An Introduction to Constructing and Assessing Overarching Properties Related Arguments (OPRAs)

Version 1.0

Kimberly S. Wasson
Joby Aviation

C. Michael Holloway
NASA Langley Research Center

Revision History

Version	Date	Remarks
1.0	2022-01-31	First published version.

Acknowledgments

Mr. Holloway’s work on this document was partially funded through an Interagency Agreement between NASA Langley Research Center and the FAA William J. Hughes Technical Center (NASA IA1-30333 / FAA IA NO. 692M15-19-T-00029) for Aviation Software and Electronics Research, specifically NASA Annex 1 / FAA Task Order 692M15-19-F-00697 Streamlining Assurance Via Overarching Properties.

Dr. Wasson's work on this document was partially funded by Joby Aviation in support of technical and regulatory advancement in assurance and certification approaches for novel aviation capabilities.

We gratefully acknowledge the helpful contributions made to this paper by the following participants in the Overarching Properties Working Group:

- James Chelini
- Cyrille Comar
- Zamira Daw
- Mallory S. Graydon
- Robert L. Green
- Tomasz Iwaszkiewicz
- Barbara Lingberg (retired)
- Srini Mandalapu
- Kevin K. Meier
- Bernie Newman
- George Romanski
- William Schnepp
- Mike Vukas

We also acknowledge the participation of the following additional people in the Overarching Properties Working Group between 2019-2021: Brian N. Allen, Clay Barber, Scott Beecher , Steve Beland, Liz Brandli, Duncan Brown, Christophe Cucuron, Hervé Delseny, Branimir Dulic, Andrew Elliott, Tom Ferrell, Louise Gregor, Brendan Hall, Todd Kilbourne, Emanuel Ledinot, Seth Mason, Thuan Nguyen, Brenda Ocker, Gordon Putsche, Dave Redman, Tammy Reeve, Manny Rios, Benedito Sakugawa, Richard Spencer, John Strasburger, Dean Thompson, Don Ward, Scott Weiss.

Table of Contents

Executive Summary

This document introduces construction and assessment of arguments in relation to the Overarching Properties. The presentation is organized and summarized as follows.

Introduction

The Overarching Properties are proposed as an organizing principle for the complex set of assurance rationale and substantiation to be accounted for in the development and fielding of a novel complex system or part thereof. They characterize at the highest level what must be established about a system to render it eligible for approval. Structured argument is an approach to the explicit statement of rationale for their substantiation. Arguments must be constructed, and assessed, to allow a determination of possession of the Overarching Properties. This document introduces the fundamentals of construction and assessment for arguments that conclude possession of the Overarching Properties.

Overarching Properties Related Arguments (OPRAs) are demonstrated here by narrated example. The examples build on each other, and highlight numerous considerations. A recurring theme throughout the demonstration is that a structured argument documents rationale to enable negotiation toward agreement between applicable parties. That is, structured argument catalyzes the development of shared understanding and provides decision support.

In scoping and conducting this demonstration, we make some important boundaries explicit:

1. A hypothesized reference system is chosen for utility to the argument demonstration objective. This work is about the argument demonstration and not about the subject system.
2. Some messaging in the assurance research community confounds notions of argument and assurance cases, and is in general self-inconsistent. This work is about structured arguments and not about assurance cases.
3. To do anything at scale, it must first be understood on its own. This work is about core principles of OPRA construction and assessment, not about scaled processes in production environments.

Prerequisites

The current document builds on several prior elements documented in associated work; these foundations are indicated and referenced in Section 2 on prerequisites. In particular, the argument primitives introduced in *A Primer on Argument* [2] are used heavily in this document and reproduced in the main text for convenient access. Further, review of selected additional foundations is provided in Appendix A. The statement and elaboration of the Overarching Properties [1] is summarized there, as are the syntax and semantics of the simple text-based Friendly Argument Notation (FAN) [3], and the iTest method of argument assessment [4].

Construction and Assessment

Every argument has both form and content, and the form and content objectives organize the construction and assessment processes. Each of construction and assessment comprises both a set of mechanics as well as a set of decision considerations, among them what to represent, how to represent it, and how to interpret it. Section 3 on construction and assessment breaks down these mechanics and decision considerations, and demonstrates them via small, narrated examples that build on each other.

For example, the construction demonstration starts with a statement of a top-most conclusion for an OPRA: the system possesses the OPs. It is then acknowledged that in order to substantiate this proposition, we need both to decompose it, and to contextualize it: what do we need to show *in order to* conclude possession, and against what specific set of understandings? The construction demonstration presents the mechanics of documentation of form and content through selections of further decomposition, and poses and responds to questions along the way regarding choices available throughout the process. The assessment demonstration proceeds similarly, using examples pulled from construction, and narrating mechanics and other considerations in determining argument cogency.

Additionally, a longer narrated example is offered in Appendix C, which documents a more detailed assessment of a compound argument comprising several atomic arguments, and traces out the nested steps and decisions in an integrated demonstration of the iTest assessment method.

Process and Practice Considerations

The current document focuses on concepts and principles of argument construction and assessment that are prerequisite to using arguments at scale and/or in production environments. Throughout the presentation, some considerations of process and practice scaling are indicated, though not elaborated, where they arise. These are then collected and characterized in Section 4 in order to set the stage for follow-on work.

Section 4.1 on process infrastructure considers challenges in establishing the enablers to project and information management specific to building and using arguments within production engineering environments, as well as the data and stakeholder interfaces thereby implicated.

Section 4.2 on practitioner maturity considers challenges in training and workforce development, to include reinforcement of core concepts, the undertaking of well-formed pilot projects, and the development of curricula.

These areas and related are excellent candidates for applied investigation and development involving applicants, regulators, researchers, and other stakeholders.

1 Introduction

The Overarching Properties (OPs) were conceived as the distillation and essence of the implicit properties that decades of practice have determined a system must possess in order to be eligible for approval [1]. The mechanisms we have conventionally relied upon to show these properties are being challenged by new applications and development methods. However, the properties themselves are simply an analytic generalization of actual technical and regulatory consensus practice. Given the challenges modern systems present to both the effectiveness and efficiency of conventional assurance methods, we now seek additional ways to demonstrate possession of these properties. One sentiment observed of late in the aviation systems certification community suggests that the Overarching Properties are too high-level to serve the considerable technical, regulatory, and process needs in play and emerging. This is a misconception of what the OPs are, and of how to use them. The OPs are not conceived as a replacement for standards such as DO-178C; rather, they name and characterize the ultimate goals that an assurance demonstration should achieve. *This document introduces the use of the OPs as an organizing principle for the complex set of assurance rationale and substantiation to be accounted for in the development and fielding of a novel complex system or part thereof.*

To adequately provide for any such set of rationale and substantiation, one must convince oneself (as well as each other applicable party) that one has identified and adequately responded to all of the relevant considerations. That is, one must argue this, implicitly or explicitly, to the point of shared belief. This community has a long history of using *implicit* argument, and a more recent history of using *explicit* argument. The trend toward performance-based standards in particular aligns well with the property-orientation of arguments vs. the process-orientation of more prescriptive approaches. As with the OPs themselves, however, there is also misconception in the community regarding the nature and use of argument in documenting and interrogating the assurance rationale for a given system. Increasing uptake of argumentation has driven a chaotic emergence of argument notations, data models, and development environments. While these continue to evolve, there remains a conspicuous lack of focus on the fundamentals of how to construct and assess an argument before considering questions of larger process and scale. If we are to get anywhere in any kind of broadly significant and sustained way with arguing properties of complex modern systems, we must establish a common baseline of fundamentals. *This document presents the fundamentals of argument construction and assessment that will underlie all applications of argument at any scale and regardless of notation and implementation choices*.

Together, then, this document introduces

1. the fundamentals of construction and assessment for arguments that
2. conclude possession of the Overarching Properties.

It is intended that this document provide a common foundational basis for the application of OP-related arguments (OPRAs) in documenting and communicating the system and/or subsystem assurance upon which approval decisions may be negotiated and reached.

1.1 Objectives

This document is part of a series of companion foundation documents establishing the framework and use of the Overarching Properties.

1.1.1 Previous Documents

The series comprises ongoing contributions of the Overarching Properties Working Group (OPWG), together with additional supports elaborated in parallel. The series thus far consists of the following documents:

- Document 1: *Understanding the Overarching Properties*, introduces the properties, their origins, definitions, and relevance [1];
- Document 2: *A Primer on Argument*, establishes an accessible, consistent lexicon for talking about and working with structured arguments [2];
- Document 3: *The Friendly Argument Notation (FAN)*, establishes an accessible, text-based, platform-agnostic notation for writing structured arguments [3];
- Document 4: *A Primer on Argument Assessment*, provides guidelines for a way (but not the only way) to assess arguments [4].

The current document is fifth in the series, and its objective is to take the foundations established by the prior four, exercise them through the introductory construction and assessment of arguments relating to the Overarching Properties, and provide narrated demonstrations accessible to a broad audience of cross-functional stakeholders.

More information on prerequisites to the current document can be found in Section 2 and Appendix A. Directions for follow-on work are identified at various points throughout the document and collected in Section 4.

1.1.2 Demonstrating Construction and Assessment

While the earlier foundation documents establish concepts, notation, and a generic argument assessment process, this document focuses on beginning application. Specifically, this document introduces the form and content principles that characterize cogent arguments, how to construct OP-related arguments respecting these principles, and how to assess OP-related arguments with regard to them.

We demonstrate these activities by constructing argument examples pertaining to a hypothesized subsystem and its possession of the Overarching Properties. A number of argument constructions are presented, with guidance and additional notes narrated. Some of these arguments are then considered again from an assessment perspective, with accompanying narration. Observations reinforce the role of argument as decision support in assurance determinations: a structured argument documents rationale to enable negotiation toward agreement between applicable parties.

The presentation is directed at cross-functional stakeholders new to OPs and/or to structured argument. Our objective is to support broad familiarization with argument-based substantiation of OPs and thereby to increase its potential value as a source of assurance within the modern aviation certification landscape. In particular, OPRAs offer a plausible means of compliance to address gaps and inefficiencies in current standards and regulations with respect to many novel system features and development methods. To get there, we need to build a reinforcing loop between a community of practice and a body of knowledge.

The approach taken here is to begin from first principles: we believe the community will benefit from development of a strong basis in fundamentals, within which diverse stakeholders can achieve a common level of competence enabling their productive interaction within this framework. That basis then provides the prerequisites necessary to enable informed follow-on discussions about scaling, integration, and process concerns connected to system development and certification.

1.2 Scope

This document introduces the construction and assessment of explicit structured arguments about the Overarching Properties in association with a hypothetical subsystem. The focus is on introduction of mechanics and presentation of examples; the examples exercise the argument primitives and precepts as defined in the Primer [2] and cast them into an accessible and utilitarian notation [3].

This document is *not* about the features or merits of the hypothesized subsystem. The reader might observe that there are directions of thought available, deriving from the argument presentations, that veer toward the system and engineering data referenced or implied. These are detours. The scope of consideration here is limited to the representation of OP-oriented rationales *about* these systems, and to arguments as vehicles for that representation. We have here neither sufficient data, motivation, nor standing to make the detour evaluations. We are rather demonstrating a decision-support approach to advance the negotiation and agreement objectives among the responsible stakeholders.

This document is also *not* about assurance cases. Throughout this document, we intentionally avoid the use of the terms *assurance case* or *safety case*. In addition to being inconsistently defined across various user populations, the associated concepts generally refer to more complex packages of entities than what we will talk about here. Rather, we make a general distinction between an *argument*, which supports a conclusion via reasoning from premises in an effort to convince another party to believe something, and an *assurance case*, which collects some situationally-specified set of entities that might include artifacts, metadata, textual components, arguments (structured or otherwise, and explicit or otherwise), as well as other possible elements, into a package, usually for an approval purpose. The current document focuses on the former, with intent to baseline (and in some cases *re*baseline) a shared set of argument fundamentals for a broad stakeholder population. Armed with argument competence, we can as a community reconceive structured argument as the nucleus, the essential core of a more disciplined notion of an assurance case. Accordingly, we can then think critically and strategically about its integration into larger entities and processes.

2 Prerequisites

To understand this document fully, a reader needs to understand the Overarching Properties, argument terminology and precepts, the Friendly Argument Notation (FAN), and argument assessment, as explained in their foundational documents [1, 2, 3, 4]. To assist readers who still wish to read this document first, and to provide otherwise convenient reference, we briefly summarize the bare essentials of the information from the prerequisite documents in Appendix A. Appendix A.1 provides essential information about the Overarching Properties, Appendix A.2 summarizes the relevant argument terminology, Appendix A.3 describes FAN, and Appendix A.4 summarizes an approach to argument assessment.

To further assist those readers, and anyone else who may benefit from a refresher about terminology, here are some of the terms from the *Primer on Argument* that will appear often in the text, where they will be denoted from now on by SMALL CAPS.

- An ARGUMENT is an attempt to convince others to BELIEVE a CONCLUSION through REASONING and one or more PREMISES.
- The CONCLUSION is the statement you want your audience to BELIEVE**.**
- A PREMISE is a statement you think your audience BELIEVES.
- Your REASONING states why you think the PREMISES should cause your audience to BELIEVE your CONCLUSION**.**
- To BELIEVE is to accept as true.
- A BINDING is an association between a term used in an ARGUMENT and the real-world information to which that term refers.

- A DEFEATER is a statement that may cause your audience to *not* BELIEVE your CONCLUSION.
- An ATOMIC ARGUMENT consists of a single CONCLUSION together with its immediate REASONING, PREMISES, BINDINGS (if present), and DEFEATERS (if present).
- A COMPOUND ARGUMENT is an ARGUMENT consisting of more than one ATOMIC ARGUMENT**.**
- An ARGUMENT is called COGENT if it rationally justifies BELIEVING its CONCLUSION to the required standard of confidence.

If any of the above definitions are unclear, or if at any point while reading further in this document you come across a foundational term, concept, or principle you do not sufficiently understand, we recommend you consult the appropriate foundation documents (or, if you are pressed for time, the relevant Appendix).

3 Construction and Assessment of OPRAs

In this section, we introduce and exercise the construction and assessment of ARGUMENTS concluding possession of the Overarching Properties.

We first consider *form* and *content*, the most basic principles of assessing any ARGUMENT that has been presented, as well as those that guide efforts to construct ARGUMENTS for presentation. Using these principles together with the foundations, we then construct several example ARGUMENTS relating to the Overarching Properties, narrating a number of development strategies, choices, and implications. Finally, we demonstrate assessment of some of these example ARGUMENTS, narrating further strategies and considerations of interest.

The example ARGUMENTS here concern a reference system hypothesized in enough detail to allow the demonstration of construction and assessment. The reader is reminded to keep the demonstration objectives top of mind when engaging with the ARGUMENTS herein, vs. the engineering merits or issues of the reference system as described. ARGUMENTS very often bring clarity to system concerns that must be negotiated among applicable stakeholders; indeed, this is central to their value. However, our focus here is on accessing that clarity, and not yet on its subsequent uses in decision support and otherwise. Similarly, we do not here consider questions of scale or industrial development process; we focus first strictly on the fundamentals that must precede such considerations.

3.1 Basic Principles

Both the construction and assessment of OPRAs rely on an inherently common set of principles. This is no surprise; when we assess something, we are investigating conformance to some expectation, and when we construct it, we are constructing toward approval by our assessing audience, with respect to that same expectation. The ARGUMENT is the vehicle for transmission of an understanding, and the objective is for the stakeholding parties to reach agreement on that understanding. We focus here on the vehicle--the ARGUMENT--that supports the subsequent negotiation toward agreement.

