√EROCEL

Using VeroTrace to support Assurance Cases and Arguments for Safety and Security Certification

Verocel, Inc.

Abstract

Verocel's VeroTrace lifecycle management tool incorporates support for structured arguments/Assurance Cases into its hyperlinked framework for certification. In this paper, Verocel provides an overview of what an Assurance Case is, how an Assurance Case and Structured Argument benefit safety certification, and how Verocel's VeroTrace tool is used to record the Assurance Case, the Structured Argument elements, and supporting certification evidence.

Keywords: *Certification, Assurance Case, Structured Argument, Safety*

1. What is an Assurance Case?

An assurance case is the summation of a semi-formal structured argument including the evidence and analyses that support the argument's conclusions. There are specific kinds of assurance cases that are directed toward specific industry sectors, most notably safety cases and security cases. Since an assurance case argues fitness for use in a given context, a sound evaluation of fitness for use in the context of a safety critical system is generally termed a safety case. According to the U.K. Ministry of Defence (Ministry of Defence, January 1996): "A safety case is a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment." Although the assurance case is typically the final deliverable product in a safety or security certification effort, the structured argument is the topic of interest here.

2. What is an Argument?

On the surface, it's a conclusion with some reasoning based on a particular set of premises. For example, the conclusion that putting money in a bank makes it hard to steal is based on the reasoning that banks keep money in a safe and the premise that it's hard to steal from a safe.

A structured argument used as part of an assurance case will have much more complexity, and each reasoning step yields additional premises, which in turn lead to more, finer-grained reasoning steps, until the premises can be directly supported with empirical evidence or analysis. This combination of the argument steps and the evidence to back up the conclusions forms an assurance case. The VeroTrace tool is configurable such that a variety of representations for structured arguments can be supported, such as:

- Toulmin's method (Toulmin, 1958, updated ed. 2003), using Claims, Warrants, Backing, Rebuttals,
- Goal Structuring Notation (ACWG, January 2018), using Goals, Strategies, Context, and
- ASPIC-type notations (Prakken, September 2009)

3. Why is a Structured Argument useful in safety or security certification?

The benefits to a program can be manifold, depending on how the argument is built and what the goals are for its production. If an argument is built around a risk assessment, for example a HAZOP, FMEA, or an ARP 4761 compliant safety assessment process, creating the argument can result in better insight into application-specific risks, yielding more effective risk mitigation strategies than just implementing prescribed safety measures. Alternatively, if the argument is built around system safety requirements and their implementation, then the stages of refinement of those requirements can be directly linked to planning and verification evidence, the contribution of each layer of specification to overall system safety, and adherence to standards such as DO-178C, IEC-61508, or ISO 26262 can be more clearly demonstrated. Structured arguments have been in use in safety-related software certification for many years. Standards such as DO-178C can be viewed as an implicit structured argument. (Holloway, 2012). Structured arguments are particularly useful in areas that are viewed as less deterministic such as machine vision, automated controls, or other probabilistic applications, where creating a reviewable, traceable, logically decomposed expression of a system's compliance with a current standard might otherwise be difficult.

4. What are the elements of an Argument?

Stephen Toulmin, in The Uses of Argument (Toulmin, 1958, updated ed. 2003), describes an argument as consisting of a conclusion (Claim), one or more premises (Grounds), and some reasoning (Warrant). The formulation is one where a stated conclusion is justified by the premises because of the reasoning. Toulmin expands on this by introducing Backing rationale to support the Warrant, as well as Qualifiers and Rebuttals. The ASD[1] research project RESSAC (Re-Engineering and Streamlining the Standards for Avionics Certification) suggests some modifications to this notation (RESSAC, REF: LIV-S-026-D6-509 -- 11/12/2018), resulting in the following formulation, currently in use at Verocel:

- Conclusion: to be derived from the current argument step

  This equates to Toulmin's Claim element.
- Reasoning: describes how the Conclusion may be derived from the given Premises

  This equates to Toulmin's Warrant element.
- Backing: supports the reasoning
- Premises: the grounds for the arguments

  This equates to Toulmin's Grounds element.
- Defeater: challenges soundness of the argument or the truth of the Conclusion

