

False Beliefs about the Overarching Properties and Overarching Properties Related Arguments

C. Michael Holloway
Safety-Critical Avionics Systems Branch
NASA Langley Research Center
Hampton, Virginia, U.S.A.
c.michael.holloway@nasa.gov
last modified: 2022-06-08 (08:00)

Abstract—False beliefs about new ideas are not new. They happen all the time, for a wide variety of reasons. Although the Overarching Properties are solidly grounded in time-honored principles, they constitute a novel expression of those ideas, and newness-based false beliefs about them are to be expected. Similarly, although Overarching Properties Related Arguments are solidly grounded in thousands of years of study of the principles of argumentation, they introduce concepts and applications that are novel to many engineers and engineering managers. So, false beliefs about them are also to be expected. Indeed, false beliefs have arisen and are spreading in the wild about both the Overarching Properties and Overarching Properties Related Arguments. This paper seeks to dispel three known false beliefs about each concept.

Index Terms—assurance, argument, Overarching Properties, certification, authorities

I. PREFACE

The original paper describing the Overarching Properties (OPs, pronounced oh-peas, not awps or oh-pea-ess.) was published in 2019 [1]. It introduced the OPs as constituting a sufficient set of properties upon which approval decisions may be made. That is, if an entity (for example, a hardware or software subsystem) for which approval is sought can be shown to possess these properties in their entirety, then granting approval for using that entity on an aircraft is technically appropriate. Hence the name: *properties* because they encapsulate the “characteristic qualities” [2] necessary to justify approval; *overarching* because they are intended to “encompass all” [3] of the necessary properties. The paper described the properties in full, including the philosophical foundation on which they rest, but left for later days a discussion about how one might go about demonstrating that an entity truly possesses the OPs.

One, but not the only one, of those later days arrived in January 2022 with the publication of *An Introduction to Constructing and Assessing Overarching Properties Related*

Arguments (OPRAs) [4]. This paper introduced an approach to demonstrating and assessing property possession based on using explicit arguments. The arguments were named, quite naturally, Overarching Properties Related Arguments, with the convenient abbreviation OPRAs. The abbreviation may be pronounced either oh-prahs or op-rahs, depending on whether you want to allude to a talk show host or to highbrow music.

Both [1] and [4] were written based on work conducted in and for the Overarching Properties Working Group (OPWG, pronounced oh-pee-dubya-gee). Both were approved by the group before publication, and both list the names of significant individual contributors. However, [4] rests on foundations established in three additional papers, which were created without direct OPWG participation or approval [5]–[7].

As originally conceived, the intended audience for this paper consisted only of people already familiar with both the OPs and OPRAs. On further reflection, restricting the audience so tightly seemed inappropriate for a conference with as large and diverse an attendee population as DASC. To remove the restriction, this paper includes background material about the OPs, arguments in general, and OPRAs intended to enable someone without previous knowledge of those topics to read it without being entirely lost. The truly interested reader will still want to consult the defining documents to fill in details, but this paper should mostly make sense without that consultation in advance.

II. INTRODUCTION

In one sense the Overarching Properties are not new. Rather they are solidly grounded in time-honored principles, which decades of practice within the aviation industry have determined are necessary to ensure safe systems. In another sense, however, the Overarching Properties are new. Specifically, they represent a novel expression of these accepted principles. Because of this novelty, false beliefs about the OPs are to be expected.

Although the meaning of the phrase ‘false beliefs’ is straightforward, its use may be jarring to some readers, who may not be accustomed to seeing the word *beliefs* used in relation to technical subjects. To any such readers I ask you to trust me that there exists a compelling (but not short enough to include in this paper) justification for why the

The work on which this paper is based has been sponsored in part by the Federal Aviation Administration through Interagency Agreements: IA1-1073, Annex 2: Assurance Case Applicability to Digital Systems; IA1-30333, Annex 1: Streamlining Assurance Via Overarching Properties (Savor); and IA1-30333, Annex 2: Using the Overarching Properties in Novel Examples (Opine). Nothing written here, however, should be considered to represent the official views of the FAA, NASA, or the Overarching Properties Working Group.

word is not only appropriate but precisely correct. I also invite you to mentally substitute whatever word or phrase suits you better whenever you encounter the phrase. Perhaps *misunderstandings* or *misconceptions* or both will do the trick.

