

A Rapid Introduction to
**the Foundations for
Assessing & Constructing
Overarching Properties Related Arguments**

C. Michael Holloway

`c.michael.holloway@nasa.gov`

International Aviation Software Summit

2021-06-23/24

A quick reminder about the OPs

<https://ntrs.nasa.gov/citations/20190029284>

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)

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 all of the *implementation*.

A Primer on Argument (OP edition)

<https://ntrs.nasa.gov/citations/20205003337>

argument: your attempt to convince others to **believe** **conclusion** through **reasoning** from one or more **premises**

conclusion: the statement you want your audience to **believe**

premise: a statement you think your audience **believes**

evidence: a name you may give to a **premise** you're certain your audience **believes**

assumption: a **premise** you are not prepared to justify if your audience does not **believe** it

reasoning : why you think the **premises** should cause your audience to **believe** your **conclusion**

binding: an association between a term used in an **argument** and the real-world information to which that term refers.

defeater: a statement that may cause your audience to not **believe** your **conclusion**

believe: accept as true

argument: your attempt to convince others to **believe** **conclusion** through **reasoning** from one or more **premises**

conclusion: the statement you want your audience to **believe**

premise: a statement you think your audience **believes**

evidence: a name you may give to a **premise** you're certain your audience **believes**

assumption: a **premise** you are not prepared to justify if your audience does not **believe** it

reasoning : why you think the **premises** should cause your audience to **believe** your **conclusion**

binding: an association between a term used in an **argument** and the real-world information to which that term refers.

defeater: a statement that may cause your audience to not **believe** your **conclusion**

believe: accept as true

An argument is called **cogent** if it rationally justifies **believing** its **conclusion** to the required standard of confidence.

atomic argument: consists of a single **conclusion** together with its immediate **reasoning**, **premises**, **bindings** (if present), and **defeaters** (if present).

compound argument: an argument consisting of more than one **atomic argument**.

argument: your attempt to convince others to **believe conclusion** through **reasoning** from one or more **premises**

conclusion: the statement you want your audience to **believe**

premise: a statement you think your audience **believes**

evidence: a name you may give to a **premise** you're certain your audience **believes**

assumption: a **premise** you are not prepared to justify if your audience does not **believe** it

reasoning : why you think the **premises** should cause your audience to **believe** your **conclusion**

binding: an association between a term used in an **argument** and the real-world information to which that term refers.

defeater: a statement that may cause your audience to not **believe** your **conclusion**

believe: accept as true

atomic argument: consists of a single **conclusion** together with its immediate **reasoning**, **premises**, **bindings** (if present), and **defeaters** (if present)

compound argument: an **argument** consisting of more than one **atomic argument**

An **argument** is called **cogent** if it rationally justifies **believing** its **conclusion** to the required standard of confidence.

The precept of **Locality** reminds us that we assess the **cogency** of a **compound argument** one **atomic argument** at a time.

The precept of **Depth** reminds us to descend no deeper than necessary.

The precept of **Certainty** reminds us that certainty is certainly not possible.

The precept of **Change** reminds us that arguments are living structures.

The precept of **Induction** reminds us that *the arguments* with which we will concern ourselves are uniformly inductive arguments.

The precept of **Plausibility** reminds us that presuppositions predetermine plausibility.

Creating arguments and ensuring they are cogent are the hard parts.

The Friendly Argument Notation (FAN)

<https://ntrs.nasa.gov/citations/20205002931>

directly embodies primitives defined in the *Primer*

The Friendly Argument Notation (FAN)



<https://ntrs.nasa.gov/citations/20205002931>

Believing

the statement you want your audience to believe

is justified by applying

why you think the premises should cause your audience to believe your conclusion

to these premises

a statement you think your audience believes

...

[with these bindings

word: definition for word for this argument . . .

reference: link to real-world information relevant to this argument . . .]

[unless

a statement that may cause your audience to not believe your conclusion

...]

Believing

<MDSS> possesses <Intent>

is justified by applying

The definition of <Intent>

to these premises

<MDSS> <DIB> is correct with respect to its <DeB>

<MDSS> <DIB> is complete with respect to its <DeB>

with these bindings

<MDSS>: subsystem as circumscribed by development artifacts X,Y,Z

<UtOPs>: the document at <https://ntrs.nasa.gov/citations/20190029284>

<Intent>: see definition in <UtOPS>

<DIB>: 'defined intended behavior' as defined in <UtOPs>)

<DeB>: 'desired behavior' as defined in <UtOPs>)

General Atomic Argument Assessment Questions

1 Is the syntax proper?

2 Are the premises acceptable?

3 Is the reasoning acceptable?

4 Is saying “Yes” to the conclusion justified?

General Atomic Argument Assessment Questions

- 1 Is the syntax proper?
- 2 Are the premises acceptable?
- 3 Is the reasoning acceptable?
- 4 Is saying “Yes” to the conclusion justified?

