DOT/FAA/TC-xx/xx

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Understanding the Overarching Properties: First Steps

September 2018

Final Report (Limited Release)

This document is currently under publication review and will be available to the U.S. public through the National Technical Information Services (NTIS), Springfield, Virginia 22161.

U.S. Department of Transportation

NOT FAA POLICY OR GUIDANCE - LIMITED RELEASE DOCUMENT

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

Disclaimer: This document is a draft deliverable of the research. This draft report is being made available as a “Limited Release” document by the FAA Software and Digital Systems (SDS) Program and does not constitute FAA policy or guidance. This document is being distributed to selected organizations only with express written permission by the Contracting Officer’s Technical Representative (COTR). The research information in this document represents only the viewpoint of authors.

The FAA is concerned that its research does not get released to outside-FAA organizations before proper and full review is completed. However, a Limited Release distribution under select conditions does allow immediate exchange of research knowledge in a way that will benefit the parties receiving the documentation and, at the same time, not damage perceptions about the quality of FAA research. When the FAA releases such research documentation, the FAA strives to insure that the receiver knows that the documentation is incomplete, limited in distribution, and should not further distribute without the express written permission by the COTR.

Technical Report Documentation Page

1. Report No.
DOT/FAA/TC-xx/xx

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Understanding the Overarching Properties: First Steps

5. Report Date
September 2018 (draft Pub)

6. Performing Organization Code

7. Author(s)
C. Michael Holloway

8. Performing Organization Report No.

9. Performing Organization Name and Address
NASA Langley Research Center, 100 NASA Road, Hampton VA 23681

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
IAI-1407

12. Sponsoring Agency Name and Address
Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport, NJ 08405

13. Type of Report and Period Covered
Draft report, under publication review, limited release

14. Sponsoring Agency Code
Barbara Lingberg, AIR-6B4

15. Supplementary Notes
The FAA William J. Hughes Technical Center Aviation Research Division Technical Monitors were John Zvanya and Srini Mandalapu.

16. Abstract

The Overarching Properties are the product of a multi-year, international effort to develop a minimum set of properties sufficient for use in the approval process. In other words, if an entity for which approval is sought is shown to possess these properties in their entirety, then granting approval for the entity to be used on an aircraft is warranted. The work is not finished.

This report explains the Overarching Properties as they are currently constituted, including the philosophical foundation underlying them, the specific text and meaning of each property, and the relationships the properties have to each other and to time. The report also discusses the remaining issues that must to be resolved in the future.

NASA Langley Research Center’s participation in the effort was supported in substantial part through an annex, “Streamlining Assurance Processes”, to a Reimbursable Interagency Agreement (Numbered IA-1407 by NASA and DTFAWA-14-C-00019 by the FAA), “Enhancement of Aeronautical Research and Technology Development”. C. Michael Holloway was the primary NASA person conducting the work, with occasional assistance from Patrick Graydon.

17. Key Words
Approval, assurance, certification, properties, philosophy

18. Distribution Statement
This document will be available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document will also be also available from the FAA William J. Hughes Technical Center at actlibrary.tc.faa.gov. Limited release.

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages

22. Price

(The document is paginated assuming 2-sided printing. Hence, some blank pages are included to provide a back side where needed.)

ACKNOWLEDGEMENTS

Mike DeWalt (the retired Chief Scientist and Technical Advisor for Software) motivated the effort resulting in the Overarching Properties. Barbara Lingberg and George Romanski (the current Chief Scientist and Technical Advisor for Software) kept it going after Mike left the scene. Srini Mandalapu provided program management support for the Interagency Agreement which partially funded NASA Langley Research Center’s involvement throughout. Thanks to all of you.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

None.

LIST OF ACRONYMS

ACE	assurance case evaluation
ALE	approved list evaluation
APE	applicant process evaluation
AVE	applicant varying evaluation
DeB	desired behavior
DiB	desired intended behavior
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
NASA	National Aeronautics and Space Administration
OPs	Overarching Properties

EXECUTIVE SUMMARY

The Overarching Properties are the product of a multi-year, international effort to develop a minimum set of properties sufficient for use in the approval process. In other words, if an entity for which approval is sought is shown to possess these properties in their entirety, then granting approval for the entity to be used on an aircraft is warranted. The work is not finished.

This report explains the Overarching Properties as they are currently constituted, including the philosophical foundation underlying them, the specific text and meaning of each property, and the relationships the properties have to each other and to time. The report also discusses the remaining issues that must to be resolved in the future.

NASA Langley Research Center's participation in the effort was supported in substantial part through an annex, "Streamlining Assurance Processes", to a Reimbursable Interagency Agreement (Numbered IA-1407 by NASA and DTFAWA-14-C-00019 by the FAA), "Enhancement of Aeronautical Research and Technology Development". C. Michael Holloway was the primary NASA person conducting the work, with occasional, always valuable, assistance from Mallory Graydon.

1. PRELUDE

The purpose of the Overarching Properties is to constitute a set of properties that are sufficient to warrant receiving approval for use on aircraft. That is, if an entity for which approval is sought possesses[1] these properties in their entirety, then granting approval is appropriate. They are called *properties* because they encapsulate the "characteristic qualities" [1] that a product must have to justify approval. They are called *overarching* because they "encompass all" [2] of the necessary properties.

The purpose of this document is to explain the Overarching Properties[2] as they currently exist, including their philosophical foundation, the specific details of each property, the relationships among them, and some practical considerations that attach to their use. Readers of this document are assumed to be at least somewhat familiar with current laws, regulations, and processes governing certification of airborne systems, software, and electronic hardware. Because the Overarching Properties are expressed at a much higher level of abstraction than is common today, however, readers *without* intimate knowledge of current practice may find understanding the Overarching Properties easier than readers with such knowledge. Readers of the document are also assumed to be aware that what is described herein is a work still in progress.

The document's structure is as follows. The remainder of this introduction presents some background information. §2 explains the philosophy underlying the Overarching Properties. The OPs themselves are then explained in detail in §3. Comments about issues that may arise in practice when the OPs are used are made in §4. The document concludes in §5 with brief speculative remarks about the future of the OPs.

1.1 BRIEF HISTORY

That which are now called the Overarching Properties originated in a workshop in December 2015. The workshop was sponsored by the Federal Aviation Administration (FAA), who selected the invitees to this workshop, seeking to ensure industry and governmental participation from across a wide area of technical disciplines, countries, and assurance viewpoints. The effort continued with two more invitation-only meetings in April and July 2016, periodic virtual meetings, and an online forum, resulting in a set of three Overarching Properties.

