Certification of a Flight Control System Implemented on an SoC

Bill Potter

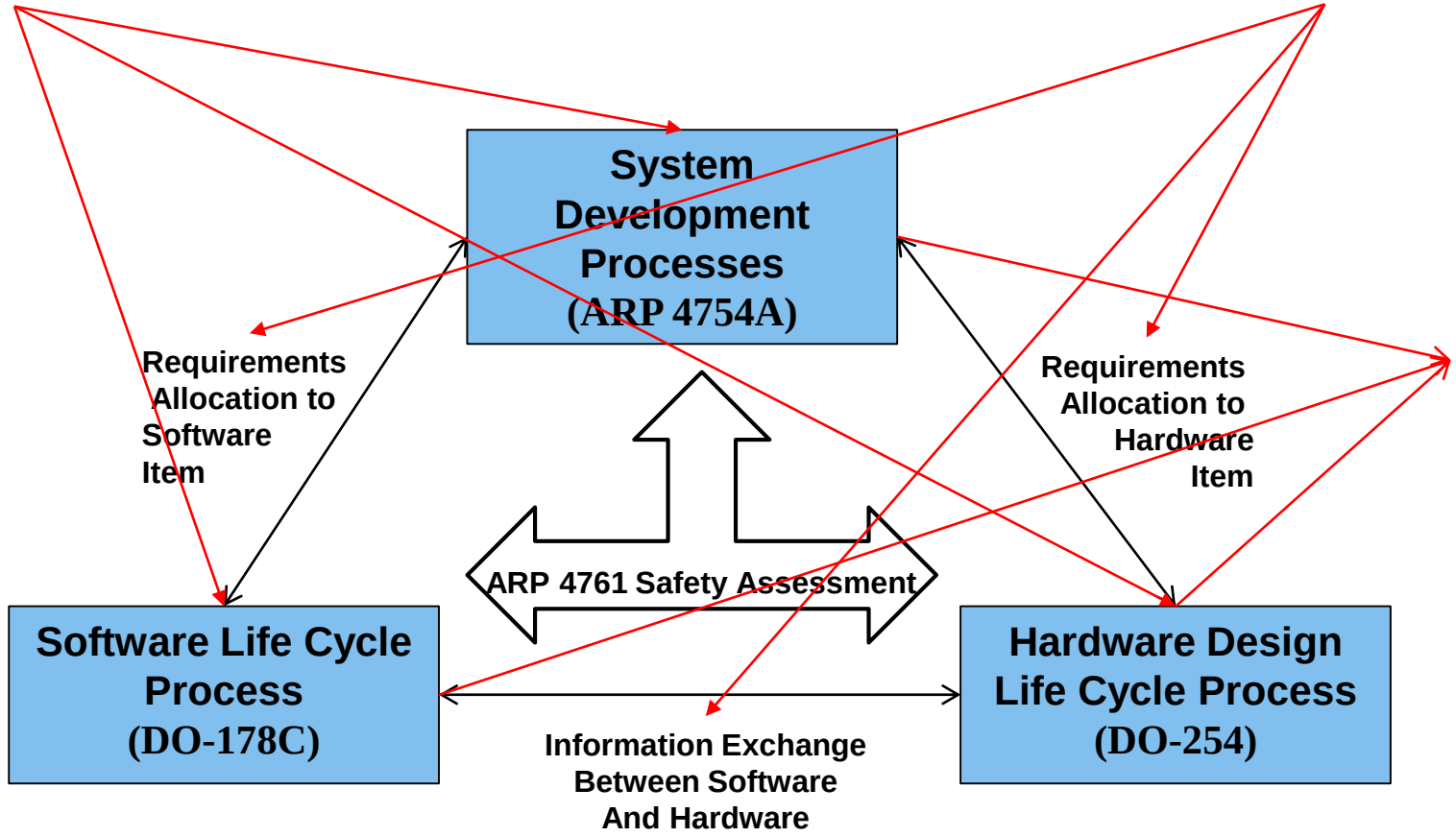
Key Takeaways

1. Model-Based Design increases productivity for development of certified systems
2. A single development environment for System on a Chip
3. Qualified tools that span ARP 4754A, DO-178C and DO-254

