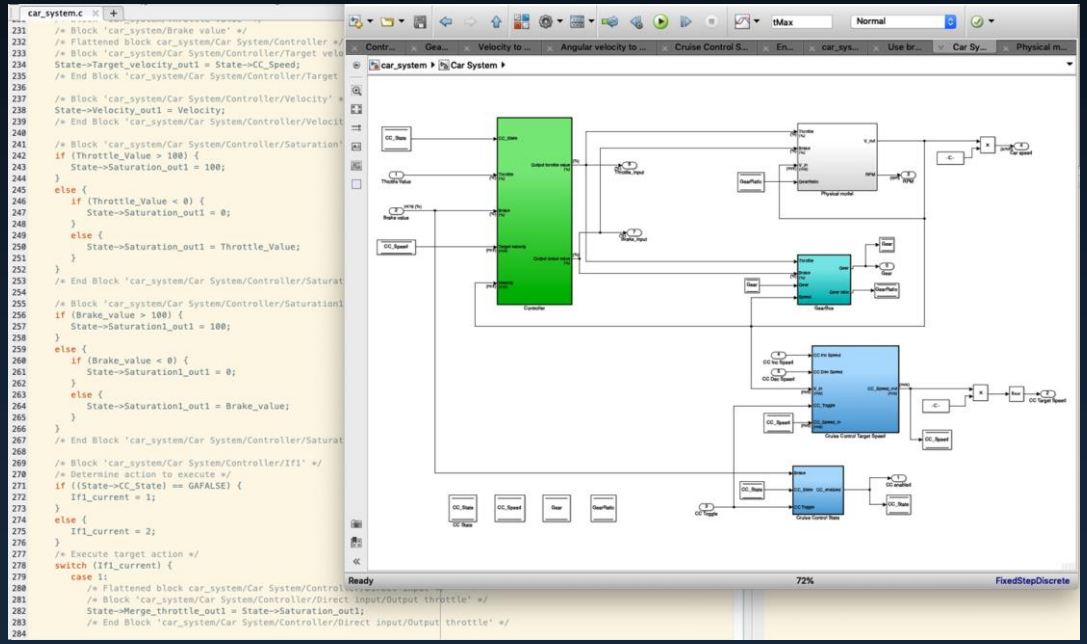
An Assurance Case based on Overarching Properties for QGen: a TQL1 Code Generator

M. Anthony Aiello, Cyrille Comar, José F. Ruiz
2020-01-30

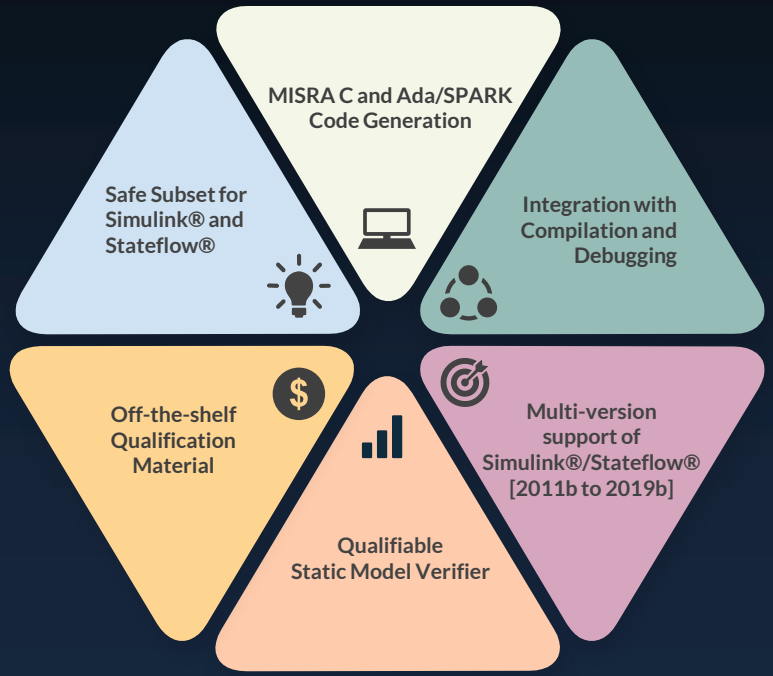
QGen

Trusted Code Generator



- 120 Simulink blocks
- Stateflow support
- MISRA C:2012 or SPARK
- Incremental code generation
- Customizable
- Model flattening at different levels
- Consistent, stable code
    - Across Simulink versions
    - Across minor layout changes