These OPs were presented to the public in September 13-15, 2016 at the 2016 FAA Streamlining Assurance Processes Workshop in Richardson, Texas. The Overarching Properties work was only one of the activities discussed, along with the other ongoing activities collected under the "streamlining assurance processes" banner. A handout containing the Overarching Properties was

[1] Two notes are appropriate here. First, henceforth for simplicity of expression the word *product* will be used as a shorthand for "an entity for which approval is sought." Second, the use of the word *possessed* instead of *satisfied* may strike some readers as odd. It is common in some circles to talk of 'satisfying' properties; such usage cannot be deemed wrong, but 'conditions' are better said to be 'satisfied' and 'properties' to be 'possessed'.

[2] The abbreviation *OPs* (pronounced "oh-peas") will be used in place of the full phrase from time to time, but not always, as it seems inappropriate in some sentences.

distributed to attendees without any additional printed explanatory material. To supplement the written material, oral presentations were delivered and several discussion sessions held.
Most workshop participants who expressed opinions about the OPs were favorable to the ideas as they understood them, with the level of enthusiasm ranging from tepid to euphoric. In the category of less-than-favorable comments, some participants expressed confusion over how the Overarching Properties work fits in with the other streamlining activities. In particular, these participants doubted that adopting a new certification regime based on the OPs would immediately, or perhaps ever, result in faster or cheaper certification. The response to these concerns was, and continues to be, that the FAA's streamlining activities are not just about reduced cost and time, but also about increasing flexibility without compromising safety, which is the emphasis underlying the Overarching Properties effort.

Other less-than-favorable comments came from participants who indicated a desire for substantially more details about how the OPs might be used in practice, especially questioning the feasibility of evaluating whether a product possesses the properties. Finally, the question was raised by a few attendees of whether the OPs as written were complete. The response to comments of these type was to acknowledge much work remained to be done.

To accomplish this remaining 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). New people joined the team, and some original team members left. Three physical meetings were held in 2017 (February, May, and September), with continuing virtual meetings throughout the year. The emphasis of the effort in 2017 was on addressing the question of evaluation. The evaluation approach pursued during this time involved the creation of a set of criteria. At first these criteria were considered to be a means by which assessors could determine whether a product possesses the OPs. Later, a switch in emphasis led to the criteria being considered as the set against which may be assessed the sufficiency of proposed processes for ensuring that a product possesses the OPs. Do not worry if this distinction seems unclear at this point; the issue of evaluation is discussed in more detail in §4.4.

The version of the Overarching Properties described in this document was finished during a physical meeting in February 2018, and refined slightly through July 2018. The changes from the version presented at the public workshop are mostly not substantial but rather subtle or editorial. The change in format from three separate pages, one for each property, to a single page is the most visible difference. Nevertheless, someone who last saw the OPs at the public workshop would recognize the version discussed here without difficulty.

1.2 PRESENTATION STYLE

This document is written in a conversational style, unlike the more formal styles usually employed in standards, guidance documents, and reports from some organizations. Two reasons motivate the choice. One, a conversational style is more likely to facilitate understanding by actively engaging the reader than is a formal style. Two, using a different writing style helps emphasize the fact that the Overarching Properties approach is substantially different in at least some respects from current approaches. The less a reader tries to make analogies between the OP approach and current approaches, the more likely he or she is to gain a correct understanding of what the Overarching Properties are all about[3].

Text from the Overarching Properties is displayed in sans-serif type. Words and phrases for which explicit definitions are an essential element of the OP are set in *italic sans-serif type*.[4] Quotations of more than a few words are set off from the surrounding text by paragraphs with slightly narrowed margins and a ragged right edge. Only the text thus displayed is normative. All other text is explanatory, instructive, or illustrative. Any apparent conflicts between the normative and non-normative parts are unintentional and should be identified for correction.

2. PHILOSOPHY

Before describing the Overarching Properties, some words are needed about the philosophy and associated principles upon which the properties are based. Hence, this section.

As a way to grasp the philosophy, the reader is invited to join in a thought experiment. Imagine, if you can, a world very much like our own, but different in one single, significant way. In this imaginary world—let's call it Earth* for ease of reference—a perfect oracle lives. Let's name this perfect oracle Quinn. Quinn is a *perfect* oracle because for any statement *P* with a truth value, if Quinn says that *P* is true, then *P* is true indeed; if Quinn says *P* is false, then *P* is false indeed.

Here are three trivial examples. If Quinn says it is raining hard outside, you need to take a sturdy umbrella with you when you leave the house. If Quinn says the dog doesn't bite, you can pet it without fearing for the physical integrity of your hand. And if Quinn says that the value of the Acme Corporation's stock will go up by 125% this year, then you should buy stock in Acme Corporation right away.

Moving to a more directly relevant example, suppose Quinn says that a particular product—software for an automated landing system, perhaps—is suitable for installation in an aircraft. In Earth* where Quinn is a perfect oracle, you can know for certain that the product is suitable. Thus, if you are charged with deciding to approve or disapprove the product, you can confidently approve it, without any fear of making the wrong decision. You don't even need to know what specific regulations the product satisfies[5].

Let's change the example a bit. Instead of Quinn stating directly that the product is suitable for installation on an aircraft, imagine that he makes an indirect conditional assessment like the following:

[3] A good analogy facilitates understanding; a bad one impedes it. Discouraging bad analogies motivated changing the original name ("meta-objectives"). The OPs are not in any useful sense similar to 'objectives' as that term is used in documents such as DO-178C [8].

[4] For added emphasis, a particular shade of blue is also used with the *italic sans-serif type*, but the color is not needed to make the necessary distinction.

[5] Just in case you are wondering, the regulations on our imaginary Earth* are identical to the regulations in our world. §4.1 and §4.3 briefly discuss, among other things, matters touching on the relationship between the OPs and real regulations.

```
If
    the product possesses the properties of Intent, Correctness, and Acceptability,
then
    the product is suitable for installation
else (that is, it does not possess the three properties)
     it is not.
```

Given Quinn's conditional statement, what must you know to warrant concluding the product is suitable for installation on an aircraft? You need to know whether the product possesses (a) the property of Intent, (b) the property of Correctness, and (c) the property of Acceptability. If you know it possesses all three, no matter what the properties mean, on our imaginary Earth* with the perfect oracle Quinn, then you also know the product definitely is suitable for installation on an aircraft, because Quinn has told you so.

To determine whether the product possesses these three properties on Earth* you need only to ask Quinn, in any order you like. Does the product possess Acceptability? Does it possess Intent? Does it possess Correctness? If he answers, "Yes," to all three questions, you can confidently approve the product. If he answers, "No," to one or more of the questions, you can confidently disapprove the product. You do not need to know anything at all about how the product was built, nor about the competency of its builders. You need no insight into the processes used in its development. You do not even need to know anything about the three properties themselves. Nor do you need to know anything about the regulations that govern the product. Not in the imaginary Earth* with the perfect oracle Quinn.

The real Earth has no Quinn; however, his non-existence does not invalidate the underlying principle:

> Given a set of properties that are sufficient to establish the suitability of a product for installation on an aircraft, a product that truly possesses all of the properties should be granted approval for installation.

