NASA/TM–2019–220292

Understanding the Overarching Properties

C. Michael Holloway
Langley Research Center, Hampton VA

July 2019

NASA/TM–2019–220292

Understanding the Overarching Properties

C. Michael Holloway
Langley Research Center, Hampton VA

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

July 2019

Acknowledgments

Special thanks are due to several specific people: Mike DeWalt (the retired Chief Scientific and Technical Advisor for Software) motivated the effort resulting in the Overarching Properties; Barbara Lingberg and George Romanski (the current Chief Scientific and Technical Advisor for Software) kept it going after Mike left the scene; Stephen Fridrick (retired from GE Aviation) ably led the Overarching Properties Group at the beginning; Jim Chelini (Verocel) does so now.

Thanks also are due to all members of the Overarching Properties Working Group, whose participation in 2015-2019 led to the creation and refinement of the properties. In particular, many of the people explicitly mentioned in the List of Contributors provided rigorous reviews of draft editions of this document. Their criticisms and suggestions contributed substantially to the accuracy and clarity of the text. Any mistakes or ambiguities that remain are entirely my fault.

Earlier drafts of this document were 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”. Thanks to Srini Mandalapu who provided program management for the agreement.

Finally, lest someone mistakenly think otherwise, **this document does not constitute official guidance.**

The use of trademarks or names of manufacturers in this report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Abstract

This document explains the purpose, history, and philosophy of the Overarching Properties, and explains the specific details of each property, the relationships among them, and some practical considerations that attach to their use. Although it has been extensively reviewed by over a dozen members of the Overarching Properties Working Group, **it does not constitute official guidance**, nor does it necessarily express a unanimously agreed view of the Working Group on every detail.

1 Prelude

The Overarching Properties are intended to define a sufficient set of properties for making approval decisions. That is, when approval is sought for using a particular entity on an aircraft, if the entity can be shown to possess these properties in their entirety, then granting approval for using that entity on an aircraft is appropriate. Hence the name: *properties* because they encapsulate the *"characteristic qualities"* [1] necessary to justify approval; *overarching* because they are intended to *"encompass all"* [2] of the necessary properties[1].

The purpose of this document is to explain the Overarching Properties including their philosophical foundation, the specific details of each property, the relationships among them, and some practical considerations that attach to their use. The abbreviation OPs (pronounced "oh-peas", *not* "awps" or "oh-pea-ess") will be used in place of the full phrase from time to time, but not always, as the abbreviation seems aesthically displeasing in some sentences.

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 might find understanding the Overarching Properties easier than readers with such knowledge.

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

[1] Some readers will be happy with this paragraph; some others will not. If you are an unhappy reader, this footnote is for you. Yes, the word "entity" is vague, intentionally so. Later sections of the document should remove the vagueness; however, if you cannot wait, you can substitute the phrase "systems, software, or airborne electronic hardware" without much harm. Similarly, if you are miffed by the use of the word "possess" instead of "satisfy", feel free to substitute the latter for the former. It is tradition 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'.

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 distributed to attendees without any additional printed explanatory material. To supplement the written material, oral presentations were delivered and several discussion sessions held.

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, recognizing that several years of effort would be needed to complete it.

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. At the same time a European research project, Re-Engineering and Streamlining the Standards for Avionics Certification (RESSAC), initiated an effort to conduct several case studies in using the OPs. Several RESSAC members were also members of the OPWG.

Most of the work throughout 2017 and 2018 involved trying to develop a collection of criteria for use in evaluating OP possession. Both direct (criteria for evaluating whether a specific product[2] possesses the OPs) and indirect (criteria for evaluating whether an applicant's proposed processes are sufficient to ensure products produced using those processes will possess the OPs) approaches were investigated. The results of RESSAC case studies completed in the summer of 2018 identified deficiencies in both the direct and indirect criteria approaches. A different approach to evaluation is currently being investigated; it is based on requiring the use of explicit arguments giving the reasons for believing a product possesses the Overarching Properties. Once the evaluation work is completed, a separate document will be written to provide information and guidelines about the subject.

The version of the Overarching Properties described in this document was finished during a physical meeting in April 2019. 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

[2] The word *product* is simply a shorthand for "an entity for which approval is sought."

single page is the most visible difference. Nevertheless, someone who last saw the OPs at the public workshop should recognize the version discussed here without much difficulty.

1.2 Presentation style

This document is written in a conversational style, unlike the more formal styles usually employed in standards and guidance documents. 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*. Quotations of more than a few words are set off from the surrounding text by typesetting them as paragraphs with slightly narrowed margins. 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. Please note: the electronic version of this document contains many internal hyperlinks, which are identified by rectangular boxes around the text.