QGen Toolset Overview



From Simulink® & Stateflow® to Ada, SPARK (Ada subset) or MISRA C

Model-level debugger with integrated Ada/C S-Function debugging

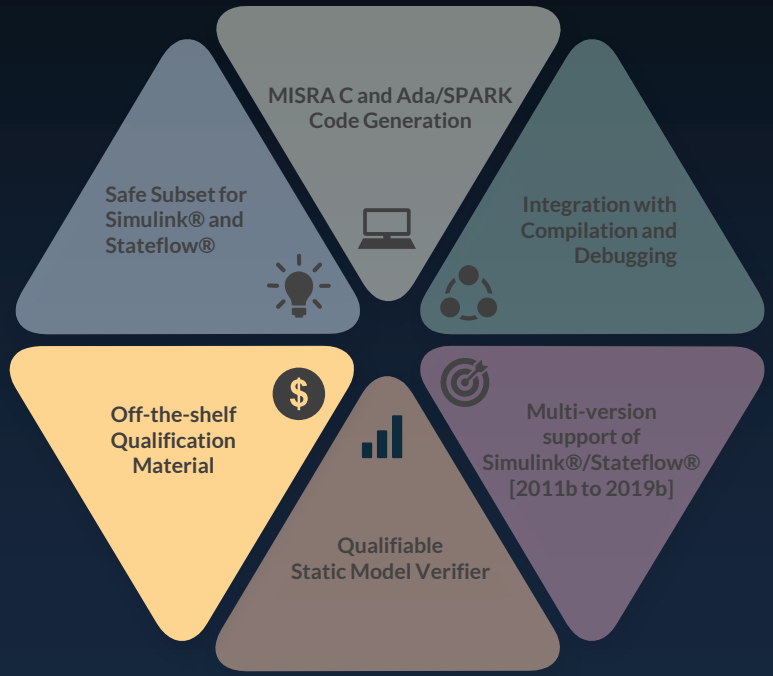
120 Simulink® blocks and expressive Stateflow® subset

AdaCore Support directly provided by QGen engineers

TQL-1 Tool Qualification for MATLAB R2018b in 2020

Static verifier detecting runtime errors and violations of functional properties at the model level

