RTRC
Raytheon Technologies Research Center

GO BEYOND




Zamira Daw
AI Systems Engineering Team Leader
Raytheon Technologies Research Center

Scott Beecher
Engineering Fellow and Certification Designee
Controls and Diagnostics Systems, Engineering
Pratt & Whitney

Overarching Properties as means of compliance: An industrial case study

This research was supported by NASA through grant no. 80NSSC20M0006.

Industrial Motivation

- Introduction of Artificial Intelligence and other likewise technologies into commercial products
- A flexible and customizable process for unconventional systems, which current standards are either not applicable or require extra resources while not adding extra safety assurance
- Existing certification standards are still good practices that should be followed when appropriate

Overarching Properties (OPs)

OPs concept has been developed by an international Overarching Properties Working Group (OPWG) with NASA and certifying agencies including FAA and EASA support

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*.

Informal Definition

Intent:
Stakeholders' intent is captured in requirements

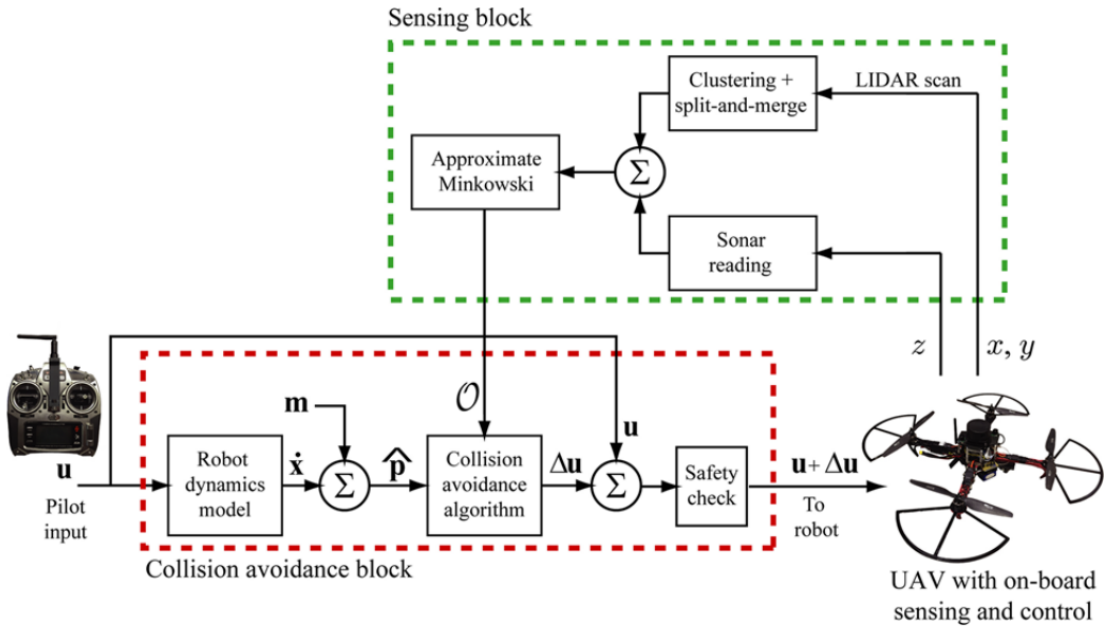
Correctness:
Implementation matches requirements

Innocuity:
Implementation contains no behavior undermining safety

Documentation:
Understanding the Overarching Properties https://ntrs.nasa.gov/citations/20190029284
A Primer on Argument (Overarching Properties Edition) https://ntrs.nasa.gov/citations/20205003337

