Software Evidence in the Aviation Domain

C. Michael Holloway

NASA Langley Research Center

c.michael.holloway@nasa.gov

Presented remotely to

14th Software Certification Consortium

4 May 2015

DISCLAIMERS

The opinions expressed in this presentation are mine alone and do not represent official opinions of my own organization or of any other organization to which I refer.

These slides are incomplete without an accompanying oral presentation.

Two Part Presentation

Part 1 – Evidence in the Concrete

In which DO-178C's approach to evidence is described

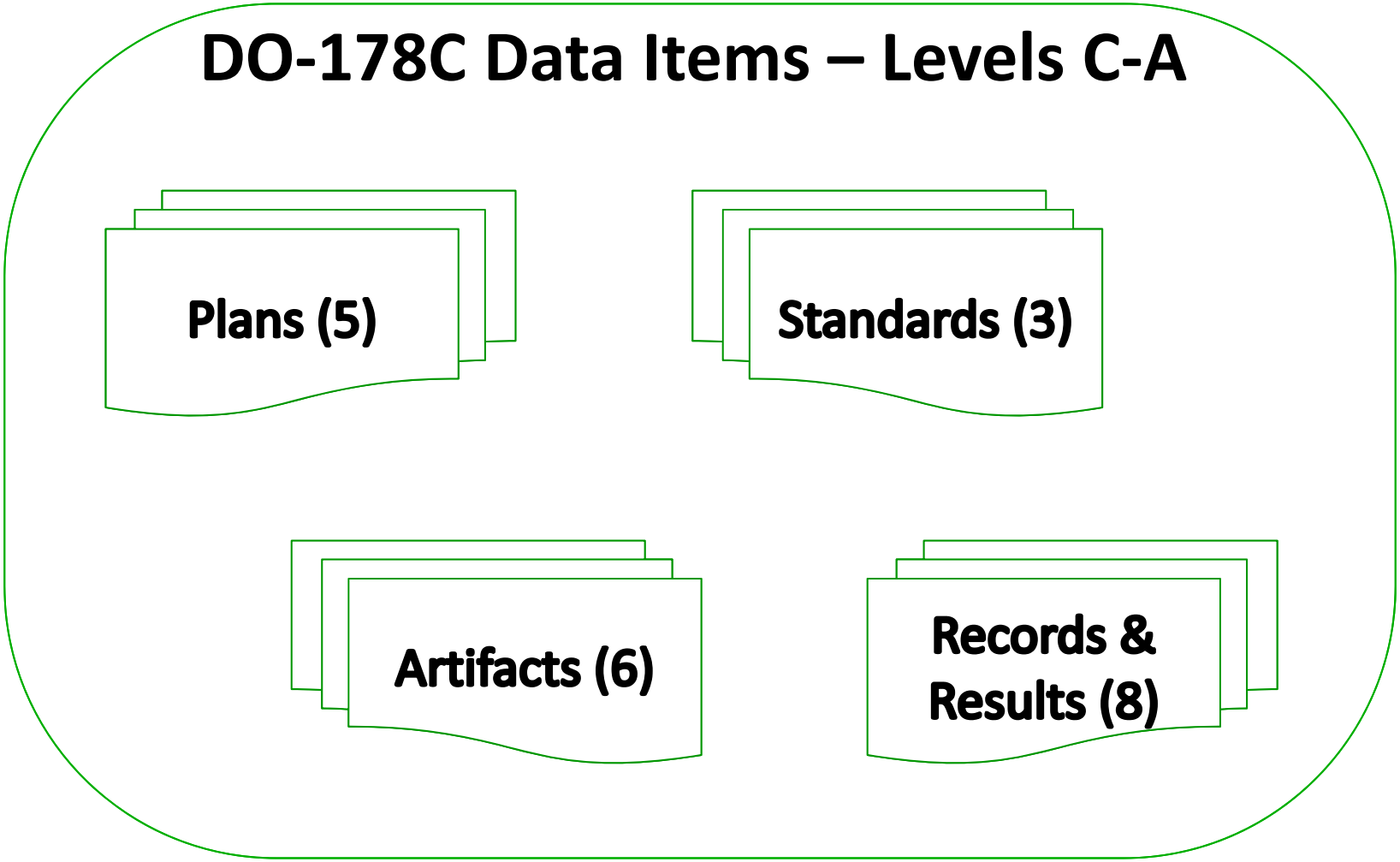
(~80% of the talk)

Part 2 – Evidence in the Abstract

In which I opine about the grave dangers of emphasizing 'evidence' over 'argument'

