Certification and Assessment Working Session

Certification by Composition
Research vehicle for bringing FAA along with new technology

What are the top 3 Lessons Learned/Technologies in the area of cert & assessment?

What are the top 3 needs not met in area?

What are the top 3 research topics/challenges (with timelines)?

What are the top 3 challenges in the area of certifification?

Education needs/topics

Transcription:

introductions:

Jim Krodel / Pratt & Whitney (moderating)
chairs committee 205 working on new DO-178B

Richard Robinson / Boeing (scribe)

Oleg Sokolsky / U Penn - formal anlysis

Tucker Taft / Softcheck Inc

Hal Pierson / FAA (in the IT dept)

Steve Jacklin / Nasa Ames (software assurance, control systems)

Jim Alfoss (U of Idaho)

Natasha Neogi / UIUC

Patrick Graydon / U Virginia

Kelly Hayhurst / NASA Langley

John Ack / U Virginia

Robin Bloomfield / London

Scott Beecher / Pratt Whitney

Darren Cofer (scribed the discussion earlier today)

===

proposed, around the room with today's presenters. what do they think critical needs in cert?

Oleg: need to move from process to evidence-based cert. big problem is, while explicit evidence
is good, there is lots of implicit evidence in minds of developers. how to document assumptions
that go into development of software and models. developers need to develop, document, present arguments.
no idea how to.

Tucker: models at different levels of abstraction. how can integration across levels
and their validation be automated. goal of component based cert. interfaces need to
be specified, documented in a formal way. examples SPARK, PRAXIS. get FAA to believe

Hal: incremental certification, not re-do whole process whenever there is a change

Frank Miller: rigorous timing analysis. also issues that arise from using COTS software.
need methodology for this. (my question, what about open source) clarifies, if you
have tools it doesn't matter. but if you don't, there's an issue because open source
changes too fast. architectural complexity, multi-threading, etc, mean these problems only become worse. second,
regardles of environments, FAF (?) sizes, cost must be controlled.

Natasha: two issues: combinations of above. certification compositions of many elements plus
the environment. environment can affect assumptions made. any two pieces of software may interact.
second, competing requirements or qualities (started in safety, now works security) safety concern
is controls must get timely inputs, but security requirements say inputs must be correct

Patrick: how to explicitly specify what you want in security. how do you formalize concept that, e.g.,
"system cannot be hacked". expressions of negative qualities difficult to express formally
argument might be that component X is proof against some set of listed vulnerabilities.

discussion:

methodology by which we currently express requirements is to express threats. this is an inefficient
and fragile way to approach the formalisms. may know the requirements at some high level, but that's
not the same as being able to detail properties of the system.

identifying the sources of influence on the system. there's no good methodology for ensuring all
have been identified.

security generally has a strategy (game structure). set up requirements, adversaries try to beat
the game. safety is a bit different, events that lead to failure are generally assumed to be
independent but security is not like that.

some have proposed safety can be analyzed in game paradigm.

with safety, concept of intent is abstracted away. assumptions are about probability of chain of
events. in security, probability does not help because of the intent. Example, in SEU to test
safety they inject random bit flips. security breaches or incidents cannot be modeled or tested
in that random way.

summarizing the discussion: deep question is where does composability work, how do we achieve
(and certify) secure system.

reasoning about a certification is not the same as reasoning about a design

Kelly: certification framework is extremely rigid today, doesn't accomodate new needs (like
security) or introduction of new technologies or methodologies. not flexible, not extensible.