The ARGUMENT as a vehicle has form and content. We both assess and construct ARGUMENTS with regard to their form and content. In a well-formed and COGENT ARGUMENT, the form and the content behave in certain ways. These are the expectations that both frame an assessment, and toward which we aim during construction. We overview these basic principles below.

3.1.1 Principles as Seen through Assessment

An ARGUMENT does its job by presenting particular content in a particular form. Assessment is an evaluation of the form and content with respect to the situational need. To assess an ARGUMENT, we look for particular properties of the form that enable us to understand the roles of the content contained therein, and also look for particular properties of the content as presented in those roles in order to determine

COGENCY. The approach developed in *A Primer on Argument Assessment* [4] and summarized in A.4 focuses on using questions to guide the assessment of whether the form of an ARGUMENT is proper and whether the content is sufficient to justify BELIEVING the CONCLUSION. In particular, the main questions are four in number:

- Is the Syntax (*a.k.a.* form) proper?
- Are the PREMISES acceptable?
- Is the REASONING acceptable?
- Is BELIEVING the CONCLUSION justified?[1]

These questions break out further into supporting interrogations of the argument in question, enabling a systematic and repeatable process.[2]

3.1.2 Principles as Seen through Construction

When we *construct* an ARGUMENT, then, we consider the content we want to present, and we place it in the appropriate form to support assessment by our intended audience. We think through the entities the ARGUMENT is to be about, the CONCLUSIONS we would like our audience to draw about these entities, and the PREMISES and REASONING available to help us support these CONCLUSIONS. We associate parts of our content to the ARGUMENT primitives, organize and relate them into well-formed structures, and add and elaborate primitives and structural relationships to the point where we have documented what we need to. We consider, while we do this, how our audience will engage with the ARGUMENT, and attend accordingly to the properties of the form and content that will best convey understanding of the target rationale.

These principles apply to all structured ARGUMENTS, whether related to the Overarching Properties or not. We abide by and elaborate them as we narrate examples of construction and assessment of OPRAs below.

3.2 Reference System

To enable the ARGUMENT demonstrations, we hypothesize here a reference system. Our reference system consists of an aircraft configuration that integrates subsystems to provide capabilities such as collision avoidance. We will focus on the application of OPRAs to organize and present rationale for the assurance of a capability that is challenging to assure using conventional means of compliance.[3]

In this case, we consider a small aircraft under partially autonomous flight control. Configurations including many unmanned aircraft systems (UAS) and electric vertical takeoff and landing systems (eVTOL) intended for a variety of applications share this feature. For purposes of illustration, we choose a UAS intended for operation at low-to-medium altitudes, providing humanitarian and/or service applications such as pipeline inspection, fire surveillance, or search and rescue.

The concept of operations (ConOps) for such a system places it in particular airspaces and with sufficient mass to indicate that the hazard of mid-air collision must be adequately mitigated. To support conflict and collision avoidance capabilities, the system includes subsystems that provide collision hazard identification

[1] For mnemonic purposes, the 4th question is worded slightly differently from what is given here; see section 3.4.1 for further information. Readers steeped in mathematical approaches to argument might prefer yet another wording of this question: Are the PREMISES and REASONING sufficient to compel BELIEVING the CONCLUSION? Go for it if you like.

[2] In addition, further interrogative detail makes clear why a step like the fourth is needed, if the first three are answered in the affirmative. As it turns out, belief sufficient for one purpose might not be sufficient for another. "COGENCY depends on how much confidence is needed and whether the ARGUMENT engenders at least that much confidence in the truth of its CONCLUSION." [4]

[3] The reader should keep in mind that the assurance challenge engaged in this document is an example, but not the only example, of challenges that can benefit from this approach.

and resolution, including maneuver determination. We will focus for current purposes on a Maneuver Determination Subsystem (MDSS).

As an architectural subsystem, it comprises some here-unspecified number of hardware and software items, and provides the function allocated to it by the aircraft system (or some intermediate system layer). The allocation comes with certain requirements, and in this case the MDSS implements these requirements via machine-learning-supported algorithms and data, in contrast to a more historically common solution such as a lookup table.

We want to establish and demonstrate requisite assurance in the behavior of the MDSS, but since it is implemented using machine learning, certain conventional assurance strategies such as requirements-based testing and structural coverage analysis are less meaningful and/or inapplicable [11]. Absent recourse to these strategies, we will here consider alternatively how we might argue that the subsystem possesses the Overarching Properties.

Though our reference system necessarily implies particular technical and engineering concerns, recall that our focus here is on making such concerns available for ARGUMENT demonstration purposes; resolution of such concerns is a separate problem out of scope for this document. Indeed, negotiation regarding the technical merits of any system assurance rationale is owned by the stakeholders; the structured ARGUMENT simply documents the rationale as a scaffold for decision support.

Similarly, though our reference system necessarily implies a development process and a certification authority, we distinguish between the problems of demonstrating OPRA construction and assessment, and the problems relating to broader issues of application in a system development and regulatory context. Process considerations and related concerns are revisited in Section 4 and are expected to be the subject of follow-on work.

3.3 Constructing an OPRA

This section introduces the construction of OP-related ARGUMENTS, using the reference system presented in Section 3.2 for illustration, and consistent with the OP and ARGUMENT foundations reviewed in Section 2 and its references.

We first describe how to state and document ARGUMENT CONCLUSIONS that we would like to substantiate. We then describe how to elaborate necessary and sufficient elements of form and content to document associated ATOMIC, and then COMPOUND ARGUMENTS.

3.3.1 Concluding Properties

We would like to argue that the Maneuver Determination Subsystem (MDSS) possesses the Overarching Properties. This constitutes the ultimate objective of our ARGUMENT: the CONCLUSION we want our audience to reach. In accordance with the purpose and meaning of the OPs [1], within a framework of OPs substantiation as a means of compliance, if we could argue this to the point of justified belief on the part of our audience, then the subsystem would be eligible for approval in support of certification of the containing system.

There are indeed three separate Overarching Properties to argue, but let’s start from the top.

3.3.1.1 Stating Conclusions

Recall from Section 2 that a CONCLUSION is a statement you want your audience to BELIEVE. It is therefore an assertion until substantiated, and we state it as a proposition. At its most generic, a CONCLUSION asserts that some entity E possesses some property P, for example, “E is a P,” “E has a P,” “E respects constraint

P," or similar. Using FAN in accordance with Appendix A.3 as our minimalist working notation, we state our ultimate CONCLUSION as follows:

```
MDSS possesses the Overarching Properties
```

In this proposition, `MDSS` is the entity, `possesses` is the asserted relationship, and `the Overarching Properties` is the property.[4]

Since we like to think ahead (sometimes to our detriment, but we'll allow it here), we can practice our CONCLUSION-stating skills and state the three CONCLUSIONS for the individual Overarching Properties that we know we will eventually need to address independently:

```
MDSS possesses Intent
MDSS possesses Correctness
MDSS possesses Innocuity
```

We have stated these compactly here; for example, we could have said:

```
The MDSS possesses the Property of Intent
```

In other words, we have choices, and most are to be made in accordance with objectives like consistency and pragmatic sufficiency. In general, the goal is to communicate what the audience needs to know, in a consistent and accessible way.

3.3.1.2 Constraining Interpretations

These propositions are the roots of our ARGUMENTS. As expressions, they define relationships among entities and properties in the world. To enable an audience to interpret them, we need to associate the variables in the expressions to the particular things in the world we mean by them, and thereby enable access to this information. To do this, we construct BINDINGS. Recall from Section 2 that a BINDING is an association between a term used in an ARGUMENT and the real-world information to which that term refers.

In deciding which BINDINGS we need and what to put in them, we can ask ourselves the following question: what real-world information does our intended audience need in order to understand the single-line expression of this CONCLUSION? For our ultimate CONCLUSION, sometimes known as a root or a top-level goal, we need to know exactly what an `MDSS` refers to, and exactly what is meant by the `Overarching Properties`. Using BINDINGs and continuing to cast in FAN, we can associate these variables to values in the real world as follows:

```
<MDSS> possesses the <Overarching Properties>
```

[4] The overloading of the term "property" here (in its generic logical meaning and as part of the "Overarching Properties" identifier) is not the only overloading with which we will contend. These collisions will be called out and clarified as they arise. In this case, use of lowercase "p" will indicate the generic logical entity, and use of uppercase "P" will indicate an Overarching Property.

<MDSS>: Maneuver determination subsystem as defined by specified development artifacts (which must eventually be named)

<Overarching Properties>: properties as defined in [1]

In accordance with FAN, we set off the variables we will bind by changing their format; here we have chosen angle brackets. Other choices are possible, consistency is critical.

Then we make the association explicit. Thus, when we say here the MDSS, we mean the subsystem circumscribed by some specified development artifacts (that will eventually need to be named in a mature ARGUMENT).[5] Likewise, when we say Overarching Properties, we mean the properties as defined in the referenced document. All such referenced artifacts and documents should be made accessible to ARGUMENT stakeholders. Considerations for how to do this are beyond scope here, but any mechanism that enables this accessibility is generally an option.[6]

In addition to development artifacts and publications, other real-world entities commonly referenced through BINDINGs include definitions (sourced if available or made explicit if new), and elaborations that add contextual information of use or interest without cluttering the ARGUMENT logic.

In general, choices exist as to whether and how to distinguish content via BINDINGS and how much information to put in them; decisions should derive from the importance of the distinction and the reference to the audience's understanding of the ARGUMENT. Once made, decisions can then be implemented in accordance with various presentation needs and options.

For example, in contrast to those terms for which we chose to provide explicit BINDINGS, we expect possesses to be interpreted in its common meaning by the target audience, and so we do not bind it further. That is, we see no further distinction necessary in order to achieve pragmatic sufficiency; this is a useful guideline to support drafting choices.

We add BINDINGs for the CONCLUSIONS about individual OPs in the same way we did for other variables above:

<MDSS> possesses <Intent>

<Intent>: The defined intended behavior is correct and complete with respect to the desired behavior [1]

<MDSS> possesses <Correctness>

<Correctness>: The implementation is correct with respect to its defined intended behavior, under foreseeable operating conditions [1]

[5] Early in a project, this means something like a concept of operations and associated early definition and specification artifacts; these delimit the system about which we're making assertions. As development proceeds, the system comes to be represented by more, and more mature artifacts, many of which will have roles in supporting propositions. Throughout, we create BINDINGS to any and all system development data to which a reviewer will need access in order to evaluate the propositions at hand. In this case the MDSS is the subsystem defined by particular artifacts at the scope of the current proposition, and in making that (or any such) association, we are also then obliged to convince ourselves of the applicability and quality of the bound reference as well as make it accessible to our audience.

[6] Options abound for presenting ARGUMENTS and supporting the mechanics of various kinds of conceptual cross-references they require. Notation, data organization, tool support, and related choices fall under process considerations, introduced later in Section 4 and available for expansion in follow-on work.

```
<MDSS> possesses <Innocuity>

<Innocuity>: Any part of the implementation that is not required
by the defined intended behavior has no unacceptable impact [1]
```

Note here that while we set off MDSS with angle brackets, we did not duplicate its BINDING. We could have repeated it if we decided it would better support audience understanding. Or, we can state in frontmatter when presenting an ARGUMENT that though BINDINGS after the first introduction are not repeated, any entity set off as bound does indeed have a BINDING that can be found in an assigned location. We could even leave *all* BINDINGS to a separate location, inclusive of first introduction of bound terms. As usual, the format is not prescriptive. The communication objectives together with situational resources and constraints drive all such decisions.[7]

For this document, we have chosen to state BINDINGS explicitly at first introduction of each bound term, and to collect all BINDINGS to a single location for reference. Appendix B provides a list of all BINDINGS used in the construction demonstration of this document, serving as reference both for the bound terms herein, and as an example of how BINDINGS might be collected to a single location.

Next, we think about how to support the CONCLUSIONS that have now been bound.

3.3.2 Elaborating Support

A CONCLUSION on its own is not an ARGUMENT. To convince an audience to BELIEVE a CONCLUSION, we need to point to other information we think they already BELIEVE, and show how the CONCLUSION follows from that information. In other words, we need to state the PREMISES from which the CONCLUSION follows, and the REASONING that allows this inference. We need to *decompose* the rationale represented by the ATOMIC ARGUMENT. In this section, we begin documenting the REASONING and PREMISES in support of our above CONCLUSIONS.

3.3.2.1 Elaborating ATOMIC ARGUMENTs

Recall that an ATOMIC ARGUMENT consists of a single CONCLUSION together with its immediate REASONING, PREMISES, BINDINGS (if present), and DEFEATERS (if present). To constitute an ARGUMENT, it is *necessary* to have a CONCLUSION, REASONING, and at least one PREMISE. An ARGUMENT for any given CONCLUSION might further require any or all of additional PREMISES, BINDINGS, and DEFEATERS in order to document what is needed in a pragmatically *sufficient* way.

Using the minimalist infrastructure of FAN syntax, we will now elaborate the ATOMIC ARGUMENTS that conclude possession of the individual OPs. Let's start with Intent. We take the bound CONCLUSION and define its PREMISES and the REASONING that connect them, as follows:

```
Believing
      <MDSS> possesses <Intent>
is justified by applying
      The definition of <Intent>
```

[7] This is not to say presentation should be a free-for all; that is, having numerous options is different from using them inconsistently or without rationale. Supported conventions are desirable *after* a stakeholder population understands its needs well and establishes a coordinated practice. See also Section 4.

```
to these premises
     <MDSS> <DIB> is correct with respect to its <DeB>
     <MDSS> <DIB> is complete with respect to its <DeB>
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by
     specified development artifacts (which must eventually be
     named)
     <Intent>: The defined intended behavior is correct and
     complete with respect to the desired behavior [1]
     <DIB>: defined intended behavior [1]
     <DeB>: desired behavior [1]
```

A CONCLUSION together with PREMISES and connecting REASONING constitutes an ATOMIC ARGUMENT. We don't know yet if this one is worthy of belief, but it at least includes the minimally required structural components. (We'll get into optional components later.)

Here are some further things to note in relation to this ARGUMENT:

1. For illustration, this time we explicated all BINDINGS vs. relying on prior presentation. Any one of these BINDINGS is likely to have come up earlier in a larger undertaking, but we're not assuming them for this particular illustration, because we want to remind you of these considerations as we introduce this process. So, for this example, we listed them all in place.
2. We leveraged the very definition of Intent to help us figure out what we need to substantiate, and thereby help us to explicate our REASONING. Words *are* associations of forms to meanings. If we want to convince someone that a system possesses Intent, we *must* understand and use and show that this system abides by the entailments of what Intent means. We turn these entailments into the ARGUMENT PREMISES.
3. A corollary to the above decomposition strategy is that difficulty in decomposing a CONCLUSION might be eased by revisiting its BINDINGS. Writing COGENT ARGUMENTS is hard. You might find that establishing or clarifying an association reveals a meaningful decomposition path.
4. Finally, since the definition of Intent is stable, the structure of this ATOMIC ARGUMENT is potentially reusable. The subject system (and its BINDING) would change, but the decomposition of Intent would not. Likewise for the other OPs, and other concepts that have stable meanings within an applicable body of knowledge.[8]

We now elaborate the ATOMIC ARGUMENT for Correctness in the same way.

```
Believing
     <MDSS> possesses <Correctness>
is justified by applying
     The definition of <Correctness>
to these premises
```

[8] Reusability is of course attractive, but not without significant considerations in application. While beyond the scope of the current work, such considerations are previewed in Section 4.

