Certification and Assessment

Azer Bestavros (Boston U)
Scalable composition analysis - interactions
Hide internals, think about interfaces
Type relationships between inputs/outputs
Natasha Neogi (tomorrow)
S. Tucker Taft (Softcheck)
Static analysis – application indep correctness, discovery of properties (max stack)
Formal proof
Model checking – requires approximations/abstractions, better for models than source code
Flow analysis – abstract interpretation
Challenges – false neg/pos, incremental analysis, SoS, static timing & performance analysis
Scott Beecher/Jim Krodel (P&W)
Complexity, certification processes insufficient, need research on highly integrated system certification techniques
Techniques that are provable to & acceptable by regulatory authorities
Components/modules with commitments/contracts, assess module's certificaiton aspects when integrated
Approach: incremental certification approval process
System composition for certification assurance
How do we convince FAA of new practices?
Gabor Karsai (Vanderbilt)
Model-based embedded SW development
"We trust platform (VxWorks) and compilers"
Need domain specific languages
Integrate verification engines
How do you know that your model transformations (code gen) are correct?
How do you know that model verification hold for the executable?
ex: emit assertions along with generated code
John C. Knight (UVA)
Prescribed SW development processes do not ensure quality
Assurance cases (safety cases) are a better mechanism
Education – shortcomings of CE/CS programs
Demand better from higher education
Oleg Sokolsky (UPenn)
Model-driven development
Conflicting assumptions in separate modeling efforts
Rance Cleaveland (not present)
Frank Mueller (NC State)
ex: A380 engine overheat detection
Governed by DO-178B
Still using cyclic executives
New – timing analysis, WCET analysis
Single event upset (no ECC in L1 cache, no protection in processor core)
Robin Bloomfield (Adelard LLP)
Assurance cases – goal-based "claims-argument-evidence" safety case approach
Shift from compliance based to behavior based certification cases

General Discussion

Moderator: David E. Corman
Scribe: Darren Cofer

David Corman's list of questions:

1. What is the "holy grail"?
2. Scale is a problem. What is biggest challenge problem we can come up with?
3. How are technologies changing?
4. Is certification going after the right problems? Too much? Not enough?
5. What does certification mean in the context of large mixed initiative systems with >1E7 lines of code? Hitting a wall?
6. What changes when UAVs enter NAS?

Lui Sha – How do we know which model to trust? Different people will come up with different versions.
Walter Storm – Support for John Knight's comments on education
Oleg Sokolsy – Must document what models are for, rationale, assumptions
John Baras – Need emphasis on architecture and hw/sw codesign from beginning to aid verification
JB – Doesn't agree with civil engineering comparison – implies over-conservative design
Barbara Lingberg – agree with JK comments, but SW has some unique properties. Are we hitting a wall? Doesn't think so. Need to identify where are the risks: integration, multiple developers, focus on the hard parts. DO-178B is de facto standard for SW, but this limits trying new ideas – higher risk.
Tucker Taft – Typical errors in C: most are unique to C language. Need tools need to facilitate good work, human engineering of tools.
John Knight – issue is teching CS people to be engineers (not programmers, stupid syntax). Civil engineers DO push the state of the art, materials. Modern buildings are not over-engineered.
Robin Bloomfield – Need standards that allow us to trust the evidence. People rarely comply with standards, they interpret them. Need to focus on goal-based approach.
Darren Cofer – Problem is not just standards. Is FAA ready to deal with new VV technology?
LS – recent major in-flight failures (777 ADIRU, A-380 blank displays) shows there are shortcomings in current process. If one thing is changed, must recertify the whole thing – need incremental certification? (scalability)
BL – DO-178B is being revised to incorporate new technologies. Applicants are encouraged to talk with FAA ahead of time about plans to use new technology.
Elroy Weems – Is 1E-9 good enough when 6000 aircraft are in the air? Why are there 2 failures in first hour of system startup? Need better customer involvement, there is an assumption that requirements are correct at start
Hal Pierson – What constitutes an adequate argument?
JK – 1E-9 is not achievable, knowable, testable
Jim Krodel – In data loaders, CRC is assumed good enough. RMA for scheduling is good enough. These are examples of acceptable analyses. Need similar standard arguments.
OS – Need to be willing to move on when demands exceed technology capabilities
LS – A653 partitions, non-critical partition failed and caused failure of critical partition. Shared cache and PCI interaction caused critical partition not to get time. SW hasn't caused crash yet, but only because pilots have been able to take control. Another example – GE engine
John Hansman – FAA needs research that can validate new certification methodologies
David Homan – What are the new technologies that could help here?
Walter Storm – Need to find problems early in development cycle

Alan Goldberg – A653 only provides partial model of non-interference, including bus contention and cache interference
LS – There is a bigger issue. DO-178B is process oriented. Need evidence-based system. Make assumptions explicit and machine checkable. Ex: Arian 4/5 overflow. Even if assumptions are documented, how do I find it in huge stack of paper? Assumptions informally captured. Interface to SW design is inadequate.
Azer Bestavros – Need to think about verification/certification ahead of time, not after the fact. We can use languages that do not permit memory leaks.
OS – Need different interface for different models for different purposes, analyses
LS – Proofs can only be partial. There will always be residual errors. System must be stable/robust, tolerant of faults.
Jim Alves-Foss – Lowest cost, lowest effort path will always be taken. Gothic features in JK cathedral slide do look like modern SW.
Xiangong Lee – Currently pilot is safety backup when SW fails. This won't be the case for UAV.
Frank Mueller – Need different methods for each property, increase reliability. Multiple approaches give more assurance. Would optional certification requirements be helpful? Purpose would be to drive development and certification process for the future.