Successfully applying this principle requires only knowing that (a) the set of properties is sufficient, and (b) a product possesses all of the properties.

The Overarching Properties rest on the assumption that they satisfy (a). To be more precise, they rest on the assumption that the text of the OPs, properly interpreted, specifies a sufficient set of properties; that is, no additional properties are needed. Or in other words, it is not possible for a product to truly possess the OPs, while also having deficiencies that should legitimately prevent it from being approved. A corollary of this assumption is the further assumption that the OP text is either unambiguous as to its meaning or, alternatively, that any ambiguities that exist resolve to equally permissible interpretations, all of which preserve sufficiency.

The word *assumption* is used in the previous paragraph because the sufficiency of the OPs has not yet been demonstrated conclusively. Because sufficiency is more a matter of practicalities than philosophy, further discussion of the issue is delayed until §4.3.

Concerning (b)—knowing that a product possesses all of the properties—the existing state of the practice does not allow certainty[6] (except perhaps for impractically simple cases). Whereas on Earth* insight into the processes used to develop a product is unnecessary, such insight is an important and essential aspect of current approval approaches. Adopting an approval process based on the Overarching Properties will not change the need for insight[7]. For a discussion about the steps being taken to help address the need, see §4.4 for more information, and a discussion of other possibilities for evaluation.

Keeping the fundamental difference between (a) and (b) clear is essential to understanding the rest of this document. A reader who does not keep the distinction clear runs the risk of conflating questions about the meaning of the OPs and questions about how to apply the OPs in practice. Both types of questions are important, but this document is intended to answer only questions of the first type.

3. PROPERTIES

We now are ready to discuss the three Overarching Properties themselves. The full description is shown in Figure 1; it consists of five parts:

- **Statements**: the three Overarching Properties themselves, including a label for each.
- **Definitions** for words or phrases used in the Overarching Properties description
- **Prerequisites** that must exist to allow Overarching Property possession to be shown
- **Assumptions** that need only be stated, not justified, in the demonstration of the possession of the Overarching Properties
- **Constraints** on how Overarching Property possession must be demonstrated

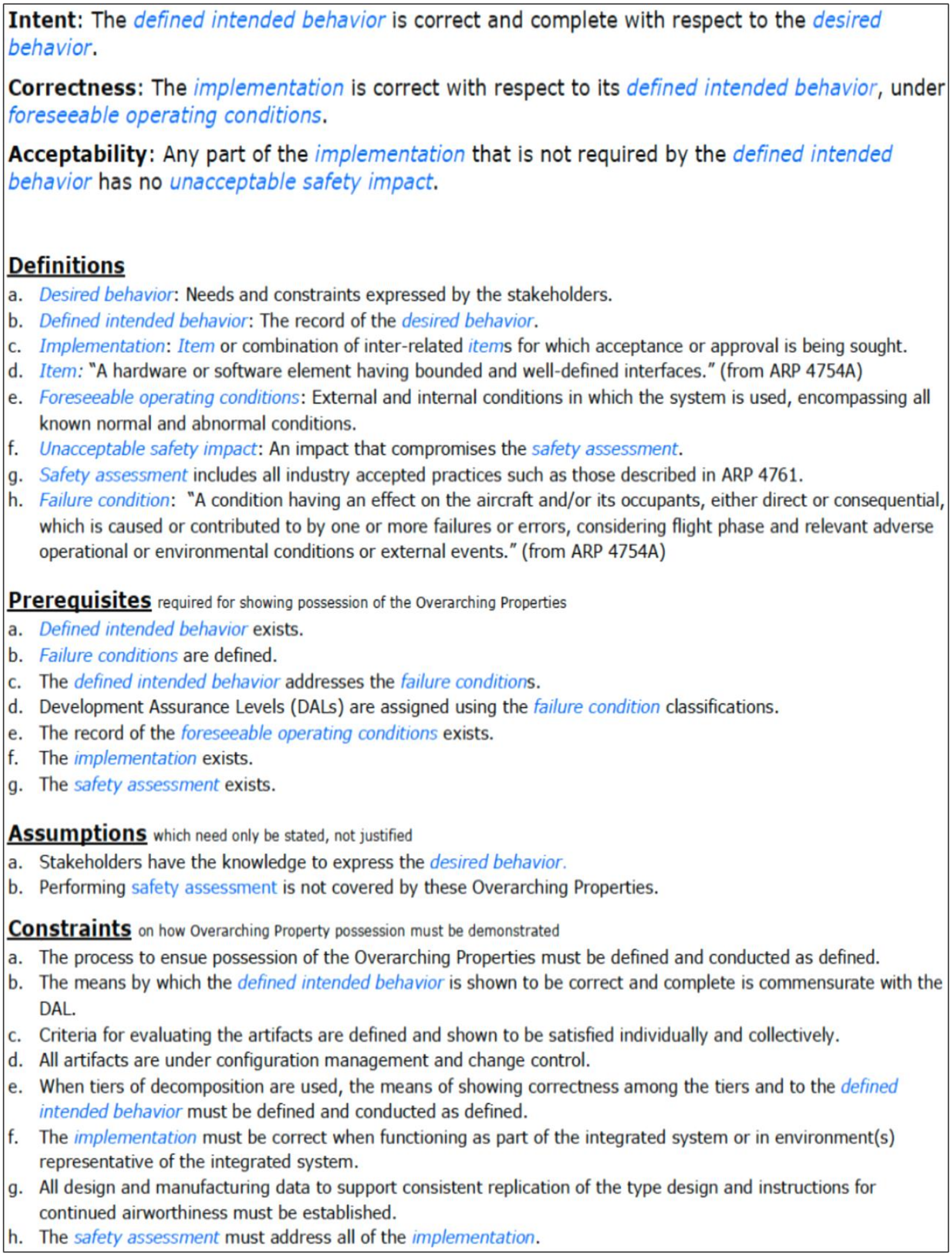
The content of these parts is discussed below. Before beginning the discussion, some preliminary comments are in order.

Only two of these 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.

The statement, the definitions in particular, and the other sections more generally, were formulated based on lessons taught by experience and research studies [3] concerning the common human tendency to ignore explicit written definitions for terms one already believes one understands. To combat this tendency, we chose to *not* use common terms such as requirements, validation, or verification in the statements. If we used these common terms, many people would naturally but subconsciously ignore the provided definitions, relying on their own definitions instead.

[6] Whether certainty may one day be possible in this area is an interesting question in epistemology.

[7] It may alter the type of insight needed, but insight into processes will still be necessary, at least until substantial breakthroughs are made in the state-of-the-art and –practice. It is important, however, to recognize that using the OPs alone, without additional generic evaluation criteria, is possible as noted in §4.4



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*.