<MDSS> <implementation> is correct with respect to its <DIB>

<Foreseeable operating conditions> are accounted for in the <DIB>

with these bindings

<MDSS>: Maneuver determination subsystem as defined by specified development artifacts (which must eventually be named)

<Correctness>: The <implementation> is correct with respect to its defined intended behavior, under <foreseeable operating conditions> [1]

<implementation>: item or combination of inter-related items for which acceptance or approval is being sought [1]

<DIB>: defined intended behavior [1]

<foreseeable operating conditions>: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions [1]

As with the earlier example for Intent, this bound CONCLUSION for Correctness has now been elaborated with REASONING and PREMISES, and thereby constitutes an ATOMIC ARGUMENT. While its further assessment is pending, it is in a form that at least renders it presentable for such, insofar as the precept of LOCALITY is concerned [2]. That is, we've not further decomposed the PREMISES, but assuming their BELIEVABILITY, this ATOMIC ARGUMENT can be assessed as is.

Here are a few additional notes about this ARGUMENT:

1. The root "correct-" is overloaded in the lexicon of the Overarching Properties.[9] This is known to many who contributed to the original framing and to subsequent related development. Within this group, terms using this root have been distinguished enough implicitly that further actions were not taken. As more people engage with this work, it seems prudent to make explicit certain uses, for the same reason we introduced in Section 3.3.1.2, that is, to support common interpretation among the full target audience. In a later example, we will bind another of the uses.
2. We used the strategy introduced above of examining the BINDINGS to help guide the decomposition, and the two stated PREMISES here derive from the definition of Correctness. That said, we stated these PREMISES to reflect an interpretation that "foreseeable operating conditions" would be accounted for in the DIB, as the DIB should already be constrained to the intended environment via a proper development process.[10] In this interpretation, stating "foreseeable operating conditions" in the definition of Correctness is redundant if the DIB if includes them. To be complete with respect to the Correctness definition, we still explicitly include this PREMISE, but state it instead as a check on the DIB.[11] Importantly, neither the interpretation used here, nor its casting into ARGUMENT, are the only available interpretation and casting choices. Alternate choices simply require respective elaborations and substantiations.

[9] For example, in addition to being part of the name of the Correctness property, it is in the definitions of both Intent and Correctness.

[10] For example, a complete DIB should include all intended safety behavior, which can only be fully identified with respect to a defined environment against which hazards and safety requirements are determined.

[11] Alternatively, we could have stated a DEFEATER of the form "Unless the DIB does not account for foreseeable operating conditions." We leave it as an exercise for the reader to consider circumstances that would motivate one presentation over the other. DEFEATERS are defined in Appendix A and discussed further in [2, 3, 4].

We will next address the Innocuity property. We invite the reader to draft an ATOMIC ARGUMENT for this property as an experiment, using the strategies introduced above, prior to reading the one provided. Upon returning, compare your draft ARGUMENT to the one below.[12]

```
Believing
     <MDSS> possesses <Innocuity>
is justified by applying
     The definition of <Innocuity>
to these premises
     Any part of <MDSS> <implementation> not required by <DIB> is identified
     Impact of <implementation> identified as not required is identified
     Impact of <implementation> identified as not required is acceptable
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by specified development artifacts (which must eventually be named)
     <Innocuity>: Any part of the implementation that is not required by the defined intended behavior has no unacceptable impact [1]
     <DIB>: defined intended behavior [1]
     <implementation>: item or combination of inter-related items for which acceptance or approval is being sought [1]
```

The above constitutes an ATOMIC ARGUMENT for Innocuity of the MDSS, presentable for assessment in accordance with LOCALITY [2].

Some further notes regarding this ARGUMENT follow:

1. This ARGUMENT is decomposed to three PREMISES via the definition of Innocuity. This perhaps seems like a lot; Innocuity is a single word and yet we've mined three separate expectations out of it. The definition, though, embeds some assumptions and relations that we have made explicit in order to force their satisfaction. Specifically, in order to evaluate the acceptability of the impact (third PREMISE), we must know what the impact *is* (second PREMISE). And in order to determine

[12] Your ARGUMENT might be similar, or it might be different in any of several ways, which might or might not detract from its potential COGENCY. If your ARGUMENT looks substantially different, evaluate the differences, their sources, and effects on the message of the ARGUMENT. Those readers interested in further practice can outline support for the well-formedness of their ARGUMENTS, or can revise them in accordance with deficiencies discovered upon review. For detailed and systematic attention to review of ARGUMENTS, see *A Primer on Argument Assessment* [4].

what the impact *is*, we have to have correctly partitioned the implementation to that required by the DIB vs. that outside of it (first PREMISE).[13] (Note: other decompositions are also possible.)[14]

2. This ARGUMENT also illustrates another available *strategy* to try when searching for an effective decomposition. Specifically, we backed out the three PREMISES by thinking through a chain of process dependencies, e.g., to do this, we need those, and to figure out those, we need these. This strategy can be quite useful, as many of us are wired to think in processes, workflows, flowcharts, etc., and such exercises can reveal critical pieces of rationale. However, we must also recall that ARGUMENTS are declarative; they propose properties subject to belief, and lay out the support for these propositions. They don't describe processes or various types of information or activity flows. But we can sometimes lean productively on process instincts as long as we learn to convert our mental models of these processes to the propositions that drive them. For example, we might habitually think in terms of *how* we identify and evaluate system behavior outside of a specification, but in doing that, what we're ultimately trying to determine is *whether* any such behavior *has some property*. To argue, we focus on the property as opposed to the process. This set of PREMISES can be seen from one angle via a familiar process view, but is converted and cast as a set of property-oriented declarative statements.
3. The reader might further notice that reuse of phrases sometimes occurs in ARGUMENT construction as a by-product of the content being worked with, and that this reuse can become cluttering to the presentation. In this example, variations of the phrase "Any part of the implementation that is not required by the defined intended behavior" occur several times. This kind of recurrence of longer strings signals an option to create a new BINDING to be used like a macro (for example, `<extra-DIB implementation>`). With some care, we could replace variations of the longer string in all of its occurrences with a single bound term and thereby achieve a simpler presentation. In this case we did not, because we wanted to direct attention to the original presentation and its properties. The reader is invited to experiment with this option to get a sense of the care to be taken in phrasing and arranging in order to preserve the intended relationships within the ARGUMENT.

These first several examples have illustrated the construction of ATOMIC ARGUMENTS concluding the individual Overarching Properties. ATOMIC ARGUMENTS for plenty of other CONCLUSIONS will also be needed, and we'll construct more as we go. But first we need to learn about how ATOMIC ARGUMENTS work together. Let's turn our attention now to COMPOUND ARGUMENTS.

3.3.2.2 Integrating into COMPOUND ARGUMENTS

An ATOMIC ARGUMENT consists of a single CONCLUSION together with its REASONING and PREMISES, but a single ATOMIC ARGUMENT will be insufficient to any of the applications we have in mind. A COMPOUND

[13] Some readers will notice that we could also have organized these PREMISES hierarchically (or into dimensions!) rather than in a flat list. For example, we might have stated here only the third PREMISE (`Impact of <implementation> identified as not required is acceptable`), which, if BELIEVABLE, might be sufficient. However, for it to be BELIEVABLE, it must itself be decomposed and supported. We would thus need a further ATOMIC ARGUMENT rooted at this PREMISE as its CONCLUSION. The reader is invited to continue this thought experiment, to consider how these alternatives might be presented in structured ARGUMENT, and to consider the reasons one might or might not choose various presentations in given scenarios.

[14] Some readers might additionally note that there is in fact a theoretical possibility of demonstrating innocuity *without* strictly identifying and separating out the impact of implementation outside of the DIB. An approach in which the implementation as a whole can be demonstrated formally correct with respect to complete and formally specified requirements addresses the impact of extraneous implementation by definition, as *all* implementation is in this case declared acceptable. This strategy was proposed in earlier work by the European Re-engineering and Streamlining Standards for Avionics Certification (RESSAC) project. As will become a refrain, practitioners have many choices in this process, and the choice of demonstration rationale is a significant one. To use the alternate rationale postulated here, one would need the implicated formal methods support, and its availability or lack thereof would provide input to the decision.

ARGUMENT, on the other hand, is an ARGUMENT consisting of more than one ATOMIC ARGUMENT, related in some way. Continuing with the ARGUMENTS from above, we can observe the following.

Elaboration of the ATOMIC ARGUMENTS in Section 3.3.2.1 generated a number of PREMISES (seven, in this case, for the three examples above). *These* PREMISES *are themselves propositions*. If we expect that our audience already BELIEVES these PREMISES, then we are done with construction; we have documented the scaffold between what we think our audience BELIEVES, and a CONCLUSION that follows from it. If, on the other hand, we have relied on PREMISES that need further support, we must then construct (or otherwise acquire) additional ATOMIC ARGUMENTS to conclude these assertions. We thus provision for one or more new ATOMIC ARGUMENT(S) upon which another depends for support.

In accordance with the precept of LOCALITY [2], we focus for such elaboration on a new CONCLUSION at hand and the REASONING and PREMISES required to support it. Here, we elaborate a new ATOMIC ARGUMENT to support the Correctness ARGUMENT, by arguing one of its PREMISES as a new CONCLUSION.

```
Believing
     <MDSS> <implementation> is correct with respect to its <DIB>
is justified by applying
     The definition of <Correct-wrt-DIB>
to these premises
     <MDSS> <implementation> meets satisfaction criteria
     The criteria are specified and acceptable
     The methods are specified and acceptable
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by
     specified development artifacts (which must eventually be
     named)
     <implementation>: item or combination of inter-related items
     for which acceptance or approval is being sought [1]
     <DIB>: defined intended behavior [1]
     <Correct-wrt-DIB>: <implementation> is shown through
     specified acceptable methods to meet specified acceptable
     satisfaction criteria (which must both eventually be named)
```

The above new ARGUMENT is still ATOMIC, since it elaborates a single CONCLUSION together with its REASONING and PREMISE(S). When together with the ARGUMENT it supports, the two constitute a COMPOUND ARGUMENT, since the two ATOMIC ARGUMENTS have a relationship (in this case the CONCLUSION of one is a PREMISE to the other).

Here are some features to note about this supporting ATOMIC ARGUMENT:

1. Earlier in this document we noted that the root "correct-" is overloaded within the OPs discourse, and indicated we would bind another of the uses in order to constrain that overload. This ARGUMENT introduces a BINDING for a use that was not previously explicit. Further, BINDING this use solved a decomposition problem for us as described next.

2. To identify an effective decomposition direction, we used the earlier-introduced strategy of re-examining the meaning of something and making it explicit. In this case, the definition of the Correctness property demands that the implementation correspond to the DIB. However, we cannot support a determination of Correctness without further clarity on what this correspondence consists of. So, we distinguish this concept with a new BINDING, `Correct-wrt-DIB`, and break out explicitly in its own definition what must be shown for this property to hold. We now have a basis from which to create meaningful PREMISES to the associated CONCLUSION. Importantly, our choices may be different from yours, or from someone else's, or even from our own under different circumstances. For example, we combined *satisfaction* of the criteria with *acceptability* of the criteria and methods in the same decomposition path. It is possible and can be appropriate to separate ARGUMENT paths about property satisfaction from ARGUMENT paths about the validity of means for showing satisfaction. Though examination of the tradeoffs among such choices is beyond current scope, the reader is invited to brainstorm on means and motivations during early experimentation with fundamentals.

By extension of the support relationship between these two ARGUMENTS, the reader can surmise that such dependencies can allow the construction of networks of ATOMIC ARGUMENTS into COMPOUND ARGUMENTS of arbitrary complexity. While true in principle, it has been our experience that COMPOUND ARGUMENTS have a practical complexity limit at the point where applicable stakeholders can no longer mentally maintain the logical storyline at a level that allows productive engagement and negotiation over the content. Without turning into a different type of artifact, this complexity tops out at tens of ATOMIC ARGUMENTS, or perhaps up to a few hundred, related with care and management into a COMPOUND ARGUMENT. There have certainly been ARGUMENT-type structures produced in the thousands of "nodes," but engagement with them, and productive use of them, becomes a different kind of exercise with a different set of objectives, in addition to the significantly increased development, management, and maintenance burden.[15]

Relating ARGUMENTS together and signposting these relationships for stakeholders can be aided by the use of labels. FAN provides a labeling mechanism to support expression of such dependencies. A FAN label is established by a string in curly braces following a FAN statement; it can then be used elsewhere to stand in for that which it labels. A full accounting of FAN syntax and semantics is available in the respective foundation paper [3]. Below, we repeat a selection of the above COMPOUND ARGUMENT using FAN labels to support documentation and navigation of the dependency relationship.

```
Believing
     <MDSS> possesses <Correctness>
is justified by applying
     The definition of <Correctness>
to these premises
     <MDSS> <implementation> is correct with respect to
     its <DIB>                                        {cwrt}
     <Foreseeable operating conditions> are accounted for in the
     <DIB>
```

[15] It is possible to construct very large and complex arguments in ways that are accessible, useful, and manageable, but the considerations for doing so are beyond the scope of the current document. Section 4 previews process and practice considerations to be addressed when contemplating argument applications at scale.

```
Believing
     {cwrt}
is justified by applying
     The definition of <Correct-wrt-DIB>
to these premises
     <MDSS> <implementation> meets satisfaction criteria
                                                       {msat}
     The criteria are specified and acceptable         {cacc}
     The methods are specified and acceptable          {macc}
```

As with many other choices, this option is available but not mandated, and the decision can take situational needs into account. For example, while use of a label to replace a statement may obscure the semantics of the statement, it can ease ARGUMENT summarization and/or visualization via abstraction of label chains. ARGUMENT visualization is introduced later in Section 3.3.3. Further, labels do not *require* the replacement of text, and so full statements can even be preserved for close review purposes while labels can still be navigated, or extracted for other kinds of views.[16]

Now, back to the ARGUMENT at hand. Since we're not yet confident our audience BELIEVES the new PREMISES either, we need to elaborate those as well. Below, we follow the above three PREMISES through further decomposition. As before, each target PREMISE becomes the CONCLUSION of a new ATOMIC ARGUMENT.

```
Believing
     <MDSS> <implementation> meets satisfaction criteria
                                                       {msat}
is justified by applying
     Qualified inspection
to these premises
     <MDSS verification report> documents satisfaction
     <MDSS verification report> conforms to <MDSS verification
     plan>
with these bindings
     <MDSS verification report>: (the real-world document, which
     must eventually be named)
```

[16] Some readers will identify many possibilities for various levels of automation in ARGUMENT presentation, and indeed, there exist options of various flavors and maturity levels. These are intentionally out of scope for this work. It is strongly advised that stakeholders planning to engage with ARGUMENTS through writing, reviewing, or any of several uses supporting a development program, start small. Work with ARGUMENTS first manually and liberally, ATOMICALLY and in small COMPOUNDS. It is also advised that stakeholders share their early exercises with each other, to present and interpret rationales, to become familiar with these structures of thinking and with the lexicon for describing them, and to establish competence in the small before considering scaling and automation. A tractable and well-bounded pilot project undertaken by a small team as a learning exercise is one way of seeding a new competency within an organization.

```
     <MDSS verification plan>: (the real-world document, which
     must eventually be named)


Believing
     The criteria are specified and acceptable        {cacc}
is justified by applying
     Qualified inspection
to these premises
     <MDSS verification plan> specifies criteria and acceptability
with these bindings
     <MDSS verification plan>: (the real-world document, which
     must eventually be named)


Believing
     The methods are specified and acceptable
     {macc}
is justified by applying
     Qualified inspection
to these premises
     <MDSS verification plan> specifies methods and acceptability
with these bindings
     <MDSS verification plan>: (the real-world document, which
     must eventually be named)
```

Some readers might note that we have chosen in this set of ATOMIC ARGUMENTS to combine criteria specification and acceptability within single CONCLUSIONS, and that we could alternatively have split these to independent CONCLUSIONS. Either can lead to a COGENT ARGUMENT, provided sufficient support is elaborated. Here, the direction would be to reference a verification plan that is defined to address both the specification and the acceptability in question, and is signed off by an empowered authority. Further ATOMIC ARGUMENTS could structure and document this support as outlined. Readers are invited to pursue this as well as alternative directions as an exercise.

