

ASCE and a production line for safety case review

Tim Clement



Background

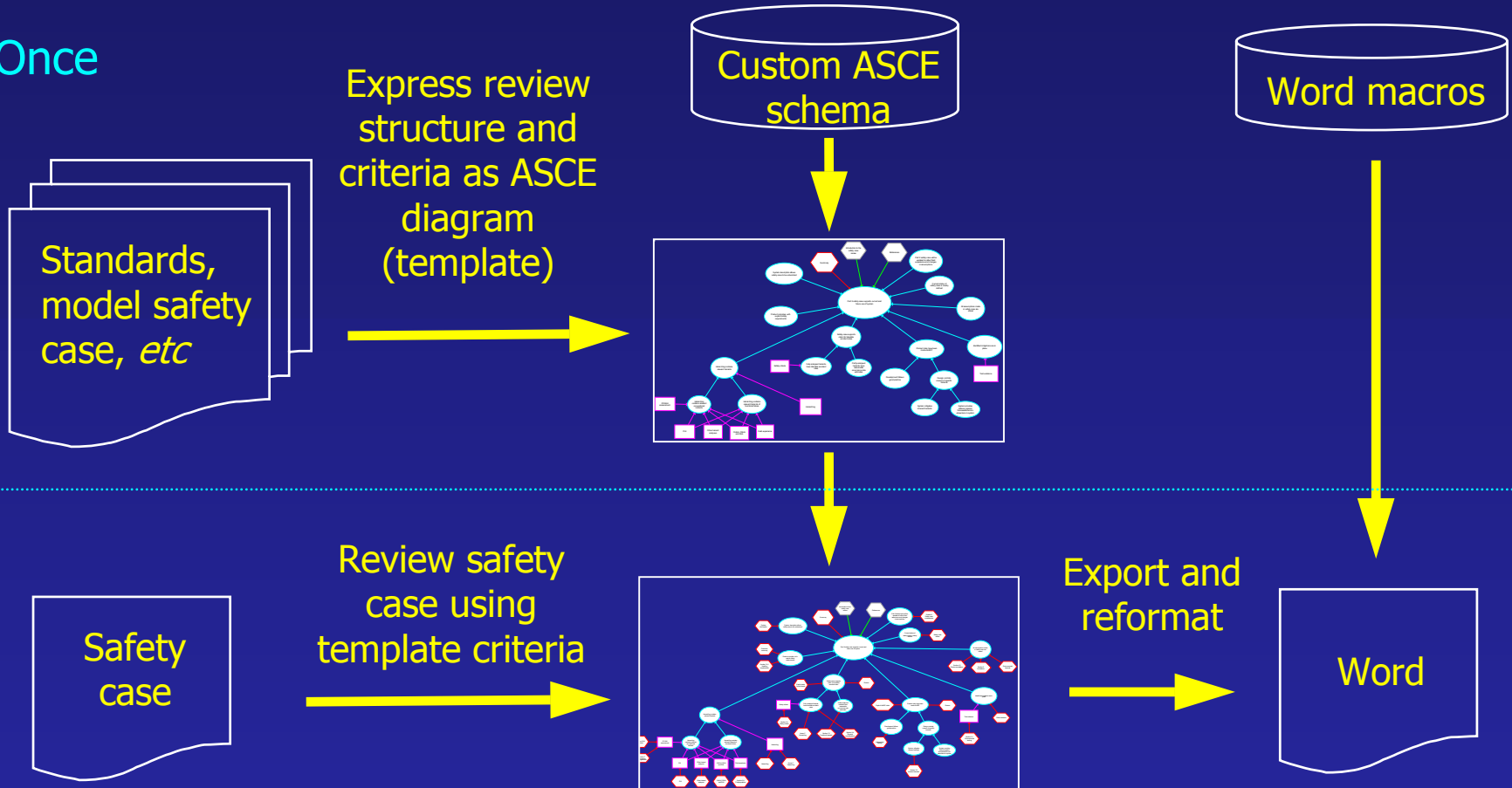
- ASCE
 - Analysing and Simplifying Complex Evidence [*Goal*]
 - But also Adelard Safety Case Editor [*Tool*]
 - Document content in editable nodes
 - ◆ With capabilities for formatting, cross-reference *etc*
 - Document structure exhibited as diagram
 - ◆ Links between node representations
 - For showing explicit safety case argument structure
 - Many other uses: shall demonstrate one here
- Production line: think Lexus rather than Leyland