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

Definitions

a. *Desired behavior*: Needs and constraints expressed by the stakeholders.
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." (from ARP 4754A)
e. *Foreseeable operating conditions*: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions.
f. *Unacceptable safety impact*: An impact that compromises the *safety assessment*.
g. *Safety assessment* includes all industry accepted practices such as those described in ARP 4761.
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 ARP 4754A)

Prerequisites required for showing possession of the Overarching Properties

a. *Defined intended behavior* exists.
b. *Failure conditions* are defined.
c. The *defined intended behavior* addresses the *failure condition*s.
d. Development Assurance Levels (DALs) are assigned using the *failure condition* classifications.
e. The record of the *foreseeable operating conditions* exists.
f. The *implementation* exists.
g. The *safety assessment* exists.

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 ensue 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 1: THE OVERARCHING PROPERTIES

Because these pre-existing definitions differ and sometimes conflict among different domains and contexts, the meaning of the Overarching Properties would inevitably be perceived quite differently by several different groups of people. Some differences in perception are unavoidable[8], but we hope that eschewing ambiguous common terms has increased the likelihood that people will read and rely on our explicit definitions to inform their understanding of the Overarching Properties. Hence, we further hope that the likelihood of unresolvable, conflicting perceptions is less than it otherwise would be.

The *label* part of the OP statement is semantically superfluous. It exists to provide a convenient means for referencing each OP. Although an OP's label was chosen to be indicative of the content, no actual meaning attaches to it. For readers familiar with computer programming, you may want to think of the label as similar to a variable name. Two otherwise textually identical programs remain semantically identical even if one program uses the variable name AltitudeAboveSeaLevel and the other uses QzwZ. So, too, is the case with the Overarching Properties. The Overarching Properties are labeled Intent, Correctness, and Acceptability, but they could be labeled Angie, Deanna, and Trish, with no change in meaning at all.

The *prerequisites* and *assumptions* do not directly affect the meaning of the Overarching Property, but they do affect when the meaning is relevant to a particular product. Finally, *constraints* apply to what is required to be demonstrated to justify that a product possesses an Overarching Property. These distinctions may not be completely clear now, but they should be clear by the time you finish reading the rest of this section.

The order of presentation in this section generally tracks Figure 1. The lone exception concerns definitions, which are discussed when a defined word or phrase first appears, not in a separate section all their own. Because definitions, prerequisites, assumptions, and constraints all use lettered lists, to distinguish clearly among them, all lettered items are preceded by D, P, A, or C as appropriate. For example, the definition for Item, which is item c, is labeled D.c. in the text.

3.1 STATEMENTS

As noted already, the three Overarching Properties are labeled Intent, Correctness, and Acceptability. Here are the statements of each.

> **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*.

[8] As the brilliant theologian and philosopher Jonathan Edwards wrote long ago, "O, how is the world darkened, clouded, distracted, and torn to pieces by those dreadful enemies of mankind called words." [4]

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

We now list and explain the definitions, which we hope provide to all readers a common understanding of the meaning of each of the three statements. We begin with the definitions applicable to the Intent statement.

3.1.1 Intent

Defined intended behavior is the first phrase in the Intent statement, and it also occurs in the statements for Correctness and Acceptability. It is a phrase that you probably have never seen before. You may be tempted to try to define it by considering separately each of the three words the phrase comprises. Resist the temptation. Instead consider the simple definition provided:

> D.b. *Defined intended behavior*: The record of the *desired behavior*.

Consider also the provided definition for *desired behavior*:

> D.a. *Desired behavior*: Needs and constraints expressed by the stakeholders.

The phrase "needs and constraints" encompasses everything the stakeholders (more about that word in a moment) want the product to do, along with anything that they want to ensure it does not do. Note in this context, the word 'needs' is used a bit more loosely than might be anticipated on first glance, because it includes both what is 'needed' and what is 'wanted'. But the phrase "needs and constraints" is fairly commonly understood to expand the connotation of 'needs' in this way.

'Stakeholders' is not further defined, because its normal meaning is appropriate. The stakeholders include anyone and everyone who has an interest in, and the authority to influence, what the product is designed to do. This group is likely to vary depending on the nature of the product, as is explained in more detail in §4.2.

So, speaking a bit loosely but without compromising accuracy, the *desired behavior* may be said to be the collective intellectual understanding of what the stakeholders want the product to do. The *defined intended behavior* is thus a physical[9] representation (that is, a record) of this intellectual understanding. One prototypical example of such a physical representation is a collection of requirements.

We can now understand the meaning of the Intent OP statement. It requires that the physical representation be correct and complete with respect to the intellectual understanding. That is, the physical representation includes everything that is part of the intellectual understanding, and does so in a way that accurately captures the meaning of that understanding.

[9] Here and elsewhere in the document the phrase *physical representation* includes representations that exist only in electronic form.

Or, in well-known colloquial phrases, the Intent OP requires that "you get the requirements right," or, "you build the right system."

3.1.2 Correctness

Here is the Correctness statement repeated:

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

In addition to the phrase we have already seen (*defined intended behavior*), three more defined phrases appear in the statement: *implementation*, *item*, and *foreseeable operating conditions*. These definitions are as follows:

> D.c. *Implementation*: *Item* or combination of inter-related *items* for which acceptance or approval is being sought.
>
> D.d. *Item*: "a hardware or software element having bounded and well-defined interfaces" [5, p.12].
>
> D.e. *Foreseeable operating conditions*: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions.

The word *implementation* is difficult to define generically[10]. The definition used here combines two distinct notions. The first of these notions incorporates the definition of *item*, which is taken directly from ARP 4754a [5], to emphasize the necessity of bounded and well defined interfaces. Prototypical examples of entities that satisfy this first part of the definition include software systems and hardware devices.

The second notion incorporated into the definition is that it applies only to something for which approval or acceptance is being sought. So, for the purposes of applying the OPs, an entity for which approval is not being sought is not considered an *implementation*.

The definition of *foreseeable operating conditions* combines the notions of the full range of (1) external circumstances that the product may encounter during its operation, and (2) internal states that may exist within the product, whether those circumstances or states occur regularly during normal operations or only during abnormal operations. The phrase all known establishes an exception for circumstances or states outside the ken of the developers and regulators.

Two extremes must be guarded against when determining the *foreseeable operating conditions* for a specific *implementation*. One extreme is adopting a dangerously weak conception of what can be known, and dismissing all circumstances or states that are conceptually

[10] Although agreeing on a generic definition is hard, identifying whether a specific something is an implementation is usually simple. As Justice Potter Stewart famously write in another context, "… I know it when I see it …" [6].

possible but deemed to be extremely improbable to occur. The other extreme is adopting an impossibly strong conception, and, for example requiring consideration of every single external circumstance that anyone can possibly imagine. Striking the balance between these two extremes is required today under current regulatory frameworks. A regulatory framework based on the OPs would not change how the balance is struck[11].