Organized as we have done here, the three ATOMIC ARGUMENTS immediately above support CONCLUSIONS that serve as PREMISES to the ARGUMENT that precedes them. All three must be satisfied together for the supported CONCLUSION to hold. This COMPOUND ARGUMENT documents in part a relationship that should be familiar to many readers: to meet a requirement, we must show not only some test or analytic result consistent with satisfaction, but we must also generate confidence that the metric used was appropriate, and that the means of measurement were appropriate. We've taken this particular path down to the level where under normal circumstances, qualified inspection of the named artifact might be sufficient for purposes. For example, DER conformance checking and signoff of plans and test reports is a terminal milestone in a given sub-process. Familiar relationships like this one are good targets of experimentation in learning argument fundamentals.

What we've added throughout this decomposition is orientation to the OPs. We've been working within a Correctness branch of a hypothetical broader tree, and have integrated familiar activities into the framework of substantiating the Overarching Properties via ARGUMENT. The reader is invited to experiment further with familiar relationships that would support and integrate into the branches for Intent and Innocuity.

What we have *not* yet done in the current ARGUMENT path is question the acceptability of the criteria and methods used in a circumstance where conventional means and/or methods of compliance are not sufficient. For example, the certification and verification plans for our reference system can conform with convention to a point, but to verify the behavior of our machine-learning enabled subsystem, we will need to rely on criteria and methods not yet standardized or broadly familiar.

We take this opportunity to remind the reader that the negotiation of technical bases of machine-learning verification is not in scope here.[17] However, how such bases might be represented in order to support that negotiation *is*. To this end, we present next a speculative piece of ARGUMENT concerning a not-yet-mature verification approach. Our intention here is to indicate a direction for ARGUMENT elaboration, using the fundamentals introduced thus far, in combination with domain-specific results that would come out of active research and/or community efforts. That is, an applicant might use ARGUMENT to help themselves to plan, communicate, and decide on verification strategies, through exercises such as the following. If the achieved ARGUMENT is COGENT, it could also contribute to an approval application. This next ARGUMENT organizes the speculative rationale for the choice of a probabilistic verification method in the verification planning for the MDSS.

```
Believing
     Probabilistic assessment method P is <fit for verification
     purpose> to verify performance of <MDSS> collision avoidance
     function
is justified by applying
     the definition of <fit for verification purpose>
to these premises
     P has property X (which must eventually be named)
     P has property Y (which must eventually be named)
with these bindings
     <fit for verification purpose>: demonstrated to have
     properties X and Y (which must eventually be named and would
     derive from current ML research)
```

Since an implementation originating through a machine learning process is resistant to conventional verification methods such as requirements-based testing and structural coverage analysis, other methods for verification of such implementations are in active research and development. We need new ways to be

[17] Indeed, the foundation definition document [1] excludes such considerations via explicit constraints and requisites. Determinations of what counts as an adequate reason to believe a given conclusion, and under which circumstances, are distinct from issues of how to represent such reasoning in an ARGUMENT. However, use of ARGUMENT as a thinking and communication support brings clarity needed to negotiate and refine these considerations. One implication for downstream process considerations is that any production ARGUMENT development undertaking requires support from a spectrum of practitioners beyond dedicated ARGUMENT writers, including from domain and competency experts.

able to demonstrate properties such as requirements satisfaction and absence (or acceptable rates) of unintended behavior for such systems.

Probabilistic approaches, formal methods approaches, and others are in investigation for these purposes. Some formal solutions rest on rationales involving demonstration that specified unsafe states cannot be reached by the implementation, for example, and this is shown through strategies such as theorem-proving based on models of the state space. Some probabilistic methods rest on rationales that model a sufficiently large number of trials of behavior and show that the behavior conforms to specified bounds at some defined rate. These and other methods have strengths and weaknesses, significant among the weaknesses being that thus far the community has few leads to satisfactorily demonstrate absence of unintended behavior.[18] However, working toward shared structural mental models of rationale can allow us to continually refine and focus the pieces in play, the PREMISES that must be substantiated, and what constitutes sufficient substantiation, in a cross-functional and broadly accessible way.

This concludes the set of construction examples provided by the current document. While we expect we have raised many questions, we hope we have also provided some answers, in particular that help interested readers feel prepared to experiment productively with OPRA construction fundamentals.

Before turning to assessment, we will take here the opportunity to address a housekeeping consideration that becomes apparent once the number of ARGUMENTS at hand exceeds a handful.

3.3.3 Visualizing Structure

The reader might have noticed that we have now littered our surroundings with a growing number of ARGUMENT pieces, and things are getting a bit chaotic.

Consider that any non-trivial ARGUMENT will require decomposition. This decomposition will impose some branching, and dependencies will unpack through some number of hierarchical levels. This usually results in some overall number of CONCLUSIONS and relationships that no stakeholder can conceptually manage in active memory. However, with some abstraction, a map of an ARGUMENT can be created that allows a different level of engagement and inquiry.

3.3.3.1 How?

There are, as usual, many ways to do this, and any mechanism that serves the applicable needs is acceptable. Text-based, tabular, and graphical approaches can all be observed in practice, though we strongly advise ignoring tool packages unless and until you determine whether you need them, why, and how you will cope with their sometimes-counterproductive constraints and impositions. Rather, consider from your own manual experiments which initial abstractions might bring good value for effort.

In Figure 1 below, we present a simple graphical dependency diagram agnostic to any particular notation. Here, boxes represent ATOMIC ARGUMENTS named by their CONCLUSIONS, and arrows represent directional dependency. Thus, any CONCLUSION that is not the root is also a PREMISE to the above CONCLUSION. Some of these ATOMIC ARGUMENTS are elaborated and decomposed above, and some are simply provisioned at this point, illustrating one use of such a visualization in construction support.[19]

[18] Architectural mitigation is a common response to this problem, but brings its own challenges and limitations. Ultimately, containment is helpful, but prevention is sought.

[19] We defer here a dedicated treatment of process considerations, but note that options clearly abound to leverage such visualizations for management of the ARGUMENT development and assessment processes. To begin with, we could have used color or other features to differentiate various types of status for nodes in the ARGUMENTS (e.g., a given node is implemented, reviewed, needs attention, etc.). We can also introduce shapes, including changing the shapes of nodes (e.g., to mark terminality), or adding shapes or other markers to signify other information. Nodes and/or text could also be hyperlinked to other entities (which could also be done within a purely text-based representation such

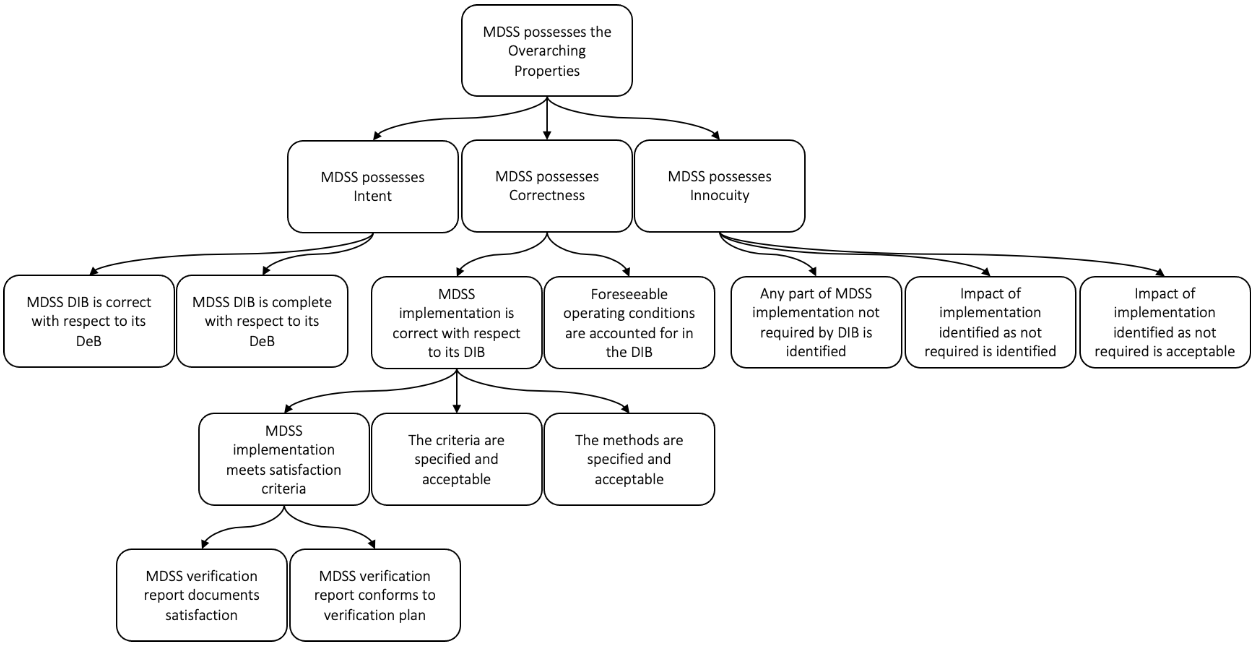

MDSS possesses the Overarching Properties
MDSS possesses Intent
MDSS possesses Correctness
MDSS possesses Innocuity
MDSS DIB is correct with respect to its DeB
MDSS DIB is complete with respect to its DeB
MDSS implementation is correct with respect to its DIB
Foreseeable operating conditions are accounted for in the DIB
Any part of MDSS implementation not required by DIB is identified
Impact of implementation identified as not required is identified
Impact of implementation identified as not required is acceptable
MDSS implementation meets satisfaction criteria
The criteria are specified and acceptable
The methods are specified and acceptable
MDSS verification report documents satisfaction
MDSS verification report conforms to verification plan

Figure 1: Visualizing argument relationships via a dependency diagram

We can characterize this diagram with some basic graph metrics: it has one root, five levels, some branching, no cycles, and sixteen total nodes at present. Some of these metrics tell us little, some more. The single root lets us know this is a single COMPOUND ARGUMENT, and that everything else is there ultimately to support it. The total number of nodes means little, as the ARGUMENT is known to be unfinished.

The branching factor is worth noting. There is no rule about how many PREMISES a CONCLUSION should rely on; the answer is the number that is needed to substantiate the given CONCLUSION at the required level of confidence. That said, we have seen "arguments" in which a single "conclusion" relies on a long flat row of undecomposed "premises" (often pointing straight to "evidence," and with no rationale to be found). That is not an ARGUMENT; it's an uninterrogated graphical checklist, and it is one of the (many) hazards of generating "arguments" without competence in ARGUMENT fundamentals. The ease of doing this faster and at larger scale with tools compounds the problem. Don't do that.

Similarly, note that propositional phrasing of CONCLUSIONS has been preserved for this diagram. This reinforces that this graphic represents a declarative set of relationships as opposed to a procedural one, that is, the ARGUMENT is oriented to properties vs. process.[20] Another hazard of developing arguments without adequate grounding in fundamentals is the production of "arguments" that are more accurately described as flowcharts or process diagrams (similarly compounded by premature use of tools).

In addition to graph structures, tables can also be used effectively to organize and support management of argument data, and can be constructed directly, or via transformation from a graphical structure. We leave it as an exercise for the reader to convert the above graphical dependency diagram into a functionally equivalent table. We further encourage the reader to organize and visualize their own experimental arguments thus far via either or both of these options, and to identify empirically some of the benefits and limitations apparent. This kind of manual manipulation should precede any efforts at automation.

as FAN). Given the breadth of possibility and the logistics of implementation, we also note that it is entirely too easy to overcomplicate an ARGUMENT development undertaking, and to create too much conceptual distance between the stakeholders and the rationale. Start small and simple.

[20] See https://en.wikipedia.org/wiki/Procedural_knowledge for a review of the differences between declarative and procedural knowledge.

3.3.3.2 Why?

The motivations for this kind of abstraction derive from benefits to both construction and assessment, as well as to use of the ARGUMENT as a shared reference during system development.

During assessment, it can provide the entry map for a reviewer, outlining the high-level storyline of the ARGUMENT.[21] Before unpacking detail, the reviewer can make some determinations regarding whether the logical progression appears plausibly convincing, whether there are obvious holes, nonsensical transitions, or irrelevant detours, and where to focus attention during the review.

During construction, a good sense of the big picture supports holistic and structural decisions regarding ARGUMENT factoring and balance, both in coverage and organization of the intended scope, as well as in the level of abstraction at which it is addressed. Keeping track of the larger storyline of the rationale as it grows, and being able to step back to review the converging series of waypoints en route to the ultimate CONCLUSION, enable things like partitioning and prioritization, for example. Upon the afforded prioritization, resources can be directed accordingly. This can impact program decisions such as putting developer support behind one solution vs another when it's determined from the ARGUMENT that CONCLUSIONS depending on the latter will be unsupportable. Abstraction and visualization can further support cross-functional communication and integration across the various competencies involved, offering entry points to detail as needed by circumstances.

Having illustrated the fundamentals of OPRA construction, we turn our attention now to assessment.

3.4 Assessing an OPRA

In this section we apply and expand on the principles and guidelines introduced in the *Primer on Argument Assessment* [4][22], to explain a way (but not the only way) to assess OPRAs. To save the reader the chore of flipping back and forth between the main body and Appendix A.4, this section begins with an even shorter summary than contained in the Appendix. Next comes an enumeration of what makes OPRAs different from ARGUMENTS that are not OPRAs, together with an accounting of the additions to the general assessment guidelines necessitated by these differences. The section concludes with several exercises in OPRA assessment.

3.4.1 Summary of a general ARGUMENT assessment approach

The *Primer on Argument Assessment* [4] sets forth a domain independent, question-based approach for assessing the COGENCY of individual ATOMIC ARGUMENTS, and a procedure called iTest for assessing the COGENCY of COMPOUND ARGUMENTS. The former is nested in the latter in all cases that require assessing more than a solitary ATOMIC ARGUMENT. Because each OPRA will inevitably be COMPOUND, we will summarize the assessment approach in this integrated manner in Figure 2 below (graphically-inclined readers may prefer the pictorial version at the end of Appendix A.4).

[21] Indeed, we could have introduced this diagram earlier in the document, to provide just such an entry map and argument navigation aid. We might have, if our focus were not to begin at the beginning. For current purposes, we worked first with single ATOMIC ARGUMENTS before considering their combination.
[22] Summarized in Appendix A.4.

I. **Isolate** one ATOMIC ARGUMENT

II. **Interrogate** it as an ATOMIC ARGUMENT by asking and answering the SPRY questions.

S. Is the **S**yntax proper?

a. Is there a single CONCLUSION that is stated in the form of a proposition?
b. Is there a statement of REASONING?
c. Is there at least one PREMISE?
d. Is each PREMISE stated in the form of a proposition?
e. If there are DEFEATERS, is each stated in the form of a proposition?
f. Does a BINDING exist for each term or phrase used in the CONCLUSION, REASONING, PREMISES, and (if any) DEFEATERS that does not have a well-known, unambiguous definition?
g. Does a proper BINDING exist for each reference to an external artifact?

P. Are the **P**REMISES acceptable?

a. Is each PREMISE BELIEVABLE? To be BELIEVABLE the PREMISE must fall into one of these categories:
(a) expresses a proposition that is 'universally' accepted as true
(b) expresses a proposition that is accepted as true within the relevant domain
(c) is supported by an ARGUMENT (provisionally presumed to be COGENT)
(d) is supported by external artifacts that are accepted within the domain as being sufficient to establish its truth
(e) will fall into category (c) or (d) at a later stage of ARGUMENT development
(f) is an assumption accepted by all stakeholders and clearly identified as such
b. Is each PREMISE relevant to the CONCLUSION?