Goals

- To support Adelard's ISA role
 - On project generating many *[100+]* safety case reports
- Completeness of review
 - Establish a set of criteria to apply to each safety case
 - Helps in commenting on omissions
- Uniformity of approach
 - Common style of response from many authors
- Guidance to safety case producers
 - Some suppliers have limited Def Stan 00-56 experience
 - Criteria can be included in safety case reviews

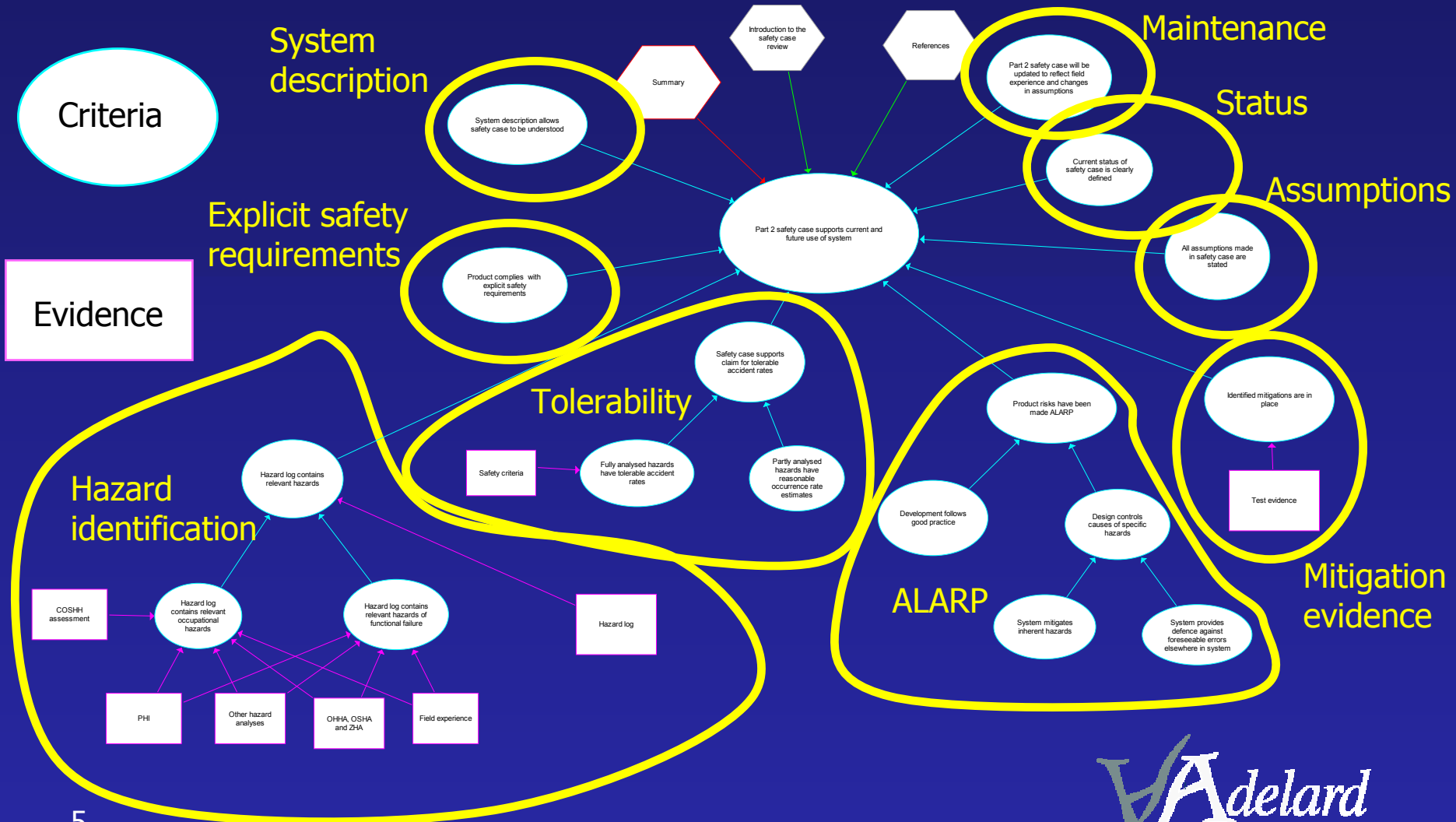
Our solution

Once



Many

The template: more detail



A typical criteria node

[CLAIM] - Hazard log contains relevant hazards - ASCE Node Editor

Node Edit View Tools Insert Format Table

B *I* U [List icons]