QGen Toolset Overview



From Simulink® & Stateflow® to Ada, SPARK (Ada subset) or MISRA C

Model-level debugger with integrated Ada/C S-Function debugging

120 Simulink® blocks and expressive Stateflow® subset

AdaCore Support directly provided by QGen engineers

TQL-1 Tool Qualification for MATLAB R2018b in 2020

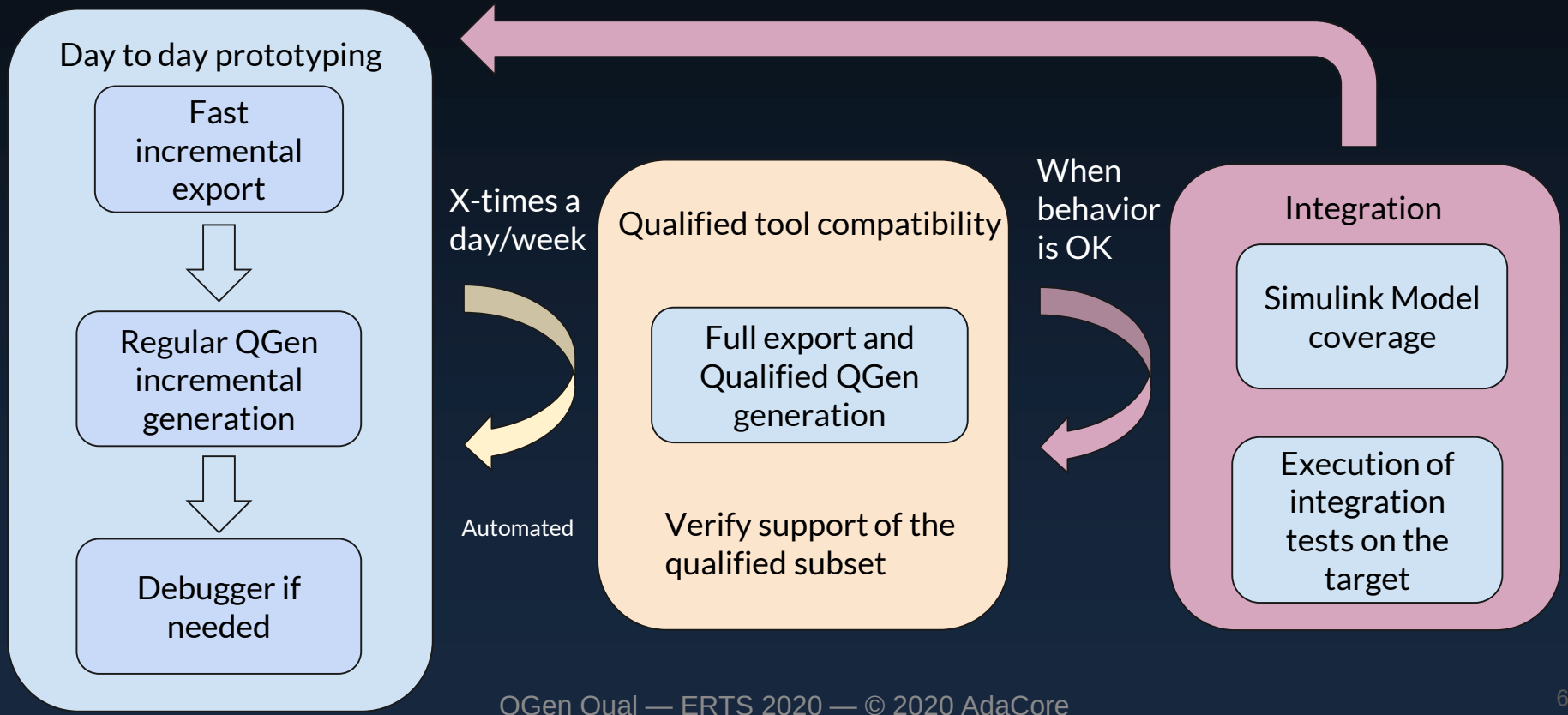
Static verifier detecting runtime errors and violations of functional properties at the model level

System Certification & Tool Qualification

- Certifying software to DO-178C Level A is expensive!
  - Many required source-code review & verification objectives, including:
    - Low-Level Requirements (LLR)-based testing of source code
    - MC/DC coverage of source code

- Through DO-331, model-based development + automatic code generation can greatly reduce that cost … but only if the code generator is qualified to TQL-1 (the highest level of qualification).

Envisioned QGen Workflow



Benefits of QGen TQL-1 Qualification

<u>Take credit for</u> certification objectives, including:

- Review of generated source code:
  - QGen TQL1 guarantees compliance with requirements & coding standards
- LLR-based testing of the generated source code
  - QGen TQL1 guarantees conformance to Simulink semantics
- Coverage analysis of generated source code
  - QGen TQL1 guarantees that model-level coverage implies code-level coverage

QGen Qualification Approach

Show Possession of the Overarching Properties

Motivation for a New Qualification Approach

DO-330, the tool-qualification supplement for DO-178C, is based on airborne-software certification

DO-330 requires substantially similar objectives to those required by DO-178C

- This approach is awkward for tools
  - Hazards for tools are different from hazards for airborne software
  - Tools are fundamentally COTS: they address multiple, heterogeneous usages
  - Tools must evolve and (re)qualification must support that evolution

FAA Initiative to Streamline Certification

The burden of current certification processes could *reduce* overall airspace safety

FAA Initiative to Streamline Certification

The burden of current certification processes could *reduce* overall airspace safety

New, different systems, like UAS are seeking certification

FAA Initiative to Streamline Certification

The burden of current certification processes could *reduce* overall airspace safety

New, different systems, like UAS are seeking certification

A novel approach is sought that will allow greater flexibility in certification

- Tailor evidence to the particular needs of the system and its application
- Reduce costs
- **Do not reduce safety**

FAA Initiative to Streamline Certification

The burden of current certification processes could *reduce* overall airspace safety

New, different systems, like UAS are seeking certification

A novel approach is sought that will allow greater flexibility in certification

- Tailor evidence to the particular needs of the system and its application
- Reduce costs
- **Do not reduce safety**

This is not about shortcuts. This is about more appropriate, more meaningful evidence given the system and its application.

