

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



### DO-178B - A Square Peg in a Round Hole?

(or whither DO-178C?)

Uma Ferrell	Tom Ferrell
Principal	Principal
Uma@faaconsulting.com	Tom@faaconsulting.com
(703)757-9777	(703)757-9777



Ferrell and Associates  
Consulting, Inc.

Slide 1

2002 FAA National  
Software Conference



### Disclaimer

- This presentation has purposefully been put together with more than just a dollop of humor and sarcasm (here or there). Our intent is to get people to think hard about the challenge we have ahead of us in formulating DO-178C – whenever that may happen.
- The views expressed in the slides and in the commentary are strictly those of the authors, also known as the devil's advocates.
- While it is hoped that much useful dialogue will occur that will ultimately help frame the DO-178C effort, no direct quotes, attributions or retributions will come of anything said behind these doors!



Ferrell and Associates  
Consulting, Inc.

Slide 2

2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



### Broaching the Question

- We all sort of know that DO-178C is coming.
- It's just a matter of when and in what form.
- The purpose of this session is to talk (interact, argue, debate, kibbutz, rant, hold a discourse...) about DO-178B and what should be done to evolve it to C!
- To set the stage a few opening thoughts (salvos)...



Ferrell and Associates  
Consulting, Inc.

Slide 3

2002 FAA National  
Software Conference



### My Oh My, How Time Flies!

- **FACT:** DO-178B will celebrate it's tenth anniversary in December of 2002.
- **FACT:** DO-178 and DO-178A take us back another ten years to 1981.
- **FACT:** Man will celebrate the 100<sup>th</sup> anniversary of human powered, controlled flight in December of 2003.
- **QUESTION:** Does it make sense that after spending more than 20% of the entire time we've been flying working issues of software assurance, we still do not have:
  - A quantifiable means of establishing that software is safe?
  - A clear and present case for the benefits of adherence to DO-178B, let alone individual objectives?
  - A more proactive rather reactive means for validating new technology (e.g. object oriented)?



Ferrell and Associates  
Consulting, Inc.

Slide 4

2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



### Killing Urban Legends

- One of the greatest reasons these issues are still dogging us is the lack of metrics data that has been made available publicly.
- It seems strange that when you look at our industry, we have found ways to share almost every other type of data that relates to safety in the name of improving safety.

#### WHY CAN'T WE DO THIS FOR SOFTWARE?

- One of the ways to give DO-178C a firm foundation is for the industry to identify a way of sanitizing data and making it available to the FAA or some other third party for collation so that at least the beginnings of a scientific and business case for individual objectives can be created.



Ferrell and Associates  
Consulting, Inc.

Slide 5

2002 FAA National  
Software Conference



### DO-178B and Safety

- You have all no doubt heard the debate about the true nature of DO-178B:
  - “It’s a development standard” - NO
  - “It’s a reliability standard” - NO
  - “It’s a design assurance standard” - MAYBE
  - “It’s a safety standard” – SORT OF (But don’t tell anybody!)
  - “It’s both a product and a process assurance standard” – YEAH!
- But, have you heard the growing debate regarding the balance between product and process assurance?



Ferrell and Associates  
Consulting, Inc.

Slide 6

2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



### Food for Thought

- During last year's System Safety Society Conference, a paper was presented that argued rather eloquently that we have collectively gone too far with process assurance in two ways, saying:

"[We tend to] focus mainly on reliability (or integrity) at the expense of functionality and performance, thereby addressing only how unsafe a system is when it fails, and ignoring the more fundamental question of how safe a system is when it is working."

- AND -

"...there is a tendency to assume (incorrectly) that not only will sound safety management processes result automatically in a 'safe' system but also that proof of adherence to such processes provides conclusive evidence of the achievement of system safety."



Ferrell and Associates  
Consulting, Inc.

Slide 7

2002 FAA National  
Software Conference



### The Nuts and Bolts

- Once you've solved the safety and software conundrum, it probably makes sense to hone in on Software Engineering and DO-178B. Here things get even murkier!
- We once again are faced with the same questions that plagued those stalwarts of SC-167 and their descendents in SC-190:
  - What constitutes a requirement and what is design?
  - What type of verification is appropriate and how much do you need?
  - How does one really prove the integrity of the new nifty partitioning scheme?
  - Is determinism really necessary or is predictability good enough?
  - And dare we even mention structural coverage?



Ferrell and Associates  
Consulting, Inc.

Slide 8

2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



### Decoupled from Reality

- With both an 85 page tutorial on MCDC and a paper that really should have been titled, "Everything You Always Wanted to Know About MCDC, but Weren't About to Ask (John – we love you, but 214 pages?), we should probably just let this flavor of structural coverage be.