Hazard identification
Review criteria

Hazard log contains relevant hazards

Hazard identification

Review criteria

The safety case should provide evidence of a preliminary hazard identification process, normally based on a structured technique such as Hazops or FMEA. The effectiveness of such methods depends on the completeness and accuracy of the product description used, and the expertise of the group conducting the analysis, both in the use of the techniques and in the application domain, and the review should assess these. Good practice is established by standards. Def Stan 00-56 Part 2 Annex B contains a suggested checklist mainly concerned with occupational hazards. Def Stan 00-58 (cited by Def Stan 00-56) provides guidance on the use of Hazops techniques for systems containing programmable electronic systems, including suggested system representations and appropriate interpretations of the guidewords. IEC 61508 cites IEC 60300, which describes Hazops and FMEA as well as the use of fault trees and reliability block diagrams.

Etc

Node label for diagram navigation

Headings give structure to review in final text

Review criteria for this area of safety case (for reviewers and reviewed)

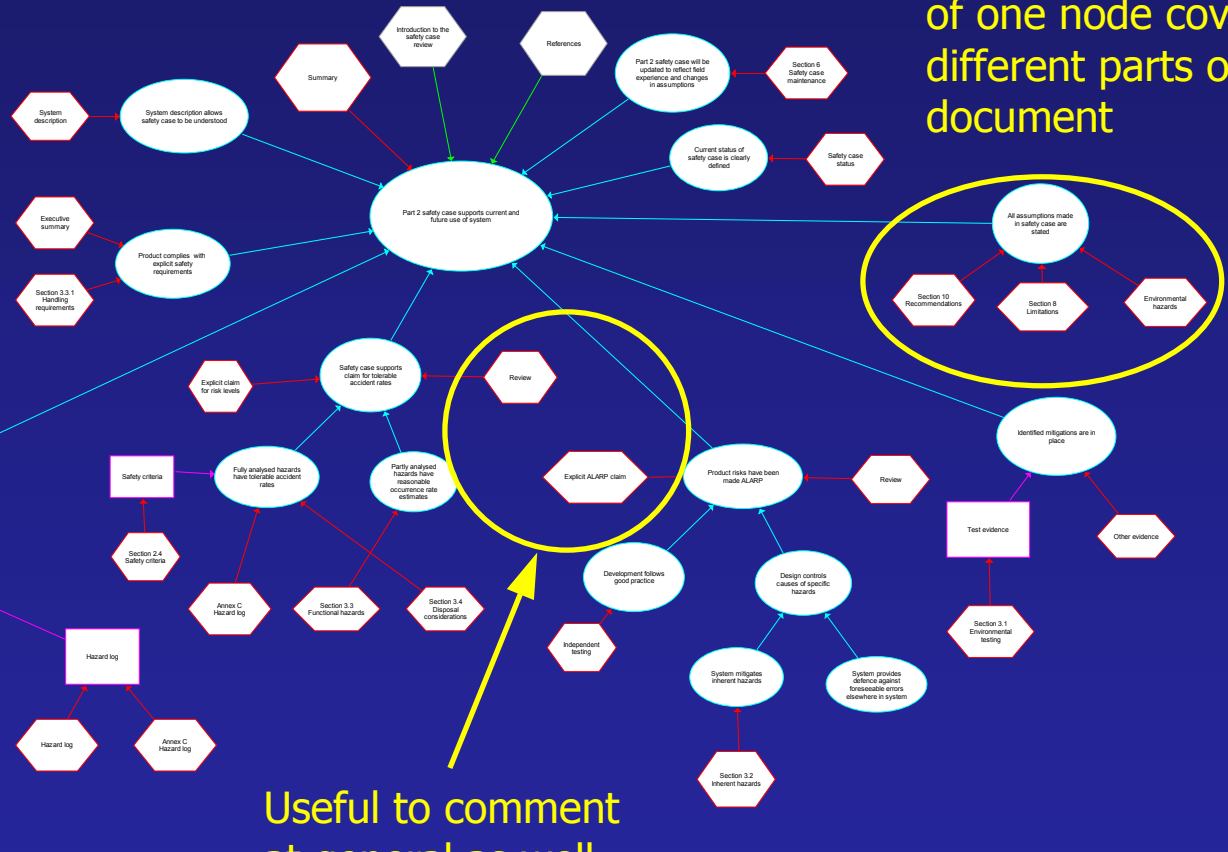
Evidence nodes

- Documents or sections we expect in safety case
 - Typically part of Def Stan 00-56 document structure
 - E.g.* PHA, safety criteria
- In diagram as part of review structure
 - Expect to comment specifically on them
- Criteria are in higher level nodes
 - But these often contain headings
 - For review structure in Word document

A populated review



Reviews attached to evidence nodes and claim nodes



Multiple reviews of one node cover different parts of document

A review node