Certification is Difficult

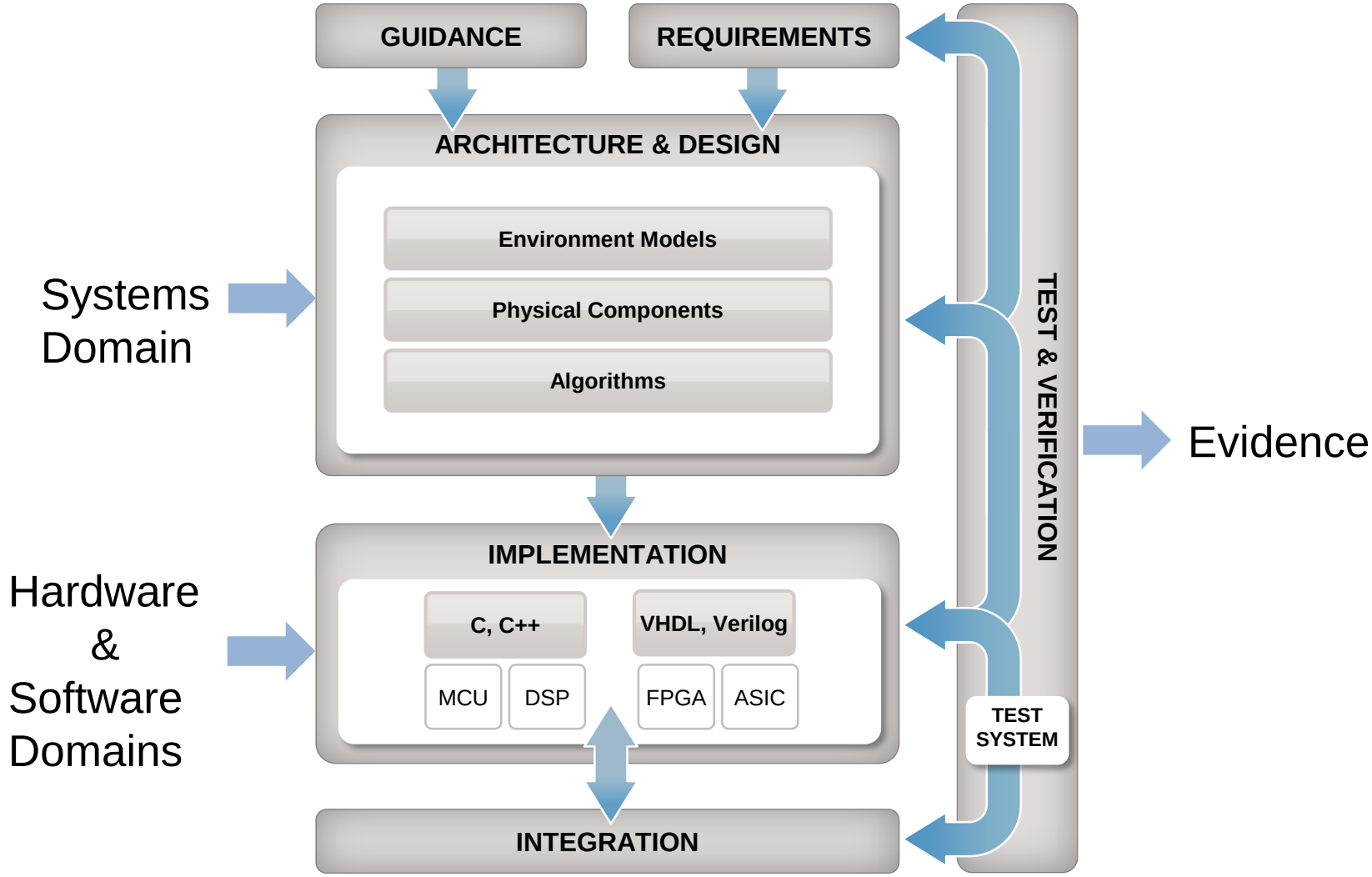
Comply with regulatory guidance

Coordinate between engineering domains



Provide evidence To regulators