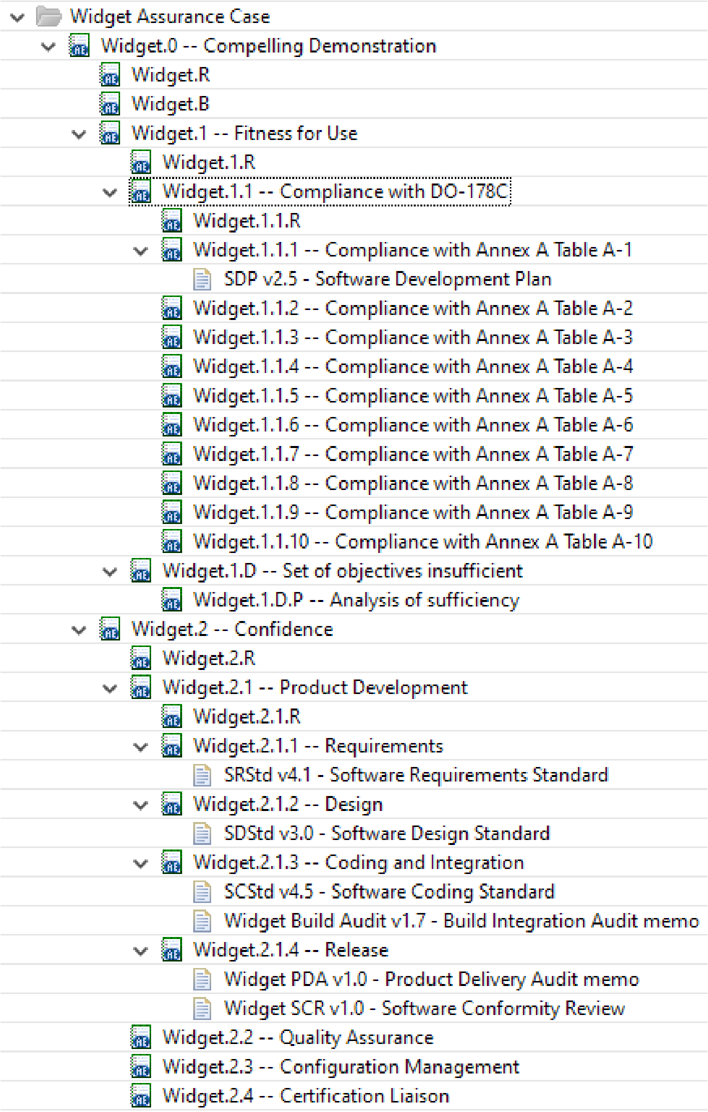
  This equates to Toulmin's Rebuttal element.

With an understanding of the terminology, the logical breakdown of an argument into its elements is simple to follow. The argument is iteratively decomposed, where each premise is the conclusion of a subordinate argument step. Decomposition continues until the lowest-level premises are all directly supported by evidence or analyses. In VeroTrace, any argument element can be linked to supporting evidence comprised of actual lifecycle wwwdata including but not limited to; requirements, tests, test results, documents, and analyses.

5. Using VeroTrace to capture an Argument

VeroTrace is able to support a number of different structured argument topologies. VeroTrace support for arguments is predicated on the understanding that a structured argument is composed of several kinds of elements, such as premises, reasoning, conclusions, etc., and different types of evidentiary artifacts that are linked to the argument elements they support through influence and dependency relationships. Each element and artifact can have its own review cycle, is configuration managed, and version controlled. VeroTrace also supports impact analysis if an artifact is modified based on the influence and dependency relationships between the argument elements and supporting artifacts.

The following example of a simple argument shows different levels of decomposition, the various elements of an argument, and how evidence artifacts, trace to different argument elements. In this example, an assurance case is made for the fitness of the Widget product for use in DO-178C avionics systems.