FAA Approach: The Overarching Properties

Overarching Properties Working Group

- International, FAA-led initiative
- Defined a set of certification meta-objectives: the Overarching Properties

The 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*.

The Overarching Properties (Definitions)

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).

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

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

Item: "A hardware or software element having bounded and well-defined interfaces." (from ARP 4754A)

Foreseeable operating conditions: External and internal conditions in which the system is used, encompassing all known normal and abnormal conditions.

Unacceptable impact: An impact that compromises the *safety assessment*.

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*.

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)

The Overarching Properties: Scope

Overarching Properties:

- are designed as different means of compliance to Airworthiness regulations
- Are more flexible in scope — can be applied to
  - a software item in place of DO-178C
  - a hardware item in place of DO-254
  - a subsystem representing several inter-related items
  - ...

For whatever the application seeks approval;
through a coherent set of artifacts

NASA/FAA document — *Understanding the Overarching Properties*:
https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190029284.pdf

FAA Approach: The Overarching Properties

Overarching Properties Working Group

- International, FAA-led initiative
- Defined a set of certification meta-objectives: the Overarching Properties

RESSAC (Re-engineering and Streamlining Standards for Avionics Certification)

- International, European-led initiative
- Investigated approaches to assessment
- Recommended approaches to presenting and providing evidence:
  - Tried to define criteria;
  - Settled on demonstration using an Assurance Case

Certification Approach

Demonstrate possession of the Overarching Properties using an Assurance Case

Assurance Case — RESSAC Definition

An assurance case is an *argument* with its supporting artifacts. In the context of the *overarching properties*, the assurance case is intended to show how the properties are possessed by an *item* or combination of *items*.

The argument introduces, summarizes, and provides context and justification for *evidence* of possession of the properties.

Evidence is a reference to a means of assessing the truth of a given premise and the artifacts created or examined in that assessment.

Certification Approach

Demonstrate possession of the Overarching Properties using an Assurance Case

Assurance case allows:

- Evidence to be proposed
- Rationale for sufficiency of the evidence to be presented
- Evidence to be provided

The argument is the means by which the justification is made.

Argument

Rationale for Justifiable Confidence in Conclusions

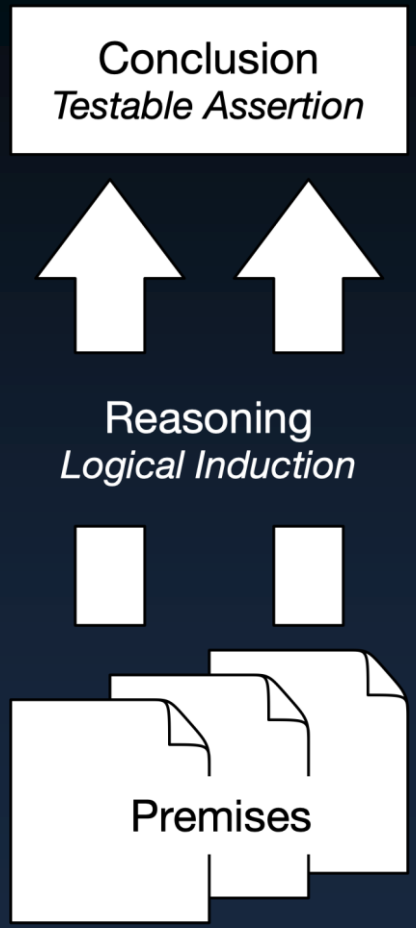
Engineers make arguments all the time:

- to themselves
- to each other

We seek arguments that are:

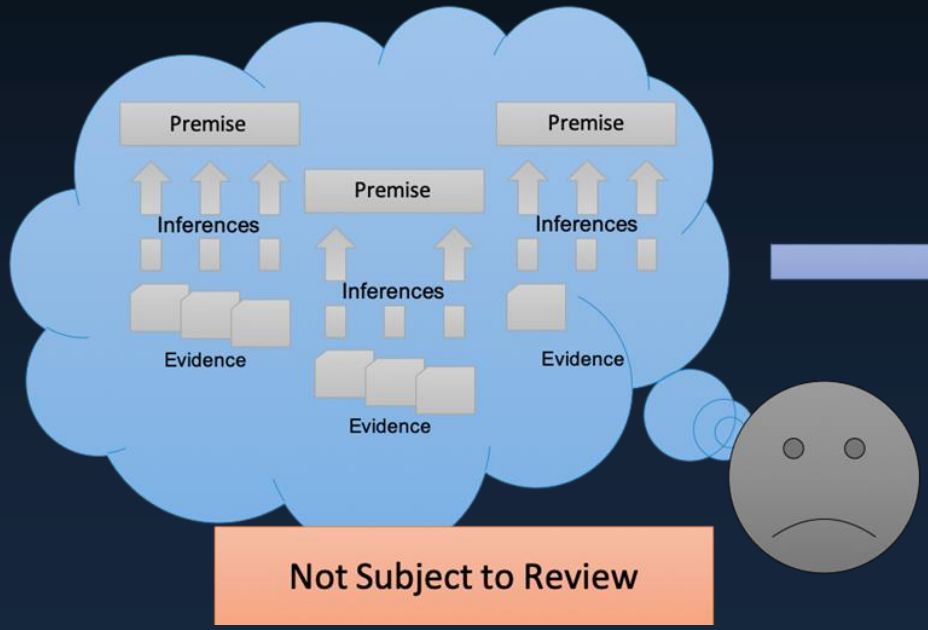
- explicit
- structured
- rigorous

We acknowledge that arguments are **not formal** because they are not based on deductive logic.

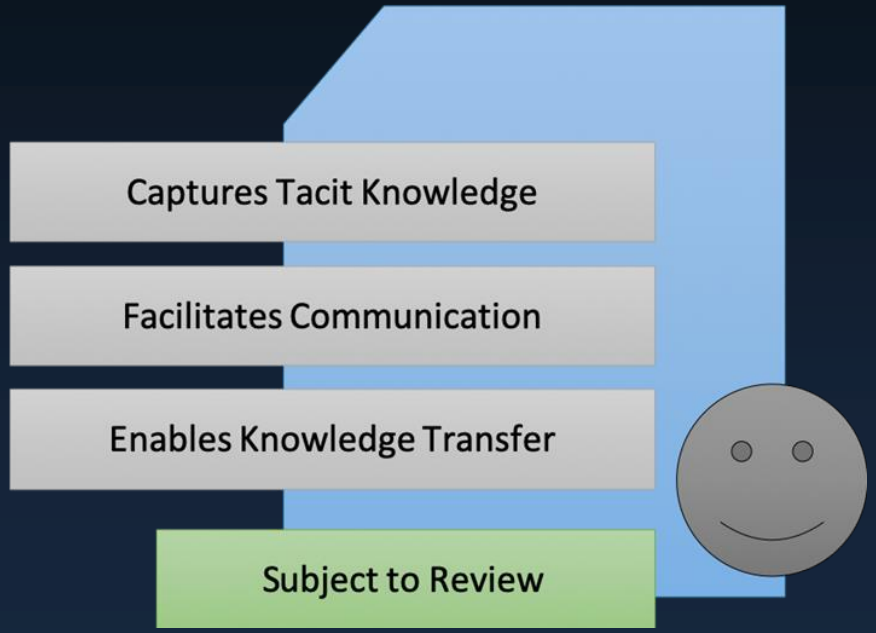


Implicit → Explicit

Implicit Argument



Explicit Argument



Unstructured → Structured

How Good is this Argument?

Rather than an unstructured flow of text that lays out the argument, we prefer to use selected, structuring forms for assurance cases. These forms enable us to present our rationale more clearly, to facilitate review, and to enable argument reuse. Structured arguments are thus superior to unstructured arguments

Conclusion. Structured Argument. Structured arguments are superior to unstructured arguments.

> Reasoning. Anecdotes are sufficient to conclude superiority.

Premise. Clearer Rationale. Structured arguments provide clearer rationale than unstructured arguments.

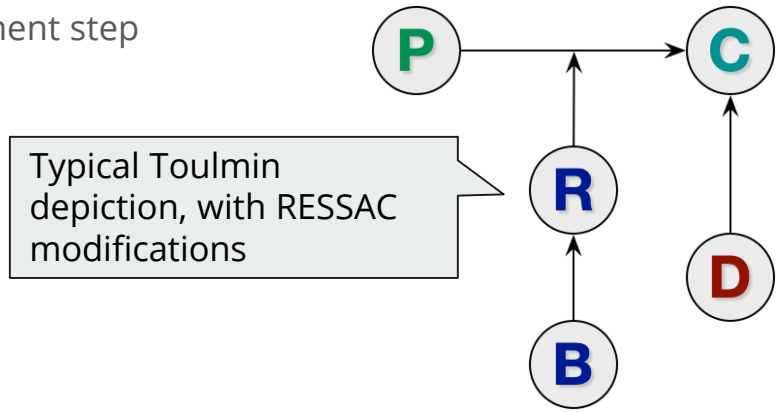
Premise. Easier Review. Structured arguments are easier to review than unstructured arguments.