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 should take a sturdy umbrella with you when you leave the house.

[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 meaningful sense similar to 'objectives' as that term is used in documents such as RTCA DO-178C [3], RTCA DO-254 [4], and ARP 4754A [5]. The non-similarity of the OPs and 'objectives' is so important to understand, repeating the previous sentence seems appropriate. The OPs are ***not*** in any meaningful sense similar to 'objectives' as that term is used in documents such as DO-178C.

- If Quinn says the dog doesn't bite, you can pet it without fearing for the physical integrity of your hand.
- If Quinn says that the value of the Acme Corporation's stock will go up by 125% this year, then you can buy stock in Acme without worrying that you might lose money this year.

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. 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 is required to satisfy[4]; Quinn's blessing is enough.

Let's change the example a bit. Suppose Quinn has a wickedly playful streak. He refuses to answer a single direct question about a product's suitability for installation on an aircraft. Instead he insists you must ask him three separate questions:

- Does the product possess the property of Intent?
- Does the product possess the property of Correctness?
- Does the product possess the property of Innocuity?

He further tells you can be confident in approving the product only if he answers "Yes" to all three questions[5].

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 Innocuity. In our imaginary Earth* with the statements from the perfect oracle Quinn, you do not need to know what these properties mean, but only if your product possesses them.

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 Innocuity? Does it possess Intent? Does it possess Correctness? If Quinn answers, "Yes," to all three questions, you can confidently approve the product. If Quinn 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

[4] Just in case you are wondering, the regulations on our imaginary Earth* are identical to the regulations in our world.

[5] As another instantiation of his wickedly playful streak, he also tells you that a "No" answer to one or more of the questions does not necessarily mean the product is unsuitable, but only that you ought not approve it without additional information.

the product. In our imaginary Earth* with the perfect oracle Quinn, Quinn's word alone is enough.

Let's now return to the real Earth. Sadly, our Earth has no perfect oracle named Quinn, nor any perfect oracle with some other name. Happily, however, the non-existence of a perfect oracle does not invalidate the underlying principle just illustrated:

> 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 can be confidently 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 Section 4.2.

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].

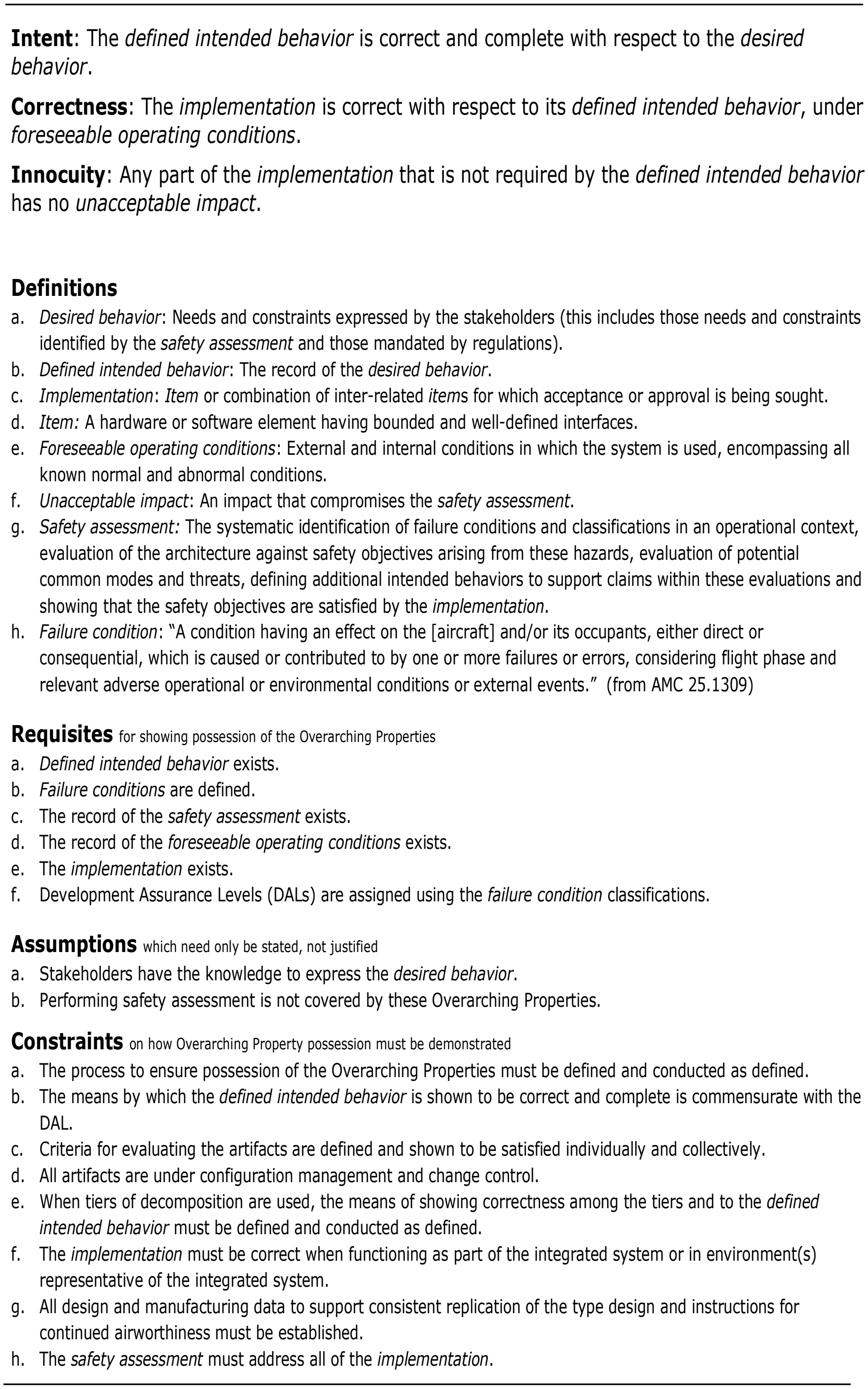
Keeping the fundamental difference between (A) and (B) clear is essential to understanding the rest of this document. A reader who does not keep clear the distinction runs a substantial risk of conflating questions about the meaning of the OPs and questions about how to evaluate possession the OPs in practice. Both types of questions are important, but this document is intended to answer only questions of the first type. As noted previously a future document will address evaluation matters.