We can now understand the meaning of the Correctness OP statement. It requires that the entity for which approval is sought correctly instantiates a physical representation of the intellectual understanding of what the stakeholders want the product to do. The product must not only be correct under normal anticipated circumstances and states, it must also be correct—or, to use a term commonly used today, robust—under abnormal circumstances and states. Or, using the well-known colloquial phrase within the software industry, the Correctness OP statement requires that "you build the system right". Thus, a product that possesses the Correctness OP will "do the right things".

3.1.3 Acceptability

Here is the Acceptability statement[12] repeated:

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

This statement introduces only one new explicitly defined phrase, but its definition introduces another, which is also listed below:

> D.f. *Unacceptable safety impact*: An impact that compromises the *safety assessment*.
>
> D.g. *Safety assessment* includes all industry accepted practices such as those described in ARP 4761 [7].

The meaning of this Overarching Property statement is at once both seemingly self-evident and subtle. The self-evidency is, well, self-evident. The subtlety stems from the reason this OP is needed at all. Why is the implementation not restricted to contain only that which is required by the defined intended behavior?

There are two primary reasons. One reason is to account for the possibility that the chosen way to build a particular product may involve the use of previously developed items, even when only part

[11] Determining the balance point is not easy today. It will not be any easier under an OP-based regime, but neither should it be any harder. History seems to show, however, that the greater danger lies in underestimating the range of circumstances and states that are feasible, than in overestimating it. Hence, we have chosen not to explicitly qualify, with phrases such as "reasonably expected to occur," the meaning of all known in the text. We are relying on established practices and common sense to supply the appropriate qualifications for each specific product. A plausible case may be made that this reliance itself violates common sense.

[12] The label and statement for this Overarching Property have changed more than for either of the other two OPs combined. It is the only one with a different label today from what was presented in the 2016 public workshop. At the workshop it was called 'Necessity'. Quite a variety of other labels, including 'Do No Harm' have also been considered.

of an item directly addresses a need or constraint recorded in the defined intended behavior. So long as the unneeded parts of the item can be shown to not compromise the safety assessment, this OP allows such use. The other reason is to ensure that those things known within the industry as “derived requirements”[13] are handled so as to not introduce any safety problems.

One additional potential subtlety, or perhaps even an ambiguity, arises from the definition of unacceptable safety impact. In the abstract the intended meaning seems clear, but in reality agreeing whether a particular change in the safety assessment compromises the assessment may be difficult. The OPWG should perhaps consider changing this definition to make it less subject to ambiguity. Alternatively, accepting the ambiguity may be necessary, and the last two sentences in this paragraph should be replaced by sentences that explain that the abstract ambiguity will have to resolved in practice on each project within the context of the project.

One colloquial phrase that expresses the meaning of this Overarching Property is, “do no wrong things” (where ‘wrong’ means ‘unsafe’). Another is “do no harm.”

3.1.4 Colloquial summary

Here are two differently worded but equivalent informal expressions of the meaning of the OP statements.

A product that possesses the three Overarching Properties will

- seek to be the ‘right’ product (Intent)
- do the ‘right’ things (Correctness)
- do no wrong things (Acceptability)

where ‘right’ is relative to the needs and constraints of the stakeholders.

Another informal summary: in a product that possesses the three Overarching Properties

- what the product is supposed to do is properly captured (Intent)
- the product does what it is supposed to do (Correctness)
- the product does not cause harm (Acceptability)

3.1.5 Relationship to each other

In one sense the three Overarching Properties are independent of one another. For example, it is possible for a product to possess Intent and Acceptability but not Correctness: what it is

[13] For readers who have not previously heard of this phrase, "derived requirements" is the name given to requirements that arise from development decisions other than requirements refinement decisions. Hence, in this phrase, unlike in normal usage, ‘derived’ is an antonym of ‘refined’ instead of a synonym. Ensuring that these “derived requirements” do not cause safety problems in the implementation is necessary for them to be acceptable. Both [5, p. 11] and [8, p. 112] have glossary entries for the phrase. The entries are not identical to one another, but they are not mutually contradictory either.

supposed to do is properly captured and it does nothing harmful, but it does not do everything it is supposed to do. As another example, consider the conventional wisdom that many (some would say, most) errors are really requirements errors. A product that conforms to this conventional wisdom does not possess Intent, but it may possess Correctness: it does what it is supposed to do, but what it is supposed to do was not properly captured. It may, or may not, possess Acceptability.

In another sense, however, the three Overarching Properties are interdependent. Possession of all three is necessary for a product to warrant approval, with one possible exception. For products that provide no safety-critical functions, an argument can be made that possessing Acceptability is unnecessary. A counter-argument can be made that possessing Acceptability is trivial, and no harm is done by saying that all products, regardless of criticality, must possess it.

Another way in which the OPs are interdependent is that no ordering among them is prescribed or implied. An applicant does not first have to do what is needed to show the possession of Intent, and then what is needed to show Correctness, followed last by Acceptability. Rather an applicant must do whatever is needed to show that the final product possesses Intent **and** Correctness **and** Acceptability.[14]

One final aspect of the relationship among the three OPs concerns how they ensure the product is appropriately safe. On a casual glance someone may think safety is only addressed in Acceptability, and thus only ensured in relation to parts of the implementation that are not required by the defined intended behavior, and not ensured in the parts of the implementation that flow from the defined intended behavior. The solution to this apparent fatal flaw is explained below in §3.2, specifically in the discussion about P.c.[15]

3.1.6 Relationship to time

One of the most difficult concepts for many people to grasp when first encountering the Overarching Properties concerns the relationship of the OPs to time[16]. The product must only be shown to possess the OPs at the end of its development[17], that is, when the product is being considered for approval. It is easy to erroneously extrapolate from this fact to a belief that an OP-based approval process would necessarily allow an applicant to "wait until the end" to engage with

[14] For a discussion related the "whatever is needed to show" see §4.4.

[15] This solution is effective, but it ruins the otherwise pristine assertion that the meaning of the OPs is fully contained in statement and definitions. Perhaps a better solution may be to expand the definition of defined intended behavior (or desired behavior) to explicitly include the notions of addressing failure conditions. The possibility of making such a change will be discussed in the future.

[16] The concept of time itself is unexpectedly difficult to understand, as Augustine explained nearly two millennia ago: "For what is time? Who can easily and briefly explain it? Who can even comprehend it in thought or put the answer into words? Yet is it not true that in conversation we refer to nothing more familiarly or knowingly than time? And surely we understand it when we speak of it; we understand it also when we hear another speak of it. What, then, is time? If no one asks me, I know what it is. If I wish to explain it to him who asks me, I do not know." [9, Bk.11, Ch. 14, Sec 17]

[17] Continued airworthiness is not considered here, but one imagines that a later showing of continuing possession of the OPs may be warranted.

approval authorities or run tests or analyses or do a host of other things that are done today throughout the development and assurance life-cycle.