John Knight: notion of evidence-based certification and assessment should itself be reviewed.
alternate approach (like assurance case analysis) present opportunities to provide better certification science

Robin: need mechanism or framework to integrate safety and security. what is certification as
a process? (my question, what specific might be integration?) - capability that you want
agency says "is it adequately safe, given all the random + malicious things that might happen"

what about throughput of certification systems?
certification challenge: deal with increasing complexity, time-to-market, etc. yet be able to
certify cost-effectively and with quality. don't want to have "false positive" i.e., certify
something "safe" that is not.

are we certifying to the right risk level? what are the safety aspects of security? (funny that's
the opposite of the way I would put the issue)

example, multi-level security. safety/fault-tolerance info being traded among multi processors
where the processors are working at different levels (top secret vs secret)

need to handle time, cost, reduction of resources and scalability of certifying large systems

Scott: Trusted tools with known pedigree and certification evidence

In a complicated case is seems that increasing automation is desirable. composability argument for
cert is distinct from composability of system. research on framing positions of safety compliance
of new research/technology.

autocoding: what about certification of generated code, generally such code can not be examined.
need to certify that the generator only makes good code.

on certifying unmanned: seems there's a higher bar where there isn't a person in control to mitigate
potential control errors.

can you identify dependency chains, where person is generating inputs to system. humans can create problems for the system, as well as be traps for trouble. and certification is a "very human" process. we tolerate human failures in a way that we don't for automated systems. again, an example from multi-level security. rate of errors in a voice transmission is much, much less than that in a data link. can models incorporate people, i.e., model the human behaviors in a system. we do certify pilots, the process is quite limited compared to what we do for software systems.

we're talking about certification issues in terms of person interacting with the system. need also to examine people roles (human interactions) in certification process itself. how to teach people to appropriately evaluate evidence (or whatever).

if you push this too far, wind up with airbus idea of envelope protection, i.e. pilot is not allowed to "overstress" the airplane. in situations where overstressing the plane may save lives, this may not be the best thing. what led to this (apparently) was an analysis that accommodated human behavior, but ended up abstracting the people out of the model.

if you elect to "pull the human out" more rigor is required. what happens is that there are trajectories that can be induced where the human must intervene. so the person is absent, except when they're not.

Darren: component based cert needs to be a big part of model based development process. model based development should improve cert process, but right now it doesn't seem that is happening (reference to the FC-205 activity).

====================================

summarizing: security and how it relates to other things

====================================

on to research challenges:

science of certification
solving false-positive problem (false indication of problems) for automated analysis tools
we can settle on "false alarms" -- want to reduce the number of false alarms

can echo the needs listed above

probabalistic aspects vs deterministic aspects of problem analysis. both approaches have viability. maybe preferable to employ both approaches, one to check or validate the other.

we have an existing certification process. what we're proposing is to automate, replace some aspects of what we have now. want to assure that we get the "same" guarantees of safety and correctness that we get today. how to show the automated methods give as good or better confidence.

general area of making tools for certification more robust, trustworthiness. discussion whether certification is an argument, or a proof. a "loose" proof is not really a proof.

do we need research on aspects of mitigations for systems where we know there will be problems arising. what are the architectural implications of fault tolerance, versus fault avoidance. certification doesn't "respect" fault tolerance. assertion this is changing, "FAA doesn't believe level A software is assured anymore" so demonstrating faults are tolerated will become new state of the art (another reference to FC-205).

complex interactions, in systems where can't prove safety guarantees.

what about certification of mitigation technologies (unstable systems, adaptive systems)

paper in recent "safe and dependable computing" on certifying mitigation techniques. evidence-based certification is important (versus "proof") because can never prove requirements are correct, and so on downstream. this argues for evidence-based certification processes over model-checking and automated techniques. and you can produce probabilistic analyses from evidence presentations.

We don't have a "set" way of putting certification arguments together.

Distinction being drawn is between evidence-based and formal. There is always a degree to which method is grounded on some judgment call. Always have something "informal" at the topmost level of the tree.

All these considerations must feed in to the "science of certification".

how to proceed: throw down some quick education ideas:

what can be done to ensure we educate next generation workforce to do adequate certification?

to do:

how to incentivize, motivate people to be educated in this area? college kids today (a "my kids" example) aren't clear what career paths are available, attractive to them.