3 Properties

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

[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 state-of-the–practice.



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

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

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

Definitions

a. *Desired behavior*: Needs and constraints expressed by the stakeholders (this includes those needs and constraints identified by the *safety assessment* and those mandated by regulations).

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

c. *Implementation*: *Item* or combination of inter-related *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." (from AMC 25.1309)

Requisites for showing possession of the Overarching Properties

a. *Defined intended behavior* exists.

b. *Failure conditions* are defined.

c. The record of the *safety assessment* exists.

d. The record of the *foreseeable operating conditions* exists.

e. The *implementation* exists.

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

Assumptions which need only be stated, not justified

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

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

Constraints on how Overarching Property possession must be demonstrated

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

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

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

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

e. When tiers of decomposition are used, the means of showing correctness among the tiers and to the *defined intended behavior* must be defined and conducted as defined.

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

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

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

Figure 1. The Overarching Properties

- **Statements** of the three Overarching Properties themselves, including a label for each
- **Definitions** for words or phrases used in the Overarching Properties description
- **Requisites** 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 [6] 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.

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 for each OP statement (that is Intent, Correctness, and Innocuity 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 Innocuity, but they could be labeled Angie, Deanna, and Trish, with no change in meaning at all.

[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" [7].

The *requisites* 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 not discussed in a separate section all their own. Because definitions, requisites, assumptions, and constraints all use lettered lists, to distinguish clearly among them, all lettered items are preceded by D, R, A, or C as appropriate. For example, the definition for *Implementation*, which is definition c, is labeled D.c in the text.

3.1 Statements

As noted already, the three Overarching Properties are labeled Intent, Correctness, and Innocuity. 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*.
>
> **Innocuity:** Any part of the *implementation* that is not required by the *defined intended behavior* has no *unacceptable 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

Here is the Intent statement repeated:

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

Defined intended behavior is the first phrase in the Intent statement, and it also occurs in the statements for Correctness and Innocuity. 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 specific definition provided, along with the provided definition for *desired behavior*:

> D.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).

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

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. The members of this group are likely to vary depending on the nature of the product. However, as the parenthetical remark emphasizes, regardless of who the specific stakeholders are for a given product, the "needs and constraints" in the *desired behavior* must always include anything identified by the *safety assessment* [9], and, of course, anything necessary to satisfy applicable regulations.

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 (including safety people and regulators) need the product to do. The *defined intended behavior* is thus a physical 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[10] 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. Or, in well-known informal phrases, the Intent OP requires that "you get the requirements right," or, "you specify 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*), two more defined phrases appear in the statement (*implementation* and *foreseeable operating conditions*) and a third (*item*) is introduced in the definition of *implementation*. These definitions are as follows:

[9] We defer discussing the specific definition of the term until a bit later in Section 3.1.3. For now, simply think of it as designating everything that is done to determine what has to be done to ensure the product is as safe as it needs to be.

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

D.c. *Implementation*: *Item* or combination of inter-related *item*s for which acceptance or approval is being sought.