R. Is the **R**EASONING acceptable?

a. Is the REASONING relevant?
b. Is the REASONING consistent with current knowledge?

Y. Is saying "**Y**es" to the CONCLUSION justified?

a. Is the required level of confidence known?
b. Does the ARGUMENT engender the required level of confidence?

III. **Iterate** until all ATOMIC ARGUMENTS have been assessed

IIII. **Integrate** the individual assessments by answering these questions:

A. Are all ATOMIC ARGUMENTS assessed as COGENT?

B. Does every path through the COMPOUND ARGUMENT terminate in BELIEVED PREMISES?

Figure 2: iTest

3.4.2 OPRA-unique assessment considerations

The assessment process for ARGUMENTS in general applies equally well for OPRAs, with minor additions as described below.

The only substantiative differences between assessing an OPRA and assessing an ARGUMENT randomly selected off the street stem from the OP Definitions and from the three sections[23] of the OP description that do not directly affect the meaning of the OPs:

- The requisites required for showing possession of the Overarching Properties
- The assumptions, which need only be stated, not justified
- The constraints on how Overarching Property possession must be demonstrated

The unique assessment considerations arising for each of these are discussed in turn.

3.4.2.1 *from the Definitions*

The easiest to explain difference between assessing a random ARGUMENT and an OPRA is that any BINDINGS provided in the ORPA must be consistent with the definitions provided in the OP description. To ensure this consistency is enforced in assessment, we add an additional clause to question II.S.f (from Figure 2): … and are these BINDINGS consistent with the OP definitions?

3.4.2.2 *from the Requisites*

The requisites require certain real-world artifacts to exist, specifically the *defined intended behavior*, the collection of *failure conditions*, the record of the *safety assessment*, the record of the *foreseeable operating conditions*, the *implementation*, and one or more assignments of development assurance levels (DALs). These requirements mean that an OPRA assessor should expect to find BINDINGS of those terms to the appropriate real-word artifacts. Within our assessment approach, the assessor will look for these appropriate BINDINGS in the Interrogate stage when considering whether the syntax is proper. Specifically, this should arise when answering question II.S.g: Does a proper BINDING exist for each reference to an external artifact?

3.4.2.3 *from the Assumptions*

The OP description specifies two permitted ASSUMPTIONS:

a. Stakeholders have the knowledge to express the *desired behavior*.
b. Performing *safety assessment* is not covered by the Overarching Properties.

One consequence for assessment is that any PREMISE equivalent to either of these assumptions falls into BELIEVABILITY category II.P.a.(f); it is "an assumption accepted by all stakeholders" and it should be "marked as such." The second consequence is that an assessor should not require an OPRA to include an ARGUMENT with a CONCLUSION about the adequacy of the knowledge of stakeholders. Nor should an assessor require ARGUMENTS with CONCLUSIONS related to the processes used to produce the *safety assessment* artifact(s) used in the OPRA. If either or both concepts (stakeholder knowledge, *safety assessment* processes) appear in an ARGUMENT, they will most likely be contained within PREMISES, REASONING, BINDINGS, or DEFEATERS.

3.4.2.4 *from the Constraints*

Unlike the relatively narrow effects on the expected content of OPRAs from the OP requisites and assumptions, the effects of the constraints are broader. Specifically, the constraints reduce the range of possible forms an OPRA might take while also demanding that any OPRA with a CONCLUSION about OP possession address certain specific matters.[24]

[23] Refer to Figure 4: The Overarching Properties in Appendix A.1 if necessary. Following the style used in the OP description, terms in italics have specific definitions provided in the description.

[24] The number and wording of the constraints engendered much debate during the creation of the Overarching Properties. Some people wanted no or very few pre-defined constraints, leaving to negotiation among each specific

We consider potential[25] assessment consequences of each of the constraints in turn, using the same identification scheme as used in *Understanding the Overarching Properties* [1].

Assessment consequences of C.a

Constraint C.a requires “The process to ensure possession of the Overarching Properties must be defined and conducted as defined.” That is, a plan must be created and then followed. Well-established processes already exist for planning, and using an ARGUMENT-based approach for demonstrating OP possession fits easily within those processes. Thus, there seems to be no reason to BELIEVE an OPRA will be needed to show satisfaction of this constraint. Existing methods should suffice, with simple references within the relevant ARGUMENTS to application of existing methods for planning. But if new planning approaches are adopted or novel applications of existing ones are used, an ARGUMENT may be needed[26].

Assessment consequences of C.b

Constraint C.b states, “The means by which the *defined intended behavior* is shown to be correct and complete is commensurate with the DAL.” Exactly how this constraint will manifest in real-world projects is not yet clear; actual case studies are needed to clarify it. Abstractly, the constraint suggests different confidence levels may be applied for different DALs. Thus, how an assessor should answer our suggested assessment questions 4.a (Is the required level of confidence known?) and 4.b (Does the ARGUMENT engender the required level of confidence?) may be DAL dependent.

Assessment consequences of C.c

C.c requires “Criteria for evaluating the artifacts be defined and that these criteria be shown to be satisfied individually and collectively.” Thus, an assessor of an OPRA that addresses artifacts should expect to need to assess ATOMIC ARGUMENTS dealing with artifact evaluation criteria, both for each artifact separately and for the whole set of artifacts collectively.

Assessment consequences of C.d

C.d says, “All artifacts are under configuration management and change control.” Analogously to C.a, well-established processes exist for configuration management and change control. Thus, often ARGUMENTS will not be needed about this subject; simple reference to application of existing methods will suffice. As the reader has likely surmised, the use of ARGUMENT adds to the collection of entities for which configuration management and change control is necessary, namely the ARGUMENTS themselves. Analogously to planning, using ARGUMENTS to justify using non-traditional approaches to configuration management and change control is a possibility.

system’s relevant parties the constraints on how OP possession could be shown for that system. Some people wanted more or tighter pre-defined constraints to correspond more closely to existing processes and guidelines. Neither side got its way; compromise eventually ruled the day.

[25] We say “potential assessment consequences” because they are based on intuition and experience and not on any empirical results from any real case studies of constructing and assessing OPRAs. Our intuition suggests that such case studies are likely to reveal additional consequences flowing from the constraints. If our intuition is correct, this document will be revised to incorporate the new information.

[26] Using ARGUMENTS when existing methods suffice is a direct violation of the principle of EFFICACY (You need *ARGUMENT* only when you *need* ARGUMENT) explained in section 3.7 of *The Primer on Argument* [2].

Assessment consequences of C.e

C.e is the most complicated constraint[27]: "When tiers of decomposition are used, the means of showing correctness among the tiers and to the *defined intended behavior* must be defined and conducted as defined." Because the constraint is so complicated, speculating on its assessment consequences in the absence of real case studies seems likely to do more harm than good. In the spirit of innocuity we decline to speculate at this time.

Assessment consequences of C.f

C.f is perhaps worded a bit clumsily ("The implementation must be correct when functioning as part of the integrated system or in environment(s) representative of the integrated system"), but its intent as explained in [1, page 19] is "to ensure that demonstrations of [the OP labeled] Correctness take place in either the actual system in which the product will be used, or in one or more environments that represent the actual system in all relevant aspects." Thus, when considering an OPRA that concerns the Correctness property, the assessor should not assess as COGENT any ARGUMENT that relies on demonstrations in environments that do not satisfy the constraint.

Assessment consequences of C.g

C.g requires, "All design and manufacturing data that is needed to support consistent replication of the type design and instructions for continued airworthiness must be established." Satisfying this constraint seems analogous to satisfying C.a and C.d. That is, applying current processes and guidelines without requiring an OPRA about it seems likely to suffice.[28]

Assessment consequences of C.h

The final constraint, C.h, demands "The *safety assessment* must address all of the *implementation*." As explained in [1], the word "address" here means that the *safety assessment* must account for all of the *implementation* either directly or by identifying any portions of the *implementation* (for example, perhaps some uses of commercial off the shelf software) that cannot be analyzed directly. Thus, the constraint precludes resting an ARGUMENT on a demonstration that employs only a partial assessment; therefore, an assessor should answer "No" to question 4 (Is saying "Yes" to the CONCLUSION justified?) for any ATOMIC ARGUMENT that does so.

Ensuring constraint enforcement

To ensure that all the consequences of the OP constraints are considered properly during assessment, we add clauses to II.R.b (and with the OP constraints) and II.Y.b (without violating any of OP constraints[29]) and add a third question to step IIII (C. Are all OP constraints satisfied?)

3.4.3 OPRA-unique iTest

This concludes the discussion of OPRA-unique assessment considerations. To incorporate these considerations into iTest requires additions to only II.S.f, II.S.g, I.P.a.(f), II.R.b, II.Y.b, and IIII.C. These additions are highlighted with italics in Figure 3.

[27] This document is not the place to try to alleviate these complications, but out of all the parts of the Overarching Properties description, this constraint is likely the one most in need of modification or (better) elimination.

[28] Alternatively, a COGENT ARGUMENT can likely be constructed that this constraint as written does not really belong, but that is a discussion for another time and place.

[29] Those folks who BELIEVE all the constraints are strictly necessary should consider this addition to be redundant. We include it in recognition of the lack of consensus within (and outside of) the OPWG about whether some of the constraints *are* strictly necessary, and to be candid, because we are among those who think some of them are not.

I. **Isolate** one ATOMIC ARGUMENT

II. **Interrogate** it as an ATOMIC ARGUMENT by asking and answering the SPRY questions.

S. Is the **S**yntax proper?

a. Is there a single CONCLUSION that is stated in the form of a proposition?

b. Is there a statement of REASONING?

c. Is there at least one PREMISE?

d. Is each PREMISE stated in the form of a proposition?

e. If there are DEFEATERS, is each stated in the form of a proposition?

f. Does a BINDING exist for each term or phrase used in the CONCLUSION, REASONING, PREMISES, and (if any) DEFEATERS that does not have a well-known, unambiguous definition*, and are these BINDINGS consistent with the OP definitions*?

g. Does a proper BINDING exist for each reference to an external artifact, *including those that are required to exist by the OP requisites*?

P. Are the **P**REMISES acceptable?

a. Is each PREMISE BELIEVABLE? To be BELIEVABLE the PREMISE must fall into one of these categories:

(a) expresses a proposition that is 'universally' accepted as true

(b) expresses a proposition that is accepted as true within the relevant domain

(c) is supported by an ARGUMENT (provisionally presumed to be COGENT)

(d) is supported by external artifacts that are accepted within the domain as being sufficient to establish its truth

(e) will fall into category (c) or (d) at a later stage of ARGUMENT development

(f) is an assumption accepted by all stakeholders and clearly identified as such*, including the OP defined assumptions?*

b. Is each PREMISE relevant to the CONCLUSION?

R. Is the **R**EASONING acceptable?

a. Is the REASONING relevant?

b. Is the REASONING consistent with current knowledge *and with the OP constraints*?

Y. Is saying "**Y**es" to the CONCLUSION justified?

a. Is the required level of confidence known?

b. Does the ARGUMENT engender the required level of confidence *without violating any of the OP constraints*?

III. **Iterate** until all ATOMIC ARGUMENTS have been assessed

IIII. **Integrate** the individual assessments by answering these questions:

A. Are all ATOMIC ARGUMENTS assessed as COGENT?

B. Does every path through the COMPOUND ARGUMENT terminate in BELIEVED PREMISES?

C. Are all OP constraints satisfied?

Figure 3: iTest for OPRAs

3.4.4 Exercises

We now present five exercises designed to enable readers to assess for themselves how well the combination of the explanations provided in this document and their understanding of those explanations works in (simulated) practice.

Including specific exercises (or even examples not in the form of exercises) here is risky[30]. To reduce (or at least not increase) the risk, these exercises follow a similar pattern to the exercises in [4], but they are fewer in number and use OPRAs instead of generic ARGUMENTS. These OPRAs are modeled after but are not always identical to examples presented in section 3.3. Following the lead of [4] and for the same reasons, we call the ARGUMENT assessor “Ashley” and the ARGUMENT creator “Cameron”[31]. For all the exercises, assume Cameron and Ashley live in a world in which the relevant approval authority has established a process allowing ARGUMENT-based substantiation of OPs as an acceptable means of compliance and has also set required confidence levels according to DALs. Answers to the exercises are given at the end. Well, answers to the first four exercises are given at the end. An answer is provided in Appendix C for the fifth exercise.

3.4.4.1 Exercise 1

Cameron presents Ashley with the following ATOMIC ARGUMENT. Ashley almost immediately tells him it is deficient. Why did Ashley say it is deficient?

```
Believing
     <MDSS> possesses <Intent>
is justified by applying
     The definition of <Intent>
to these premises
     <MDSS> <DIB> is correct with respect to its <DeB>
     <MDSS> <DIB> is complete with respect to its <DeB>
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by
     specified development artifacts (which must eventually be
     named)
     <OPsDefinition>: as given in presentation by Michael Holloway
     on 2017-11-04
     <Intent>: The definition of Intent in <OPsDefinition>
     <DIB>: defined intended behavior as defined in
     <OPsDefinition>
```

[30] The riskiness is rooted in the difficulty (some might say impossibility) of developing exercises that are appropriate for an audience encompassing a wide range of knowledge and expertise. Some folks with deep knowledge may find some of the exercises to not contain as much information as they want. On the other hand, if that information were included some (perhaps many) people with less knowledge would find the exercises too complicated and confusing. We hope (and perhaps BELIEVE) that by mimicking to a large extent the pattern of the exercises in [4] we will not annoy any more people with these additional exercises than would be annoyed by the [4] exercises alone.

[31] These names were chosen because they are gender neutral; “Ashley” and “assess” both begin with the letter ‘a’, and “Cameron” and “construct” both begin with the letter ‘c’ pronounced similarly.

```
     <DeB>: desired behavior as defined in <OPsDefinition>
```

3.4.4.2 Exercise 2

Early in the system development process, Cameron presents Ashley with the following ATOMIC ARGUMENT, asking if it is acceptable at the current point in time within a DAL C system. Ashley says it is. Why did Ashley say so?

```
Believing
     <MDSS> possesses <Correctness>
is justified by applying
     The definition of <Correctness>
to these premises
     <MDSS> <implementation> is correct with respect to its <DIB>
     <Foreseeable operating conditions> are accounted for in the
     <DIB>
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by
     specified development artifacts (which must eventually be
     named)
     <foreseeable operating conditions>: as defined in [1]
     <Correctness>: The <implementation> is correct with respect
     to its defined intended behavior, under <foreseeable
     operating conditions> [1]
     <implementation>: item or combination of inter-related items
     for which acceptance or approval is being sought [1]
     <DIB>: defined intended behavior [1]
```

3.4.4.3 Exercise 3

Ashley finds the following ATOMIC ARGUMENT in e-mail from Cameron one morning. The subject of the e-mail is, “Would you buy this?” Assuming the elided BINDINGs are provided in the e-mail, and each is proper, should Ashley reply in the affirmative or the negative?

```
With
     . . . all needed bindings . . .
Believing
     <MDSS> <implementation> is correct with respect to its <DIB>
is justified by applying
     Inspection of <simulation results>
to these premises
     The <implementation> was tested in a <simulation environment>
     The <simulation results> were correct with respect to the
     <DIB>

     The <simulation environment> was developed for a different
     aircraft
```

3.4.4.4 Exercise 4

Cameron asks Ashley to assess the following ATOMIC ARGUMENT. Ashley responds with several questions. What are these questions?

```
Believing
     <MDSS> <implementation> is correct with respect to its <DIB>
is justified by applying
     The definition of <Correct-wrt-DIB>
to these premises
     <MDSS> <implementation> meets satisfaction criteria
     The criteria are specified and acceptable
     The methods are specified and acceptable
with these bindings
     <MDSS>: Maneuver determination subsystem as defined by
     specified development artifacts A, B, and C
     <implementation>: item or combination of inter-related items
     for which acceptance or approval is being sought [1]
     <DIB>: defined intended behavior [1]
     <Correct-wrt-DIB>: <implementation> is shown through
     specified acceptable methods to meet specified acceptable
     satisfaction criteria
```

3.4.4.5 Exercise 5

The following COMPOUND ARGUMENT makes up a part of Cameron's overall COMPOUND ARGUMENT about MDSS possessing the Overarching Properties. Ashley has quit her job to train for a try at making the U.S. team in the marathon for the Games of the XXXIII Olympiad. You are solely responsible for assessing the ARGUMENT. Apply iTest, under these conventions:

(a) The required level of confidence is known.
(b) Wherever it is used `Conjunction` is relevant REASONING, consistent with current knowledge and the OP constraints, and sufficient when applied to BELIEVED PREMISES to justify BELIEVING the CONCLUSION.
(c) `BelProp1` represents a proposition that is BELIEVED universally and known to be relevant.
(d) `BelProp2, BelProp3` represent propositions that are accepted as true within the domain and known to be relevant.
(e) `Assu7` represents an assumption accepted by all stakeholders and known to be relevant.
(f) `Reas1`, `Reas2` represents REASONING known to be relevant, consistent with current knowledge, sufficient when applied to appropriate PREMISES to justify BELIEF in a CONCLUSION, and consistent with the OP constraints.