Solution - Model-Based Design

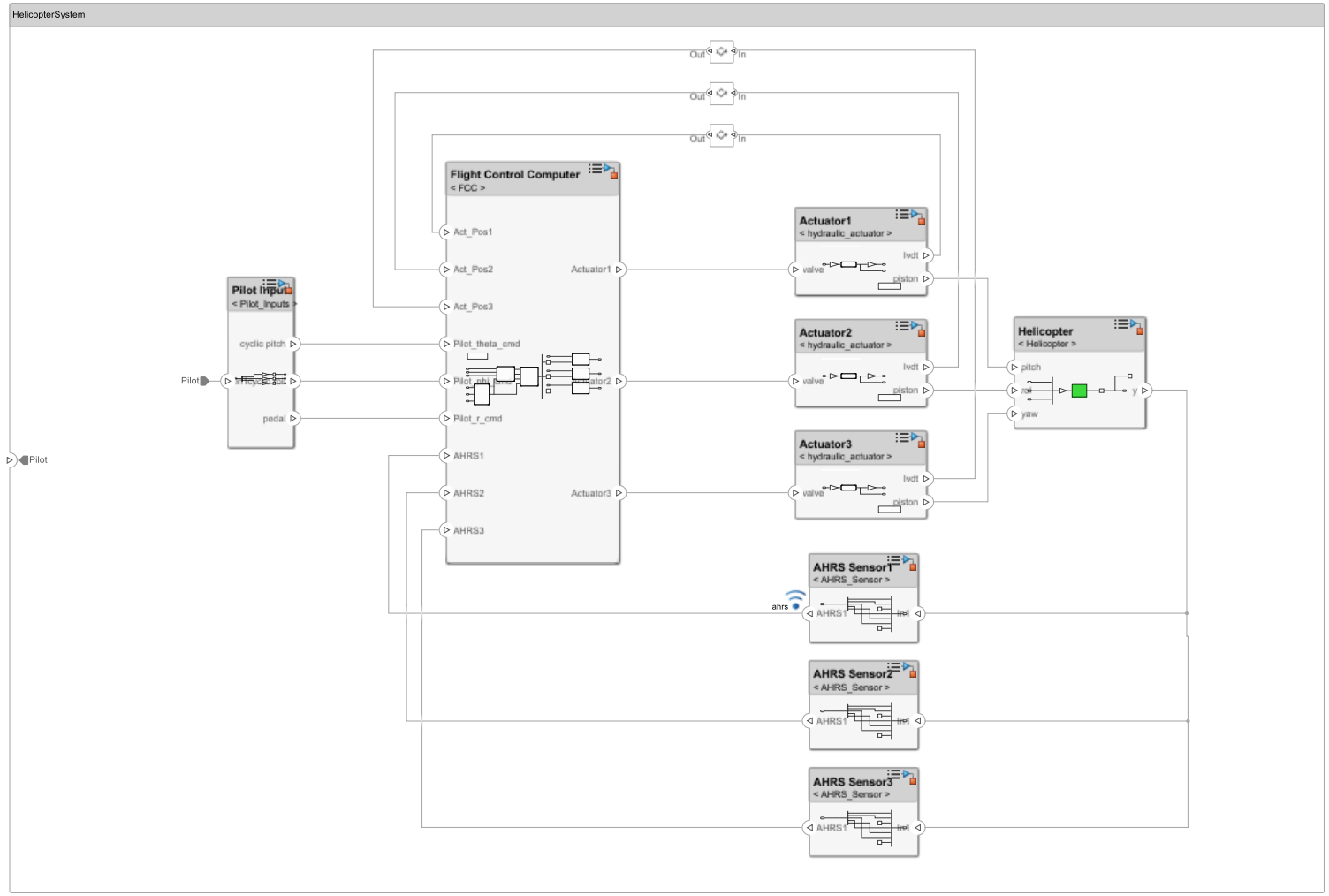


System Model Development

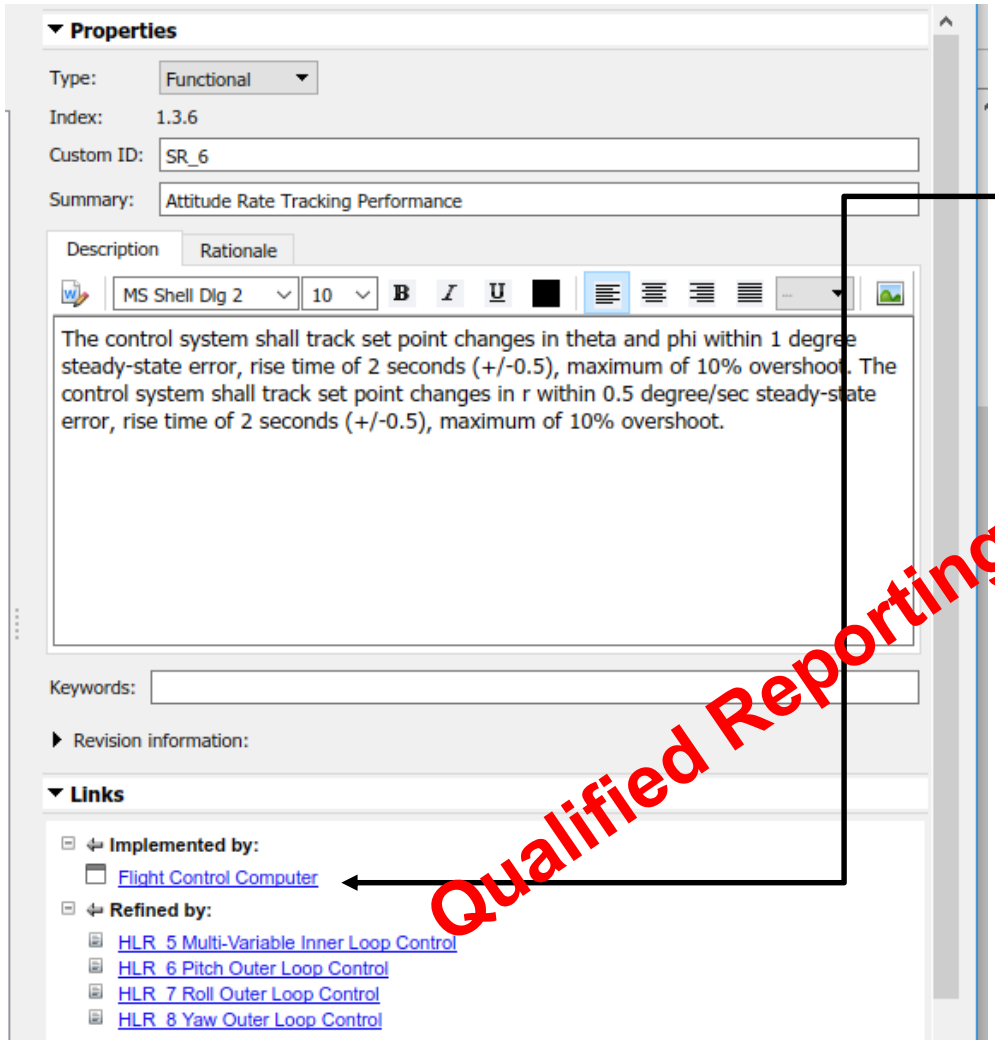
System Level Architecture Model of Helicopter Flight Controls