Similarly, the concept of Overarching Properties Related Arguments is not new, in that it is solidly grounded in thousands of years of study of the principles of argumentation. In another sense, however, OPRAs are new, in that many engineers and engineering managers have encountered principles of argument only in passing, if at all. Also, the specific application of the principles to OPs is novel. Thus, false beliefs about OPRAs are also to be expected.

Indeed, false beliefs have arisen about both the Overarching Properties and Overarching Properties Related Arguments. The purpose of this paper is to dispel three observed false beliefs about each¹. Dispelling these false beliefs is important for at least three reasons: (1) the full potential of the OPs and OPRAs can be realized only if everyone is working from the same foundation; (2) propagation of falsehoods may enable influential critics to cause further research and experimentation to cease prematurely; and (3) truth should always be preferred over falsity, perhaps especially so in times like these.

The structure of the remainder of this paper is as follows. Section III provides an overview of the OPs. Readers who truly know all about the OPs can skip it without fear of missing any vital information. Section IV tackles three false beliefs about the Overarching Properties. For each false belief, the paper will explicate the belief, speculate briefly about possible causes for it, and articulate a countervailing true belief. Section V provides an overview of the concepts involved in OPRAs. Readers who already know all about OPRAs can skip it without fear of missing anything important. Section VI tackles three false beliefs about OPRAs. Finally, section VII wraps everything up by collecting all six countervailing true beliefs.

In neither section IV nor section VI will citations be made to any papers or presentations expressing any of the false beliefs. This is for two reasons. First, the purpose of this paper is to clarify the misunderstandings or misconceptions not to condemn or embarrass anyone who holds them. Second, some of the false beliefs have been expressed so far only in conversations or unpublished presentations for which no citation is possible.

III. ABOUT THE OVERARCHING PROPERTIES

This section presents a summary of the Overarching Properties. It begins by explaining a bit of history and then proceeds to presenting the essentials of the OPs.

A. History

What we now call the Overarching Properties originated in a workshop in December 2015 sponsored by the Federal Aviation Administration (FAA). The FAA selected the invitees

¹Let's make it four false beliefs about OPs. One trivial false belief that has reared its head recently is that the abbreviation for Overarching Properties is OaP (or OAP). How this false belief came about is difficult to understand, because it is refuted in the second paragraph of [1].

to this workshop, seeking to ensure industry and governmental participation from across a wide area of technical disciplines, countries, and assurance viewpoints. The goal of the workshop was to seek to generalize existing assurance objectives for software, hardware, and systems containing both into a small set of what were initially called "meta-objectives." The effort continued with two more invitation-only in-person meetings in April and July 2016, periodic virtual meetings, and the use of an online forum, culminating in a set of three, as they were now more appropriately named, Overarching Properties.

These OPs were presented to the public at the 2016 FAA Streamlining Assurance Processes Workshop, which was held September 13–15, 2016, in Richardson, Texas. Workshop participants expressed opinions across a wide spectrum ranging from (to use slang appropriate to the location) "madder than a wet hen" to "ready and rarin' to go." A sufficient number (and percentage) of opinions were positive that the decision was made to continue the work. Virtual meetings and forum activity continued through the remainder of 2016, resulting in some relatively minor changes to the OPs.

In early 2017 the team was dubbed the Overarching Properties Working Group (OPWG). Most of the work throughout 2017 and 2018 involved trying to develop a collection of criteria for use in evaluating OPs possession, with the intent of publishing a single document describing the OPs and the possession criteria. However, the results of several case studies completed in 2018 identified deficiencies in criteria based approaches. Consequently, the OPWG decided to publish a description of the Overarching Properties alone. A few minor changes were made during a meeting of the group in April 2019, leading a few months later to the publication of [1].

B. Description

This section provides a rapid introduction to the details of the Overarching Properties as they were described in the defining document. The description is divided into labeled property statements, definitions, requisites, assumptions, and constraints. The meaning of the properties is fully described by the three property statements (not including the labels) and the eight definitions.