D.d. *Item*: a hardware or software element having bounded and well-defined interfaces.

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. Although agreeing on a generic definition is hard, identifying whether a specific something is an *implementation* is usually simple[11].

The definition used here combines two distinct notions. The first of these notions incorporates the definition of *item*, which is the same here as it is in some existing standards (for example [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 (that is, something we have called a "product" in early text). 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 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.

Just as 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, not overestimating, the range of circumstances and states that are feasible. 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, as has been done in aviation for decades.

[11] As Justice Potter Stewart famously wrote in another context, "... I know it when I see it ..." [8].

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 need 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 informal 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 Innocuity

Here is the Innocuity[12] statement repeated:

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

This statement introduces only one new explicitly defined phrase, but its definition uses the phrase *safety assessment*, which we saw earlier and deferred discussing until now.

> D.f. *unacceptable impact*: An impact that compromises the *safety assessment*.

The definition of *unacceptable impact* is another instance in which greater specificity in the general case is not feasible. But for any given specific product, reaching agreemment about whether a particular change compromises the *safety assessment* will often be easy. When agreeing is not easy, applying existing methods for assessing hazard severity should still make it possible. Whether easy or hard the need to reach agreement between applicant and approval authority on this issue is no different in an OP-based regime than it is using current approval practices.

> D.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*.

Although this definition of *safety assessment* may seem a bit complicated, the intent of the definition is simple: to encompass all of the activities that are done to determine the needs and constraints on the product necessary to ensure the

[12] For readers unfamiliar with this word, it is identical in meaning to the longer, less aesthetically pleasing word *innocousness*. Both mean (unhelpfully), "The quality of being innocuous" [9], or (helpfully) substituting the meaning of innocuous [10], "The quality of being not hurtful or injurious; harmless." Since that meaning expresses the essence of the quality this OP demands from a product, the label fits well.

product is as safe as it needs to be. In keeping with long-standing practice within the aviation industry these activities center around identifying *failure conditions*, for which we have our final explicit definition. It is identical in all substantive aspects to the definition in AMC 25-1309 [11], and hence any further explanation is more likely to cause confusion than enlightment[13].

> 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.

With these three definitions in mind, we see that the meaning of the Innocuity OP statement is at once both seemingly self-evident and subtle. The self-evidency is, well, self-evident: nothing extra in the *implementation* can negatively affect safety.

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 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 it to be used.

The other reason is to provide additional assurance that those things known within the industry as "derived requirements"[14] are handled so as to not introduce any safety problems. These "derived requirements" should be included within the *desired behavior* as "needs and constraints" and industry-standard practices should be followed to ensure that all such requirements are passed to safety people to analyze.

One informal phrase that expresses the meaning of this Overarching Property is, "do no wrong things" (where *wrong* means *unsafe*). Another is "do no harm."

[13] If you are taken aback by the concentration on failures, this footnote is for you. The aviation industry is aware of the school of thought that defines 'failure' so narrowly as to include only instances in which an entity does not do what it is explicitly *specified* to do (or, to use the language of the OPs, the entity does not possess the property of Correctness). But the industry does not adopt this narrow definition. An instance in which an entity does not do what it is *intended* to do is a failure, even if the cause can be traced to mistakes in properly recording the intent. In OP language, not possessing Intent or Innocuity may also contribute to failures.

[14] 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 [3] [p. 112] have glossary entries for the phrase. The entries are not identical to one another, but they are not mutually contradictory either.

3.1.4 Informal 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
>
> - be specified properly (Intent)
> - do the right things (Correctness)
> - do no wrong things (Innocuity)
>
> 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 (Innocuity)

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 Innocuity but not Correctness: what it is supposed to do (*desired behavior*) *is* properly captured (in the *defined intended behavior*) and it *does nothing harmful*, but the *implementation* is *not correct* in some way. 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 (that is, it has requirements errors) would 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 Innocuity.

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 functions that can possibly impact safety. An argument can be made that possessing Innocuity is unnecessary for such a product. A counter-argument can be also be made that possessing Innocuity in such a case is trivial, and thus no harm is done by saying that all products, regardless of criticality, must possess it.

Another way in which the OPs are *independent* 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 Innocuity. Rather an applicant must do whatever is needed to show the final product possesses Intent **and** Correctness **and** Innocuity.

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[15]. The product must only be shown to possess the OPs at the end of its development[16], 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 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: requisites, assumptions, and constraints. In doing so, we will also need to introduce two more definitions.

3.2 Requisites

Recall from Section 3 that requisites encompass that which must exist to allow the possibility of demonstrating 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 certain conditions that must be true before a successful demonstration of property possession is even possible. Or, because each of the conditions involve existence of something, another way to look at the requisites is as setting a minimal set of necessary evidence.