The following double conditional is theoretically true: *if* an applicant waited until the end to produce evidence that their product possessed the Overarching Properties, and *if* that evidence was in fact sufficient to demonstrate possession, then their product *would* warrant approval. But in practice, even without considering time-based requirements that may be imposed by the process evaluation criteria, it is nearly impossible for the second conditional to true. Evidence produced only at 'the end' will almost certainly result in moving 'the end' to a much later date than originally planned and at much higher cost, in order to demonstrate that the properties are actually possessed. An applicant attempting to claim otherwise should not expect to obtain approval.

This completes the discussion of the first two parts of the description of the Overarching Properties: statements and definitions. We now consider in turn the remaining three parts: prerequisites, assumptions, and constraints. In doing so, we will also need to introduce two more definitions.

3.2 PREREQUISITES

Recall from §3 that prerequisites encompass that which must exist to allow the possibility of demonstrating that a product possesses the Overarching Properties. They do not constrain how the demonstration must be done, nor affect directly the meaning of the OPs, but simply establish preconditions that must be true before a successful demonstration of property possession is even possible. The following seven prerequisites are identified:

P.a. *Defined intended behavior* exists.

P.b. *Failure conditions* are defined.

P.c. The *defined intended behavior* addresses the *failure conditions*.

P.d. Development Assurance Levels (DALs) are assigned using the *failure condition* classifications.

P.e. The record of the *foreseeable operating conditions* exists.

P.f. The *implementation* exists.

P.g. The *safety assessment* exists.

The means by which the defined intended behavior is created is not prescribed in any way by the Overarching Properties, but its existence is essential for all three.

The second prerequisite introduces another phrase with an explicitly defined meaning. The phrase also appears in the next two prerequisites. The definition is taken directly from ARP 4754a:

D.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." [5, p.11]

Since this definition has been around for a long time, we presume that our readers understand it.

The third prerequisite, combined with the first two, ensures that safety considerations are included in the defined intended behavior. Otherwise, the possibility would exist that unsafe aspects of the desired behavior (if any such aspects exist) might be propagated to the final product through the defined intended behavior and the implementation.

The assignment of DALs[18] based on the failure conditions (P.d) serves to allow the possibility of differing levels of confidence applying to the evidence supporting OP possession claims. Note, however, that the concept of DALs appears nowhere else in the Overarching Properties.

Prerequisite P.e ensures that the *foreseeable operating conditions* are recorded and not simply an intellectual understanding, which might vary from one person to another.

The need for the existence of an implementation (P.f) may seem so obvious as to not require its statement. It is included, however, to preclude the possibility that someone might try to demonstrate that a product possesses the Overarching Properties without using the actual product in the demonstration. Certainly some aspects of, or related to, the demonstration of property possession may be doable before the actual implementation is finished, but not all of the demonstration.

The final prerequisite (P.g) emphasizes the critical place occupied by safety assessment within an OP-based approval regime.

3.3 ASSUMPTIONS

Recall from the opening of §3, assumptions need only be stated, not explicitly justified, in the demonstration of the Overarching Properties. Two assumptions are included in the Overarching Properties description:

A.a. Stakeholders have the knowledge to express the *desired behavior*.

A.b. Performing *safety assessment* is not covered by these Overarching Properties.

Some readers from outside the aviation domain may wonder why Stakeholder knowledge is an assumption and not a requirement. The long-standing and successful practice in aviation has been to infer competence from the successful adherence to the applicable guidelines and regulations. The OPs assume that the practice will continue to be successful.

While the existence of safety assessment is required by the OPs, the actual assessments are not themselves something that can be shown to possess the Overarching Properties.

[18] In the absence of a generally accepted generic term for the concept of differing levels of assurance, we use DALs here generically. It is not identical to any specific current collection of levels.

3.4 CONSTRAINTS

Constraints are different from the other four parts of the Overarching Properties description. They 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. Eight constraints are enumerated. We list and comment on each separately.

The first constraint concerns the entire process of showing OP possession:

> C.a. The process to ensure possession of the Overarching Properties must be defined and conducted as defined.

This constraint does not prescribe what particular processes[19] must be used, but it does require that an applicant define the processes that will be used, and follow those processes once they are defined. It is consistent with current practices, which require the documentation of the process that will be used in developing and assuring a product, and the showing that the documented process has been followed.

The second constraint applies specifically to the demonstration of Intent possession:

> C.b. The means by which the *defined intended behavior* is shown to be correct and complete is commensurate with the DAL.

This constraint explicitly allows for different means to be used to show possession of the Intent property depending on the product's DAL. The phrase commensurate with indicates that higher DALs should require stronger demonstration.

The third and fourth constraints concern the artifacts that are produced throughout the development and assurance of the product. The third constraint reads as follows:

> C.c. Criteria for evaluating the artifacts are defined and shown to be satisfied individually and collectively.

This constraint does not prescribe the criteria[20] for evaluating artifacts (more on this word in a moment), but it does require that criteria be defined, and that these criteria be applied to the individual artifacts and to the collection of artifacts.

The fourth constraint applies to the management of these artifacts:

> C.d. All artifacts are under configuration management and change control.

Similarly, this constraint does not prescribe the particular configuration management and change control processes or tools that must be used, but it does require that both configuration management

[19] 'Process' and 'processes' are used interchangeably here, because the two seemingly different words (one singular, one plural) are used interchangeably by nearly everyone within the aviation domain. The 'process' contains a bunch of 'processes'.

[20] The 'criteria' mentioned here are not to be confused with the process evaluation criteria mentioned elsewhere in the document. The criteria here are the means of evaluating the acceptability of specific artifacts and collections of artifacts. One example of criteria that an applicant may define for evaluating software test results is "The testing-related objectives from DO-178C are satisfied."

and change control be applied to all artifacts. In this constraint, the terms configuration management and change control are used broadly to encompass all aspects of ensuring the artifacts are managed well. These terms should not be thought of as being restricted in meaning to the meaning specified in any existing standard or guidance document.

Before we discuss the next constraint, here is the promised more about the word ‘artifact’. The current version of the Overarching Properties does not include the word among the definitions. Some earlier versions did, while others did not. An explicit definition is not included now, under the assumption that the general meaning of the word is sufficiently well established within the aviation community. The intent is that the word applies only to the entities that play a role in the demonstration of a product’s possession of one or more of the OPs. There may be some entities produced during development that are not used in any demonstration. These constraints do not apply to those entities.

The fifth constraint applies specifically to the acceptable means for showing possession of the Correctness property:

> C.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.

This constraint exists to address concerns about the amount of flexibility that should be allowed within decomposition based-approaches to product development. These concerns are motivated by the comparatively high degree of prescription on the subject that exists in typical aviation guidance documents today. DO-178C [8] for example is usually perceived to mandate the use of multiple tiers[21] of decomposition, the establishment of specified attributes at each tier, and the showing of specified relationships among the tiers.