(g) Reas8 represents REASONING known to be relevant, consistent with current knowledge, sufficient when applied to appropriate PREMISES to justify BELIEF in a CONCLUSION, but inconsistent with OP constraint C.e.

(h) Arti3, Arti4, Arti5 represent artifacts for which appropriate bindings are provided (despite not being shown here), and which are accepted within the relevant domain as sufficient to establish compliance with the relevant standard.

(i) Unless otherwise stated, the OP constraints are satisfied.

Answer these questions. How many ATOMIC ARGUMENTS are there? How many did you initially assess as COGENT? How many remained assessed as COGENT after the iTest integration step? What is your final assessment of the COMPOUND ARGUMENT?

```
With these bindings
    <UtOPs>: The document Understanding the Overarching Properties,
          NASA/TM-2019-220292
          [https://ntrs.nasa.gov/citations/20190029284]
    <MDSS>: Maneuver determination subsystem as defined by
          specified development artifacts (which must eventually be
          named)
    <Intent>: “The defined intended behavior is correct and complete
          with respect to the desired behavior” as defined in
          <UtOPs>
    <Correctness>: “The <implementation> is correct with respect to
          its defined intended behavior, under <foreseeable
          operating conditions>” as defined in <UtOPs>
    <Innocuity>: “Any part of the <implementation> that is not
          required by the <defined intended behavior> has no
          <unacceptable impact>” as defined in <UtOPs>
    <DIB>: abbreviation for <defined intended behavior>
    <DeB>: abbreviation for <desired behavior>
    <desired behavior>: "Needs and constraints expressed by the
          stakeholders (this includes those needs and constraints
          identified by the <safety assessment> and those mandated
          by regulations)." as defined in <UtOPs>
    <defined intended behavior> "The record of the desired behavior"
          as defined in <UtOPs>
    <implementation>: “<item> or combination of inter-related
          <item>s for which acceptance or approval is being sought”
          as defined in <UtOPs>
    <foreseeable operating conditions>: “External and internal
          conditions in which the system is used, encompassing all
          known normal and abnormal conditions” as defined in
          <UtOPs>
    <unacceptable impact>: as defined in <UtOPs>
```

```
   <Correct-wrt-DIB>: <implementation> is shown through specified
        acceptable methods to meet specified acceptable
        satisfaction criteria (which must both eventually be
        named)

   <safety assessment>: see description in <UtOPs>

   <item>: see description in <UtOPs>


Believing
    <MDSS> possesses the <Overarching Properties>  {pOPs}
is justified by applying
    conjunction
to these premises
    <MDSS> possesses <Intent>      {pIntent}
    <MDSS> possesses <Correctness> {pCorrectness}
    <MDSS> possesses <Innocuity>   {pInnocuity}



Believing {pIntent}
    <MDSS> possesses <Intent>
is justified by applying
    The definition of <Intent>
to these premises
    <MDSS> <DIB> is correct with respect to its <DeB>   {DIBcorrect}
    <MDSS> <DIB> is complete with respect to its <DeB>  {DIBcomplete}


Believing {pCorrectness}
    <MDSS> possesses <Correctness>
is justified by applying
    The definition of <Correctness>
to these premises
     <MDSS> <implementation> is correct with respect to its <DIB>
        {ImpcrtDIB}
     <Foreseeable operating conditions> are accounted for in the
        <DIB> {FOCinDIB}


Believing {pInnocuity}
    <MDSS> possesses <Innocuity>
```

```
is justified by applying
    The definition of <Innocuity>
to these premises
    Every part of <MDSS> <implementation> is required by its <DIB>
         {impReq}

Believing {DIBcorrect}
    <MDSS> <DIB> is correct with respect to its <DeB>
is justified by applying
    conjunction
to these premises
    BelProp1
    BelProp2

Believing {DIBcomplete}
    <MDSS> <DIB> is complete with respect to its <DeB>
is justified by applying
    Reas1
to these premises
    Assu7
    BelProp3

Believing {ImpcrtDIB}
    <MDSS> <implementation> is correct with respect to its <DIB>
is justified by applying
    Reas8
to these premises
    Arti3
    Arti4
    Arti5

Believing {FOCinDIB}
    <Foreseeable operating conditions> are accounted for in the
    <DIB>
is justified by applying
    Reas2
```

```
to this premise
    The <DIB> accounts for everything in <prevFOC>. {DIBprevFOC}
with
    <prevFOC>: the collection of <foreseeable operating
      conditions> developed for the predecessor to <MDSS>
```

3.4.4.6 Ashley's Answers

Ashley said the ATOMIC ARGUMENT in Exercise 1 (3.4.4.1) is deficient because it binds `<OPsDefinition>` to an unpublished, comparatively old presentation instead of to the current version of *Understanding the Overarching Properties*, thus requiring a "no" answer to assessment question 1.g ("Does a proper BINDING exist for each reference to an external artifact?"). In real life a decent configuration management system should prevent analogous errors from happening, as explained in 3.4.2.4 *Assessment consequences of C.d.*

Ashley said the ATOMIC ARGUMENT in Exercise 2 (3.4.4.2) is acceptable for the current point in time (early in the development process) because its syntax is proper; the PREMISEs are category (e) BELIEVABLE and relevant; the REASONING is relevant and (in our assumed world) consistent with current knowledge; the required confidence level is known; and the ARGUMENT (under all the assumptions relevant for early in the development cycle) seems sufficient to engender the required confidence level. Ashley does, however, suggest to Cameron that good practice includes checking the consistency of BINDINGs, citing the discrepancy apparent in the BINDING of `<foreseeable operating conditions>`.

For Exercise 3 (3.4.4.3) Ashley should reply in the negative. The ARGUMENT appears to violate constraint C.f ("The implementation must be correct when functioning as part of the integrated system or in environment(s) representative of the integrated system"), because it refers to a `<simulation environment> developed for a different aircraft`. It seems unlikely that a different aircraft's simulation environment will be one that is representative of the integrated system of the aircraft on which the `<MDSS> <implementation>` is intended to fly.

Ashley's questions for Exercise 4 (3.4.4.4) include the following:

- Why is `methods` unbound?
- Why is `criteria` unbound?
- Are `criteria` and `satisfaction criteria` meant to be the same thing?
- Are `methods` and `specified acceptable methods` meant to be the same thing?

Other questions are also possible.

Although not involved in officially assessing the ARGUMENT in Exercise 5 (3.4.4.5), Ashley nevertheless did an assessment, which is provided in full in Appendix C.

4 Process and Practice Considerations

In this section, we collect some of the considerations we have noted pertaining to the use of OPRAs within production-scale development and assessment processes. We log these considerations here to recognize them, and to set the stage for future work.

Production use of structured argument in the service of aircraft assurance and certification implies at least 1) processes on the parts of both the applicant and assessing authority, and 2) competent execution of these processes by the responsible practitioners.

4.1 Process Infrastructure

ARGUMENTS are living structures, and those intended to support system approvals will be larger and more complex than the examples shown here. ARGUMENTS are grown and refined both during the initial drafting process, throughout the associated system development process, as well as in response to reviews, both internal as well as by approval authorities, and in response to in-service experience.

This means we have considerations for things like development planning, configuration management, decision history, larger scale review, status tracking, issue tracking, visualization, coherence monitoring, error reporting, responsibility, authority, tooling, packaging, and a number of other information and engagement needs of various stakeholders, all of which must be coordinated to the associated development and certification process for the target system and/or subsystem.

Where would support for such considerations come from and how should energy be directed? Remember that internal consistency sufficient to pragmatic needs is the priority; respect first principles first. Drivers and actions should start small, from within a program, and as a learning exercise first. No applicant should run headlong into a major ARGUMENT development effort without having first established some organizational competence and familiarity via some combination of trial projects and training. Then, dedicated personnel with some understanding and experience can design, maintain, improve, and extend a local practice that supports applicant-specific ARGUMENT development needs. In the course of seeding and growing an organizational competency, engagement with the approving authority will provide additional feedback on the accessibility, utility, and value of various options in ARGUMENT organization and presentation.

This brings us to another consideration for advancing an ARGUMENT practice.

4.2 Practitioner Maturity

Process definition is a significant need. It is also not sufficient. To execute processes on the applicant and authority sides, we need trained practitioners, competent in both construction and assessment. What makes a competent practitioner? This question requires investigation commensurate with those above on process definition. Some directions are previewed in the current work and considered below.

4.2.1 Reinforcement of Core Concepts

Recall here the primitives and precepts as introduced in the Primer on Argument [2], the foundation upon which the rest of this approach rests. Recall further the distinction between ARGUMENT and assurance case we described in Section 1.2, the distinction between the container and the contained as addressed in Section 3.3.2.2, and the declarative vs. procedural nature of ARGUMENT. Both the research and practitioner communities would do well to establish a broader, common understanding of these notions, their relationships with each other, and with adjacent and containing processes, before attempting to activate them all together in production scenarios.

Regarding the development of conventions, we've made a repeated point of identifying various choices that exist in conceiving and writing down an ARGUMENT. Though we have encouraged consistency, it is completely reasonable to imagine two authors or teams or organizations both practicing with internal consistency, though differently from each other, with regard to various choices. THIS IS OK, as long as sufficient direction in navigation and interpretation is provided to the intended audience upon presentation. This said, it is also reasonable and appropriate to consider collaboration toward community-supported conventions. To get there, stakeholders need to develop the requisite command of concepts and judgement to build quality ARGUMENTS independently. Then, they must engage intentionally with other stakeholders to assess combined experience for insights.

Indeed this document is certainly not the beginning of community discussion on ARGUMENTS, though the muddy lexicon and chaotic application in the assurance case community has contributed to churn and lack of broad coherence despite valuable contributions. Similarly, notations and tools abound, but none has established itself as a consensus solution to a need. This is largely because a notation or tool won't fix a lack of clarity, coherence, and competence in fundamentals. One must understand a concept before attempting to scale or automate it. Conventions and tools are desirable *after* a stakeholder population understands its needs well and has resourced the requisite competency for their application. Competent application should then feed experience back into refinement of those conventions and tools, ideally from broad, cross-functional use.

4.2.2 Training

How do we get either a whole practitioner population over this hill, and/or establish dedicated trusted pools of competence within organizations? This is beyond the scope of this document, again, but training and curriculum have come up at places like the Software Certification Consortium, and others have identified the need for an empirical program [10].

A direction for further discussion begins as follows: which stakeholders are going to consider OPRAs and for what uses? Which roles, processes, interfaces, entities, and dependencies are implicated? What in-house applicant competencies need to be acquired to support those, and how can this be done? And what authority-side competencies? What are the first, most tractable, most valuable steps to take in establishing a trainable body of knowledge, and in establishing local practice? How should the conversation proceed between applicants and authorities? What more general implications arise for higher education and workforce development? These are all questions in need of investigation.

5 Summary

This is the fifth in a series of foundation documents addressing definition and application of the Overarching Properties. In it, we took concepts established in the prior documents and exercised them, demonstrating and narrating the construction and assessment of ARGUMENTS that conclude possession of the OPs. The presentation was aimed at a broad population of potential users and stakeholders new to either the OPs, structured ARGUMENT, or both. We believe that a broad base of foundational competence will be one prerequisite to building an effective community of practice.

Several themes and observations characterized this document, among them:

- ARGUMENT-based substantiation of the OPs is plausible as a future means of compliance;
- stakeholders should focus on fundamentals before scale and automation;
- effective use of ARGUMENT will depend on competent application and situationally appropriate use;
- a main objective is the support and achievement of cross-functional shared understanding of rationales.

We highlighted these themes throughout a set of narrated examples of ARGUMENT construction and assessment, noted a number of additional issues and decisions that arise, and logged a number of considerations to be addressed next. We expect follow-on work to consider practical application, including integration into development and certification processes, specific stakeholder needs, and appropriate use of conventions, notations, and tools.

6 References

1. Holloway, C. Michael. 2019. Understanding the Overarching Properties. NASA/TM-2019-220292. https://hdl.handle.net/2060/20190029284 (last visited September 20, 2021).

2. Holloway, C. Michael and Kimberly S. Wasson. 2021. A Primer on Argument. https://ntrs.nasa.gov/citations/20210019993 (last visited September 20, 2021). An earlier version was published as A Primer on Argument (Overarching Properties Edition). https://ntrs.nasa.gov/citations/20205003337 (last visited October 17, 2020).

3. Holloway, C. Michael. 2020. The Friendly Argument Notation (FAN). NASA/TM–2020-5002931. https://ntrs.nasa.gov/citations/20205002931 (last visited September 20, 2021).

4. Holloway, C. Michael and Kimberly S. Wasson. 2021. A Primer on Argument Assessment. https://ntrs.nasa.gov/citations/20210022807 (last visited December 20, 2021).

5. Greenwell, William S, John C. Knight, C. Michael Holloway, and Jacob J. Pease. 2006. A Taxonomy of Fallacies in System Safety Arguments. *24th International System Safety Conference*. July 31 - August 4. Albuquerque, NM. https://ntrs.nasa.gov/citations/20060027794 (last visited November 4, 2021).

6. The Assurance Case Working Group. 2018. Goal Structuring Notation Community Standard Version 2. SCSC-141B.

7. Govier, Trudy. 2010. A Practical Study of Argument. 7th edition. Belmont, CA: Cengage Learning.

8. Toulmin, Stephen E. 2003 (1958). The Uses of Argument. Cambridge, UK: Cambridge University Press.

9. Holloway, C. Michael. 2018. Understanding Assurance Cases: An Educational Series in Five Parts. https://shemesh.larc.nasa.gov/arg/uac.html (last visited October 17, 2020)

10. Habli, I., *et al*., Safety Cases: An Impending Crisis? 29th Safety-Critical Systems Symposium Virtual Conference, 2021.

11. Bhattacharyya, S., *et al*., Certification Considerations for Adaptive Systems. National Aeronautics and Space Administration (NASA), Langley Research Center, Hampton, VA, NASA/CR-2015-218702, 2015. https://ntrs.nasa.gov/citations/20150005863 (last visited November 4, 2021).

12. Wikipedia contributors (2021). List of fallacies. In *Wikipedia, The Free Encyclopedia*. Retrieved May 12, 2021, from https://en.wikipedia.org/w/index.php?title=List_of_fallacies&oldid=1022453908.