R.a *Defined intended behavior* exists.

Although the means by which the *defined intended behavior* is created is not prescribed in any way by the Overarching Properties, *defined intended behavior* must exist to allow possession of any of the OPs to be shown.

[15] 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." Bk.11, Ch. 14, Sec 17. [12]

[16] Continued airworthiness is not considered here, but one imagines that a later showing of continuing possession of the OPs would likely be necessary.

R.b *Failure condition*s are defined.

R.c The record of the *safety assessment* exists.

Requisites (R.b) and (R.c) emphasize the critical place occupied by *safety assessment* within an OP-based approval regime. Without it, the *desired behavior* might not contain all the needs and constraints necessary to ensure adequate safety.

R.d The record of the *foreseeable operating conditions* exists.

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

R.e The *implementation* exists.

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

R.f Design Assurance Level (DAL) assignments based on *failure condition* classification exist.

The assignment of DALs[17] based on the *failure condition*s serves to allow the possibility of applying differing levels of confidence to the evidence supporting OP possession claims. Note, however, that the concept of DALs appears nowhere else in the Overarching Property statements themselves, but is included in constraint C.b. Additional material about DALs will be included in the future document about using and evaluating OPs.

3.3 Assumptions

Recall from the opening of Section 3 that 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.

[17] In the absence of a generally accepted generic term for the concept of differing levels of assurance, we use DAL here generically. It should not be thought of as identical to any specific current collection of levels.

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 the practice will continue to be successful. Should future events, however, be inconsistent with past history, the OPs can be easily modified by converting A.a into a constraint.

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. The future document about evaluating OP possession will provide additional information about the practical implications of this fact.

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[18] 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. To use the simpliest terms, this constraint requires that planning be done and the plans followed. It is consistent with current practices, which require the recording 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. Similar constraints are not explicitly imposed on the means for showing Correctness or Innocuity. Satisfying C.b should result in DAL-commensurate activities

[18] *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. For example, the process is said to contain a bunch of processes.

being applied for those OPs, also[19].

The third and fourth constraints concern the artifacts that are produced throughout 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 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 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. Constraints C.c and C.d 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.

[19] If it turns out in practice that this constraint as written does not ensure DAL-commensurate activities for the other two OPs, then a simple solution is to remove C.b and modify C.a to read as follows: The process to ensure possession of the Overarching Properties must be defined, conducted as defined, and commensurate with the DAL.

[20] The criteria mentioned here are not to be confused with the evaluation criteria mentioned in Section 1.1. 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."

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 in typical aviation guidance documents today. DO-178C [3] 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 OP 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. Because the current state-of-the-art does not provide a trustworthy way to make such a demonstration (except in unrealistically simple cases), the constraint 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 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.

Here is an example illustrating what this constraint does and does not require. Consider an *implementation* developed using three intermediate tiers of decomposition, yielding a total of five tiers. Let's lable the *defined intended behavior* as tier 0, the *implementation* as tier 4, and the intermediate tiers as tier 1, tier 2, and tier 3.

The Correctness property by itself only requires showing tier 4 is correct with respect to tier 0. C.e, however, adds the additional requirement of addressing correctness among the tiers. One means to do so is serially: show tier 1 is correct with respect to (icwrt) tier 0; tier 2 icwrt tier 1; tier 3 icwrt tier 2; tier 4 icwrt tier 3; and then explain why these serial relationships are sufficient (for this particular product) to establish tier 4 icwrt tier 0. A separate demonstration of tier 4 icwrt tier 0 is not required to satisfy C.e[22].

The sixth constraint also applies to demonstrating Correctness:

[21] DO-178C does not use the word tiers, but instead refers to levels of requirements. Each level of requirements constitutes a tier (as described in [13]), as does any other instance of refinement, such as source code, which is refined from low-level requirements.

[22] Which does not mean, of course, that for a specific product an approval authority is forbidden from adding additional constraints on what constitutes an acceptable means for demonstrating tier-based 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.

This constraint 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.

Constraint (C.f) 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 concerns the handoff from development organizations to manufacturing and operations organizations. It exists to ensure that the product for which OP possession has been demonstrated is the same product that is manufactured and operated. It thus requires that the demonstration of OP possession includes evaluation of the means established to ensure the integrity of the manufacturing or replication processes, and also of the means of passing on any needed instructions for maintaining continued airworthiness.

The final constraint addresses the adequacy of the safety analysis:

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

The *safety assessment* must account for all of the *implementation* either directly or by indentifying limits on portions of the *implementation* that cannot be analyzed directly (such as COTS).