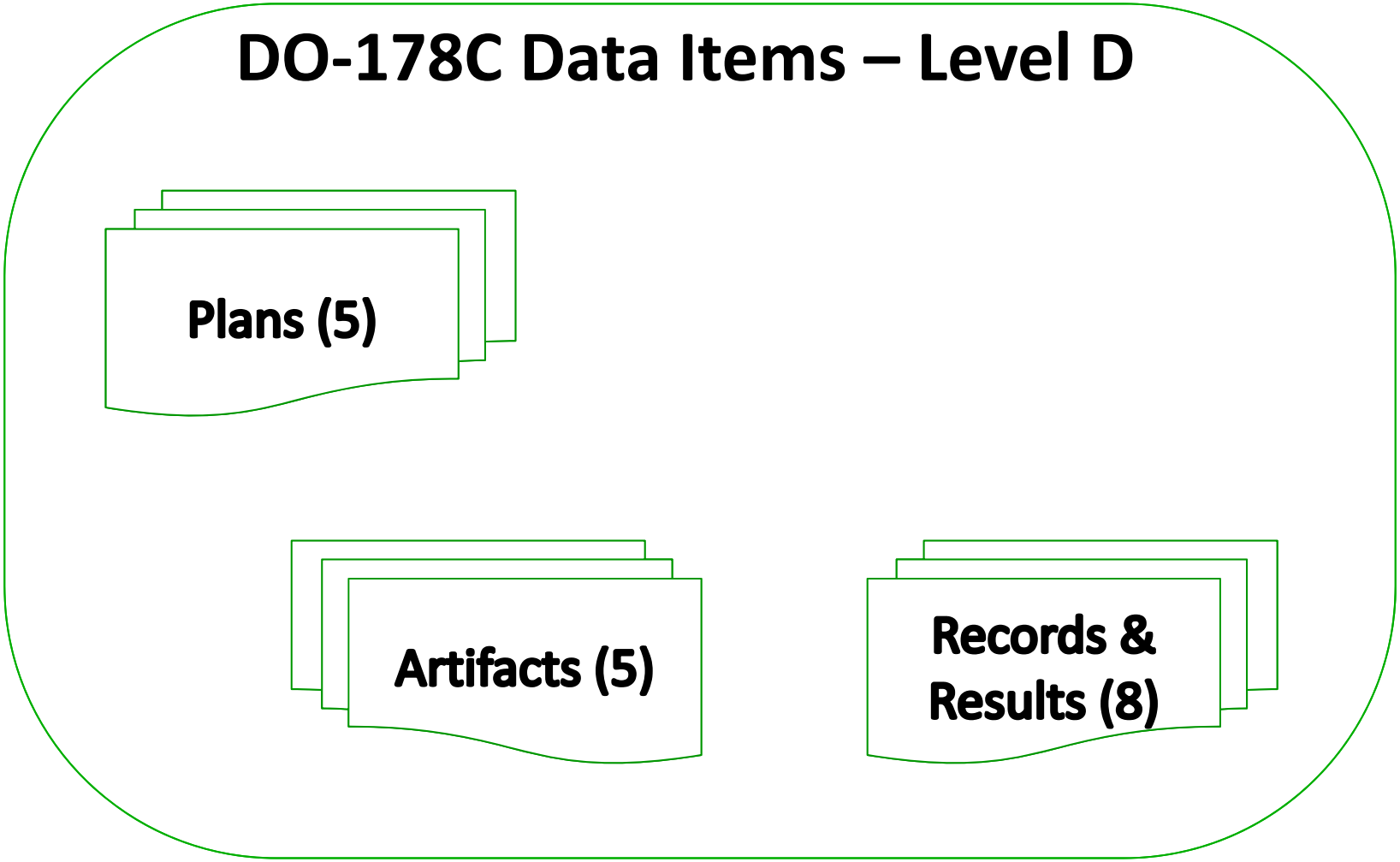
(~20% of the talk)

DO-178C Data Items – Levels C-A



See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C.
Section 11 Software Life Cycle Data
(division into 4 categories is my doing alone – not part of the document)

DO-178C Data Items – Level D



See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C.
Section 11 Software Life Cycle Data
(division into 4 categories is my doing alone – not part of the document)

PLANS

- Plan for Software Aspects of Certification
- Software Development Plan
- Software Verification Plan
- Software Configuration Management Plan
- Software Quality Assurance Plan

See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Sections 11.[1-5]

STANDARDS

- Software Requirements Standards
- Software Design Standards
- Software Code Standards

Not required for Level D

See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Sections 11.[6-8]

ARTIFACTS

- Software Requirements Data
- Design Description
- Source Code - not required for Level D
- Executable Object Code
- Trace Data
- Parameter Data Item File