System Architecture Components

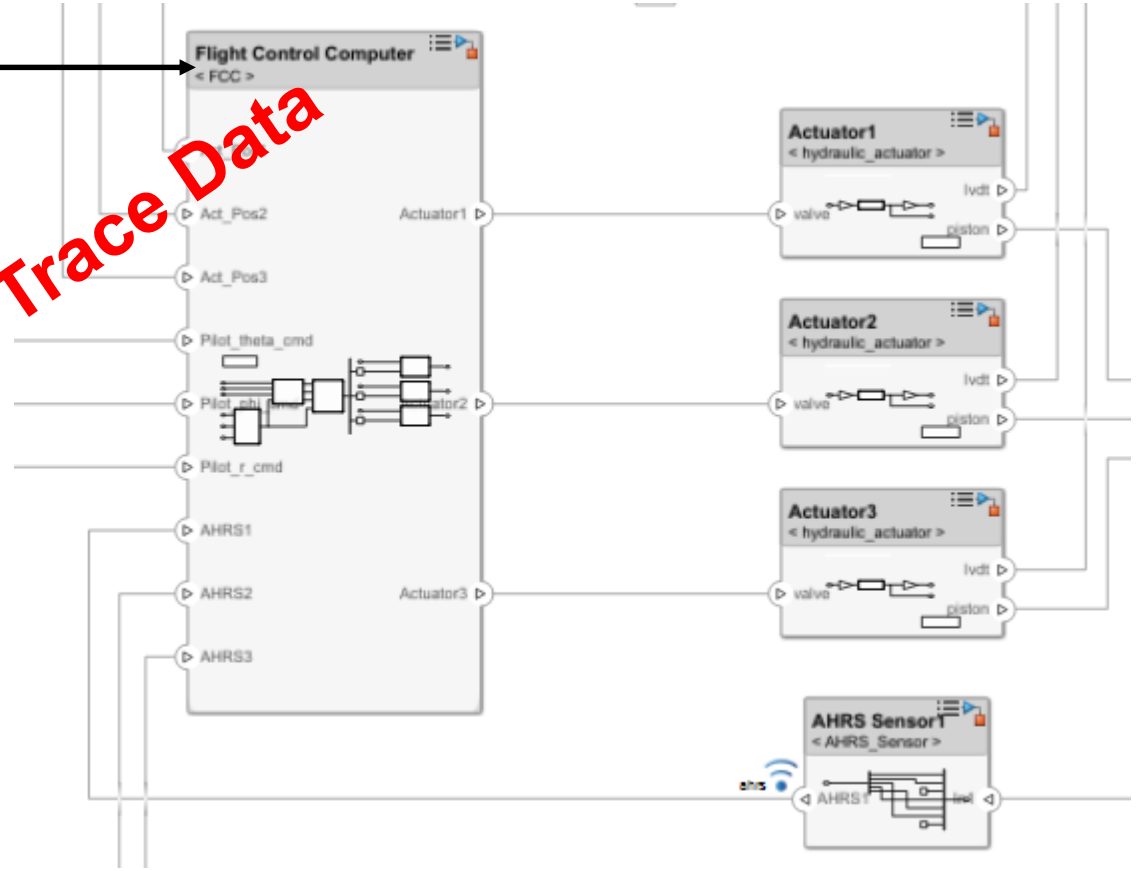
- Plant Models
- Physical Items
- Digital Hardware Items
- Software Items
- Redundancy



