
False Beliefs about the Overarching Properties & Overarching Properties Related Arguments

— C. Michael Holloway —

NASA Langley Research Center
c.michael.holloway@nasa.gov

September 2022

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

Sponsorship

This work has 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).

The foundational papers

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

Three-part tutorial

Part 1 - The Overarching Properties

https://www.youtube.com/watch?v=Z2nDdxnoD_k

Part 2 - Argument

https://www.youtube.com/watch?v=Nw1LDrV_EqI

Part 3 - Overarching Properties Related Arguments

<https://www.youtube.com/watch?v=TqcuXx0NISO&t=2s>

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*.

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 *items* 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)

From False to True Beliefs about the OPs

The constraints alter the meaning of the OPs.

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

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

From **False** to **True** Beliefs about the OPs

The constraints have no effect on the meaning of the Overarching Properties.

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

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

From **False** to **True** Beliefs about the OPs

The constraints have no effect on the meaning of the Overarching Properties.

The OPs are intended to provide an organizing foundation from which a means of compliance may be built.

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

From **False** to **True** Beliefs about the OPs

The constraints have no effect on the meaning of the Overarching Properties.

The OPs are intended to provide an organizing foundation from which a means of compliance may be built.

The OPs may be used for a part of a system while some other approach is used for other parts.

From False to True Beliefs about OPRAs

OPRAs must be created for everything.

OPRAs are based on formal logic.

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

From False to True Beliefs about OPRAs

OPRAs are needed only when OPRAs are needed.

OPRAs are based on formal logic.

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

From False to True Beliefs about OPRAs

OPRAs are needed only when OPRAs are needed.

OPRAs are based on informal logic.

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

From False to True Beliefs about OPRAs

OPRAs are needed only when OPRAs are needed.

OPRAs are based on informal logic.

Assessing the cogency of OPRAs is not necessarily too hard to be practical.