Appendix A: Summary of Prerequisite Material

To truly understand this document, one must first understand the four prerequisite documents. To assist readers who still wish to read this document first, and to provide otherwise convenient reference, we briefly summarize the bare essentials of the information from the prerequisite documents here. Whether the summaries presented in this Appendix will suffice for a particular reader will depend on the reader and the circumstances. The reader is directed to consult the full prerequisite documents as needed.

A.1 Bare Essentials of the Overarching Properties

The Overarching Properties were first presented and explained in *Understanding the Overarching Properties* [1]. The OPs are intended to define a sufficient set of properties for making approval decisions. That is, when approval is sought for using a particular aviation system or subsystem, if the entity can be shown to possess these properties in their entirety, then granting approval for using that system or subsystem should be appropriate.

The full description of the OPs fits on a single page, as shown in Figure 4. Here are some additional things to know:

- The Overarching Properties are a novel expression of time-honored principles.
- The Overarching Properties description consists of the property labels, the property statements, the definitions section, the requisites section, the assumptions section, and the constraints section.
- The meaning of the properties is *fully defined* by the three property statements and eight definitions.
- The property labels (Intent, Correctness, and Innocuity) do not affect the meaning of the properties in any way; they are included only for convenience of reference.
- The requisites, assumptions, and constraints sections do not affect the meaning of the properties in any way; they only affect the means by which property possession may be shown.
- Using the Overarching Properties for assurance of some aspects of an entity while using something else for other aspects is acceptable.
- Argument-based approaches to the Overarching Properties for assurance are presumed to offer advantages over other approaches; whether this presumption holds true will be determined through application in realistic and real projects.
- Advances in assurance methods may eventually justify cancelation of some constraints, refinement of requisites, and/or alteration of assumptions.

Intent: The *defined intended behavior* is correct and complete with respect to the *desired behavior*.

Correctness: The *implementation* is correct with respect to its *defined intended behavior*, under *foreseeable operating conditions*.

Innocuity: Any part of the *implementation* that is not required by the *defined intended behavior* has no *unacceptable impact*.

Definitions

a. *Desired behavior*: Needs and constraints expressed by the stakeholders (this includes those needs and constraints identified by the *safety assessment* and those mandated by regulations).
b. *Defined intended behavior*: The record of the *desired behavior*.
c. *Implementation*: *Item* or combination of inter-related *item*s for which acceptance or approval is being sought.
d. *Item:* A hardware or software element having bounded and well-defined interfaces.
e. *Foreseeable operating conditions*: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions.
f. *Unacceptable impact*: An impact that compromises the *safety assessment*.
g. *Safety assessment:* The systematic identification of failure conditions and classifications in an operational context, evaluation of the architecture against safety objectives arising from these hazards, evaluation of potential common modes and threats, defining additional intended behaviors to support claims within these evaluations and showing that the safety objectives are satisfied by the *implementation*.
h. *Failure condition*: "A condition having an effect on the [aircraft] and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events." (from AMC 25.1309)

Requisites for showing possession of the Overarching Properties

a. *Defined intended behavior* exists.
b. *Failure conditions* are defined.
c. The record of the *safety assessment* exists.
d. The record of the *foreseeable operating conditions* exists.
e. The *implementation* exists.
f. Development Assurance Level (DAL) assignments based on the *failure condition* classifications exist.

Assumptions which need only be stated, not justified

a. Stakeholders have the knowledge to express the *desired behavior.*
b. Performing *safety assessment* is not covered by these Overarching Properties.

Constraints on how Overarching Property possession must be demonstrated

a. The process to ensure possession of the Overarching Properties must be defined and conducted as defined.
b. The means by which the *defined intended behavior* is shown to be correct and complete is commensurate with the DAL.
c. Criteria for evaluating the artifacts are defined and shown to be satisfied individually and collectively.
d. All artifacts are under configuration management and change control.
e. When tiers of decomposition are used, the means of showing correctness among the tiers and to the *defined intended behavior* must be defined and conducted as defined.
f. The *implementation* must be correct when functioning as part of the integrated system or in environment(s) representative of the integrated system.
g. All design and manufacturing data to support consistent replication of the type design and instructions for continued airworthiness must be established.
h. The *safety assessment* must address all of the *implementation*.

Figure 4: The Overarching Properties

A.2 Bare Essentials of ARGUMENT

A Primer on Argument [2] identifies a collection of primitives, precepts, and practical considerations important for discussing, constructing, and assessing ARGUMENTS. The document includes an Appendix summarizing the essential things to know. The content of that Appendix is reproduced here.

- An ARGUMENT is an attempt to convince others to BELIEVE a CONCLUSION through REASONING and one or more PREMISES.
- The CONCLUSION is the statement you want your audience to BELIEVE.
- A PREMISE is a statement you think your audience BELIEVES.
- Your REASONING states why you think the PREMISES should cause your audience to BELIEVE your CONCLUSION.
    - (EVIDENCE is the name you *may* give to a PREMISE you're certain your audience BELIEVES.)
    - (ASSUMPTION is the name you *may* give to a PREMISE you are not prepared to justify if your audience does not BELIEVE it.)
- A BINDING is an association between a term used in an argument and the real-world information to which that term refers.
- A DEFEATER is a statement that may cause your audience to *not* BELIEVE your CONCLUSION.
- To BELIEVE is to accept as true.
- An ATOMIC ARGUMENT consists of a single CONCLUSION together with its immediate REASONING, PREMISES, BINDINGS (if present), and DEFEATERS (if present).
- A COMPOUND ARGUMENT is an ARGUMENT consisting of more than one ATOMIC ARGUMENT.
- An ARGUMENT is called COGENT if it rationally justifies BELIEVING its CONCLUSION to the required standard of confidence.
- The precept of EFFICACY reminds us that *you need argument only when you <u>need</u> argument.*
- The precept of PLAUSIBILITY reminds us that *presuppositions predetermine plausibility*.
- The precept of INDUCTION reminds us that *the arguments with which we will concern ourselves are uniformly inductive arguments*.
- The precept of CERTAINTY reminds us that *certainty is certainly not possible*.
- The precept of LOCALITY reminds us that *compound arguments are always assessed one atomic argument at a time.*
- The precept of DEPTH reminds us to *descend no deeper than necessary*.
- The precept of CHANGE reminds us that *arguments are living structures.*

A.3 Bare Essentials of FAN

The Friendly Argument Notation (FAN) was developed to facilitate the creation, understanding, and assessment of structured ARGUMENTS [3], particularly, but not exclusively, ARGUMENTS about safety-critical systems. FAN intentionally corresponds closely to traditional ARGUMENT concepts. Unlike most existing notations commonly used within safety and assurance cases (see [6, 9]), FAN can be understood by someone without knowledge of computer science concepts or graphical conventions. It is designed to be efficient to write and read, with sufficient semantic and syntactic rigor to capture the necessary distinctions. We use it in this document specifically for its minimalist nature. Our choice does not mean that every OPRA from this day forward must do the same. Any notation that adequately expresses ARGUMENTS may be considered a legitimate choice. We chose FAN to minimize to the extent possible the likelihood of notational nuances getting in the way of important basic ideas about ARGUMENT creation and assessment.

An ATOMIC ARGUMENT in FAN is expressed using the following structure:

```
Believing
     CONCLUSION
is justified by applying
     REASONING
to these premises
     PREMISE-1
     . . .
     PREMISE-P
[with
     BIND-1: definition, link, etc.
     . . .
     BIND-B: definition, link, etc.]
[unless
     DEFEATER-1
     . . .
     DEFEATER-D]
```

The CONCLUSION follows a line containing the keyword `Believing`. The REASONING follows a line containing "`is justified by applying`".[32] The PREMISES follow the phrase "`to these premises`", with each PREMISE starting on its own line and being visually distinguishable from any other PREMISES. This visual distinction may be done in a variety of ways, such as using blank lines, numbering, or trailing backslashes.

The keyword `with` begins a BINDING section, which may contain as many BINDINGS as needed. In this document each bound phrase is surrounded by angle brackets (< >) to identify it as such. Different conventions (such as, **`mortal`**, *`mortal`*, or `mortal`) are also allowed, so long as they are used consistently. FAN allows DEFEATERS to be expressed following the keyword `unless`.

To express a COMPOUND ARGUMENT in FAN, one need only to write sequentially each of its constituent ATOMIC ARGUMENTS. FAN facilitates understanding and navigating COMPOUND ARGUMENTS in four ways: (1) allowing statements to be labeled; (2) treating BINDINGS as having global scope; (3) permitting a FAN COMPOUND ARGUMENT to begin with a free-standing BINDING section; and (4) allowing comments to be included.

A.4 Bare Essentials of ARGUMENT Assessment

A *Primer on Argument Assessment* [4] describes one way, but not the only way, to assess the COGENCY of ARGUMENTS. Its Appendix "You Must Remember This" summarizes the essential information from the document as follows:

[32] The FAN definition is a bit less restrictive than this sentence implies. Any text whatsoever may follow the initial keyword `is`. This document always uses the longer phrase `is justified by applying`. Similarly, to identify the beginning of PREMISES, FAN only requires the single keyword `to`, but the longer `to these premises` is used consistently here.

One way to assess the COGENCY of an ATOMIC ARGUMENT is to answer the SPRY questions:

1. Is the **S**yntax proper?
2. Are the **P**REMISES acceptable?
3. Is the **R**EASONING acceptable?
4. Is saying "**Y**es" to the CONCLUSION justified?

One way to answer the **S** question is to answer these additional questions:

a. Is there a single CONCLUSION that is stated in the form of a proposition?
b. Is there a statement of REASONING?
c. Is there at least one PREMISE?
d. Is each PREMISE stated in the form of a proposition?
e. If there are DEFEATERS, is each stated in the form of a proposition?
f. Does a BINDING exist for each term or phrase used in the CONCLUSION, REASONING, PREMISES, and (if any) DEFEATERS that does not have a well-known, unambiguous definition?
g. Does a proper BINDING exist for each reference to an external artifact?

One way to answer the **P** question is to answer these additional questions:

a. Is each PREMISE BELIEVABLE? To be BELIEVABLE it must fall into one of these categories:
    (a) expresses a proposition that is 'universally' accepted as true
    (b) expresses a proposition that is accepted as true within the relevant domain
    (c) is supported by an ARGUMENT (provisionally presumed to be COGENT)
    (d) is supported by external artifacts that are accepted within the domain as being sufficient to establish its truth
    (e) will fall into category (c) or (d) at a later stage of ARGUMENT development
    (f) is an assumption accepted by all stakeholders and clearly identified as such
b. Is each PREMISE relevant to the CONCLUSION?

One way to answer the **R** question is to answer these additional questions:

a. Is the REASONING relevant?
b. Is the REASONING consistent with current knowledge?

One way to answer the **S** question is to answer these additional questions:

a. Is the required level of confidence known?
b. Does the ARGUMENT engender the required level of confidence?

One way, but not the only way, to assess the COGENCY of a COMPOUND ARGUMENT is to apply iTest.

Applying iTest involves completing the following steps:

I. **Isolate** ONE ATOMIC ARGUMENT.

II. **Interrogate** it as an ATOMIC ARGUMENT using the SPRY questions.

III. **Iterate** until all ATOMIC ARGUMENTS have been assessed.

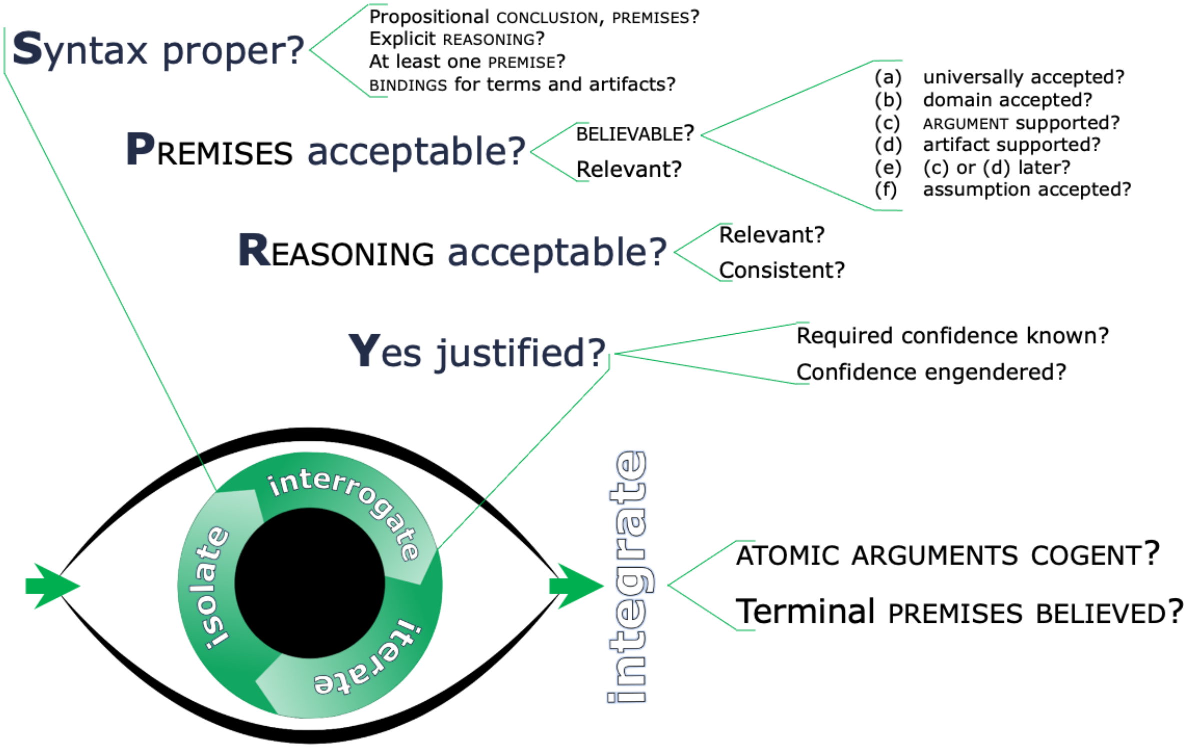
IIII. **Integrate** the individual assessments by answering these questions:
    A. Are all ATOMIC ARGUMENTS assessed as COGENT?
    B. Does every path through the COMPOUND ARGUMENT terminate in believed PREMISES?

One way, but not the only way, to propagate the effect of non-COGENT ATOMIC ARGUMENTS on a COMPOUND ARGUMENT is to follow these five steps:

1. For each non-COGENT ATOMIC ARGUMENT, list its CONCLUSION.
2. For each listed CONCLUSION, find all ATOMIC ARGUMENTS for which it serves as a PREMISE. Note that each such PREMISE will have been identified as falling into BELIEVABILITY category (c).
3. Change the PREMISE'S BELIEVABILITY from category (c) to "No."

4. Reassess the COGENCY of the ARGUMENT in which the PREMISE appears.
5. Repeat until no new non-COGENT ARGUMENTS are revealed.

Readers who prefer graphical depiction of information over purely textual ones may prefer the following summary:



Appendix B. List of Bindings

This appendix serves as a reference for both content and form. That is, these are all of the BINDINGS used in this document, in one place for reader reference. This is also an example of how an applicant might consider providing such information.

Within an ARGUMENT, BINDINGS may be presented as they occur. Here, BINDINGS are presented alphabetically for ease of retrieval.

The following list comprises the BINDINGS used throughout the construction demonstration portion of this document.