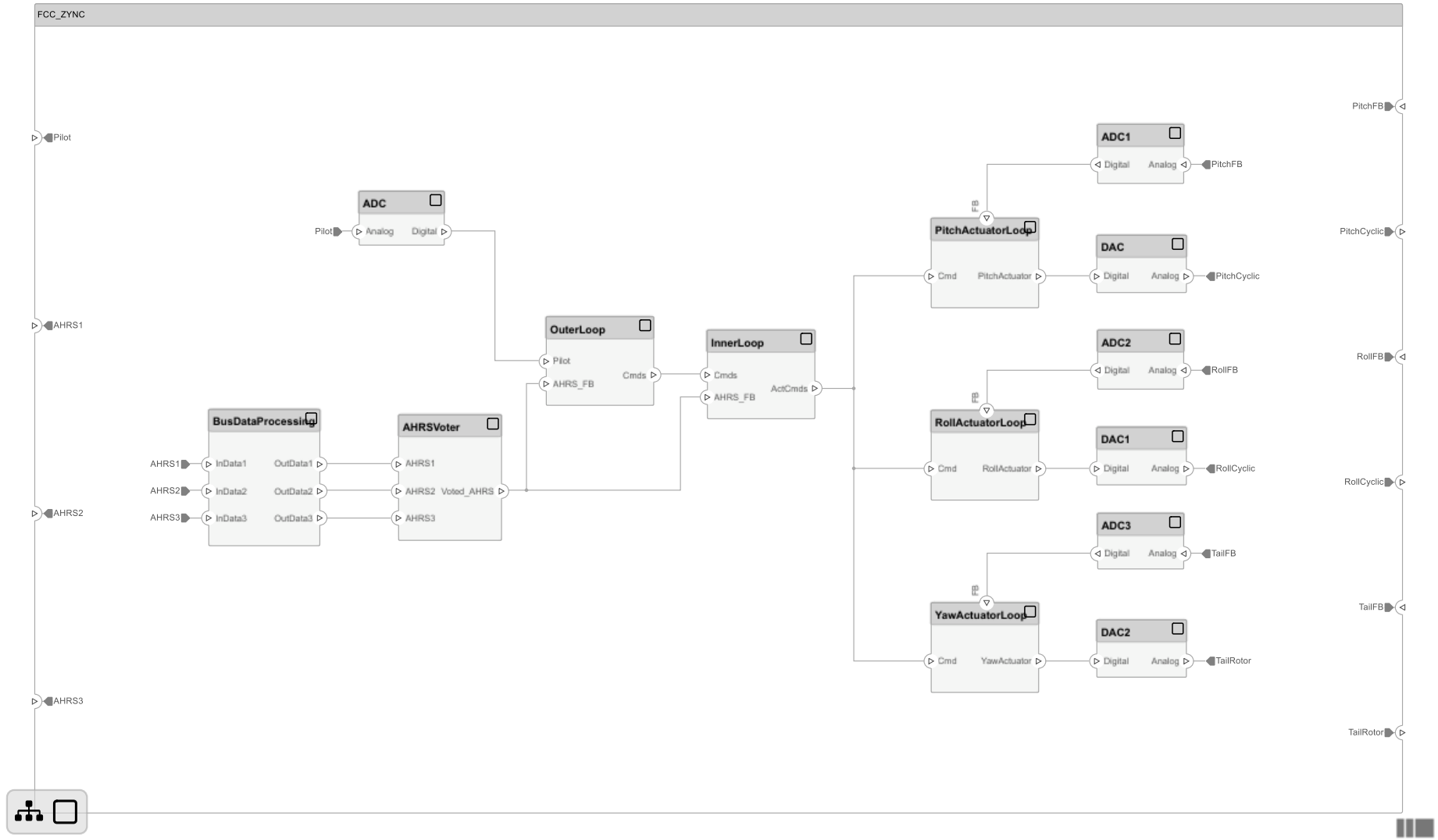
System Requirements to Architecture Traceability