Labeled Property Statements

The property labels (Intent, Correctness, and Innocuity) do not affect the meaning of the properties in any way. The labels were created only for convenience of reference. For example, the meaning of the property labeled 'Intent' would not change if we replaced 'Intent' with 'A,' 'Drumstick,' 'Property One,' or even 'Correctness.' Correctness would be a very unwise replacement, almost as unwise as the decision years ago to label as 'derived requirements' precisely those requirements that are most certainly *not* derived from higher-level requirements, but it wouldn't change the actual meaning of the property. Here are the statements as they appear in [1]:

- a. **Intent:** The **DEFINED INTENDED BEHAVIOR** is correct and complete with respect to the **DESIRED BEHAVIOR**.

- b. **Correctness:** The **IMPLEMENTATION** is correct with respect to its **DEFINED INTENDED BEHAVIOR**, under **FORESEEABLE OPERATING CONDITIONS**.
- c. **Innocity:** Any part of the **IMPLEMENTATION** that is not required by the **DEFINED INTENDED BEHAVIOR** has no **UNACCEPTABLE IMPACT**.

The meaning of words and phrases shown **LIKE THIS** (for example, **DESIRED BEHAVIOR** and **DEFINED INTENDED BEHAVIOR**), must not be assumed based on prior experience, nor by considering the meaning of the individual words in the phrases. Rather the meaning of such words and phrases is explicitly given in a definitions section replicated here:

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 **ITEMS** 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.” [8]

In [1] these definitions are explained in detail. For this paper, I will only write a little bit more about two of them: **DESIRED BEHAVIOR** and **DEFINED INTENDED BEHAVIOR**. **DESIRED BEHAVIOR** is the term we chose to give to the needs and constraints expressed by the stakeholders. Crucially, these needs and constraints must include those identified by safety assessment and regulations. **DEFINED INTENDED BEHAVIOR** is the phrase used for the written down expression of the needs and constraints².

²Nearly everyone shortens **DEFINED INTENDED BEHAVIOR** to DIB. Thus far, no one but me shortens **DESIRED BEHAVIOR** to DeB.

Some readers are likely wondering why we did not use more familiar words such as ‘requirements’ and ‘specifications’. To paraphrase the discussion of the issue in [1], we chose to not use common but overloaded terms such as requirements, validation, or verification, to combat the natural tendency of people to subconsciously ignore explicitly provided definitions in favor of relying on their own internal definitions instead. We hoped that eschewing ambiguous common terms would increase the likelihood that people would read and rely on the explicit definitions, but ’tis not entirely clear to what extent the hope has been realized.

The statements and definitions fully define the Overarching Properties. The remaining sections of the description—requisites, assumptions, and constraints—only affect the means by which property possession may be shown (see subsection IV-A for additional discussion).

Requisites enumerate things that must exist to allow the showing of 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 **FAILURE CONDITION** classifications exist.

Assumptions 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 directly circumscribe 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**.

This concludes the rapid overview of the OPs. We move on to refuting three false beliefs that have arisen about them.

IV. FALSE BELIEFS ABOUT THE OVERARCHING PROPERTIES

False beliefs concerning the Overarching Properties sprang up during the initial public unveiling of them, and have continued to this day. The publication of [1] quashed some of the false beliefs among some people, but not others. Three false beliefs that are still out there are as follows:

- The constraints alter the *meaning* of the OPs.
- The OPs are intended to be *a means of compliance by themselves*.
- The OPs must be used in an *all or nothing* fashion.

Each of these is explained and refuted below. Readers are reminded that neither the labeling of the belief as false, nor its explanation, nor its refutation should be considered to express the collective opinions of the OPWG, FAA, or NASA.

A. False: The constraints alter the meaning of the OPs

One of the most pervasive false beliefs about the Overarching Properties is that the constraints section of the description contributes to the meaning of the properties. This belief persists despite explicit text in [1] saying otherwise:

Only two of the five parts are strictly necessary: *statements* and *definitions*. That is, the meaning of each Overarching Property is fully specified by the statement of the property as interpreted according to the relevant definitions. (p. 7)

Constraints ... apply directly and only *to the means by which OP possession may be demonstrated*. That is, they constrain what is considered a legitimate demonstration, but without changing the meaning of the OPs in any way (p. 16)

Why does this false belief persist despite foundational text refuting it? I believe the most likely reason³ arises from the underlying opinions that led to the constraints being written in the first place. I will explain by simplifying the convoluted and occasionally contentious history.

In the early days of the creation of the OPs, deep and wide differences existed among participants concerning how tightly to couple the OPs to existing practices and knowledge. On one side were those who sought solely to use existing knowledge to generalize existing practice. On the other side were those who sought to incorporate existing knowledge and practice while

also making provisions for future advances in knowledge and practice to be accommodated without requiring changes to the properties.