Premise. Easier Reuse. Structured arguments are easier to reuse than unstructured arguments.

Argument Format: Modified Toulmin

The argument is presented in a modified Toulmin form inspired by the recommendations of the RESSAC working group.

- **Conclusion**: to be derived from the current argument step
- **Reasoning**: describes how the Conclusion may be derived from the given Premises
- **Backing**: supports the Reasoning
- **Premises**: the grounds for the argument
- **Defeater**: challenges soundness of the argument or the truth of the Conclusion



Argument Format: Textual Representation

Conclusion. **Argument-fragment Conclusion.** This is the conclusion to be derived from the fragment.

Reasoning. How the premises may be seen to be sufficient to conclude the conclusion.

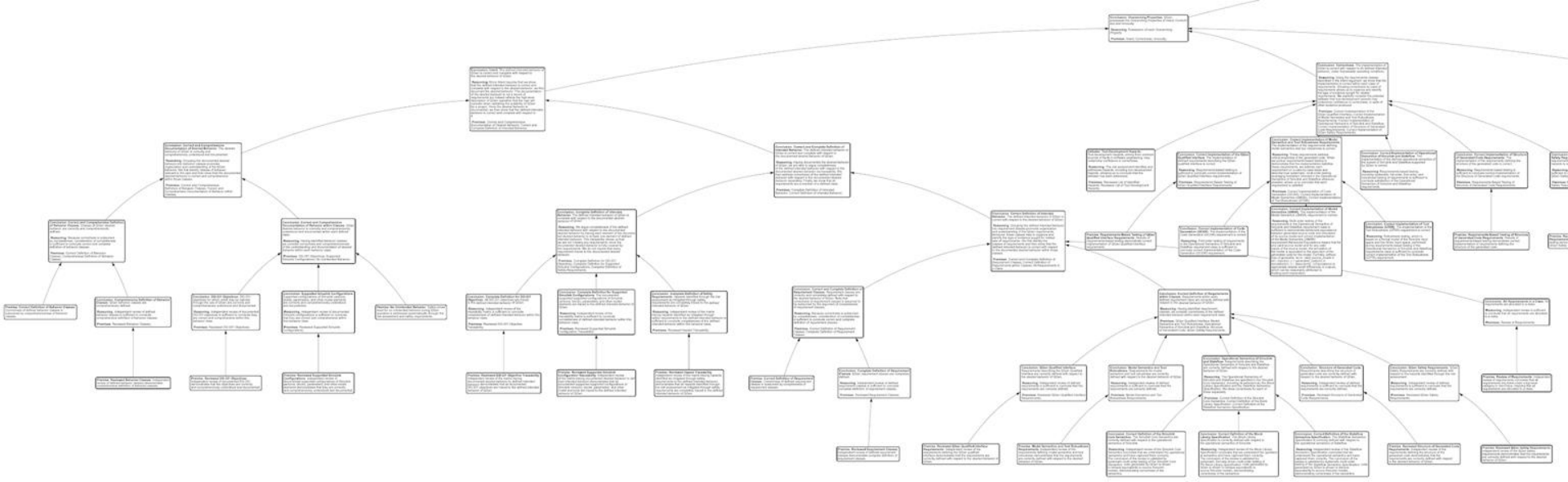
Backing. Support the reasoning, as necessary.

Defeater. Identified threats to the validity of the reasoning or conclusion, as appropriate.