The screenshot shows the ASCE Node Editor interface. The title bar reads "[REVIEW] Annex C - Hazard log - ASCE Node Editor". The menu bar includes "Node", "Edit", "View", "Tools", "Insert", "Format", and "Table". The toolbar contains icons for bold, italic, underline, bulleted list, numbered list, indent, outdent, and link. The main content area is titled "Occupational hazards" and contains the following text:

Occupational hazards

The hazard log shown in Annex C does not give the complete view of the hazard analysis that it should. It describes each hazard, but not the accident or accidents that it may give rise to and their severity. The hazard probabilities seem more likely to be accident probabilities, taking the external mitigations into account: these are certainly more useful in the risk assessment. It is not clear how the target probabilities have been set, and there is no statement of the risk class of the hazard-accident combinations. (This would require the risk classification matrix to be included in the safety criteria, as requested in [Section 2.4 - Safety criteria.](#))

Section 3.5 describes the contents of the hazard history sheets, which do appear to provide a complete description of the analysis but have not been provided for review. Other safety case reports have presented the hazard analysis in this form, and given the small number of hazards involved we suggest that this should be done here.

Annotations in the image include:

- A callout box pointing to the "Annex C" and "Hazard log" fields: "ASCE node labels help with ASCE navigation".
- A callout box pointing to the "Occupational hazards" heading: "Subheadings subdivide final text form".
- A callout box pointing to the "Section 2.4 - Safety criteria." link: "ASCE supports cross-references to (headings in) other nodes, including bibliography".
- A callout box pointing to the "Section 3.5" heading: "Explicit section references support final text form".

Preparing the Word version

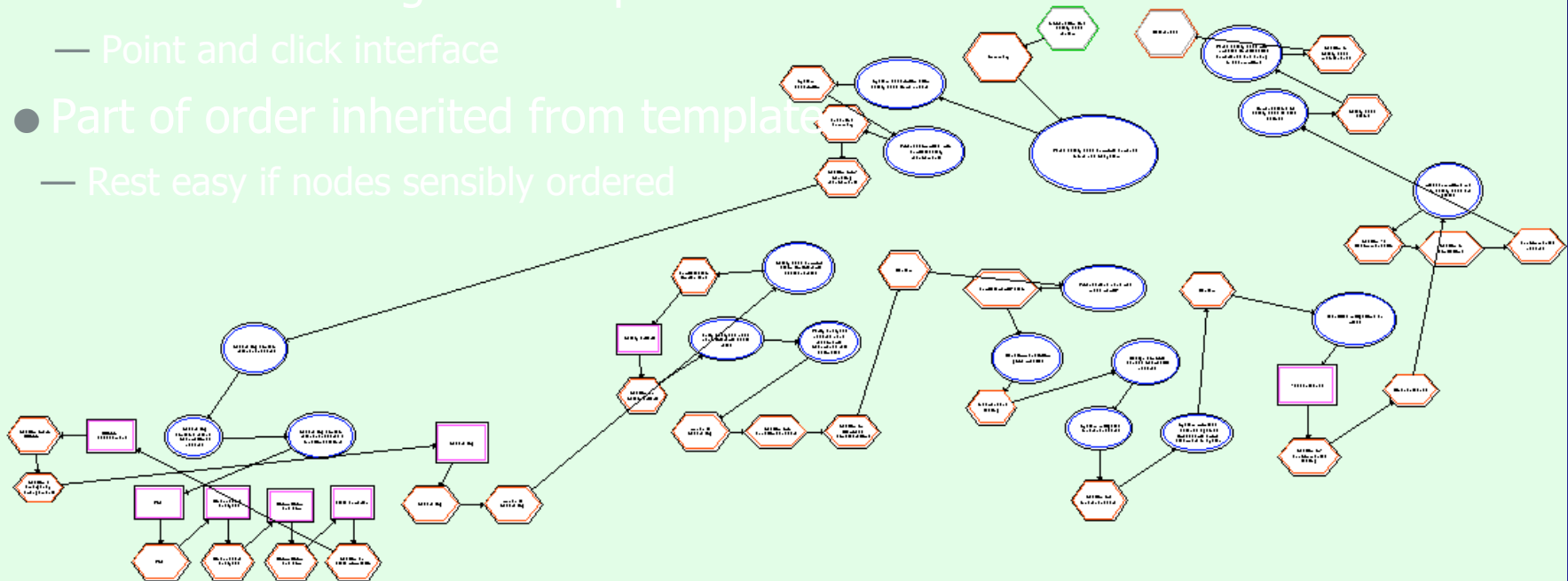
- Word document needs linear ordering of nodes