"testers are always coder wannabes". traditional career trajectory has been disincentive to software quality / testing / verification type of work. we desire to move out of the "hand crafted" software world.

education being used today in Europe to motivate young people in this area.
Benchmarking US capability vs world standards

example of culture shift in Boeing, when emphasis moved toward "lean" goals of designing plane in order to be produced. look for similar culture shift where software is designed and built in a way that's directed toward certification. back to the national competitiveness initiative. example, sikorsky outsources everything except their "core" competency. focus should be on certification as the high-value software capability.

exemplary systems for use in university research. one perspective is such developments
are expensive to make but have a short shelf-life. need pedagogical structure, then when
the need for exemplars arises it will appear as a standard persistent need.

again on culture change: is going through V & V a way to get into high level executive management?

Certification Breakout Session 2:

Jim Krodel
Richard Robinson
David von Oheimb
Tucker Taft
Hal Peirson
Jim Alfoss
Kelly Hayhurst
Patrick Graydon
Scott Beecher
Natasha Neogi
Robin Bloomfield

Jim K notes working group 72 (EuroCAE) is being looked at for coordination with FC-205

"top 3" needs from yesterday bulleted out, consolidated somewhat, categorized by topic.

first bit of time directed at review of yesterday's notes

context from one of this morning's talks:
certification vs qualification: cert means airworthy, ie can fly.
qualification is support of component toward cert of a system that can fly.
qualification says evidence for qual can be cited in support of cert.

what about IMA system approval basis, a prescriptive and very process oriented engagement (297). some amount may be helpful here. CM, for example, a big part of it. Maybe not so helpful in our context. Doesn't give mechanism for showing assurance of system based on qualities of components.

Gap between validating properties of individual components versus demonstrating safety of a whole aircraft. reason for liking the qualification/certification distinction.

added, consideration of certifying where legacy components are incorporated in new systems (per Natasha N talk this morning).

In Service Oriented Architecture, interfaces specified by "contract".
Hal thinks this can be a mechanism supporting "argument" or reasoning

about how components behave in context.

define certification framework: example motivated by fact that FAA current regulations inhibit component-level qualification. we're talking about the process of certification (not some evidenciary bus).

illustrative: to use a new technology today, can do, but process is quite informal. no policy governs it, therefore it's quite ad hoc.

realistic goals. we hear a lot of "anomaly" stories. how many would be "expected" in a year? can certification framework accommodate incorporation of realistic goals or targets, in addition to tools, methods.

propose wording: "certification criteria consistent with systems analysis" in place of "certification framework"

between certification of COTS vs open source. for COTS there is (may be) an organization that can be identified with a financial or other stake in providing evidence. not so for open source. for open source, may have behavioral or direct evidence, but not development process evidence.

see that knowledge management is needed in addition to formal methods, etc.

don't believe certification process can be fully automated, because of need for judgment. same as system architecture.

to what degree is the science of certification the same as the science of risk analysis?

decision of level at which evidence should be examined is a policy matter.

on paradigm shift: if we're proposing a new science of certification, how can we know that the new processes introduced are "right"? how to know when verification system is done? how to show that new approach to certification gives better, cheaper, faster, safer results? if it's a "science" of certification, what's the role of experimentation.
again, how to prove that the revolutionized process is valid? mainly, how can it be known that a new certification approach guarantees safe systems. what are success criteria for a certification approach?

note, we would like to put some priorities on these "needs". how are the outcomes of this workshop going to be used? community here includes research (academic) community, industry, suppliers, and regulatory institutions.   would be useful to direct "needs" at each segment of the community. approach needs acceptance/working together with academic, regulatory, and industry.

Hal weighs in on prioritizing needs. His view of the top level issue is cost of certification, especially in light of expanding effort required to individually qualify components in their contexts.

Top three needs (summarizing): (see Jim's notes)

Top three research topics (review points from John's talk this morning, on "Science For Certification")

Need to get consensus on most important, highest priority needs and research topics. current list is unwieldy

top three challenges:

better, richer way of specifying component interfaces, component commitments (contracts for timing, assumptions, limitations, side effects). a language for reasoning about how components aggregate. have argument that we have adequate languages. but current methods allow us to talk about component properties, want to have a methodology for reasoning about emergent properties.

as a "starting point" for a certification framework or discipline, toward making the process more rigorous, suggest collecting and analyzing "patterns" for certification.

need to engage certifiers with certifyees.