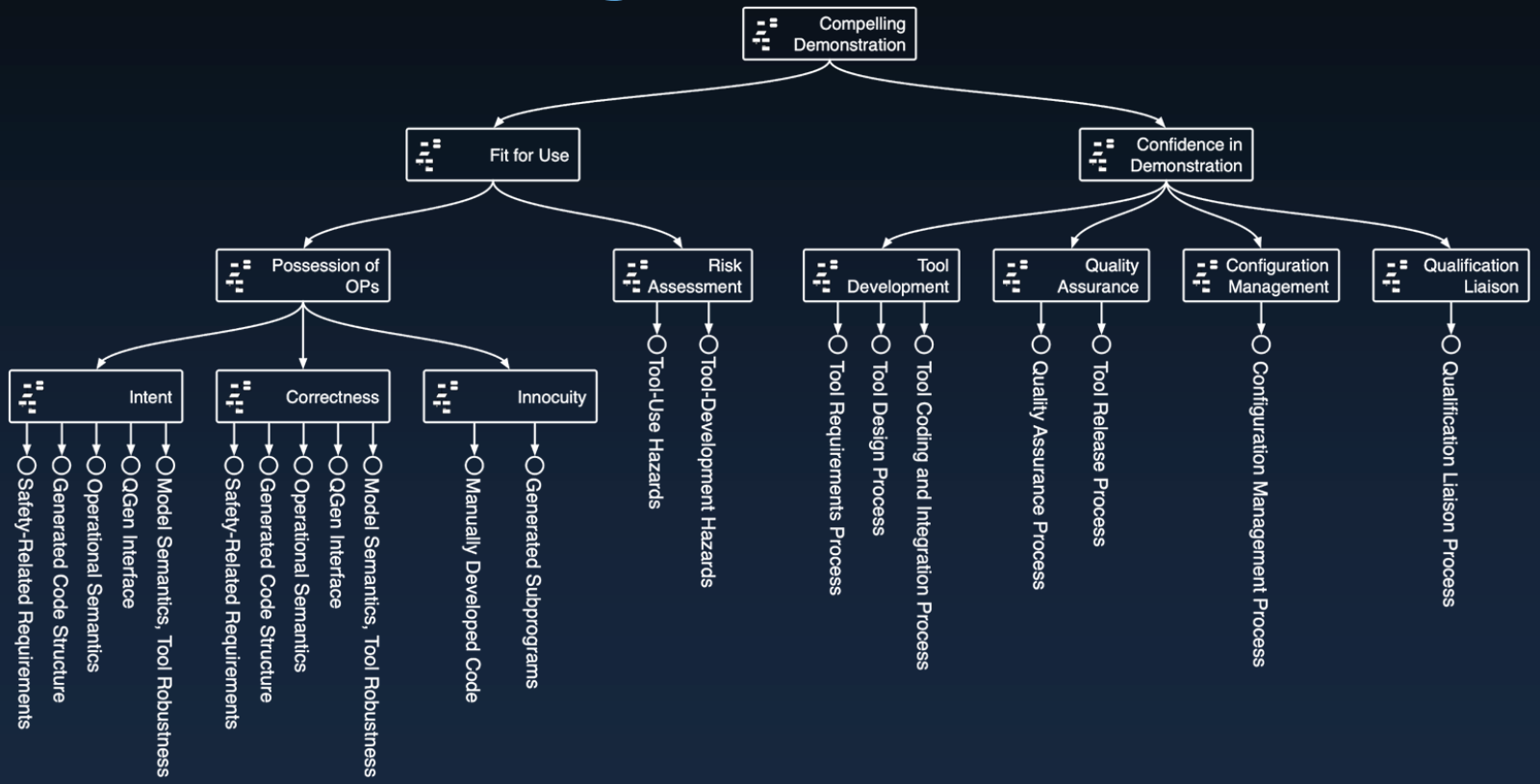
Premise. **Premise 1.** The first premise, used to derive the conclusion.
[supported by conclusion of another argument step]

Premise. **Premise 2.** The second premise, used to derive the conclusion.
[supported by evidence]