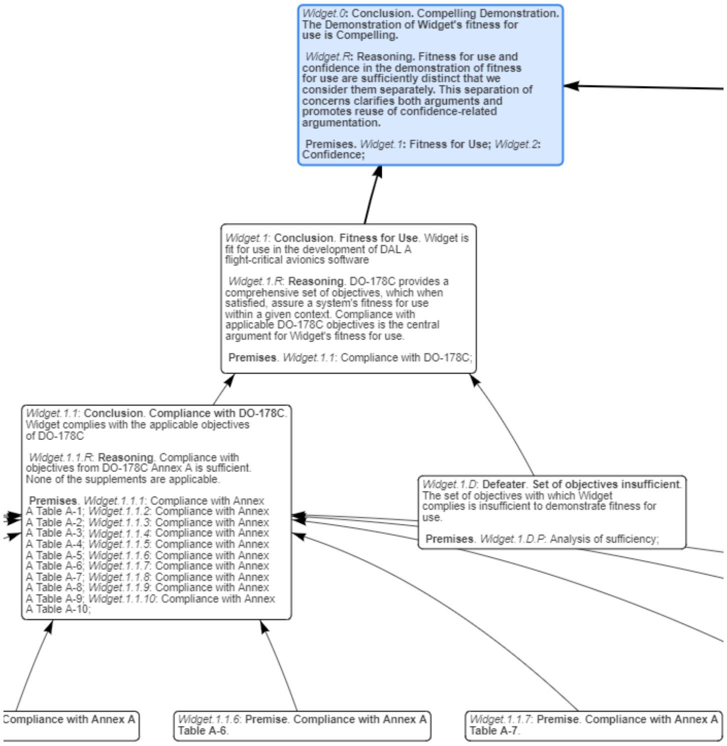


```
Widget Assurance Case
  Widget.0 -- Compelling Demonstration
    Widget.R
    Widget.B
    Widget.1 -- Fitness for Use
      Widget.1.R
      Widget.1.1 -- Compliance with DO-178C
        Widget.1.1.R
        Widget.1.1.1 -- Compliance with Annex A Table A-1
          SDP v2.5 - Software Development Plan
        Widget.1.1.2 -- Compliance with Annex A Table A-2
        Widget.1.1.3 -- Compliance with Annex A Table A-3
        Widget.1.1.4 -- Compliance with Annex A Table A-4
        Widget.1.1.5 -- Compliance with Annex A Table A-5
        Widget.1.1.6 -- Compliance with Annex A Table A-6
        Widget.1.1.7 -- Compliance with Annex A Table A-7
        Widget.1.1.8 -- Compliance with Annex A Table A-8
        Widget.1.1.9 -- Compliance with Annex A Table A-9
        Widget.1.1.10 -- Compliance with Annex A Table A-10
      Widget.1.D -- Set of objectives insufficient
        Widget.1.D.P -- Analysis of sufficiency
    Widget.2 -- Confidence
      Widget.2.R
      Widget.2.1 -- Product Development
        Widget.2.1.R
        Widget.2.1.1 -- Requirements
          SRStd v4.1 - Software Requirements Standard
        Widget.2.1.2 -- Design
          SDStd v3.0 - Software Design Standard
        Widget.2.1.3 -- Coding and Integration
          SCStd v4.5 - Software Coding Standard
          Widget Build Audit v1.7 - Build Integration Audit memo
        Widget.2.1.4 -- Release
          Widget PDA v1.0 - Product Delivery Audit memo
          Widget SCR v1.0 - Software Conformity Review
      Widget.2.2 -- Quality Assurance
      Widget.2.3 -- Configuration Management
      Widget.2.4 -- Certification Liaison
```

This example is not intended to be complete, and only shows some of the possible relationships between argument elements and evidentiary artifacts that VeroTrace supports.

[1] AeroSpace and Defence Industries Association of Europe (ASD)

Through the use of the context reporting feature, VeroTrace also allows the argument, or argument-fragments, to be rendered in a navigable HTML pictographic view that also allows the user to zoom in and out to show more or less of the argument structure and contents:



Widget.0: **Conclusion. Compelling Demonstration. The Demonstration of Widget's fitness for use is Compelling.**

Widget.R: **Reasoning. Fitness for use and confidence in the demonstration of fitness for use are sufficiently distinct that we consider them separately. This separation of concerns clarifies both arguments and promotes reuse of confidence-related argumentation.**

Premises. *Widget.1*: **Fitness for Use;** *Widget.2*: **Confidence;**

Widget.1: **Conclusion**. **Fitness for Use**. Widget is fit for use in the development of DAL A flight-critical avionics software

Widget.1.R: **Reasoning**. DO-178C provides a comprehensive set of objectives, which when satisfied, assure a system's fitness for use within a given context. Compliance with applicable DO-178C objectives is the central argument for Widget's fitness for use.

Premises. *Widget.1.1*: Compliance with DO-178C;

Widget.1.1: **Conclusion**. **Compliance with DO-178C**. Widget complies with the applicable objectives of DO-178C

Widget.1.1.R: **Reasoning**. Compliance with objectives from DO-178C Annex A is sufficient. None of the supplements are applicable.