See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Sections 11.[9-12,21.22]

RESULTS & REPORTS

- Software Verification Cases and Procedures
- Software Verification Results
- Software Life Cycle Environment Configuration Index
- Software Configuration Index
- Problem Reports
- Software Configuration Management Records
- Software Quality Assurance Records
- Software Accomplishment Summary

See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Sections 11.[13-20]

CONCERNING DATA ITEMS

- No specific form or packaging method is mandated by the standard
- Configuration management control categories (CC1, CC2) are specified by software level
- May be adapted to the needs of the project
- Each data item is expected to have desirable characteristics

See RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Sections 11.0.[bcda]

Desired Data Item Characteristics

- Unambiguous
- Complete
- Verifiable
- Consistent
- Modifiable
- Traceable

"Information is unambiguous if it is written in terms which only allow a single interpretation, aided, if necessary, by a definition."

"Information is complete when it includes necessary and relevant requirements and/or descriptive material; responses are defined for the range of valid input data; figures used are labeled; and terms and units of measure are defined."

"Information is verifiable if it can be checked for correctness by a person or tool."

"Information is consistent if it is used and has a uniform notation, terminology, and symbology within it."

"Information is modifiable if it is structured and has a style such that changes can be made completely, consistently, and correctly while retaining structure."

"Information is traceable if the origin of its components can be determined."

What do you think these words mean?

Words in this font are quoted from
RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Section 11.0.a

THAT IS, A DATA ITEM SHOULD ...

- be written in terms which only allow a single interpretation, aided, if necessary, by a definition
- include necessary and relevant requirements and/or descriptive material; define responses for the range of valid input data; label figures used; define terms and units of measure
- be checkable for correctness by a person or tool
- have no conflicts within it
- be structured and have a style such that changes can be made completely, consistently, and correctly while retaining structure
- have components whose origins can be determined

Summary of RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Section 11.a

SOFTWARE REQUIREMENTS DATA (EX. 1)

- … definition of the high-level requirements including the derived requirements.
- should include
  - a. Description of the allocation of systems requirements to software, with attention to safety-related requirements and potential failure conditions.
  - d. Timing requirements and constraints.
  - g. Failure detection and safety monitoring requirements.
  - Also b, c, e, f, h

Words in this font are quoted from
RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Section 11.9

DESIGN DESCRIPTION (EX. 2)

- … definition of the software architecture and the low-level requirements that will satisfy the high-level requirements.
- should include
  - a. A detailed description of how the software satisfies the specified high-level requirements, including algorithms, data structures, and how software requirements are allocated to processors and tasks.
  - d. The data flow and control flow of the design.
  - h. Partitioning methods and means of preventing partition breaches.
  - j. Derived requirements resulting from the software design process.
  - Also b, c, e, f, g, i, k, l

Words in this font are quoted from
RTCA (2011) Software Considerations in Airborne Systems and Equipment Certification. DO–178C. Section 11.10