This constraint also precludes a demonstration that employs only a partial *safety assessment*. As an example of something that could happen without this constraint, consider Innocuity. Someone might erroneously believe demonstrating possession of Innocuity could consider in isolation only the part of the *implementation* that is not required by the *defined intended behavior*. As a result they might use only part of the results of the *safety assessment*, which would likely 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

Although the purpose of this document is to explain the meaning of the Overarching Properties and not to provide guidance on using them, a few remarks about potential questions that are likely to arise in practice seem appropriate. As mentioned several times already, another document will be written explaining the use and evaluation of the OPs.

4.1 Supplant or supplement?

Despite many statements to the contrary at the public unveiling of the Overarching Properties in 2016, and even more statements 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 for software aspects of certification will be required to stop it and use the OPs instead on future projects. 'Tis not true. Not true at all.

The current intent is for the OPs to provide a different 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 greater 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 constraint C.a).

4.2 What about sufficiency?

Recall this foundational concept from Section 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 exists anecdotal evidence to suggest the plausibility of assuming sufficiency at this point. Beginning at the 2016 public 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 flaws that should prevent it from being approved for installation on an aircraft. To date, no one has produced a counter example. Of course, absence of a counter example is not proof, but it is suggestive, and consistent with how most scientific hypotheses are evaluated.

Suggestive also of sufficiency is the informal argument sketched in Section 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 close enough to sufficient that any actual insufficiencies can 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.

4.3 How many DIBs are allowed?

The Overarching Properties are clear. For the purpose of gaining (if you are an applicant) or granting (if you are an authority) approval for a product to be installed on an aircraft, there exists the *desired behavior* for the product, along with its associated *defined intended behavior* (affectionately referred to by many as the DIB) and *implementation*. Nothing is mentioned about multiple instances of the DeB[23] and DIB pairs.

This lack of mention should not be interpreted as prohibiting multiple instances. Whether having them is a good idea depends 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 entity 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, using only a single DeB and DIB seems absurd. Ultimately the subsystem will have to be demonstrated to possess the three OPs, but that demonstration will certainly compromise 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 may well be different.

4.4 Whither evaluation?

Despite previous explicit statements consigning to another paper the issue of how to evaluate OP possession, some readers are assuredly still hoping to read some useful words on the subject here. Abandon your hope now.

Abstractly, evaluating whether a product possesses Intent, Correctness, and Innocuity is not necessarily difficult. An applicant following an OP-based approval path could be required to create an argument[24] 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. Standard methods for evaluating the cogency of arguments would be applied.

Concretely, however, it is too soon to know whether such an approach can work in practice. Standard ways of evaluating arguments are not foolproof, require training and experience to use, and are not necessarily always straightforward to apply

[23] Inexplicably, using this word to refer to *desired behavior* has not yet caught on. It will.

[24] 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.

even for experienced people. Only time will tell if a suitable argument-based evaluation approach (or collection of approaches) can be developed.

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 will go beyond intellectual appeal to practical application is an open question. The question remains open, but steps are underway to close it. A European consortium recently completed a series of case studies. The National Aeronautics and Space Administration (NASA) is conducting a different case study and continues to pursue avenues for conducting additional ones. And small, but real, industry-based projects are underway with legitimate hopes for more to begin soon. A promising future for the OPs appears plausible.

References

1. property, n. OED Online. June 2017. Oxford University Press. URL `http://www.oed.com/view/Entry/152674`.

2. overarching, adj. OED Online. June 2017. Oxford University Press. URL `http://www.oed.com/view/Entry/134273`.

3. RTCA: DO-178C: Software Considerations in Airborne Systems and Equipment Certification. RTCA, Inc., Washington DC, USA (Also published as EUROCAE ED-12C), 2011.

4. RTCA: DO-254: Design Assurance Guidance for Airborne Electronic Hardware. RTCA, Inc., Washington DC, USA (Also published as EUROCAE ED-80), 2000.

5. Society of Automotive Engineers: Guidelines for Development of Civil Aircraft and System. , SAE ARP 4754a, 2010.

6. Edwards, B. S.; and Ward, M. B.: Surprises from Mathematics Education Research: Student (mis) Use of Mathematical Definitions. *The American Mathematical Monthly*, vol. 1111, no. 5, May 2004, pp. 411–24. Doi:10.2307/4145268.

7. Edwards, J.: The "Miscellanies": (Entry Nos. a-z, aa-zz, 1-500) (WJE Online Vol. 13). Entry 4. URL `https://bit.ly/jewords`.

8. Stewart, J.: Jacobellis v. Ohio. 378 US 184, 197, 1963.

9. innocuity, n. OED Online. March 2019. Oxford University Press. URL `http://www.oed.com/view/Entry/962997`.

