s, a, s' \rangle$ where $a \in \Sigma = \Sigma^{in} \cup \Sigma^{int} \cup \Sigma^{out}$
  - W - set of trajectories over $V = U \cup X \cup Y$
- Input actions are always enabled
- Environment action, e, will arbitrarily change the input variables
- Two HIOAs can be composed into one if they are compatible
- Implementation relation

Overview of the TCAS Design



The Aircraft Model

Variables:

Input:

$a_i \in \mathbf{R}^3$

Output:

$ModeS_i \in \mathbf{N}$ initially empty

$Equipment_i \in \{\text{None, Report, TCAS}\}$ initially arbitrary

$p_i \in \mathbf{R}^3$ initially arbitrary with $z_i \geq 0$

$v_i \in \mathbf{R}^3$ initially empty

Actions:

Input:

e the environment action

Discrete Transitions:

e: **Effect: Arbitrarily reset the input variables**

Trajectories:

Input variables follow arbitrary trajectories.

$ModeS_i$ **and** $Equipment_i$ **remain constant**

$$\begin{bmatrix} \dot{p}_i(t) \\ \dot{v}_i(t) \end{bmatrix} = \begin{bmatrix} v_i(t) \\ a_i(t) \end{bmatrix}$$

Sensors

Input: position and velocity of all aircraft

Output: estimates of the altitude, vertical rate, distance and rate between all pairs of aircraft

No input or internal actions.
Output action: $Sample_i$

Discrete Transitions:

$Sample_i$**:**

Precondition: $t_{S_i} = T_{S_i}$

Effect:

$t_{S_i} \leftarrow 0$

$h_{ij} \in \left[z_j \pm \frac{n_{Ai}}{2}\right]$

...

Trajectories: $\dot{t}_{S_i} = 1$**, etc.**

Simplifications of the Safety analysis

- **All aircraft are TCAS equipped**
- **Sensors are exact**
- **Pilots always abide the RAs issued by the TCAS system**
- **Aircraft always have constant horizontal velocities**
- **The pilot can apply infinite vertical acceleration**
- **The aircraft have equal strength**
- **... and more**

Execution Categorisation

- Conflict_Free_Execs - TCAS protocol not invoked
- Non_Crossing_Execs - noncrossing RA issued
- Crossing_Execs - crossing RA issued, eventually becomes noncrossing
- Reversing_Execs - crossing RA changed and becomes noncrossing

Derive safety conditions for each of the categories.

Safety Analysis

- Conjunction of Per-Category Safety Properties:

If the initial state of a conflict satisfies all per-category safety conditions, then the execution is safe.

- Isolating Noncrossing Executions:

Since the majority of advisories will be noncrossing ones, by isolating them and distinguishing them from the crossing ones will yield less conservative results.

- Aircraft Close in Altitude:

Crossing advisories are most likely to be given when aircraft are close.

Questions

- The discussion about model refinement in the article is based on the implementation relation (cf. page 929). This relation means that if we know that a more detailed HIOA is an implementation of a more abstract HIOA then we know that any previously proven properties of the abstract model automatically hold also for the finer model. How is the model refinement done in practice? How do you guarantee that a refinement of a certain HIOA actually will result in a HIOA that is an implementation of the original one?
/Martin Enqvist

Questions

- The authors believe that conventional analyzing/engineering techniques for complex systems like the TCAS are unsatisfactory, since the intuitive understanding of the system behaviour often becomes overshadowed by the details and technicalities present in the detailed low-level specifications. The techniques proposed in the paper aims, amongst other things, at overcoming these problems by "...obtaining precise mathematical models of all core components...". Have they been sucessful, does the HIOA give the intuitive understanding of very complex systems?
/David Lindgren

Questions

- In the example in the paper with two aircraft with their sensors, conflict dectection & resolution systems, communication equipment and pilots constitute a feedback control system. In all feedback control the issue of stability is important. In the TCAS II-7 system the controller (the two conflict resolution systems) is able to adjust its control signals (the "resolution advisories") during a threat situation. The adjustment is in the form of the opposite control signal ("climb" or "decend") and the adjustment is only allowed once for each aircraft. I think this restriction to maximum one adjustment is a means to avoid instability. Would it not be better to use "standard" control theory and allow the controller to continuously adjust its control signals to fulfill the requirement, e.g. avoid a collision? Of course the controllers must be designed to make the whole feedback control system stable.

What is "nmi"?

How is it possible for two HIOAs A1 and A2, that "A1 implements A2 if every external behavior of A1 is allowed by A2"? Should it not be the opposite? Could you explain this more?

/Svante Björklund

Questions

- What is the actual contribution with this article? In my opinion, they make such huge simplifications that I cannot see the value of ,e.g., their "safety analyze". Why not use realistic assumptions from start instead of leaving everything to "future research"? Or is it the large amount of definitions and the problem specification which are the actual contributions?

/Erik Wernholt

Questions

- The paper presents a comprehensive analysis and verification technique of TCAS which is a very complex safety critical system. In the presented approach several simplifying assumptions are made. One of this simplifying assumption is that multiple aircraft can never be simultaneously involved in a conflict. This assumption seems extremely important to me because near to airports you can easily end up in multiple conflicting situations .There is also military TCAS system called Enhanced Traffic Alert & Collision Avoidance System (ETCAS) which provides military aircraft operators with an extended surveillance range and the capability to coordinate formation flying in addition to standard TCAS operations. With the above mentioned simplifying assumption the usefulness of the analysis and verification technique for ETCAS especially in coordinating formation flying is questionable. What are the difficulties of extending the analysis and verification techniques presented in the paper to deal with this simplifying assumptions?

/Peter Bunus

Questions

- A realistic scenario around an airport should be a very complex system to perform verification etc. to. What do you think about the applicability of the kind of methods described in the article?

/Jacob Roll

- A widely used system is modeled and tested from a safety aspect. I sincerely hope that this also has been done prior to the use of the system. What is the contribution of doing it again (in a new way, perhaps)?

/Frida Gunnarsson

- In the beginning of the paper they talked about verification through simulation. Can you please tell me about the analysis method they use to ensure for instance safety?

/Peter Aronsson