#### But what of Data and Control Coupling?

- In a paper published in the 1995 Proceedings of COMPASS, twelve different levels of coupling were discussed:
  - Independent Coupling
  - Scalar Data Coupling
  - Scalar Control Coupling
  - Scalar Data/Control Coupling
  - External Coupling
  - Global Coupling
  - Call Coupling
  - Stamp Data Coupling
  - Stamp Control Coupling
  - Stamp Data/Control Coupling
  - Nonlocal Coupling
  - Tramp Coupling



Ferrell and Associates  
Consulting, Inc.

Slide 9

2002 FAA National  
Software Conference



### Adding OOT to the Mix

- In the recent OOT conference, we expanded the dialogue on coupling to address:
  - Class Coupling
    - Attributes
    - Methods
  - Subclass Coupling
  - Client Coupling
- Now, the \$64,000 question, if you sat a group of DERs and FAA Specialists down in a room and asked what must be done to satisfy objective A-7, 8:  
"Test coverage of software structure (data coupling and control coupling) is achieved."

Hmmmm...



Ferrell and Associates  
Consulting, Inc.

Slide 10

2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



---

### The Dirty Little Secrets...

- What about:
  - The debate regarding what is and isn't a viable lifecycle. How much difference is there (really) between spiral or prototype development models and reverse engineering?
  - Do we really want to exclude large classes of COTS components because of some missing data when those components have been built by subject matter experts?
  - How does one answer the broader safety community that is pushing hard down the path of formal methods (Z anyone?) and independent verification and validation?
  - How do we deal with 4<sup>th</sup> and 5<sup>th</sup> generation languages for which code generation is a way of life, not an option?
  - And isn't it time to really do at least a little qualification on those integrated CM tools that are really the last things to touch the code in many instances?



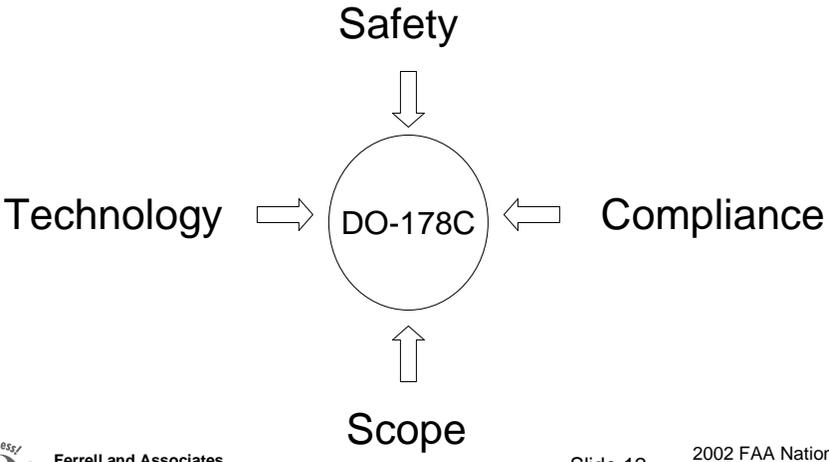
Ferrell and Associates  
Consulting, Inc.

Slide 11      2002 FAA National  
Software Conference



---

### The Challenge is NOW...



The diagram illustrates the challenge of DO-178C. At the center is a circle labeled "DO-178C". Four arrows point towards this central circle from the top, bottom, left, and right. The top arrow is labeled "Safety", the bottom arrow is labeled "Scope", the left arrow is labeled "Technology", and the right arrow is labeled "Compliance".