In one meeting in 2016, the differences between the sides seemed certain to derail the entire effort forever. As an attempt to keep the effort on the tracks, a couple of folks proposed the notion of constraints on how possession of the OPs could be shown. Under this proposal, which after some discussion was enthusiastically adopted, the OPs would be written generally (so as to endure for a long time no matter how much more advanced knowledge and practice becomes), and the constraints would be written to encapsulate existing limits imposed by current practice and knowledge (with the recognition that advances might one day enable some constraints to be removed or changed). This compromise led to the OPs description you see today.

Although [1] clearly explains the results of this happy compromise, as the quoted text above shows, it does not explain the reasoning that led to it. Thus, someone who is unaware of the history may be predisposed by experience or natural inclination or both to assume that all parts of the OP description affect what the OPs mean. My own predisposition is to believe that this explains why the false belief continues to be held by some. But those who hold it should replace it with this true belief: The constraints have *no effect* on the meaning of the OPs.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? Because without it, the potential future flexibility of the OPs cannot be properly appreciated.

B. False: The OPs are intended to be a means of compliance by themselves

Another fairly common false belief about the Overarching Properties is that they are intended to be *a means of compliance in and of themselves*. This belief was first expressed at the public workshop in 2016 by a small, but vocal minority of attendees. We explained then that it was a false belief, and that more work was needed to figure out how to create an OP-based means of compliance. Similar statements were made in [1]. Nevertheless, the false belief has continued to be held by some to this day. At least two likely explanations for the persistence of this false belief are discernible.

One explanation is that Overarching Properties proponents, myself included, have not always been as careful with our language as we ought to be. For example, the title of a paper published in last year's conference [9] suggests (rather strongly) that the OPs can be a means of compliance. Nevertheless, the full paper is a bit more careful with terminology, explaining how the OPs are being used in a case study as the *foundation for* developing a possible new means of compliance. The work is ongoing, and greater precision is being used in the language concerning compliance.

Another, perhaps more likely, explanation for why some people continue in this false belief stems from the delay in publishing anything explaining the OPWG's position about

³To be fully transparent, there is a plausible reason for believing that one constraint (but only one) may alter the meaning of one of the OPs. Consider the (relatively) subtle interaction between constraint h ("The SAFETY ASSESSMENT must address all of the IMPLEMENTATION") and the definition a (for DESIRED BEHAVIOR), which includes "... this includes those needs and constraints identified by the SAFETY ASSESSMENT". A case can be made that the constraint on what the SAFETY ASSESSMENT must address necessarily contributes to the meaning of DESIRED BEHAVIOR, which thus necessarily affects the meaning of the property labeled INTENT. Suppose, without deciding, that the case is compelling enough to justify believing it. Then, the optimal response would be to rewrite the definition so as to make constraint h unnecessary, not to generalize an exception to supersede the general.

what a new means of compliance might look like. Almost three years passed between the publication of [1] and [4]. It is understandable that some folks might interpret this delay as signaling that nothing more would be said, and thus the OPs must be intended to be it.

The actual reasons for the delay are multi-faceted, but the main reason rests in the OPWG pursuing an approach that was eventually decided to be unworkable. Specifically, the group spent nearly two years trying to come up with a set of predefined criteria similar to DO-178 [10]-type objectives, the idea being that these criteria would have to be satisfied by someone wanting to use OPs. As noted the effort ultimately failed, as some of us suspected it would. The OPWG moved on to exploring argument-based approaches, as [1] suggested was likely.

Although the publication delay may have provided a plausible reason for thinking the OPs were intended to constitute a means of compliance themselves, the publication of [4] has eliminated the plausibility. The following quotation from the introduction suffices to do so:

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.

Given this refutation, any reader holding the false belief discussed here should replace it by the following true belief: The OPs are intended to provide *an organizing foundation from which* a means of compliance may be built.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? Because without it, a person is likely (and justifiably) to believe no future for the OPs exists within any aviation regulatory environment.

C. False: The OPs must be used in an all or nothing fashion

Another false belief about the Overarching Properties, and the last one we will discuss, is that they must be used in an all or nothing fashion. That is, if you have some entity for which you would be seeking approval, and you want to use an OPs-based approach for some aspects of it, you must use an OPs-based approach for everything related to that entity.