A spry argument is a cogent argument.

*Are the **premises** acceptable?*

a. Is each **premise** **believe**-able?

b. Is each **premise** relevant to the **conclusion**?

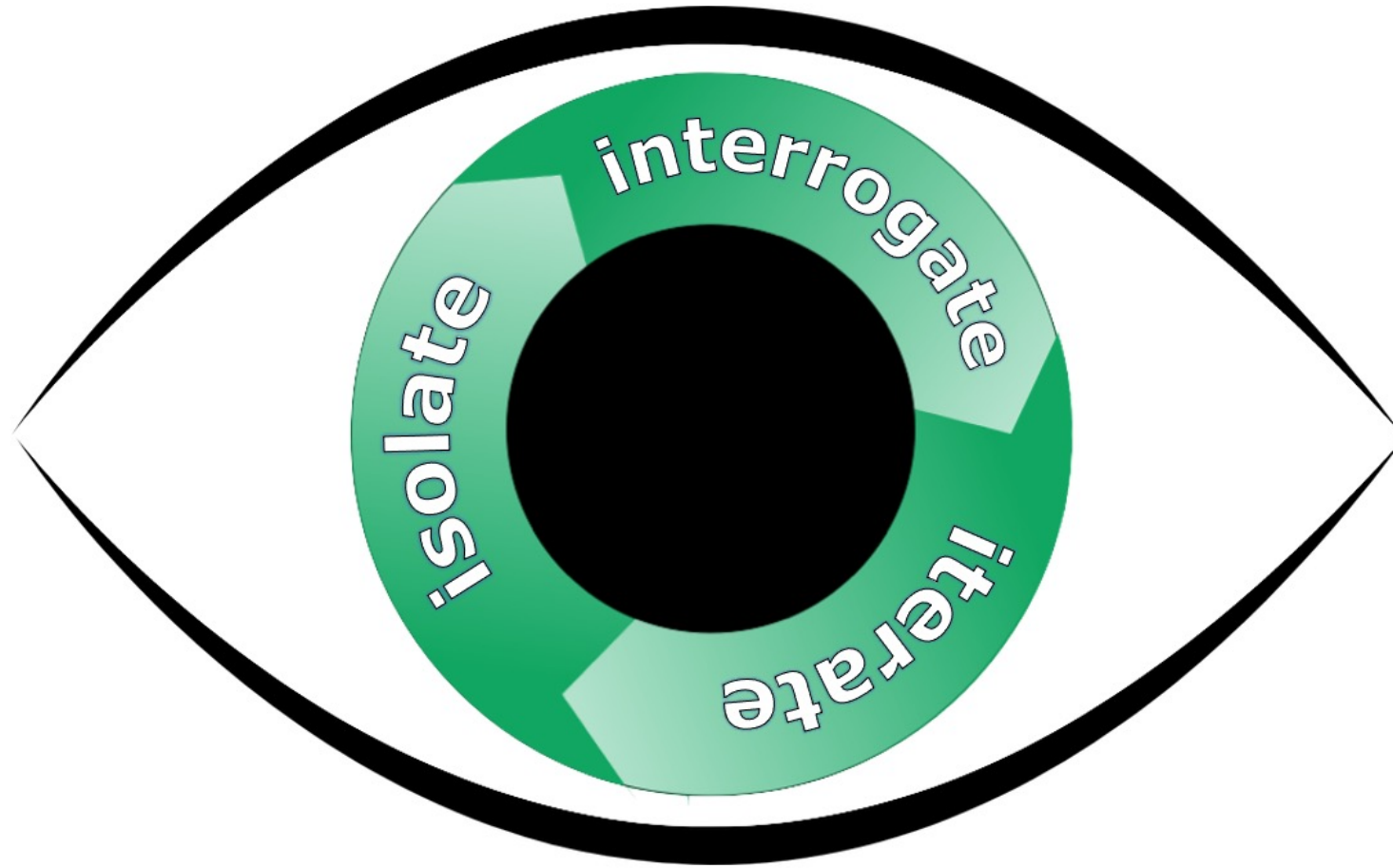
*Are the **premises** acceptable?*

a. Is each **premise** **believe**-able?

Must fall into one of these categories:

- (a) expresses a proposition that is ‘universally’ accepted as true
- (b) expresses a proposition that is accepted as true within the relevant domain
- (c) supported by an **argument** (provisionally presumed to be **cogent**)
- (d) supported by external artifacts that are accepted within the domain as being sufficient to establish its truth
- (e) at a later stage of argument development, it will fall into category (c) or (d)
- (f) is an assumption accepted by all stakeholders and clearly identified as such

Compound Argument Assessment Approach



Questions?