The Overarching Properties & Overarching Properties Related Arguments

Part 1

C. Michael Holloway
NASA Langley Research Center
c.michael.holloway@nasa.gov

July 2022

photo credit: C. Michael Holloway, 2009-07-27

Batting order

1. **Preliminaries**
2. **The Overarching Properties (OPs) :** philosophy & history
3. **The Overarching Properties:** details
4. **Argument:** terminology and principles
5. **Argument:** assessment
6. **Argument:** the Friendly Argument Notation (FAN)
7. **OP Related Arguments (OPRAs):** uniqueness
8. **OPRAs:** assessment
9. **Loose ends**

Batting order

1. **Preliminaries**
2. **The Overarching Properties (OPs) :** philosophy & history
3. **The Overarching Properties:** details

Preliminaries

Sponsorship

This work has also been sponsored in part by the **Federal Aviation Administration** through Interagency Agreements: IAI-1073, Annex 2, Assurance Case Applicability to Digital Systems; IA1-30333, Annex 1: Streamlining Assurance Via Overarching Properties (Savor); IA1-30333, Annex 2: Using the Overarching Properties in Novel Examples (Opine).

About Michael

As a teenager Michael Holloway could run really fast and catch baseballs well. Unrelatedly, he planned to become a constitutional lawyer and eventually a Justice of the Supreme Court of the United States. For non-academic reasons, he ended up as a senior research computer engineer at NASA Langley Research Center, where he explores epistemic issues in safety-critical systems.

photo credit: Annette D. Holloway, 2018-06-01

Preliminaries

Understanding the Overarching Properties. [2019]
ntrs.nasa.gov/citations/20190029284

A Friendly Argument Notation (FAN). [2020]
ntrs.nasa.gov/citations/20205002931

A Primer on Argument. [2021] ntrs.nasa.gov/citations/20210019993

A Primer on Argument Assessment. [2021]
ntrs.nasa.gov/citations/20210022807

An Introduction to Constructing and Assessing Overarching Properties Related Arguments (OPRAs). [2022]
ntrs.nasa.gov/citations/20210025425

Preliminaries

I will consider this talk **highly successful** if a 'substantial portion' of listeners …

- … were **not bored**
- … have thought, or will soon **think**, about at least one concept more intensely than they ever have before
- …(optionally) experienced, or will soon experience, **happy feelings** about the OPs, arguments, and/or OPRAs

Batting order

1. Preliminaries
2. **The Overarching Properties (OPs) :** philosophy & history

Consider our world …

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Now imagine with me …

… a world very much like our own.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

It's so much like our own, there is only …

… one exception.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Earth* has a perfect oracle …

… called Quinn.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Quinn is never wrong, …

… but he has limitations.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Quinn can only respond to inquiries …

… about propositions.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Quinn can only respond to inquiries …

For any P, he will respond with

True, if P is true

False, if P is false

… about propositions.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Quinn can only respond to inquiries …

For any P, he will respond with

True, if P is true

False, if P is false

Remember Quinn is never wrong.

If someone thinks Quinn is wrong, ‘tis they who are wrong, not Quinn.

… about propositions.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

What on Earth* does any of this have to do with Overarching Properties?!

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

What on Earth* does any of this have to do with Overarching Properties?!

Quinn can't answer because the question is not about a proposition.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

What on Earth* does any of this have to do with Overarching Properties?!

Quinn can't answer because the question is not about a proposition.

Quinn can, however, identify the following as **True**:

A connection to the OPs will soon be revealed.

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

Us: Our system is safe enough to be approved.

Quinn: **True**

Us: Our system is safe enough to be approved.

Quinn: **True**

The system should be approved

Nothing at all needs to be known about how the system was developed and assured.

Us: A system that possesses three specific properties is safe enough to be approved.

Quinn: **True**

Us: Our system possesses the three specific properties.

Quinn: **True**

Thus …

Us: Our system is safe enough to be approved.

Quinn: **True**

Thus …

Us: Our system is safe enough to be approved.

Quinn: **True**

The system should be approved

Nothing at all needs to be known about how the system was developed and assured.

Suppose the three specific properties are called Alpha, Beta, and Rho …

Us: Our system possesses Alpha, Beta, and Rho.

Quinn: **True**

means

Us: Our system is safe enough to be approved.

Quinn: **True**

Back to Quinn-less Earth …

photo credit: NASA as13-60-8588, 1970-04-17, https://images.nasa.gov/details-as13-60-8588 (black background removed)

… the general principle remains

Given a sufficient set of properties the possession of which ensures a system is safe enough to be approved …

then

deciding whether to approve a system requires **only** determining whether the system possesses those properties.

The Overarching Properties were created to constitute such a set.

Origin story - motivators

2005 – 2011	DO-178C + supplements (officially endorsed in 2013)
2012 - 2016	Explicate ‘78 work (published 2018)
2014	DeWalt/McCormick Technology Independent Assurance Method paper
2014 - 2015	FAA internal conversations …
2015	FAA invitation only “Meta Objectives” workshop

Origin story

2015	FAA invitation only "Meta Objectives" workshop
2016	Additional meetings (virtual and in-person)
2016-09	Public unveiling of Overarching Properties
2017-19	Refining OPs, pursuing ways to demonstrate possession
2019	*Understanding the Overarching Properties* published
2020-22	Case studies, pilot projects, eventually OPRAs
2022-2?	Actual use of OPRAs & other techniques

Batting order

1. **Preliminaries**
2. **The Overarching Properties (OPs) :** philosophy & history
3. **The Overarching Properties:** details

Overarching Properties

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*.

See *Understanding the Overarching Properties* (NASA/TM-2019-220292)
https://bit.ly/UtOPs

Overarching Properties

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

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

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

Definitions

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

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

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

d. *Item*: "A hardware or software element having bounded and well-defined interfaces." (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 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)

Overarching Properties

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*.

Requisites required for showing possession of the Overarching Properties

a. *Defined intended behavior* exists.

b. *Failure conditions* are defined.

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

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

e. The *implementation* exists.

f. 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.

Overarching Properties

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*.

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*.

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

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

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

Definitions

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

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

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

d. *Item*: "A hardware or software element having bounded and well-defined interfaces." (from ED-79A/ARP4754A)

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 required for showing possession of the Overarching Properties

a. *Defined intended behavior* exists.

b. *Failure conditions* are defined.

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

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

e. The *implementation* exists.

f. 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 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 e[illegible] f the *implementation*.

The Overarching Properties are a novel expression of time-honored principles.

The meaning of the properties is fully defined by the three property statements and eight definitions.

- The property labels do not affect the meaning of the properties in any way; they are included only for convenience of reference.
- The requisites, assumptions, and constraints sections do not affect the meaning of the properties in any way; they only affect the means by which property possession may be shown.

Advances in assurance methods may eventually justify

- cancellation of some constraints
- refinement of requisites
- alteration of assumptions

Applying the Overarching Properties to some parts of a system while using something else for other parts is acceptable.

Batting order

1. **Preliminaries**
2. **The Overarching Properties (OPs) :** philosophy & history
3. **The Overarching Properties:** details
4. **Argument:** terminology and principles
5. **Argument:** assessment
6. **Argument:** the Friendly Argument Notation (FAN)
7. **OP Related Arguments (OPRAs):** uniqueness
8. **OPRAs:** assessment
9. **Loose ends**