BREAK-----------------

Certification Breakout Session Final

1. What are the Top 3 Lessons Learned/technology in the area of certification and assessment?

2. What are the Top 3 needs that have not been met?

Cost & Cost of rework
Cope with complexity
Handling New Technologies

Cert Approaches

- Alternate approaches to acceptance (eg. Product Evidence based vs Process based)
- Composition cert approach including environmental aspects of the system
- Component based qualification/certification with cert. expressive interfaces in a formal manner (links to Model based design, Incremental Certification, When does composablity work and where, Models at different levels and how to validate)
- Consideration of certifying with legacy components and systems
- How do you know the cert of the system meets with a success criteria (Analysis of experimentation used in the cert process.)
- Approaches need acceptance/working together with the academic, certification & industry

Cert Criteria Consistent with Systems Analysis

- Cert framework process to handle new technologies, both flexible or extensible.
- Analysis methods to consider integration of Safety vs. other complex system attributes or requirements (eg. Human Factors, Security can have competing requirements)

Tools

- Need a methodology/tools for Certification of COTS (with evidence) & Open source (without development process evidence) (SW & ICs)
- Trusted tools with known pedigree to support qualification/certification evidence (Risk analysis needed to determine level of trust)

Human Factors

- Human Factors certification considerations (both helping and hurting) in large complex systems
- Human interactions in the certification process itself
- Component interactions including people as a component

Other

- Complete Documentation of System Assumptions (implicit/explicit)
- Rigorous Timing Analysis
- Need to handle time, cost, reduction of resources and scalability of certifying large systems
- Inability to achieved a secure system even with formal security requirements

3. What are the Top 3 Research topics/challenges (with timelines) being/should be pursued in your domain of expertise related to certification.

- Probabilistic approaches for levels of confidence (how to do?)
- Risk mitigation of highly complex systems, and can't provide guarantee because of the complexity (e.g. adaptive systems for one) (being worked now)
- Research on framing positions of safety compliance of new research/technology
- Science for Certification
    - *Clarify verification and certification differences, interfaces (cannot look inside*
    - *Specifiation & verification of integration frameworks*
    - *High Performance automated verification for strong properties of model-based design (mostly infinite state and hybrid systems) and automation of related processes (test generation, Fault Tree Analysis)*
    - *Compositional certification of hybrid systems*
    - *Tool qual – evidence management*
    - *Integrated methods and arguments, probabilities assisting the qualification/certification argument*
- Solving (reducing) false alarms of automated tools

4. What are the Top 3 challenges (with timelines) in the area of cert (including outside your domain of expertise?

Component Composability attributes/interfaces commitments (timing, assumptions, limitations, side affects, tracability) such that the aggregate product is safe.

Need to engage certifiers

Collect patterns of certified systems

5. Education needs/topics

- Incentives / motivate people to enter the domain & stay current
- Assessment of systems a career option
- Benchmarking US education capability vs. world standards (both higher education & industry)
- Shift culture such that cert is an integral part of system development (high level stuff inhouse/ low level stuff outsource?)
- Exemplary systems for use by education institutions
-

Participants

Jim Krodel / Pratt & Whitney (Moderator)
Richard Robinson / Boeing (Scribe)
Oleg Sokolsky / U Penn
Tucker Taft / Softcheck Inc
Hal Pierson / FAA (IT)
Steve Jacklin / NASA Ames
Jim Alves Foss / U of Idaho
Natasha Neogi / U of Illinois - UC
Patrick Graydon / U Virginia
Kelly Hayhurst / NASA Langley
John Knight / U Virginia
Robin Bloomfield / Adelard
Scott Beecher / Pratt Whitney
Darren Cofer / Honeywell
Frank Mueller / NC State U