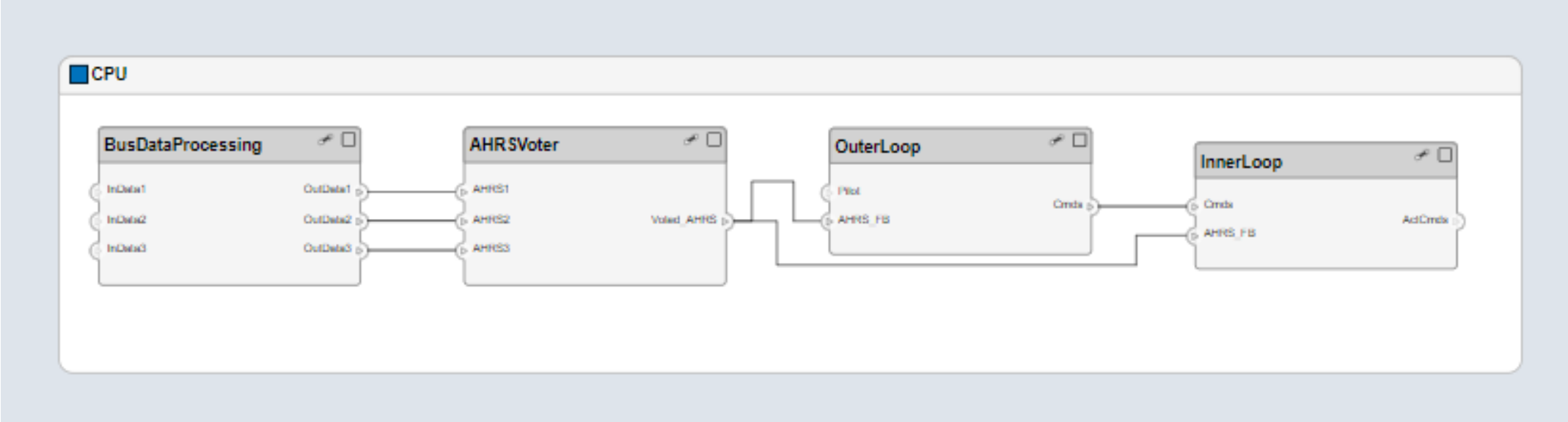
Qualified Reporting and Trace Data



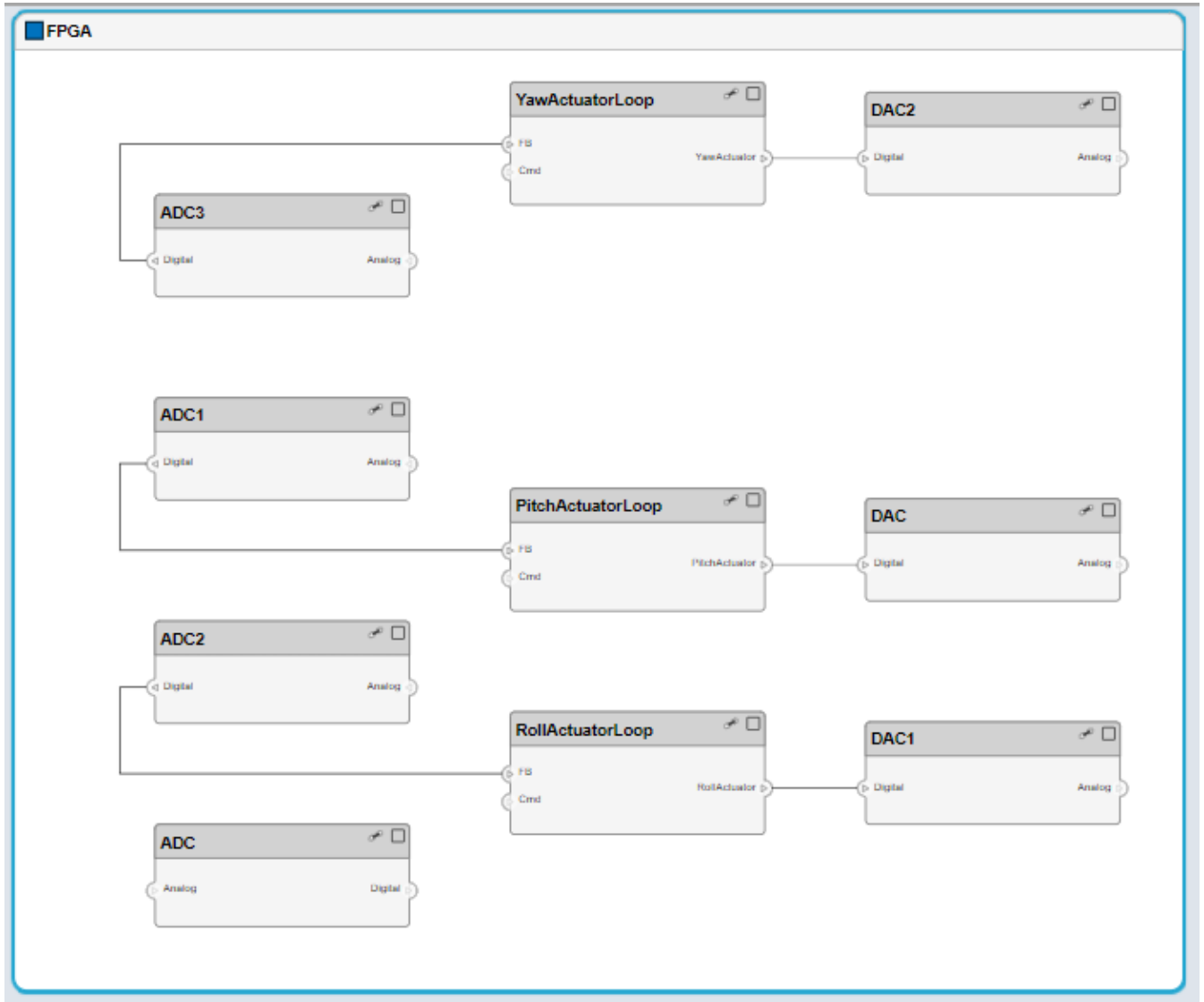
Flight Control Computer Architecture for Xilinx Zynq SoC