The Correctness Overarching Property statement mentions only two tiers: the highest (defined intended behavior) and the lowest (implementation). It says nothing about anything in between the two. From an abstract standpoint, this is exactly right. All that ultimately matters is whether the product does what it is supposed to do.

From a practical standpoint, however, given the current state-of-the-practice, the implementation for all but extremely simple products will almost certainly be developed through multiple tiers of decomposition, even if multiple tiers are not explicitly required. For these tier-based developments, the constraint requires more than just a demonstration that the lowest tier is correct with respect to the highest tier. It also requires a means to be defined for demonstrating that one tier is correct with respect to the tier above it, and that this defined means be followed (that is, conducted as defined).

Please note that the constraint does *not* prescribe what the means must be. Nor does it prescribe that the means for showing correctness of tier n with respect to tier n-1 must be the same as the

[21] DO-178C [8] does not use the word tiers, but instead refers to levels of requirements. Each level of requirements constitutes a tier (as described in [10]), as does any other instance of refinement, such as source code, which is refined from low-level requirements.

means for showing correctness of tier n-1 with respect to tier n-2. Nor does it prescribe that the defined means must permit demonstrating correctness of any arbitrary tier with respect to any arbitrary higher level tier.

The sixth constraint also applies to demonstrating Correctness:

> C.f. The *implementation* must be correct when functioning as part of the integrated system or in environment(s) representative of the integrated system.

It exists to ensure that demonstrations of 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.

The penultimate constraint may seem out of place to readers who are familiar only with software aspects of aviation systems. On the other hand, readers familiar with hardware products will likely understand immediately why the constraint is included.

> C.g. All design and manufacturing data to support consistent replication of the type design and instructions for continued airworthiness must be established.

This constraint applies to products that will be manufactured or replicated. It exists to ensure that the demonstration of OP possession includes evaluation of the means established to ensure the integrity of the manufacturing or replication processes.

The final constraint addresses the adequacy of the safety analysis:

> C.h. The *safety assessment* must address all of the *implementation*.

This constraint exists to preclude a demonstration that employs only a partial safety assessment. Someone might erroneously think that such an assessment would be acceptable for demonstrating possession of Acceptability. This partial safety assessment would consider in isolation only the part of the implementation that is not required by the defined intended behavior, but ignore the potential interactions with the part of the implementation that is required.

Having brought to a close the explanation of the Overarching Properties, we turn now to a brief discussion of four practical questions.

4. PRACTICALITIES

In earlier sections we postponed discussing the sufficiency of the Overarching Properties and how to evaluate whether a product possesses them. Both of these issues are discussed below. But first, we discuss two other matters, one of which has engendered some confusion within the community, and the other of which has engendered considerable confusion with the Overarching Properties Working Group. Devising solutions to these confusions must be a primary focus of future work.

4.1 SUPPLANT OR SUPPLEMENT?

Despite many statements to the contrary at the public unveiling of the Overarching Properties in 2016, and even more since, the perception still exists within parts of the community that the OPs are intended to supplant the existing approval processes and guidance documents. That is, if an OP-based approach is recognized, then companies who would prefer to continue using, for example, DO-178C [8] for software aspects of certification will be required to stop it and use the OPs instead on future projects. This perception is not true. It is not true at all.

The current intent is for the OPs to provide an alternative path for approval, a path that does not supplant the current path, but rather supplements it with another choice to consider. The new choice is intended to be more abstract and less prescriptive, and thus allow greatly flexibility.

No one who prefers the current path will be forced to choose the new one. Also, for those who want to try the OP path, an easy way to try it the first time would be to propose complying with an existing guidance document as the process to ensure possession of the Overarching Properties (see §3.4, C.a.).

4.2 WHO HAS DIBS?

Of all the subjects that the Overarching Properties Working Group has discussed over the last two-plus years, perhaps none has occupied more time than how the concepts of defined intended behavior (affectionately referred to by many as the DIB) and desired behavior (inexplicably never before referred to by anyone as the DeB) will play out in practice. The most confounding questions have concerned whether multiple tiers may exist, how multiple tiers should be handled, and what constitutes the DeB and the DIB for software. The flippant answers to these questions are “yes,” “carefully”, and “we don’t agree.” We consider slightly less flippant answers now.

The two questions concerning multiple tiers of DeBs and DIBs have different answers depending on the specific product to which the OPs are being applied and also, perhaps, to the organizational structure being used to develop it. Consider a simple example: a hardware device to accomplish a single task being developed within a single company for use by that company. In this simple case, a single DeB instantiated in a single DIB seems appropriate, with OP possession being demonstrated accordingly. Identifying the stakeholders who will produce the DeB should be simple.

Consider, on the other hand, a highly complex example: the product for which approval is sought is a subsystem implementing multiple functions containing several software elements running on different hardware devices, each of which will be developed by different companies. In this complex case, a single DeB and DIB seems ludicrous. Ultimately the subsystem will have to be demonstrated to possess the three OPs, but that demonstration will certainly consist of multiple instantiations of demonstrations of the subsystem components possessing the OPs with respect to specific DeBs and DIBs refined from the originals. The stakeholders for each of these DeBs are likely to be different.

The question of what constitutes the DeB and DIB for software has not yet been resolved. Some people believe that no DeB exists for software, and thus the Intent OP does not apply. These folks rationalize their belief based on an analogy between Intent and requirements validation, asserting that DO-178C [8] does not prescribe validating requirements.

Other people[22] believe that a clear analogy exists between the DeB and the system requirements allocated to software, and similarly between the DIB and the software high level requirements. Further, these people rationalize their belief as being consistent with the original understanding of the desired relationship between DO-178C [8] and the Overarching Properties, namely that the former should be considered a means to satisfy the latter for software. Without Intent applying to software, this cannot be.

Two approaches for resolving the conflict between these very different opinions seem feasible. The conflict could be left active, with each software project negotiating with the approval authority about which opinion will govern the project. Alternatively, the conflict could be closed by a binding decision of either the OPWG or the FAA.

4.3 DOES SUFFICIENCY EVEN MATTER?

Recall this fundamental concept from §2. The Overarching Properties rest on the assumption that they constitute a sufficient set of properties to establish the suitability of a product for installation on an aircraft. Recall also the admission that the sufficiency of the OPs has not yet been demonstrated conclusively.

Although no conclusive demonstration has been made, there does exist anecdotal evidence to suggest the plausibility of assuming sufficiency at this point. Beginning at the 2016 workshop and continuing to this day, doubters of the sufficiency of the OPs have been challenged to produce a counter example demonstrating insufficiency. That is, to conceive of a product that can be demonstrated (conceptually) to possess the OPs and to also have flaw that should prevent it from being approved for installation on an aircraft. To date, no one has produced a counter example. Readers of this document are encouraged to try their hand at conceiving a counter example.