10. innocuous, adj. OED Online. March 2019. Oxford University Press. URL `http://www.oed.com/view/Entry/96300`.

11. European Aviation Safety Agency: AMC 25.1309 System Design and Analysis. *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS-25)*, 2012, pp. 2–F–38–65. URL `https://www.easa.europa.eu/sites/default/files/dfu/agency-measures-docs-certification-specifications-CS-25-CS-25-Amdt-12.pdf`.

12. Augustine: *The Confessions of Saint Augustine*. Translated by E. B. Pusey. URL `https://www.gutenberg.org/files/3296/3296-h/3296-h.htm`.

13. Dewalt, M.; and McCormick, G. F.: Technology Independent Assurance Method. *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, 2014. Doi:10.1109/dasc.2014.6979529.

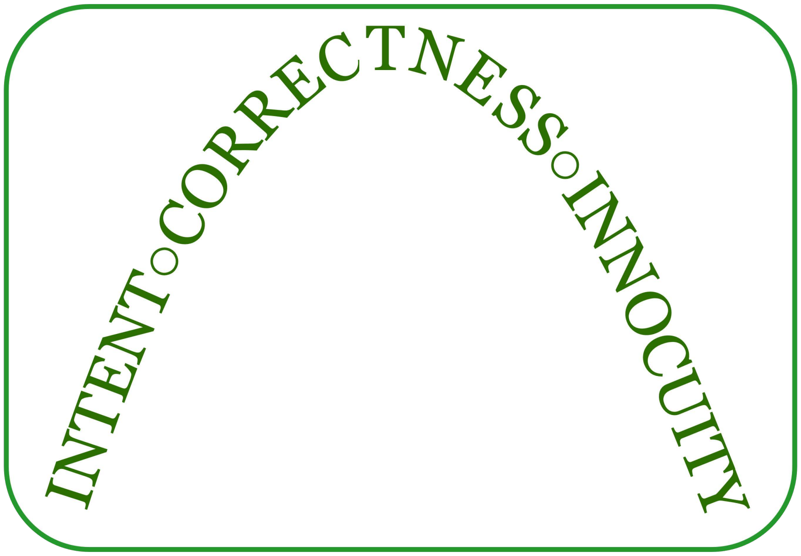
Note: The OED Online is cited to provide authoritative definitions. Similar definitions can be found in many other dictionaries. Readers without personal or institutional access to the OED can consult one of those other dictionaries without excessive danger of being misled.

Appendix: Images

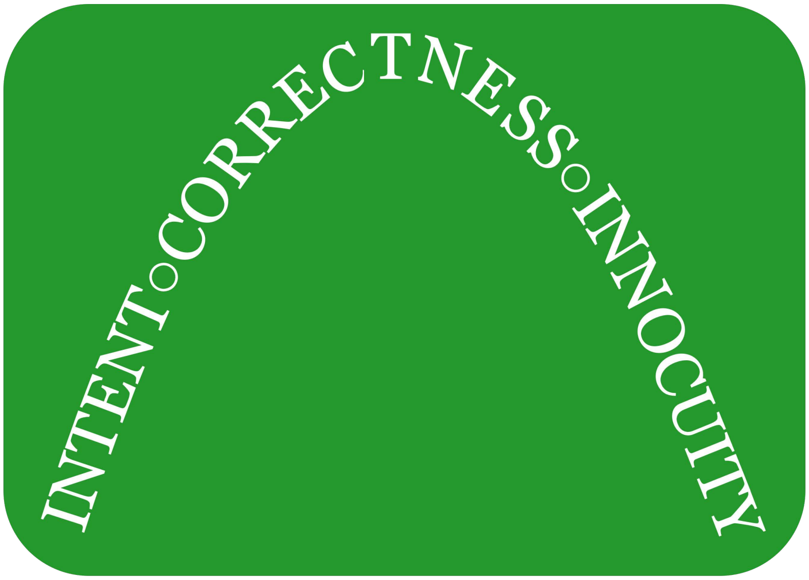
This appendix displays several variations of images that seem appropriate for providing a graphical identity to the Overarching Properties. Readers who would like copies of these images may get them by contacting the author.