Allocation of System Requirements to Software – CPU View



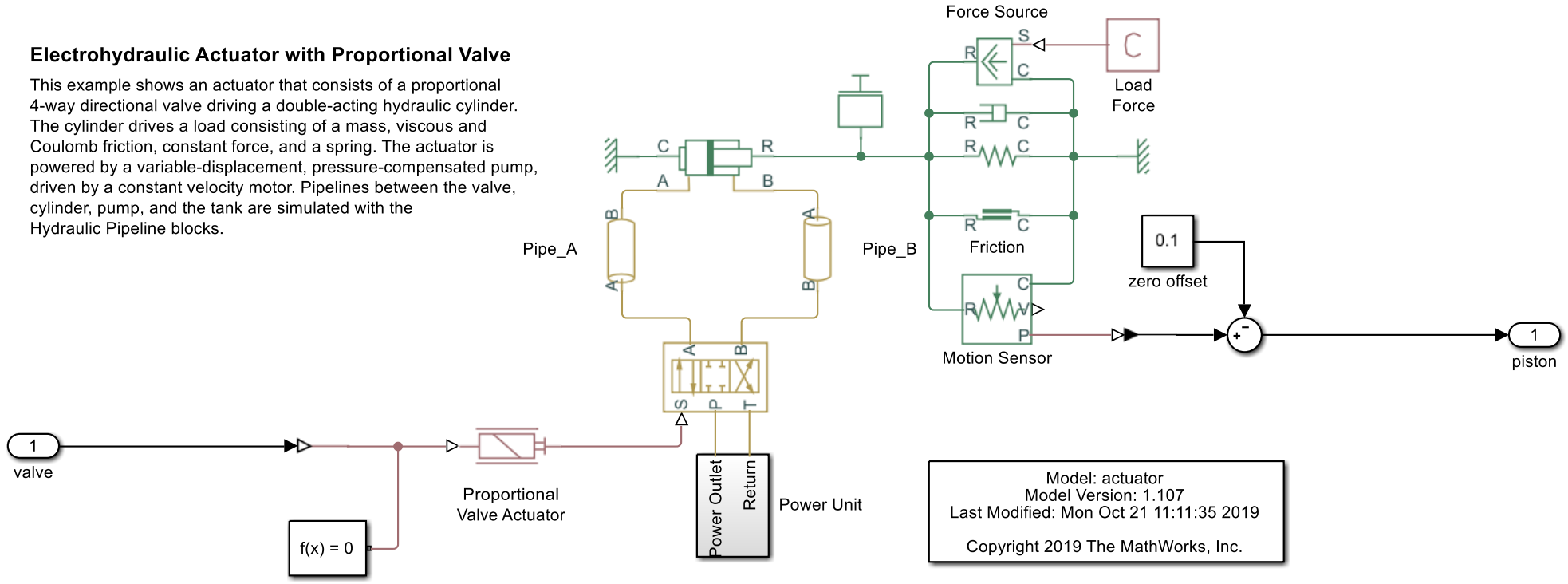
Allocation of System Requirements to Hardware – FPGA View



Plant Models can be used with System Composer Components

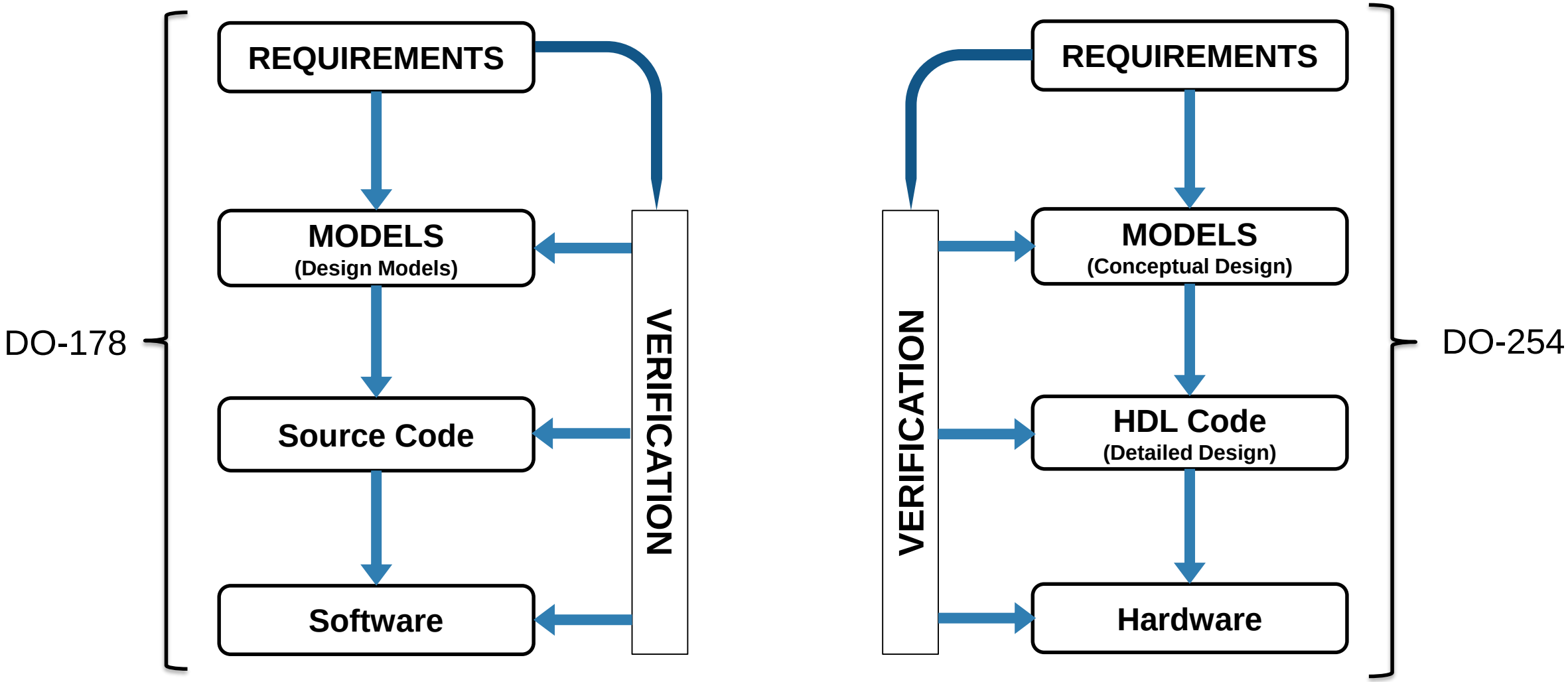
Electrohydraulic Actuator with Proportional Valve