Specimen scope

Robot dynamic model for UAV with Model-based collision avoidance

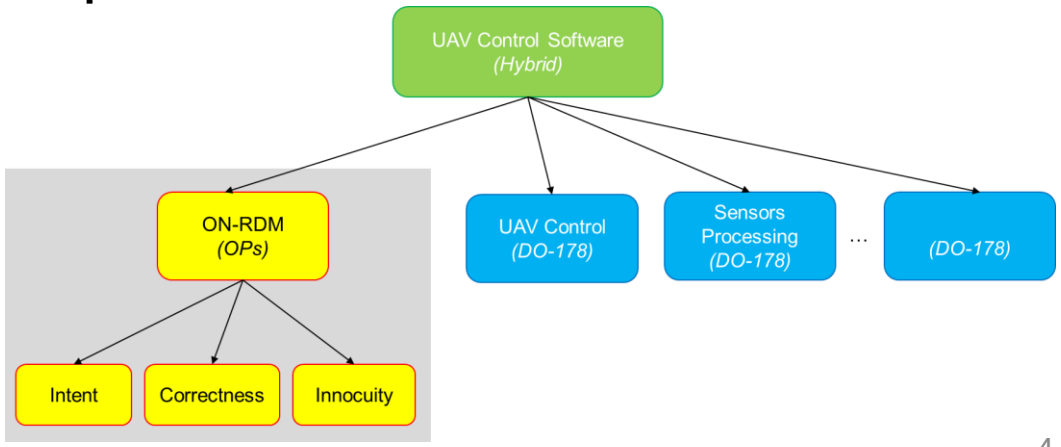


Bareiss, Daman, Joseph R. Bourne, and Kam K. Leang. "On-board model-based automatic collision avoidance: application in remotely-piloted unmanned aerial vehicles." Autonomous Robots 41.7 (2017): 1539-1554.

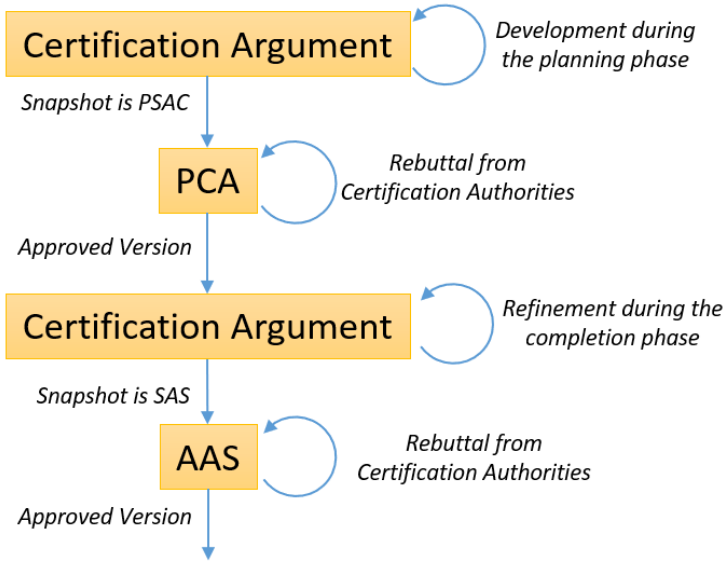
Hybrid certification approach

- OPs for an on-board robot dynamic (**ON-RDM**) model and DO-178C for the rest of the UAV
- The on-board model should ensure:
  - Deterministic timing results
  - Estimated values have to be accurate and robust ***in relation to*** the off-board robot dynamics model
- The off-board robot dynamic model (**OFF-RDM**) is a accurate representation of the robot

Scope of the OPs:

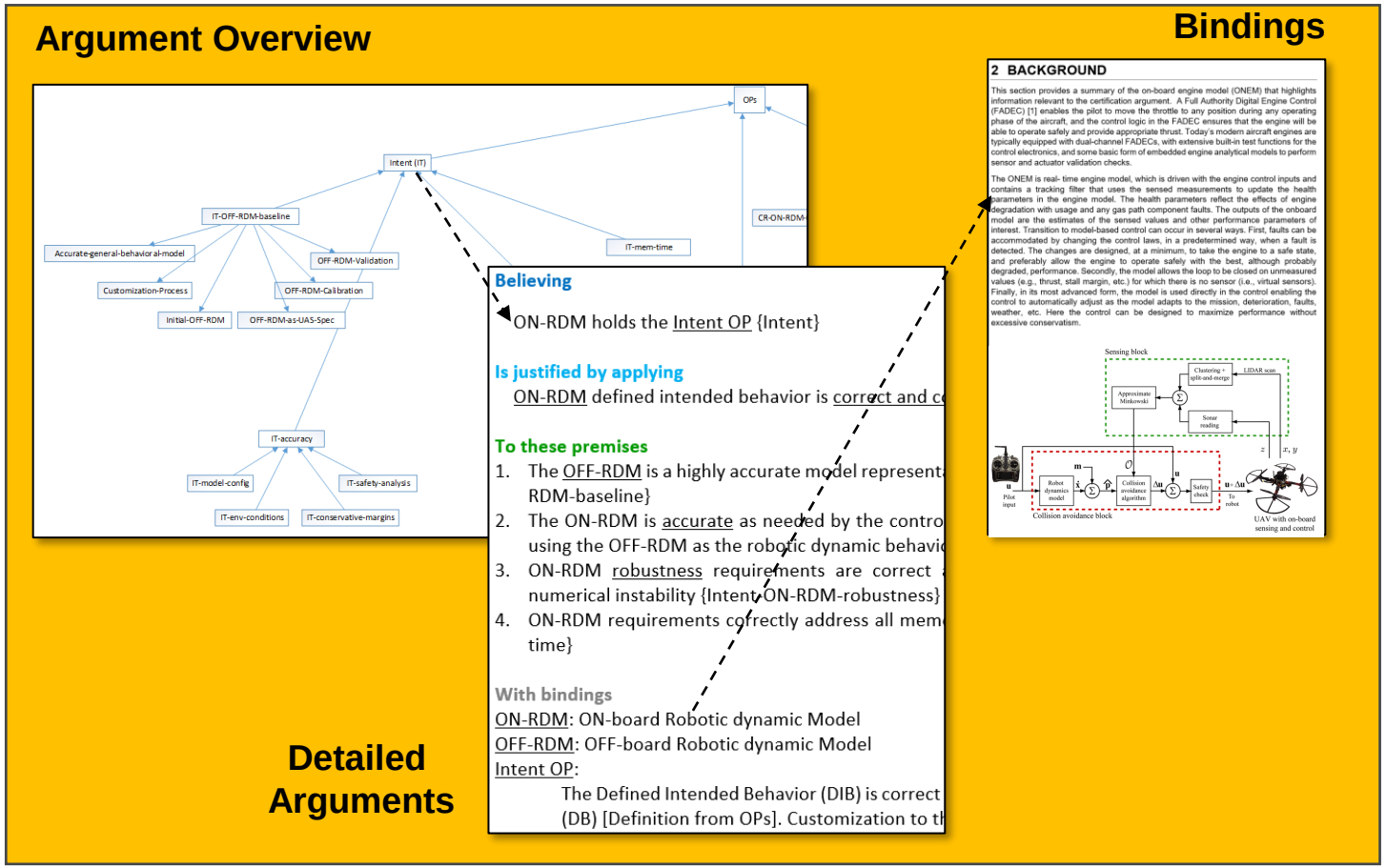


Certification Process using OPs



PCA: *Planned Certification Argument*
AAS: *Argument Accomplishment Summary*

Certification Argument



Assurance Cases

An **assurance case** is an explicit argument that a system or service is acceptable for its intended use

Argument: An attempt to convince others to believe a conclusion through reasoning and one or more premises.

Conclusion: The statement you want your audience to believe.

Premise: A statement you think your audience believes.

Reasoning: States 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: Statement that may cause your audience to not believe your conclusion.

***Documentation**:*
The Friendly Argument Notation (FAN) https://ntrs.nasa.gov/citations/20205002931

The Friendly Argument Notation

- Developed by Michael Holloway, NASA.
- Writing argument in an easy and understandable way
- *Major focus on the content of the argument*
- Accepted by OPWG

Believing
ON-RDM holds the Intent OP {Intent}

Is justified by applying
ON-RDM defined intended behavior (DIB) is correct and complete with respect to the DB

To these premises

1. The OFF-RDM is a highly accurate model representation of the robot dynamics {IT-OFF-RDM-baseline}
2. The ON-RDM is accurate as needed by the control in relation with the robot dynamics by using the OFF-RDM as the robot dynamics representation {IT-accuracy}
3. ON-RDM robustness requirements are correct and complete for off-nominal input values and numerical instability {IT-robustness}
4. ON-RDM requirements correctly address all memory and timing constraints {IT-mem-time}