BOTTOM LINE

The Data Items constitute

*A **means***

the evidence

from which the determination is made

about whether

*to an **end***

*which is a **means***

the required objectives are satisfied

for approving the system for deployment

Two Part Presentation

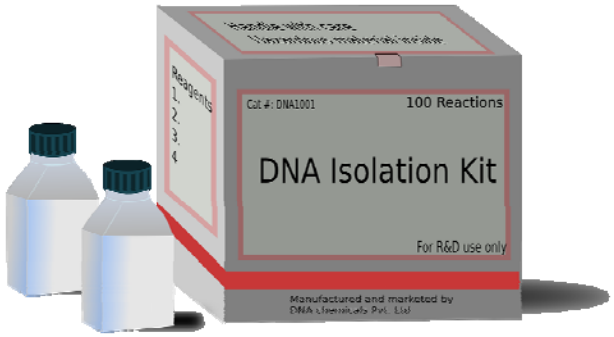
Part 1 – Evidence in the Concrete

In which DO-178C's approach to evidence is described

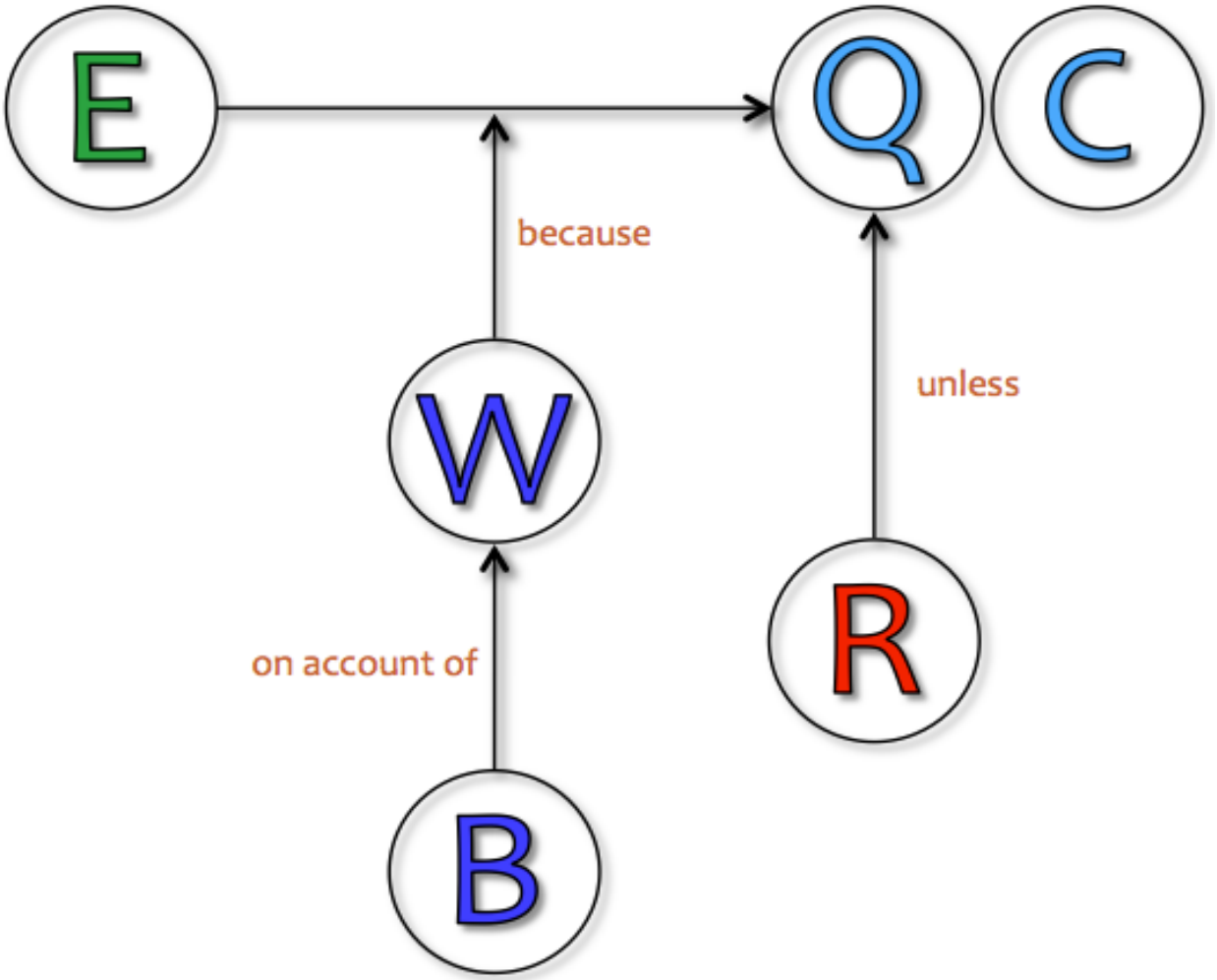
Part 2 – Evidence in the Abstract

In which I opine about the grave dangers of emphasizing 'evidence' over 'argument'

Evidence w/o Argument



EVIDENCE IN CONTEXT



Evidence
Conclusion
Warrant

Qualification
Rebuttal
Backing

Based on *The Uses of Argument*, Stephen E. Toulmin, updated edition, 2003 (1958)

CURRENT PRACTICE SEEMS TO …

- … emphasize production of evidence
  - Data items showing compliance with level A objectives
- … rely on mostly implicit warrants & backing
  - Why is level A compliance data deemed sufficient?
- Thus it is hard to know
  - The relative importance of different types and instances of evidence
  - What can be changed or eliminated without adversely affecting outcome

EXPLICATE '78 PROJECT

- Multi-year activity to (among other things)
  - Identify the arguments contained in, or implied by DO-178C, which implicitly justify the assumption that the document meets its stated purpose …
  - Express the arguments explicitly in the form of an assurance case
- Funded by FAA & NASA

C. Michael Holloway, 'Explicate '78: Discovering the Implicit Assurance Case in DO-178C', in *Engineering Systems for Safety*, M. Parsons and T. Anderson (eds). Proceedings of 23rd Safety-critical Systems Symposium, 2-5 February 2015, Bristol, UK.

Bottom Line – Part 2

Evidence is always necessary
but never sufficient.