Argument Format: Tree



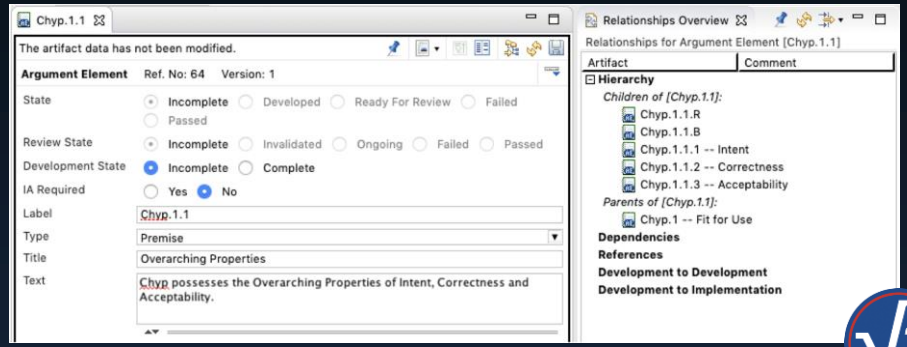
The Structured Argument: Overview



Argument Elements Stored in VeroTrace

Each argument element is individually stored in VeroTrace

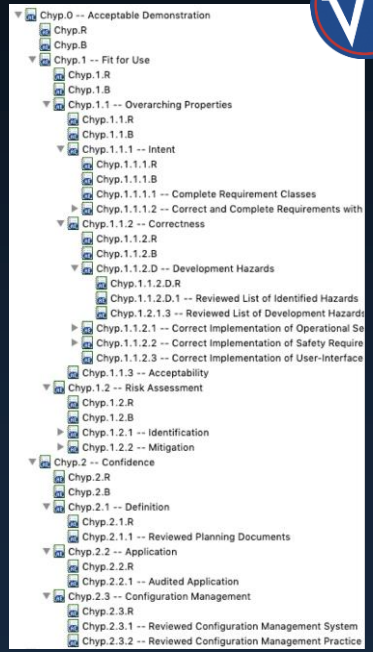
- Premises, Reasonings, Backings, Defeaters
- Parent/child relationships amongst elements



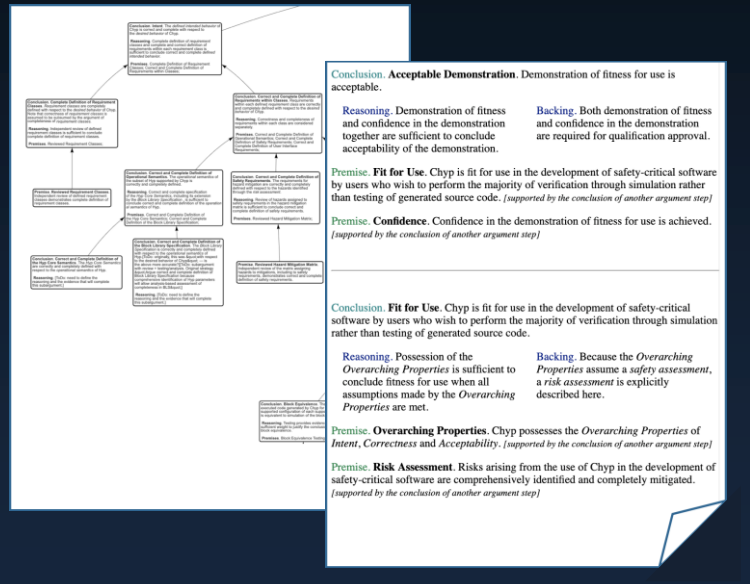
VeroTrace Provides

- links to artifacts and dependencies
- impact analysis
- configuration management and version control
- review and artifact management, including state information: development, review, audit

Argument Views are VeroTrace Reports



VeroTrace Report Generator



Other views / representations could easily be generated.

Conclusion

The Overarching Properties and their assurance case seek **more appropriate activities** to **improve confidence** in critical systems and software.

AdaCore is using an Overarching Properties assurance case to seek TQL-1 qualification for QGen.

AdaCore is currently working with its launch customer and is targeting qualification by the end of 2020.

Conclusion

For the avionics domain, QGen TQL-1 qualification brings significant benefits:

- We are using the Overarching Properties to achieve TQL-1 for QGen
- Our customers **do not** need to also use the OPs
- Customers using DO-178C / DO-331 can take advantage of QGen TQL-1 qualification

For the automotive domain:

- We are planning adaptations to our qualification results for 26262 tool qualification

For the railway domain

- We are planning adaptations to our qualification results for EN-50128 tool qualification
- We are envisioning T3 — the highest level of tool qualification

Conclusion

Many other domains call for explicit assurance cases (safety cases), including:

- UK Air-Traffic Management
- UK MoD
- UK Nuclear
- EU, Australian, NZ process industries
- US FDA (certain medical devices)
- US Navy (certain UAS operations)

The Overarching-Properties-based approach shown here could naturally support these domains.

QGen's qualification evidence could naturally fit into these domains.