With bindings
ON-RDM: ON-board Robot Dynamic Model
OFF-RDM: OFF-board Robot Dynamic Model

Intent OP:
The Defined Intended Behavior (DIB) is correct and complete with respect to the Desired Behavior (DB) (Definition from OPs)
Customization to this project:
DIB = Requirements of ON-RDM
DB = Model of the robot dynamics at a level of accuracy **as needed by the control system**

Correct and complete:
- The complete detailed description of the behavior of the ON-RDM correctly captures the **robot dynamics** plus **accuracy**, **robustness**, **memory** and **timing** requirements defined by the control system {ON-RDM-behavior}
- Correctness within the context of the intent of ON-RDM means **functional equivalency to the robot dynamics**

Highly accurate: aims to qualify the accuracy of the ON-RDM and the OFF-RM in relation to the robot dynamics

Accuracy: represents the difference between the ON-RDM against the robot dynamics, which is defined by the difference of the ON-RDM output parameters against the OFF-RDM output parameters under the same inputs due to premise [IT-OFF-RDM-baseline]

Robustness: corresponds to "The extent to which software can continue to operate correctly despite abnormal inputs and conditions" (Definition from RTCA DO-178C/ED-12C). Additional to abnormal inputs and conditions common to embedded software, ON-RDM is affected by other abnormal conditions, such as, instability due to discrete mathematical abstraction and abrupt changes in the inputs

Believing

ON-RDM holds Innocuity {Innocuity}

Is justified by applying

Any part of the executable ON-RDM that is not required by the DIB has no unacceptable impact

To these premises

1. Open/retained problems represent non-required behaviors {IO-open-problems}
2. Unexpected behaviors caused by implementation choices, such as, numerical instability, inaccuracy, and exceptions are addressed by the DIB {IO-impl-choices-DIB}
3. Other unexpected behaviors caused by implementation choices that are not addressed in the DIB are uncovered by system regression testing and robustness testing {IO-impl-choices-noDIB}
4. Common software functionalities or technologies that might cause unintended behaviors are not used in ON-RDM implementation {IO-NA-common-unint-beh}
5. Safety assessment addresses all open/retained problems and unexpected behaviors caused by implementation choices {IO-safety-assess}
6. Open/retained problems and implementation choices have no unacceptable impact as concluded by the safety assessment {IO-safety-impact}

With bindings

ON-RDM: ON-board Robot Dynamic Model

Innocuity: Any part of the implementation that is not required by the Defined Intended Behavior (DIB) has no unacceptable impact. Customization to this project:

- Implementation = Executable ON-RDM
- DIB = Requirements of ON-RDM defined in intent (robot dynamics, accuracy, robustness, memory and timing requirements). **Any additional requirements added during the development process are added to the DIB**.

Open/retained problems: Throughout verification activities when the implementation does not match the requirements a problem report is created. Based on a control board assessment, the problem can remain open for a specific software release.

Implementation choices: unintended behaviors that can emerge due to approximation of the OFF-RDM (accuracy), and due to additional behaviors related directly to the ON-RDM implementation. ON-RDM Implementation:

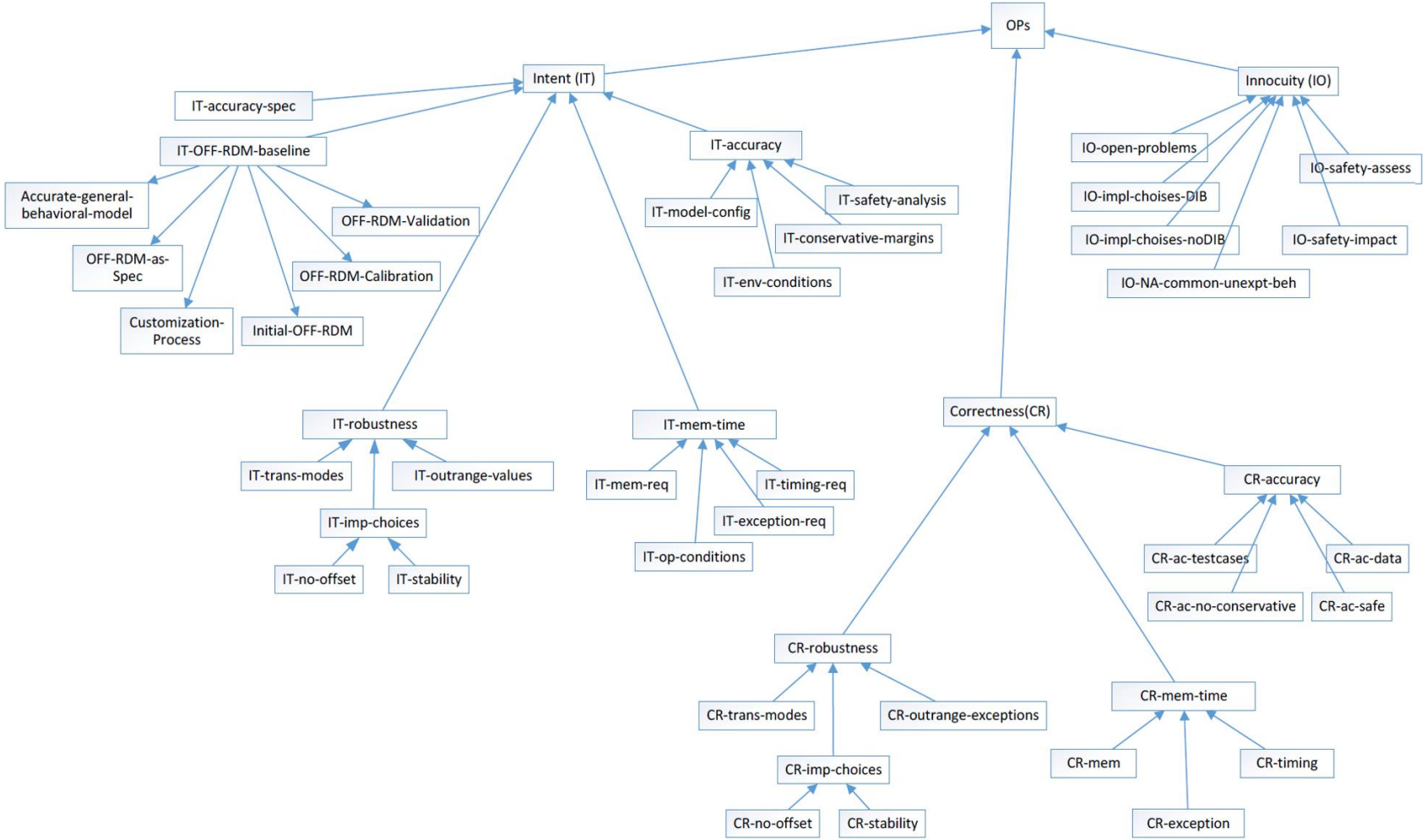
- ON-RDM can be implemented using component-based physics equations, lookup tables, approximations using linear equation systems, physic-based algorithmic approximation or neural networks.
- In this specific implementation *physic-based algorithmic approximation*, unintended behaviors are numerical instability due to discretization of the calculation and the constraints of the target platform, such as timing and memory.

Common software functionalities or technologies: External developed libraries, COTS, multi-tasking and multi-core, Non-deterministic algorithms, and machine learning functions.

Argument Structure

Raytheon Technologies Research Center

Planned Certification Argument (PCA)