Words only

Green on white

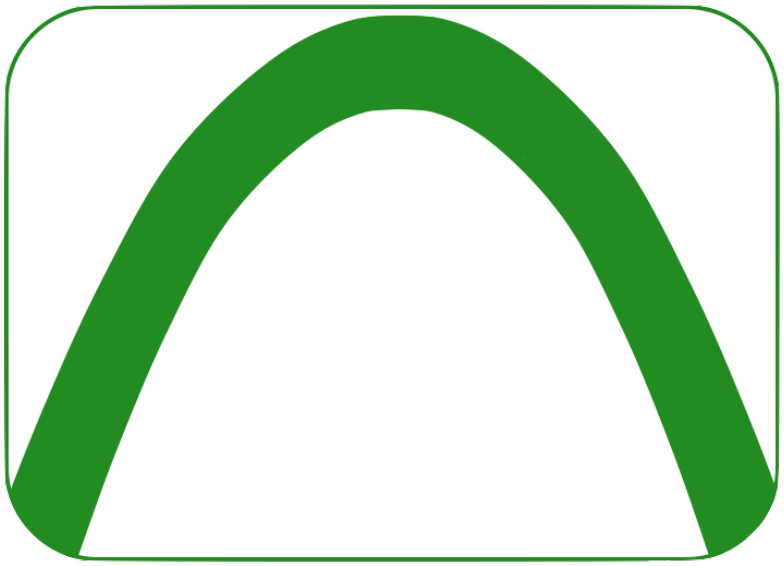


White on green

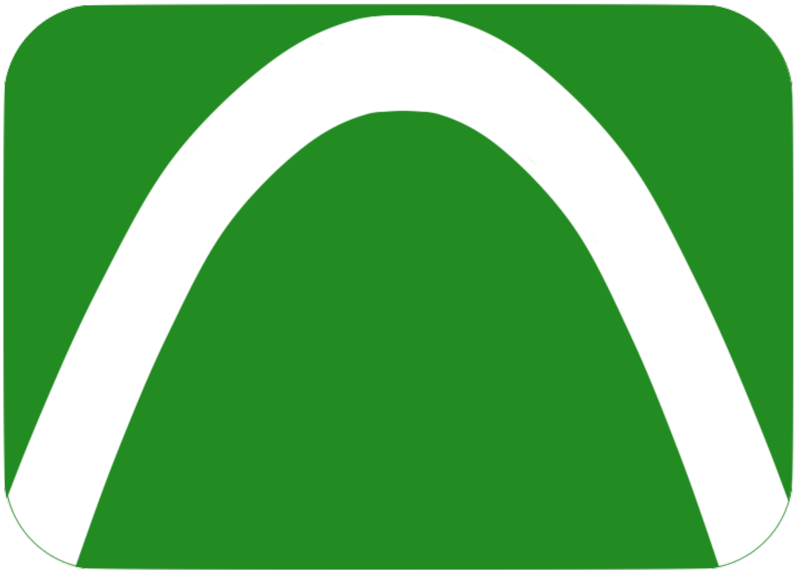


Arch only

Green on white



White on green



List of Contributors

The following members of the Overarching Properties Working Group contributed to the content of this paper in myriad ways.

M. Anthony Aiello, AdaCore
Clay Barber, Garmin International Inc.
Scott Beecher, Pratt & Whitney
Steve Beland, Boeing Commercial Airplanes
Duncan Brown, Rolls-Royce
Cyrille Comar, AdaCore
James Chelini, Verocel
Christophe Cucuron, AIRBUS
Zamira Daw, Raytheon Technologies Research Center
Tom Ferrell, Joby Aero Inc.
Mallory Graydon, NASA Langley Research Center
Robert Green, BAE Systems
Louise Gregor, Honeywell International
Chris Hubbs, Collins Aerospace
Tomasz Iwaszkiewicz, Verocel
Barbara Lingberg, Federal Aviation Administration
George Romanski, Federal Aviation Administration
Rodrigo Valério Magalhães, Brazillian National Civil Aviation Agency
Bernie Newman, Astronautics Corporation of America
Tammy M. Reeve, Patmos Engineering Services Inc.
Kimberly S. Wasson, Federated Safety LLC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
01-07-2019

2. REPORT TYPE
Technical Memorandum

3. DATES COVERED *(From - To)*
2016-2019

4. TITLE AND SUBTITLE
Understanding the Overarching Properties

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
C. Michael Holloway

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
340428.02.10.07.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, Virginia 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L–21043

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM–2019–220292

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES
An electronic version can be found at http://ntrs.nasa.gov.
This document does not constitute official guidance.

14. ABSTRACT

This document explains the purpose, history, and philosophy of the Overarching Properties, and explains the specific details of each property, the relationships among them, and some practical considerations that attach to their use. Although it has been extensively reviewed by over a dozen members of the Overarching Properties Working Group, **it does not constitute official guidance**, nor does it necessarily express a unanimously agreed view of the Working Group on every detail.

15. SUBJECT TERMS
philosophy, certification, guidance, safety, argument, cool

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
U	U	U	UU	31

19a. NAME OF RESPONSIBLE PERSON
STI Help Desk (email: help@sti.nasa.gov)

19b. TELEPHONE NUMBER ***(Include area code)***
(443) 757-5802