Premises. *Widget.1.1.1*: Compliance with Annex A Table A-1; *Widget.1.1.2*: Compliance with Annex A Table A-2; *Widget.1.1.3*: Compliance with Annex A Table A-3; *Widget.1.1.4*: Compliance with Annex A Table A-4; *Widget.1.1.5*: Compliance with Annex A Table A-5; *Widget.1.1.6*: Compliance with Annex A Table A-6; *Widget.1.1.7*: Compliance with Annex A Table A-7; *Widget.1.1.8*: Compliance with Annex A Table A-8; *Widget.1.1.9*: Compliance with Annex A Table A-9; *Widget.1.1.10*: Compliance with Annex A Table A-10;

Widget.1.D: **Defeater**. **Set of objectives insufficient**. The set of objectives with which Widget complies is insufficient to demonstrate fitness for use.

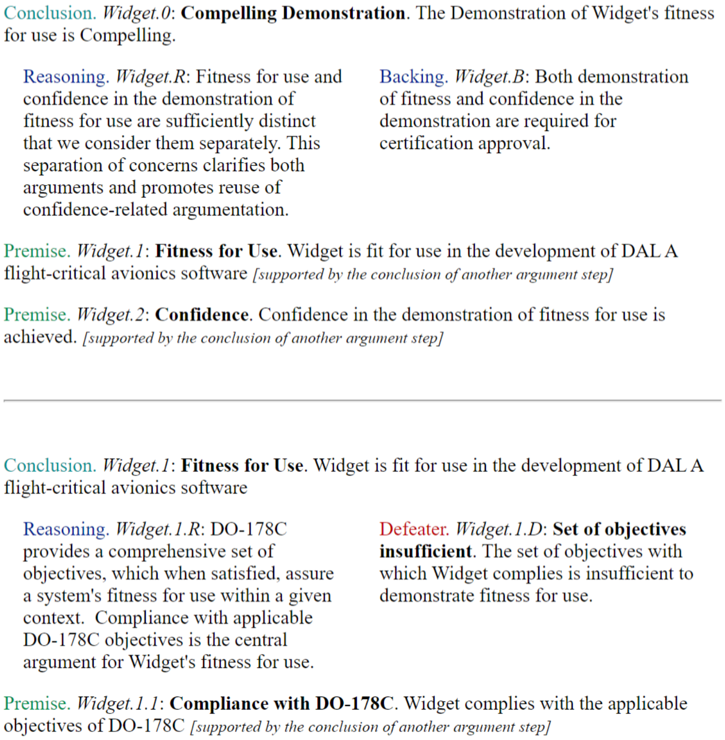
Premises. *Widget.1.D.P*: Analysis of sufficiency;

Compliance with Annex A

Widget.1.1.6: **Premise**. **Compliance with Annex A Table A-6**.

Widget.1.1.7: **Premise**. **Compliance with Annex A Table A-7**.

A textual representation of the argument can also be generated using the VeroTrace context-sensitive reporting feature:



Conclusion. *Widget.0*: **Compelling Demonstration**. The Demonstration of Widget's fitness for use is Compelling.

Reasoning. *Widget.R*: Fitness for use and confidence in the demonstration of fitness for use are sufficiently distinct that we consider them separately. This separation of concerns clarifies both arguments and promotes reuse of confidence-related argumentation.

Backing. *Widget.B*: Both demonstration of fitness and confidence in the demonstration are required for certification approval.

Premise. *Widget.1*: **Fitness for Use**. Widget is fit for use in the development of DAL A flight-critical avionics software *[supported by the conclusion of another argument step]*

Premise. *Widget.2*: **Confidence**. Confidence in the demonstration of fitness for use is achieved. *[supported by the conclusion of another argument step]*

Conclusion. *Widget.1*: **Fitness for Use**. Widget is fit for use in the development of DAL A flight-critical avionics software

Reasoning. *Widget.1.R*: DO-178C provides a comprehensive set of objectives, which when satisfied, assure a system's fitness for use within a given context. Compliance with applicable DO-178C objectives is the central argument for Widget's fitness for use.

Defeater. *Widget.1.D*: **Set of objectives insufficient**. The set of objectives with which Widget complies is insufficient to demonstrate fitness for use.

Premise. *Widget.1.1*: **Compliance with DO-178C**. Widget complies with the applicable objectives of DO-178C *[supported by the conclusion of another argument step]*

6. Establishing confidence in the Argument

Having confidence in the conclusions of a structured argument is critical to acceptance of an assurance case as sufficient evidence to accept a system as being fit for use. Confidence is established in several ways.

- A determination must be made that the argument is well-formed and structurally complete.
- There must be confidence in the argument's conclusions and the evidence used to support those conclusions.
- There must be confidence in the processes used to develop the argument and its supporting evidence (integral processes including quality assurance and configuration management).