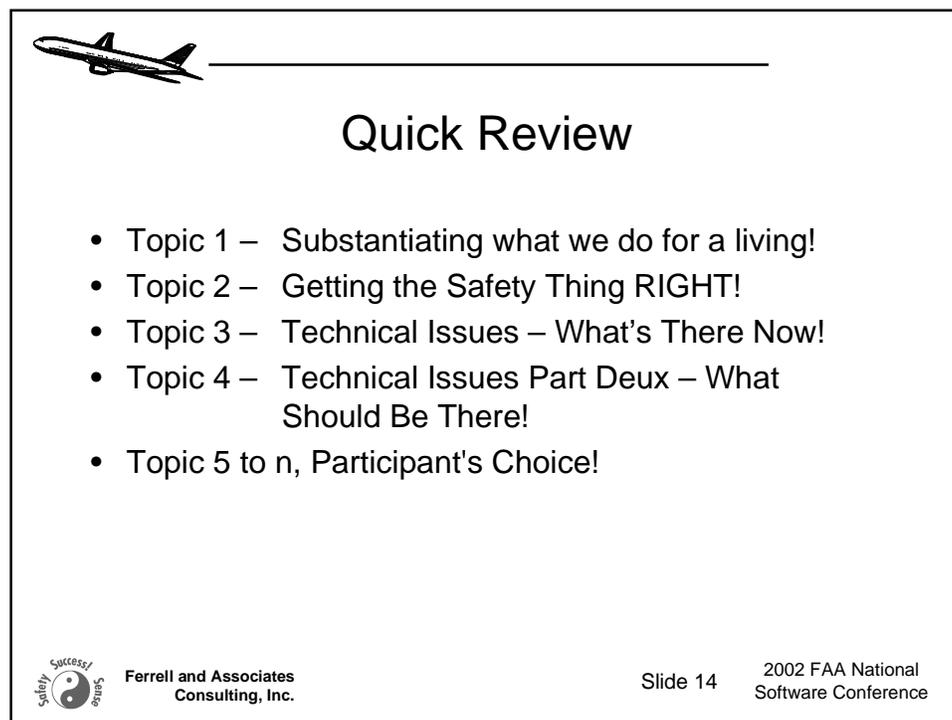
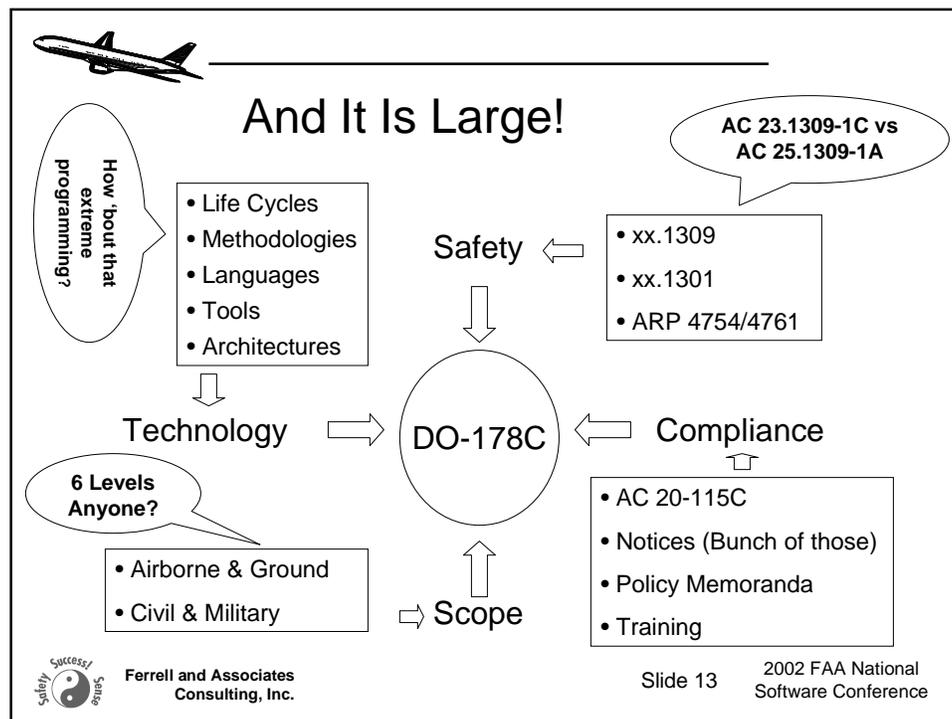


Ferrell and Associates  
Consulting, Inc.

Slide 12      2002 FAA National  
Software Conference

# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



# FAA National Software Conference, May 2002

## DO-178B - A Square Peg in a Round Hole?



---

**WHAT DO YOU THINK??**



Ferrell and Associates  
Consulting, Inc.

Slide 15      2002 FAA National  
Software Conference



---

**References**

- “DO-178B, Software Considerations in Airborne Systems and Equipment”, RTCA, Inc, 1992.
- “Safety Assurance of Air Traffic Management and Similarly Complex Systems”, Fowler, D., Tiemeyer, B., Eaton, A., Proceedings of the 19<sup>th</sup> System Safety Society Annual Conference, September 2001.
- “A Practical Tutorial on Modified Condition / Decision Coverage”, Hayhurst et al, NASA / TM-2001-210876, May 2001.
- “An Investigation of Three Forms of Modified Condition Decision Coverage (MCDC) Criterion”, Chilenski, J., DOT/FAA/AR-01/18, April 2001.
- “Integration Testing Based on Software Couplings”, Zhenyi, J., and Offut, A.J., COMPASS Proceedings, June 1995.



Ferrell and Associates  
Consulting, Inc.

Slide 16      2002 FAA National  
Software Conference