- Constructed using ASCE export order tool

- Point and click interface

- Part of order inherited from template

- Rest easy if nodes sensibly ordered



The report format

Heading formats and numbering
generated from ASCE headings
by Word macros

7.4 Occupational hazards

60. The hazard log shown in Annex C does not give the complete view of the hazard analysis that it should. It describes each hazard, but not the accident or accidents that it may give rise to and their severity. The hazard probabilities seem more likely to be accident probabilities, taking the external mitigations into account: these are certainly more useful in the risk assessment. It is not clear how the target probabilities have been set, and there is no statement of the basis for the target probabilities. (This would require the risk assessment requested in §59.)

Review exported from
ASCE as HTML, then read
into Word

61. Section 3.5 provides a complete description of the hazards, which do appear to provide a basis for review. Other safety case reports have presented the hazard analysis in this form, and given the small number of hazards involved we suggest that this should be done here.

7.5 Functional failures

62. The Isengard safety case will need to show that the palantir is sufficiently reliable to support its intended use within Isengard. Section 3.3 addresses functional failures even though these do not appear in the hazard log. It assumes that they result in degradation or complete loss of performance, but does not consider the possibility of data corruption (e.g. from software errors). It gives the MTBF of the palantir as 42 120 years but does not say whether this is for hardware failures alone. To be useful, software failures must also be included.

Cross-references formatted and linked by Word
macros (paragraphs, sections, bibliography)



Paragraph
numbers
added by
Word
macro to
support
responses

Our experience

- Framework useful in generating reviews
 - Reviewers' guidance on areas to cover
 - Particularly useful for first reviews on project
 - Flexible staffing has helped keep reviews timely
 - Easy to place comments from document in structure
 - Helps with PDF cases which are less easily annotated
 - Emphasises substantive comments rather than typos
 - And positive comments as well as negative ones
- Final editing and internal review use Word form
 - Need to consider linear flow as well as technical content
 - All changes propagated back to ASCE diagram

Field experience

- Client concern: lack of comment classification
 - Safety *vs* presentation, major *vs* minor
 - Summary and comment guidance not enough
 - Could implement using ASCE status fields
- Our main issue: responses and re-reviews
 - Client comments in a variety of *[Word]* formats
 - Need to close the ASCE-Word-ASCE loop
 - Word macros could generate tabular formatting
 - With space for response from SCR authors
 - Could then extract comments to maintain ASCE form

Summary

- Analysing and Simplifying Complex Evidence
 - In this case, evidence presented as safety case
- Using Adelard Safety Case Editor
 - Coming to appreciate that it is rather more than this
 - Have exploited flexibility given by
 - Custom ASCE schema definitions
 - Control of linear ordering of presentation
 - Control of HTML export format by templates
 - All supported by ASCE 1.6 [*As demonstrated*]
- Automated Support for Commenting on Evidence?