To establish the structural completeness and correctness of the argument, as shown above, VeroTrace supports both textual and graphical representations of the argument structure and elements, and provides for review of the argument-fragments and evidence elements. The review process is captured within VeroTrace. The review process may lead to changes in the argument or precipitate the creation of defeaters and defeater mitigations to strengthen the argument. The review process leads to a determination of completeness.

When a conclusion or premise has defeaters associated with it, the mitigation or negation of the defeaters increases confidence in correctness of the conclusion (John B. Goodenough, September 2012). Formal review of evidentiary artifacts captured in VeroTrace (such as tests, test results, or analyses that support the argument's premises or reasoning) instills additional confidence in the argument's conclusions.

Evidence of the use of integral development processes for the argument and its evidentiary artifacts is supported within the argument structure in VeroTrace using:

- Premises with linked evidence of defined development and verification processes,
- Documented practices for configuration management, and
- Quality assurance audits to support the confidence-related premises.

Confidence in the argument's conclusions is established through formal reviews of the version-controlled argument elements.

7. What makes an Argument a good Argument?

When an argument is recorded in VeroTrace and the development of an argument-fragment is complete, the elements are deemed ready for review and a review checklist is assigned to that specific version of each artifact. The contents of the checklist and the criteria to be met are configurable. Careful consideration of the checklist criteria is necessary to ensure that an argument is acceptable and to provide high confidence in the validity of the argument (Holloway, 2015-16).

Typically, review of argument-fragments is bottom-up, meaning the leaf or lowest level argument-fragments of the overall argument are reviewed first. The considerations for each higher-level argument-fragment are the same until the top-level conclusion is reached. For example, is the argument-fragment complete? Does it have a valid reasoning with necessary backing? Are its defeaters mitigated or negated? Are its premises valid? A premise can be deemed valid based on additional argument-fragments, or empirical evidence, and/or analysis at the lowest level.

The assurance case has a different set of review criteria than the argument elements. An analysis of the complete assurance case is typically produced as a white paper, analysis, or report. The criteria for review might include validation that the argument is comprehensible and has the expected structure. Is the argument well-formed, meaning is it free from circularity, unsupported conclusions, or informal logical fallacies?

When all the review criteria for the argument elements and the assurance case as a whole are met, then it is reasonable to deem the system to be fit for use.

8. Why use VeroTrace?

Tools exist that capture different aspects of structured arguments or safety cases. Few tools offer the ability to represent so many different argument topologies, but only VeroTrace allows the user to capture not only the assurance case analysis, but also the argument elements, and related evidentiary artifacts.

VeroTrace supports integral processes for:

- Document development and review
- Configuration management, including baseline management
- Change control and corrective action, including problem reporting and impact analysis

During the development phase, VeroTrace enables the user to capture and manage:

- The argument structure.
- The evidence that supports the argument.
- Traceability between the argument elements and the evidentiary artifacts.
- The assurance case analysis.

During the review phase, VeroTrace enables the user to independently review:

- The individual argument elements and argument-fragments.
- The individual evidentiary artifacts.
- The traceability between argument elements and evidence.
- The assurance case analysis.

VeroTrace also provides robust reporting mechanisms that allow the argument structure to be displayed or manipulated in graphical, textual, or hierarchical representations.

References

Holloway, C. M., 2012. Making the Implicit Explicit: Towards An Assurance Case for DO-178C, Hampton, VA: NASA Langley Research Center.

Holloway, C. M., 2015-16. Understanding Assurance Cases Module 3: Evaluation, Hampton, VA: NASA Langley Research Center.

John B. Goodenough, e. a., September 2012. Toward a Theory of Assurance Case Confidence, Pittsburgh, Pennsylvania: Research, Technology, and System Solutions Program, Carnegie Mellon University.

Ministry of Defence, January 1996. JSP 430 - Ship Safety Management System Handbook, s.l.: Ministry of Defence.

RESSAC, REF: LIV-S-026-D6-509 -- 11/12/2018. Recommendations for the use of Assurance Cases for demonstrating and assessing Overarching Properties, s.l.: Re Engineering and Streamlining the Standards for Avionics Certification (RESSAC).

Toulmin, S. E., 1958, updated ed. 2003. The Uses of Argument. Cambridge, UK: Cambridge University Press.

About Verocel

Verocel provides expertise and services for Software Verification in the safety critical software industry covering unmanned systems, airborne, industrial and automotive applications. Our services include the development and review of software plans and standards, software requirement and test development, software structural coverage analyses, life cycle data traceability, and outsource support. Founded in 1999, Verocel is privately held and headquartered in Westford, Massachusetts.