Although it is possible that an approval authority might one day choose to impose such a requirement on some specific project, there is nothing in the material produced so far under the auspices of the OPWG, or in any associated foundational documents, that implies such a thing is intended. In fact, the material clearly acknowledges the possibility of selected use of OPs. The "... or part thereof" from the quote above shows it, as does the running example throughout [4] concerning applying the OPs to a particular subsystem only.

Even without the textual refutations, imagining why this false belief exists is difficult. Neither the history nor tradi-

tion of approval authority behavior seems to compel such a belief. Nor does it comport with common sense. If existing approaches work well for some part of system, there is no reason to use something else. If existing approaches do not work well for some other part, and an OPs-based approach shows promise, then there is good reason for trying it on that part. (Assuming, of course, that the approval authority concurs.)

The true belief to replace this false one can be stated as follows: The OPs *may be used for a part of a system* while some other approach is used for other parts.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? Because without it, the costs of trying to use the OPs will seem excessive, except perhaps to brand new organizations without any established procedures.

V. ABOUT OVERARCHING PROPERTIES RELATED ARGUMENTS

This section presents a summary of relevant information about OPRAs⁴. In particular, it distills information from *A Primer on Argument* [6], *A Primer on Argument Assessment* [7], and *An Introduction to Constructing and Assessing Overarching Properties Related Arguments (OPRAs)* [4]. Because of the depth and breadth of the material covered in those documents, this summary is necessarily incomplete. It should be complete enough to enable the rest of the paper to be read and mostly understood on its own.

A. Argument terms

A Primer on Argument [6] identifies a collection of primitives, precepts, and practical considerations important for talking about ARGUMENTS. For our purposes the primitives (that is, the enumeration and definition of terms) is the crucial part. Here are the relevant definitions.

- An ARGUMENT is an attempt to convince others to BELIEVE a CONCLUSION through REASONING and one or more PREMISES.
- To BELIEVE is to accept as true.
- 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.
- A BINDING is an association between a term used in an argument and the real-world information to which that term refers.
- An ATOMIC ARGUMENT consists of a single CONCLUSION together with its immediate REASONING, PREMISES, and BINDINGS (if present).
- A COMPOUND ARGUMENT is an ARGUMENT consisting of more than one ATOMIC ARGUMENT.

⁴People who have previously read [4] and remain confident they continue to understand its content may wish to skip this section, moving immediately to Section VI.

- An ARGUMENT is called COGENT if it rationally justifies BELIEVING its CONCLUSION to the required standard of confidence.

B. Argument assessment

A *Primer on Argument Assessment* [7] explains one way to assess whether an ARGUMENT is COGENT. The assessment approach presented is generic; it is not tied to OPRAs, but can be applied to ARGUMENTS about anything. The approach has two primary components: the SPRY questions and iTest.

The SPRY questions for assessing the COGENCY of an ATOMIC ARGUMENT are as follows:

- S. Is the syntax proper?
- P. Are the PREMISES acceptable?
- R. Is the REASONING acceptable?
- Y. Is saying “Yes” to the CONCLUSION justified?

Each of these questions encompasses additional questions, the details of which are not necessary to include here.

The iTest procedure for assessing the COGENCY of a COMPOUND ARGUMENT is as follows:

- 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.
- IV. Integrate the individual assessments.

As with SPRY, iTest encompasses additional details that are not relevant for this paper.

C. OP-unique aspects

Tailoring of argument assessment to OPRAs is one of two main topics of *An Introduction to Constructing and Assessing Overarching Properties Related Arguments (OPRAs)* [4]. Only relatively minor additions and no deletions are needed to either the SPRY questions or iTest to accommodate assessing OPRAs. The other topic, as the title suggests, concerns how to construct OPRAs. Those details are not necessary for current purposes.

VI. FALSE BELIEFS ABOUT OPRAS

For Overarching Properties Related Arguments, the paper tackles these false beliefs:

- OPRAs must be created for *everything*.
- OPRAs are *based on formal logic*.
- Assessing the cogency of OPRAs is *necessarily too hard* to be practical.

Each of these is explained and refuted below. Readers are reminded that neither the labeling of the belief as false, nor its explanation, nor its refutation should be considered to express the collective opinions of the OPWG, FAA, or NASA.

