Certification Opportunities for IMA

John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA USA
Imagine... 

- Maybe 10 years from now
- New guidelines: DO-297B and DO-178D
- What might we hope for?
- And what might we have to deal with?
What Might We Have To Deal With?

- A lot of code for health monitoring
- And a lot of (possibly adaptive) code for recovery
  - Take a pretty safe airplane, add a lot of complex, seldom-executed code to make it safer
- Aircraft-to-aircraft negotiation
  - NextGen: distributed airspace management
- Some of the pilots may be remote, on the ground
- Frequent updates, product families, customization
- Complex, outsourced, development and supply chain
What Might We Hope For (From DO-178x)?

- **Justifiable confidence** in its effectiveness
  - In the face of the new challenges on previous slide
    - e.g., it’s not productive to view a learning system, say, as merely a different means for implementing software
    - And then to try to apply DO-178B to it
    - It’s a more radical change than that

- **Manageable cost**

- **Credible and inexpensive recertification** for product evolution
  - Incremental cost for incremental changes
What Might We Hope For (From DO-297x)?

- Truly **compositional** certification
  - Components are qualified (certified standalone)
  - The certification of the system considers its (IMA) architecture
  - And the component qualifications
  - But need not go inside the component or architecture implementations

- Credible and inexpensive **recertification** with changed/new components

- IMA concept extends **beyond individual aircraft:**
  - Distributed, cooperating, elements
    (remote piloting, NextGen)

John Rushby, SRI

Certification Opportunities for IMA: 5
Credibility: A Recent Incident

- Fuel emergency on Airbus A340-642, G-VATL, on 8 February 2005 (AAIB SPECIAL Bulletin S1/2005)
- Toward the end of a flight from Hong Kong to London: two engines flamed out, crew found certain tanks were critically low on fuel, declared an emergency, landed at Amsterdam
- Two Fuel Control Monitoring Computers (FCMCs) on this type of airplane; they cross-compare and the “healthiest” one drives the outputs to the data bus
- Both FCMCs had fault indications, and one of them was unable to drive the data bus
- Unfortunately, this one was judged the healthiest and was given control of the bus even though it could not exercise it
- Further backup systems were not invoked because the FCMCs indicated they were not both failed

John Rushby, SRI Certification Opportunities for IMA: 6
Standards-Based Software Certification

- E.g., airborne s/w (DO-178B), security (Common Criteria)
- Applicant follows a prescribed method (or processes)
  - Delivers prescribed outputs
    - e.g., documented requirements, designs, analyses, tests and outcomes; traceability among these
  - Certification examines the outputs
- Works well in fields that are stable or change slowly
  - Can institutionalize lessons learned, best practice
    - e.g. evolution of DO-178 from A to B to C
- But less suitable with novel problems, solutions, methods
  - Might work only because of implicit factors
    - Conservative practices, safety culture
  - Can become a barrier to innovation
Standards and Goal-Based Assurance

- All assurance is based on arguments that purport to justify certain claims, based on documented evidence.
- Standards usually define only the evidence to be produced.
- The claims and arguments are implicit.
- Hence, hard to tell whether given evidence meets the intent.
- E.g., does MC/DC coverage provide evidence for good testing, or good requirements, or absence of unintended function?
- Recently, goal-based assurance methods have been gaining favor: these make the elements explicit.
The Goal-Based Approach to Software Certification

• E.g., UK air traffic management (CAP670 SW01), UK defence (DefStan 00-56), growing interest elsewhere
  ○ Recommendation of NRC report: Sufficient Evidence?

• Applicant develops a safety case
  ○ Whose outline form may be specified by standards or regulation (e.g., 00-56)
  ○ Makes an explicit set of goals or claims
  ○ Provides supporting evidence for the claims
  ○ And arguments that link the evidence to the claims
    ★ Make clear the underlying assumptions and judgments
    ★ Should allow different viewpoints and levels of detail

• Generalized to security, dependability, assurance cases

• The whole case is evaluated by independent assessors
  ○ Explicit claims, evidence, argument
Relation to Current Practice

- Fairly consistent with top-level certification practice
- Applicants propose means of compliance
  - cf. ARP4754, ARP4761
  - Apply safety analysis methods (HA, FTA, FMEA etc.) to an informal system description
- And a Plan for Software Aspects of Certification
  - Typically DO-178B
  - To be sure implementation does not introduce new hazards, require it exactly matches analyzed description
  - Hence, DO-178B is about correctness, not safety
- It’s the latter that we propose to change
  - Analyze the implementation for preservation of safety, not correctness
  - This may be a way to deal with adaptive systems

John Rushby, SRI
Software Hazards:
Standards Focus on Correctness Rather than Safety

- Premature focus on correctness inappropriate for adaptive systems, *goal-based methods could reduce this*
Safety Cases and Monitoring

- Health monitoring implies **online checking**
- We know how to do this (runtime verification)
- But what (source of) properties to monitor?
- Low Level SW requirements unlikely to be useful
  - DO-178B ensures these are implemented correctly
- Similarly with High Level SW requirements
- Most likely it’s the **requirements** that are in error
- We need an **independent** source of properties to monitor
- **Aha**: the safety case
  - Monitor against the claims of the safety case
IMA and Compositional Certification

• Profound insight (Ibrahim Habli & Tim Kelly)
  ○ The safety case may not decompose along architectural lines

• So what is an architecture?

• A good one supports and enforces the safety case

• Cf. MILS approach to security: yesterday afternoon
  ○ Explicitly compositional
  ○ Relates to IMA

• Intuitively, it’s what partitioning is all about

• But I think the idea of a MILS Policy Architecture provides a useful interface between policy and mechanism
Closing Thoughts And Questions

• Is it time to rethink the approach to software certification?

• And are safety cases the way to go?

• What other approaches could cope with the challenges we face?

• Do we want to move toward explicitly compositional certification?

• Are we doing it anyway, but implicitly?

• Can the safety and security worlds benefit from a common foundation?

• What did I leave out?