

Overarching Properties

29 August 2016

Overarching Property Statement:

Intent: The defined intended functions are correct and complete with respect to the desired system behavior.

Definitions: words / phrases in the Overarching Property description

- a. Desired system behavior: System needs and constraints expressed by the stakeholders.
- b. Defined intended functions: The record of the system needs and constraints as expressed by stakeholders.
- c. Failure Condition(s): A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events. (From ARP 4754A)

Pre-requisites: which must exist to allow Overarching Property satisfaction to be shown

- a. Defined intended functions exists.
- b. Failure conditions are defined for the aircraft systems.
- c. Design Assurance Levels (DALs) are assigned using the failure condition classifications.

Constraints: on how Overarching Property satisfaction must be demonstrated

- a. The process to satisfy this Overarching Property must be defined and conducted as defined.
- b. The defined intended functions must address the failure conditions.
- c. Criteria for evaluating the artifacts are defined and shown to be satisfied individually and collectively.
- d. All artifacts required to establish the Overarching Property are under configuration management and change control.

Assumptions: which need only be stated, not justified (if any)

- a. Stakeholders have the system knowledge to express the desired system behavior.
- b. Performing system safety assessments is not covered by these Overarching Properties.

Overarching Properties

Overarching Property Statement:

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

Definitions: words / phrases in the Overarching Property description

- a. *Implementation*: Item or collection of items contributing to system realization, for which acceptance or approval is being sought; item (from ARP 4754A) is a hardware or software element having bounded and well-defined interfaces.
- b. *Defined intended functions*: The record of the system needs and constraints as expressed by stakeholders.
- c. *Foreseeable operating conditions*: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions.

Pre-requisites: which must exist to allow Overarching Property satisfaction to be shown

- a. *Defined intended functions* exists.
- b. The *implementation* of the functions exists.
- c. The record of the *foreseeable operating conditions* exists.

Constraints: on how Overarching Property satisfaction must be demonstrated

- a. The process to satisfy this Overarching Property must be defined and conducted as defined.
- b. When tiers of decomposition are used, the means of showing correctness among the tiers and to the *defined intended functions* must be defined and conducted as defined.
- c. The *implementation* must be correct when functioning as part of the integrated system or in environment(s) representative of the integrated system.
- d. Criteria for evaluating the artifacts are defined and shown to be satisfied individually and collectively.
- e. All artifacts required to establish the Overarching Property are under configuration management and change control.
- f. All design and manufacturing data to support consistent replication of the type design and instructions for continued airworthiness must be established.

Assumptions: which need only be stated, not justified (if any)

None.

Overarching Properties

Overarching Property Statement:

Necessity: All of the *implementation* is either required by the *defined intended functions* or is without *unacceptable safety impact*.

Definitions: words / phrases in the Overarching Property description

- a. *Unacceptable Safety Impact*: An impact which compromises the system safety assessment.
- b. *Defined intended functions*: The record of the system needs and constraints as expressed by stakeholders.
- c. *Implementation*: Item or collection of items contributing to system realization, for which acceptance or approval is being sought; item (from ARP 4754A) is a hardware or software element having bounded and well-defined interfaces.

Pre-requisites: which must exist to allow Overarching Property satisfaction to be shown

- a. *Defined intended functions* exists.
- b. The *implementation* or a representation of the implementation exists.
- c. The system safety assessment exists.

Constraints: on how Overarching Property satisfaction must be demonstrated

- a. The process to satisfy this Overarching Property must be defined and conducted as defined.
- b. The system safety assessment must address all of the implementation.
- c. Criteria for evaluating the artifacts are defined and shown to be satisfied individually and collectively.
- d. All artifacts required to establish the Overarching Property are under configuration management and change control.

Assumptions: which need only be stated, not justified (if any)

- a. For a TSOA appliance there may not be a complete system safety assessment for the final installation at the appliance level.