Evidence

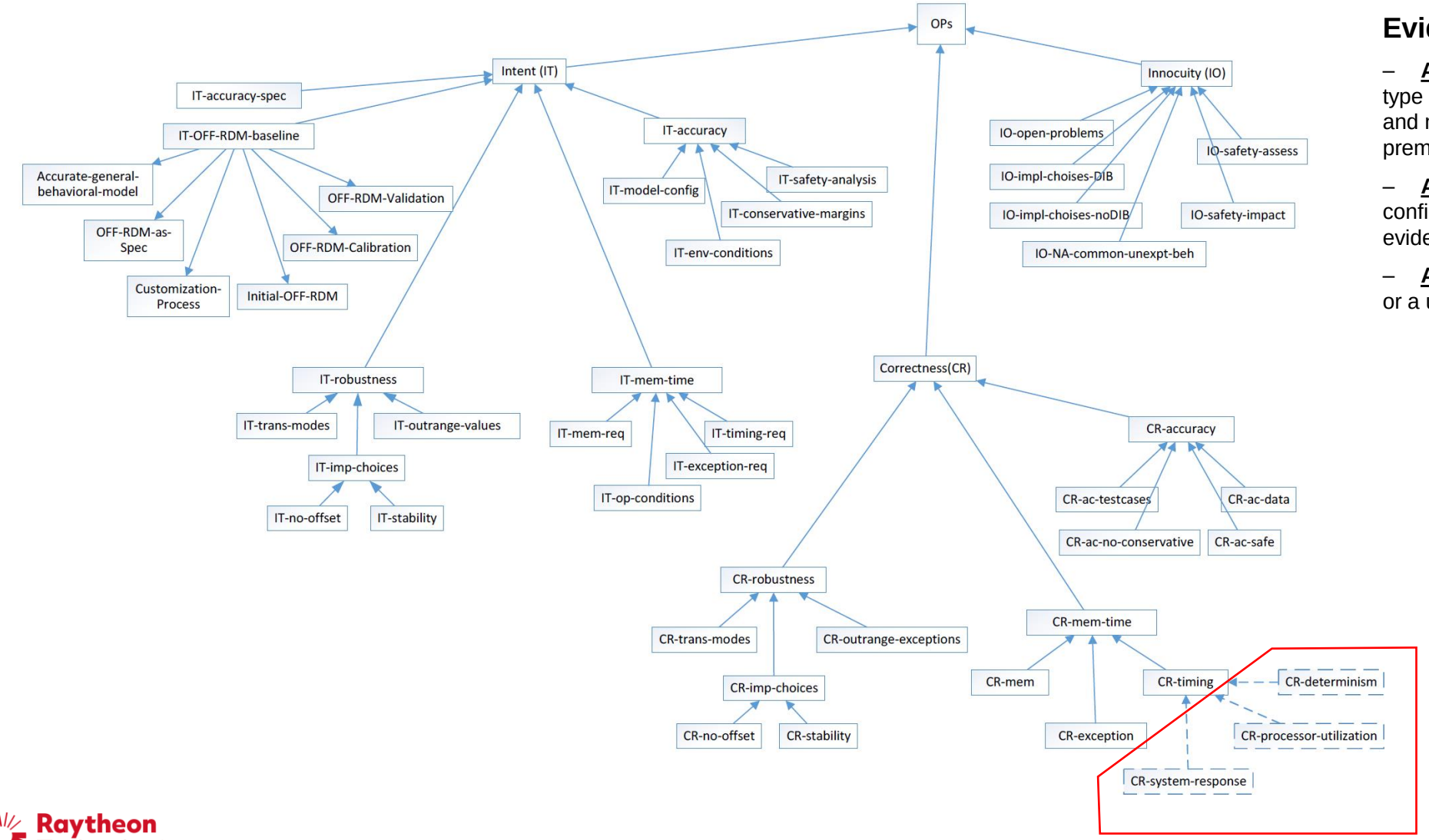
– **Artifact Type:** Description of the artifact type that is enough to understand the scope and nature of how the artifact supports the premise.

– **Artifact Control Category:** Establish the configuration control category of the evidence.

Argument Structure

RTRC
Raytheon Technologies Research Center

Argument Accomplishment Summary (AAS)



Evidence

– **Artifact Type:** Description of the artifact type that is enough to understand the scope and nature of how the artifact supports the premise.

– **Artifact Control Category:** Establish the configuration control category of the evidence.

– **Artifact:** Link to the evidentiary artifacts or a unique identifier or a title.

Takeaways

1. OPs potentially enable more flexible, safe, yet complete and efficient approaches to certification approval

2. The hybrid approach combines OPs with existing standards, where existing standards are not sufficient or require additional effort without commensurate additional safety assurance
   – We envision that the hybrid approach will be the common approach

3. Required skills to create an OP-argument are certification/domain background and argumentation expertise (suggested two team members)

4. The industrial example shows that the high-level properties are held by the system component effectively using a formal certification argument
   – Practical use of OPs with realistic certification artifacts
   – Multi-domain and criticality leveling examples are needed (Phase II)