Of course, absence of a counter example is not proof, but it is suggestive. Suggestive also of sufficiency is the informal argument sketched in §2, as are some incomplete, but promising, attempts to formalize an argument. It seems reasonable to believe that the OPs are either truly sufficient or closely enough to sufficient that any actual insufficiencies may not be revealed except by attempting application in the real world, or something close to it.

Also, the consideration of sufficiency should be done within the historical context. Actual abstract sufficiency of current approaches has never been demonstrated, but these current approaches have a long track record of impressive practical sufficiency. Perhaps an OP-based approach does not need a definitive demonstration of actual sufficiency either, so long as it is shown to have practical sufficiency.

[22] Such as the author of this document.

4.4 CAN ANYTHING GO?

We have postponed until last discussing the issue of evaluating whether a product possesses the Overarching Properties. Two reasons motivate the postponement: (1) the issue is mostly beyond the intended scope of this document, and will be discussed in great detail in another one; and (2) a final decision about what to recommend for evaluation seems further away now than it did a few months ago. Having delayed the discussion as long as possible, this section explains the current situation with respect to evaluation.

A common, but not unanimously held, understanding among the participants at the first workshop (see §1.1) in December 2015 was that the preferred approach would be based on an assurance case. That is, an applicant following the OP-based approval path would create an argument[23] explaining why they have justified belief (to an appropriate level of confidence) their product possesses the OPs. The argument would constitute the approval basis, serve as a primary means of communication between the applicant and the approval authority, and be the object of evaluation. For ease of reference a bit later, let's use the label "assurance case evaluation" (ACE).

Rather quickly, beginning with the second workshop, this understanding became the preferred approach of only a tiny minority of the participants. Instead the emphasis switched to developing a set of criteria against which a product's possession of the OPs could be evaluated. Although the original version of these criteria were based on graphical representations of generic assurance-case-like arguments, the criteria, also rather quickly, become unanchored from those arguments. The end result was a document consisting of requirements (apologies for using the word but it really is the best one here) on the processes that an applicant would be allowed to use to show possession of the OPs. Think of constraints (§3.4) writ large. The idea is simple: satisfaction of these requirements will serve as the means for determining whether a proposed collection of development and assurance processes is capable of producing a sufficient demonstration that a product possesses the Overarching Properties.

Two similar, but not identical, methods for applying these process evaluation criteria are feasible. One method is to allow an applicant to propose any collection of processes they wish to propose and evaluate those processes against the criteria. If the proposed processes satisfy the criteria, then the applicant would then use these processes to develop the product, with the evidence produced during the development evaluated for compliance with the approved processes. Let's call this method "applicant process evaluation" (APE).

The other method is to evaluate various published process standards and guidelines against the criteria, producing a list of approved standards and guidelines. An applicant wanting to follow the OP-based approval path would be constrained to choose from the approved list, developing the

[23] The word 'argument' is used here, as it has been used for centuries, to include not only the reasoning but also the claims and the evidence associated with the reasoning. Unfortunately, the assurance case community moved away from traditional usage by applying the word 'argument' only to the reasoning, with evidence (or a variety of other words) and claims (or a smaller variety of other words) being treated as separate entities. Even more unfortunately I once contributed to this perversion of language. No more.

product following their choice, with the evidence produced during the development evaluated for compliance with that choice. “Approved list evaluation” (ALE) will be the name.

In addition to ACE, APE, and ALE, at least one more plausible approach exists. One can easily imagine a regime in which evaluation criteria are handled on a product-by-product basis, with a proposal for the specific criteria to be used being part of the agreement between an applicant and the approval authority. An appropriate name for this approach is “applicant varying evaluation” (AVE).

Of these four approaches, ACE provides the most flexibility to applicants in choosing how to develop a product that will possess the Overarching Properties. AVE comes next, followed by APE, with ALE bringing up the rear. Concerning the likely costs incurred in the first use of the OP approach using the evaluation method, AVE probably has the least costs in the general case, because it facilitates doing things nearly identically to how they are done now. APE probably comes next; it, too, facilitates repeating current processes, but necessitates evaluating those current processes against a fixed set of criteria. In a general case ALE is next; but in a specific case using a standard already used that is on the approved list, it may well have to the least new costs. ACE certainly has the highest, first-time new costs, because of the novelty of assurance cases in the aviation community.

At this point, a question has probably formed in the minds of many readers: Is there anything wrong with allowing all four possibilities? In the abstract, the obvious answer to this question is, “No.” In the concrete, taking into account the finite resources available to companies and approval authorities and the desirability of repeatability in approval decisions, the equally obvious answer is, “Yes!” If an Overarching Properties path for approval is to become a reality, a decision must be made about how property possession will be evaluated.

5. POSTLUDE

The Overarching Properties provide an intellectually appealing new approach for obtaining justified belief in the suitability of a product for inclusion on an aircraft. Whether the OPs can go beyond intellectual appeal to practical application is an open question. The question remains open, but steps are underway to close it. The results of small case studies completed by a European consortium were released in mid-summer 2018. Motivated in part by those results, the FAA, EUROCAE, and industry representatives developed a plan for continuing work. Resolving the unsolved issues mentioned in this report will constitute an important component of the effort. NASA will participate. Also, NASA is independently conducting at least one case study, and considering more. The future looks cautiously promising.

6. REFERENCES

[1] “property, n.” OED Online. September 2017. Oxford University Press. Accessed October 9, 2017. http://www.oed.com/view/Entry/152674

[2] “overarching, adj.” OED Online. September 2017. Oxford University Press. Accessed October 9, 2017. http://www.oed.com/view/Entry/134273.

[3] Edwards, Barbara S., and Michael B. Ward. “Surprises from Mathematics Education Research: Student (mis) Use of Mathematical Definitions.” *The American Mathematical Monthly* 1111, no. 5 (May 2004): 411-24. Accessed January 30, 2018. doi:10.2307/4145268.

[4] Edwards, Jonathan. *The “Miscellanies”: a-500*. Edited by Thomas A. Schafer. Vol. 13. The Works of Jonathan Edwards. New Haven: Yale University Press, 1994.

[5] *Guidelines for Development of Civil Aircraft and Systems.* ARP4754a. Washington, D.C.: SAE International, 2010.

[6] *Jacobellis v. Ohio*, 378 US 184, 197 (1963) (Stewart, J. concurring).

[7] *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* ARP4761. Washington, D.C.: SAE International, 1996.

[8] *Software Considerations in Airborne Systems and Equipment Certification*. DO-178C. Washington, D.C.: RTCA, 2011.

[9] Saint Augustine. *The Confessions of Saint Augustine*. Translated by E. B. Pusey. Accessed December 19, 2017. https://www.gutenberg.org/files/3296/3296-h/3296-h.htm.

[10] Dewalt, Mike, and G. Frank McCormick. “Technology Independent Assurance Method.” *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, 2014. doi:10.1109/dasc.2014.697952