A. False: OPRAs must be created for everything

This false belief about OPRAs is analogous to the previously discussed “all-or-nothing” false belief about OPs. It is equally pernicious, and perhaps more prevalent. A person who holds this false belief thinks that a decision to use an OPRA about one thing necessitates using OPRAs for everything else, even

when there exist already well-accepted non-argument-based approaches for demonstrating that thing.

I am not sure why some people hold this false belief. Perhaps it stems from prior exposure to overly complicated, elaborate “assurance cases” or “safety cases” in which standard techniques such as hazard analysis methods are forced into a particular argument-like notation. Whatever the reason for this false belief, it is easily shown to not apply. These two quotations suffice.

Although ARGUMENTS are subjectively cool and objectively useful for prompting thinking about why a particular CONCLUSION is BELIEVABLE, not everything needs to, or should, be expressed as an ARGUMENT. Rarely will a CONCLUSION that is part of the accepted body of knowledge within a discipline need to be justified by ARGUMENT. If it needs to be justified at all within a particular application, the already accepted approaches should usually be sufficient. [6] (p. 8)

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. [4] (p. 26)

For these reasons, the true belief is as follows: Overarching Properties Related Arguments are needed *only when OPRAs are needed*. That is, the principles that ARGUMENTS in general apply equally to OPRAs in particular.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? Because creating unnecessary OPRAs takes time and effort that can be better allocated elsewhere. Because having to assess the COGENCY of unnecessary OPRAs does, too. Because believing you have to put everything into an argument form is likely to be discouraging to applicants and regulators alike.

B. False: OPRAs are based on formal logic

The most surprising false belief that I have heard arose earlier this year in a rather large virtual meeting. A fellow expressed deep skepticism about whether the Overarching Properties would ever be used in practice because, “they require you to make arguments in formal logic.” There were others who agreed with this sentiment.

Holding such a belief is possible only if one has not read about OPRAs or the foundations on which they rest. For example, *A Primer on Argument* [6] states the following (footnotes included):

The study of argument differentiates CONCLUSIONS that can be proven through the application of for-

mal logic to sufficient PREMISES (deductive ARGUMENTS), and those that are in contrast BELIEVABLE through the application of any other type of reasoning (inductive ARGUMENTS)¹⁰. ... the ARGUMENTS with which we will concern ourselves are uniformly¹¹ inductive ARGUMENTS.

¹⁰ We are simplifying things a little bit here, as modern philosophers of logic often speak of additional categories or sub-categories such as analogical, explanatory, and defeasible ARGUMENTS. Most of the ARGUMENTS likely to be used in engineering applications would properly fit into the defeasible category. We shall not speak of this again.

¹¹ Note a COMPOUND inductive ARGUMENT might include occasional nested deductive ARGUMENTS, which does not CHANGE the fact that at the relevant level of abstraction, it is still an inductive ARGUMENT.

Equally fatal to this false belief is the fact that none of the examples of ARGUMENTS given in [7] and [4] are formal. Truthfully, without possibility of question, OPRAs are *based on informal logic*.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? Because informal logic corresponds more directly than formal logic to what people do naturally, and thus it will be typically easier to understand, and simpler to use in constructing OPRAs. In practice, many OPRAs may well turn out to be constructed by simply making explicit the implicit ARGUMENTS that are already used. Finally, assessing the COGENCY of non-deductive ARGUMENTS requires less mathematical training. None of which is to suggest assessment is easy, as we will discuss now.

C. False: Assessing the cogency of OPRAs is necessarily too hard to be practical

The precise wording of the final false belief was chosen carefully. With the adverb ‘necessarily’, the belief implies that we know beforehand without even trying anything that assessing the COGENCY of OPRAs will be too hard. Thus, there is no reason to give it a go.

Skepticism of this magnitude may stem from prior bad experiences, perhaps by being exposed to poorly constructed, impossible to understand, overly complicated “assurance cases.” The skepticism may also stem from lack of exposure to informal argumentation, or from being exposed to it only through the eyes of radical formalists. Whatever the causes of the skepticism, the current state of efforts in this area refute it.

The initial reception to the SPRY questions and iTest has been uniformly positive. Thus far, no reason has surfaced to doubt the possibility that these techniques will turn out to be a practical way to assess the COGENCY of OPRAs.