<Correctness>: The <implementation> is correct with respect to its defined intended behavior, under <foreseeable operating conditions> [1]

<Correct-wrt-DIB>: <implementation> is shown through acceptable methods to meet specified satisfaction criteria ABC

<DeB>: desired behavior [1]

<DIB>: defined intended behavior [1]

<fit for verification purpose>: demonstrated to have properties X and Y (which must eventually be named and would derive from current ML research)

<foreseeable operating conditions>: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions [1]

<Implementation>: item or combination of inter-related items for which acceptance or approval is being sought [1]

<Innocuity>: Any part of the <implementation> that is not required by the defined intended behavior has no unacceptable impact [1]

<Intent>: The defined intended behavior is correct and complete with respect to the desired behavior [1]

<MDSS>: Maneuver determination subsystem as defined by specified development artifacts (which must eventually be named)

<MDSS verification plan>: (the real-world document, which must eventually be named)

<MDSS verification report>: (the real-world document, which must eventually be named)

<Overarching Properties>: properties as defined in [1]

Appendix C. Exercise 5 as completed by Ashley

For recording the application of iTest Ashley used the same notational conventions used in Appendix B of *A Primer on Argument Assessment* [4]. This convention is based on numbering ATOMIC ARGUMENTS according to the order in which they are assessed, identifying iTest steps using its own roman numeral scheme, and identifying the SPRY questions by the appropriate S-P-R-Y and lower-case letter.

Ashley began the assessment of Exercise 5's ARGUMENT by Isolating the top-level ATOMIC ARGUMENT and recording the work as shown below. All text except that enclosed within square brackets is text produced by Ashley.

I. **Isolate** ARGUMENT 1 - the ARGUMENT for {pOPs}.

```
Believing
    <MDSS> possesses the <Overarching Properties>  {pOPs}

is justified by applying
    conjunction

to these premises
    <MDSS> possesses <Intent>      {pIntent}
    <MDSS> possesses <Correctness> {pCorrectness}
    <MDSS> possesses <Innocuity>   {pInnocuity}
```

II. **Interrogate** using SPRY questions.

1 S: Yes. The syntax is proper because the answers to all questions S.a – S.g are affirmative.

1 P.a: Yes. All PREMISES are in BELIEVABILITY category P.a.(c).

1 P.b: Yes. All PREMISES are relevant.

1 R.a: Yes. By convention (b) `conjunction` is relevant REASONING.

1 R.b: Yes. By convention (b) `conjunction` is consistent with current knowledge and with the OP constraints.

1 Y.a: Yes. By convention (a) the required level of confidence is known.

1 Y.b: Yes. By the reasoning explained in {UtOPs}, showing possession of the three properties engenders the required level of confidence

1 Assessment: The ARGUMENT for {pOPs} is **COGENT**, subject to the COGENCY of the ARGUMENTS for {pIntent}, {pCorrectness}, and {pInnocuity}.

[Ashley decided to isolate the ARGUMENT for {pIntent} for the next iteration. You may have made a different choice. No choice is wrong. For this iteration and this one only Ashley also used the same graphic from Appendix B to denote the second isolated ATOMIC ARGUMENT.]

III. Iterate and **I. Isolate** ARGUMENT 2 - the ARGUMENT for `pIntent`.

```
Believing {pIntent}
    <MDSS> possesses <Intent>

is justified by applying
    The definition of <Intent>

to these premises
    <MDSS> <DIB> is correct with respect to its <DeB>   {DIBcorrect}
    <MDSS> <DIB> is complete with respect to its <DeB>  {DIBcomplete}
```

II. Interrogate using the SPRY questions.

2 S: Yes. The syntax is proper.

2 P.a: Yes. Both PREMISES are in BELIEVABILITY category P.a.(c).

2 P.b: Yes. Both PREMISES are relevant as they simply encapsulate the definition from {UtOPs}.

2 R.a: Yes. Unpacking a definition is relevant REASONING.

2 R.b: Yes. Unpacking a definition is consistent with current knowledge and with the OP constraints.

2 Y.a: Yes. By convention (a) the required level of confidence is known.

2 Y.b: Yes. Showing that both parts of a definition are satisfied justifies BELIEVING the definition is satisfied (assuming the definition is not internally inconsistent or incoherent[33]).

2 **Assessment:** The ARGUMENT for {pIntent} is **COGENT**, subject to the COGENCY of the ARGUMENTS for {DIBcorrect} and {DIBcomplete}.

[Ashley decided to isolate next the ARGUMENT for {pCorrectness}. You may have chosen differently, for example selecting the ARGUMENT for {DIBcorrect}. Both you and Ashley made reasonable choices. The same freedom of choice applies to the rest of the assessment, but we will not repeat it anymore.

From this point forward, Ashley began using shortcuts to record the assessment results.]

[33] Because the phrases ‘complete with respect to’ and ‘correct with respect to’ are well-established and accepted as consistent and coherent within the aviation community, no good purpose would be served in this paper by delving into a discussion about the philosophical impossibility of completeness. So, delve we shall not.

III/ I 3 - ARGUMENT for pCorrectness.

```
Believing {pCorrectness}
    <MDSS> possesses <Correctness>

is justified by applying
    The definition of <Correctness>

to these premises
    <MDSS> <implementation> is correct with respect to its <DIB> {ImpcrtDIB}
    <Foreseeable operating conditions> are accounted for in the <DIB> {FOCinDIB}
```

II. 3

3 S: Yes.

3 P.a: Yes. BELIEVABILITY category P.a.(c) for both PREMISES.

3 P.b: Yes. 'Tis a reasonable decomposition of the definition.

3 R.a: Yes.

3 R.b: Yes.

3 Y.a: Yes. By convention (a).

3 Y.b: Yes.

3 **Assessment:** The ARGUMENT for {pCorrectness} is **COGENT**, subject to the COGENCY of the ARGUMENTS for {ImpcrtDIB} and {FOCinDIB}.

III/I 4 - ARGUMENT for pInnocuity

```
Believing {pInnocuity}
    <MDSS> possesses <Innocuity>

is justified by applying
    The definition of <Innocuity>

to these premises
    Every part of <MDSS> <implementation> is required by <DIB> {impReq}
```

II. 4

4 S: Yes.

4 P.a: Yes. Presumed to fall into BELIEVABILITY category P.a.(e) at this stage of ARGUMENT construction.

4 P.b: Yes.

4 R.a: Yes. By definition, the definition of a property is relevant to whether it is possessed.

4 R.b: Yes.

4 Y.a: By convention (a).

4 Y.b: Yes. If there is no part of the <implementation> that is "not required by the {DIB}", then there is no part of the <implementation> for which a separate showing of "no <unacceptable impact>" is needed.

4 **Assessment:** The ARGUMENT for {pInnocuity} is **COGENT**, subject to the future elaboration of a COGENT ARGUMENT for {impReq}.

III/I 5 - ARGUMENT for `DIBcorrect`

```
Believing {DIBcorrect}
    <MDSS> <DIB> is correct with respect to its <DeB>

is justified by applying
    conjunction

to these premises
    BelProp1
    BelProp2
```

II. 5

5 S: Yes.

5 P.a: Yes. By convention (c) `BelProp1` is in BELIEVABILITY category P.a.(a). By convention (d) `BelProp2` is in BELIEVABILITY category P.a.(b).

5 P.b: Yes. By conventions (c) and (d), the PREMISES are relevant.

5 R.a: Yes. By convention (b).

5 R.b: Yes. By convention (b).

5 Y.a: Yes. By convention (a).

5 Y.b: Yes. By convention (b).

5 **Assessment:** The ARGUMENT for {pInnocuity} is **COGENT**.

III/ I 6 - ARGUMENT for `DIBcomplete`

```
Believing {DIBcomplete}
    <MDSS> <DIB> is complete with respect to its <DeB>

is justified by applying
    Reas1

to these premises
    Assu7
    BelProp3
```

II. 6

6 S: Yes.

6 P.a: Yes. By convention (e) `Assu7` is in BELIEVABILITY category P.a.(f). By convention (d) `BelProp3` is in BELIEVABILITY category P.a.(b).

6 P.b: Yes. By conventions (d) and (e), the PREMISES are relevant.

6 R.a: Yes. By convention (b).

6 R.b: Yes. By convention (f).

6 Y.a: Yes. By convention (a).

6 Y.b: Yes. By convention (f).

6 **Assessment:** The ARGUMENT for {DIBcorrect} is **COGENT.**

III/I 7 - ARGUMENT for `ImpcrtDIB`

```
Believing {ImpcrtDIB}
    <MDSS> <implementation> is correct with respect to its <DIB>

is justified by applying
    Reas8

to these premises
   Arti3
   Arti4
   Arti5
```

II. 7

7 S: Yes.

7 P.a: Yes. By convention (h), all three premises fall into P.a.(d).

7 P.b: Yes. By convention (h).

7 R.a: Yes. By convention (g).

7 R.b: No. By convention (g), which says that REAS8 is inconsistent with constraint C.e (the one about tiers).

7 Y.a: Yes. By convention (a).

7 Y.b: No. Because the answer to R.b is negative.

7 **Assessment:** The ARGUMENT for {ImpcrtDIB} is **not COGENT.**

III/ I 8 - the ARGUMENT for FOCinDIB

```
Believing {FOCinDIB}
    <Foreseeable operating conditions> are accounted for in the <DIB>

is justified by applying
    Reas2

to this premise
    The <DIB> accounts for everything in <prevFOC> {DIBprevFOC}

with
    <prevFOC>: the collection of <foreseeable operating conditions>
               developed for the predecessor to <MDSS>
```

II. 8

8 S: Yes.

8 P.a: Yes. With the assumption that the PREMISE falls into category P.a.(e).

8 P.b: Yes. [Ashley properly understands that without knowing the precise contents of <prevFOC>, assessing this PREMISE as *irrelevant* would be inappropriate. By itself it is clearly *insufficient*, but sufficiency is assessed with the Y questions, not the P questions.]

8 R.a: Yes. By convention (f).

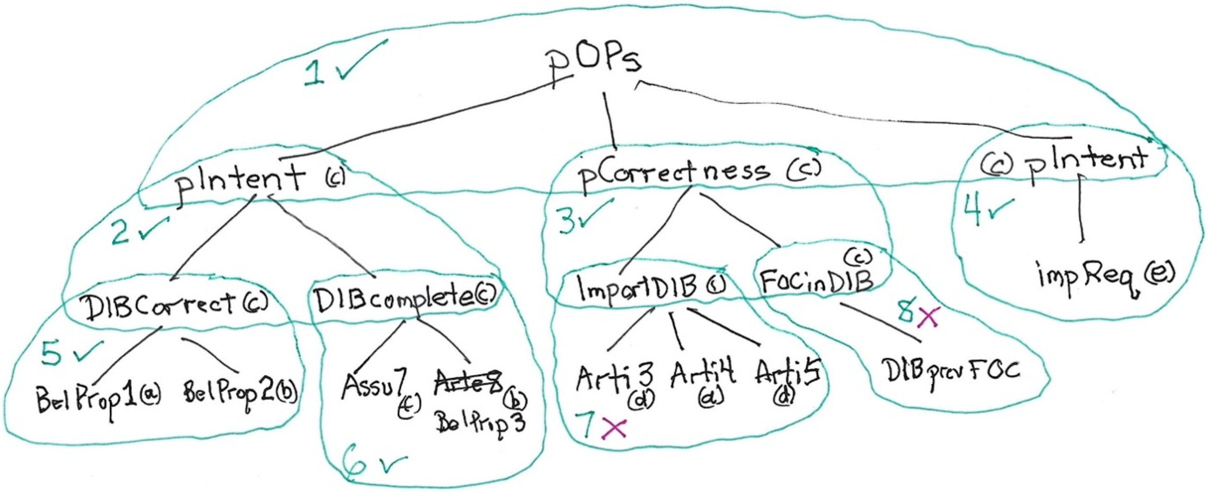
8 R.b: Yes. By convention (f).

8 Y.a: Yes. By convention (a).

8 Y.b: No. The argument does not explain the relationship between <prevFOC> and the <foreseeable operating conditions> for <MDSS>.

8 **Assessment:** The ARGUMENT for {FOCinDIB} is **not COGENT.**

[In honor of Ashley's former boss, Leslie, who preferred graphics over words, Ashley drew a rough diagram to explain the results so far.]



IIII. Integrate ATOMIC ARGUMENT assessments.

A. Are all ATOMIC ARGUMENTS assessed as COGENT?

No. ARGUMENT 7 and ARGUMENT 8 are assessed as not COGENT. ARGUMENT 7 is assessed as having unknown COGENCY.

[Ashley's numbering scheme for the steps comes from the description of steps in section 3.2.1 of [4] for propagating non-COGENCY.]

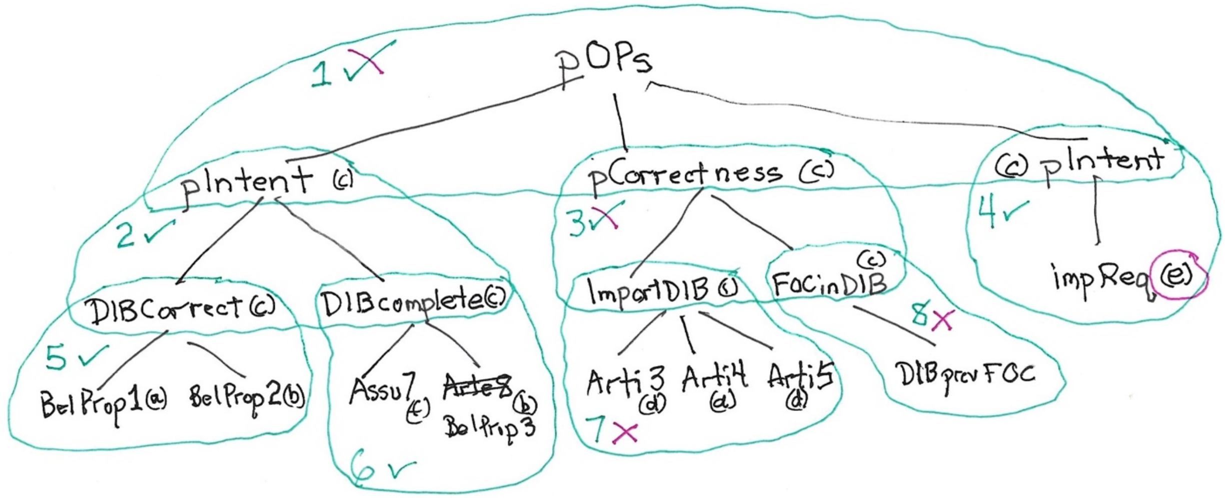
1. ARGUMENT 7 CONCLUSION is ImpcrtDIB
2. ImpcrtDIB is a PREMISE in ARGUMENT 3
3. Change ImpcrtDIB BELIEVABILITY category from (c) to "No"
4. This changes ARGUMENT 3's assessment from COGENT to non-COGENT.

1. ARGUMENT 8 CONCLUSION is FOCinDIB
2. FOCinDIB is a PREMISE in ARGUMENT 3
3. Change FOCinDIB BELIEVABILITY category from (c) to "No"
4. ARGUMENT 3's assessment has already been changed to non-COGENT.

5. Next iteration

1. ARGUMENT 4 CONCLUSION is `pCorrectness`
2. `pCorrectness` is a PREMISE in ARGUMENT 1
3. Change `pCorrectness` BELIEVABILITY category from (c) to “No”
4. This changes ARGUMENT 1’s assessment from COGENT to non-COGENT.

[For Leslie, Ashley shows the following drawing.]



B. Does every path through the COMPOUND ARGUMENT terminate in BELIEVED PREMISES?

This question does not have to be asked for the non-COGENT ARGUMENT in exercise 5. But if it is asked, the answer is Not Yet.. ARGUMENT 4 has a sole premise; it is in BELIEVABILITY category (e), which is appropriate only during ARGUMENT construction

C. Are all OP constraints satisfied?

No. One of the reasons the ARGUMENT is not COGENT is that ARGUMENT 7 (the one for `ImpcrtDIB`)uses REASONING that violates constraint C.e.