More importantly case studies and pilot projects with approval authority participation are ongoing, some with existing or planned publications, others being conducted in a proprietary way. The one such case study with which I am deeply familiar remains promising, and good things are being said, but

not yet published, about some of the others. Not all of these use OPRAs exactly as we have defined, but all are based on the same general concept.

Consequently, the skepticism expressed by the false belief is not warranted. It should be replaced with this belief: Assessing the COGENCY of OPRAs is *not necessarily too hard to be practical*.

Besides the *truth > falsity* principle, why does holding a true belief on this matter matter? This is the simplest of the six instantiations of the question to answer. Because holding a false belief on this matter results in giving up. Rather than giving up, we want to continue to give it a go.

VII. CONCLUDING REMARKS

This paper discussed the Overarching Properties, Overarching Properties Related Arguments, and false beliefs about both. For each false belief, a true belief was provided. Here are all six of these true beliefs:

- The constraints have *no effect* on the meaning of the Overarching Properties.
- The Overarching Properties are intended to provide an *organizing foundation* from which a means of compliance may be built.
- The Overarching Properties *may be used for a part of a system* while some other approach is used for other parts.
- Overarching Properties Related Arguments are needed *only when OPRAs are needed*.
- Overarching Properties Related Arguments are *based on informal logic*.
- Assessing the cogency of Overarching Properties Related Arguments is *not necessarily too hard to be practical*.

The truth of these beliefs, and the corresponding falsity of their negatives as shown above, justifies ending this paper by quoting the final sentence of [1]: “A promising future for the OPs appears plausible.”

ACKNOWLEDGMENT

In previous papers I have acknowledged many of the essential contributors to the Overarching Properties work, from its initial conception by the incomparable Mike DeWalt to its current state. Here, I want to thank my co-author on three of the foundational papers, Kim Wasson, who is a brilliant thinker, careful writer, and since Kelly Hayhurst’s retirement in 2018, my closest professional friend. I also want to thank my student interns in 2020-2022 for their insightful comments, helpful suggestions, and (most importantly) for helping me to feel from time to time a bit less old than I am: Sydney Filler, Katelyn Crockett, Marie-Helena Peeters (2 summers), Asha Maran, Angelica Bonilla (2 semesters), and Abel Peña.

REFERENCES

- [1] C. M. Holloway, “Understanding the overarching properties,” Technical Memorandum NASA/TM-2019-219650, available at <https://ntrs.nasa.gov/citations/20190029284>, National Aeronautics and Space Administration, Hampton, VA, USA, July 2019.
- [2] “property, n.” OED Online. March 2022. Oxford University Press.
- [3] “overarching, adj.” OED Online. March 2022. Oxford University Press.

- [4] K. S. Wasson and M. Holloway, "An introduction to constructing and assessing overarching properties related arguments (OPRAs)," white paper, available at <https://ntrs.nasa.gov/citations/20210025425>, NASA Langley Research Center, January 2022.
- [5] C. M. Holloway, "The friendly argument notation (FAN)," Technical Memorandum NASA/TM-2020-5002931, National Aeronautics and Space Administration, Hampton, VA, USA, June 2020.
- [6] C. M. Holloway and K. S. Wasson, "A primer on argument," white paper, available at <https://ntrs.nasa.gov/citations/20210019993>, National Aeronautics and Space Administration, Hampton, VA, USA, June 2021.
- [7] C. M. Holloway and K. S. Wasson, "A primer on argument assessment," white paper, available at <https://ntrs.nasa.gov/citations/20210022807>, National Aeronautics and Space Administration, Hampton, VA, USA, October 2021.
- [8] European Aviation Safety Agency, "AMC 20-115C software considerations for certification of airborne systems and equipment," available at [http://easa.europa.eu/system/files/dfu/annexEuropean Aviation Safety Agency](http://easa.europa.eu/system/files/dfu/annexEuropean%20Aviation%20Safety%20Agency.pdf), December 19 2013.
- [9] Z. Daw, S. Beecher, M. Holloway, and M. Graydon, "Overarching properties as means of compliance: An industrial case study," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, pp. 1–10, Oct 2021.
- [10] RTCA, "DO-178C: Software considerations in airborne systems and equipment certification." RTCA, Inc., Washington DC, USA (Also published as EUROCAE ED-12C), 2011.