This example shows an actuator that consists of a proportional 4-way directional valve driving a double-acting hydraulic cylinder. The cylinder drives a load consisting of a mass, viscous and Coulomb friction, constant force, and a spring. The actuator is powered by a variable-displacement, pressure-compensated pump, driven by a constant velocity motor. Pipelines between the valve, cylinder, pump, and the tank are simulated with the Hydraulic Pipeline blocks.

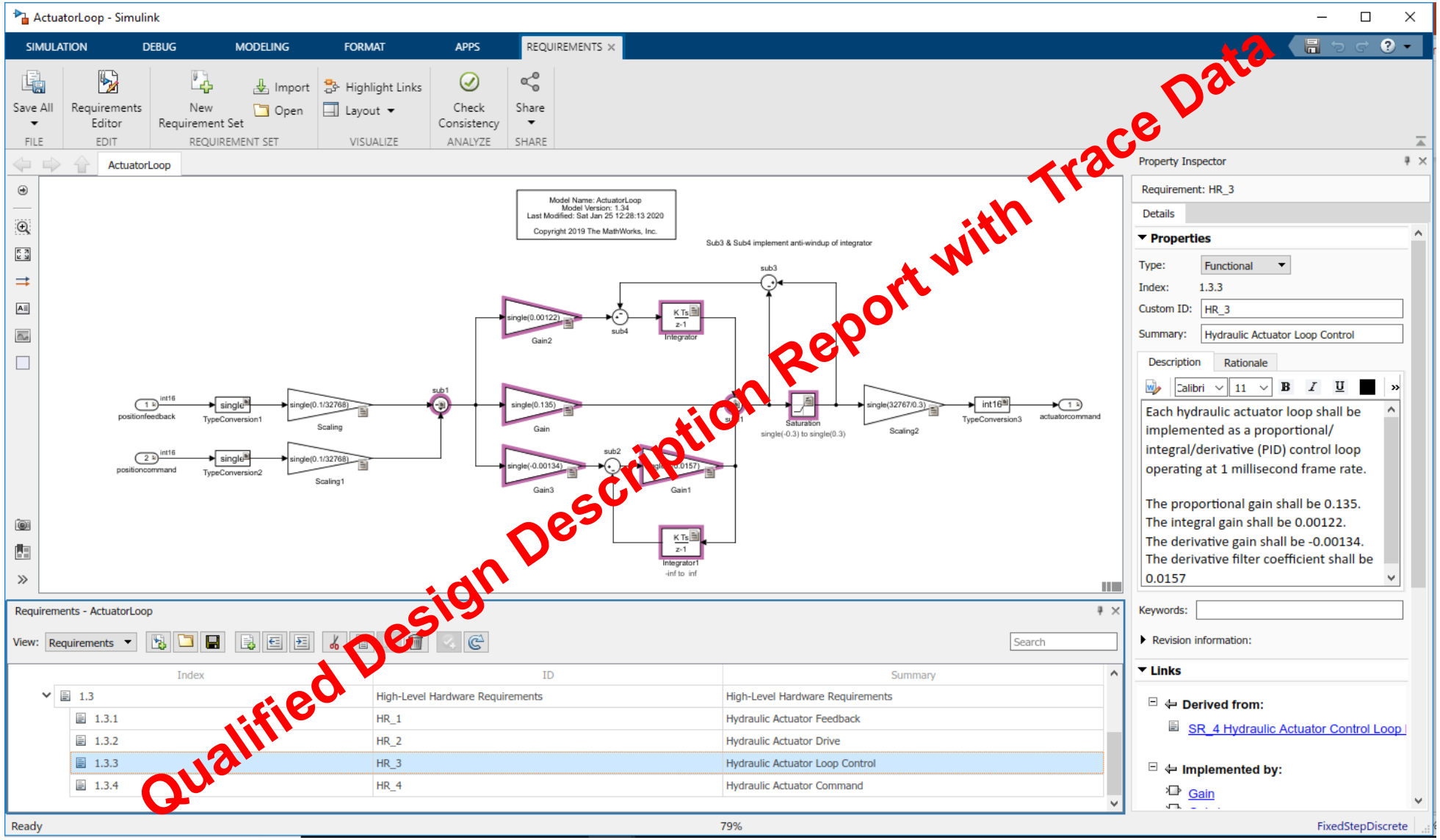


Software and Hardware Model Development

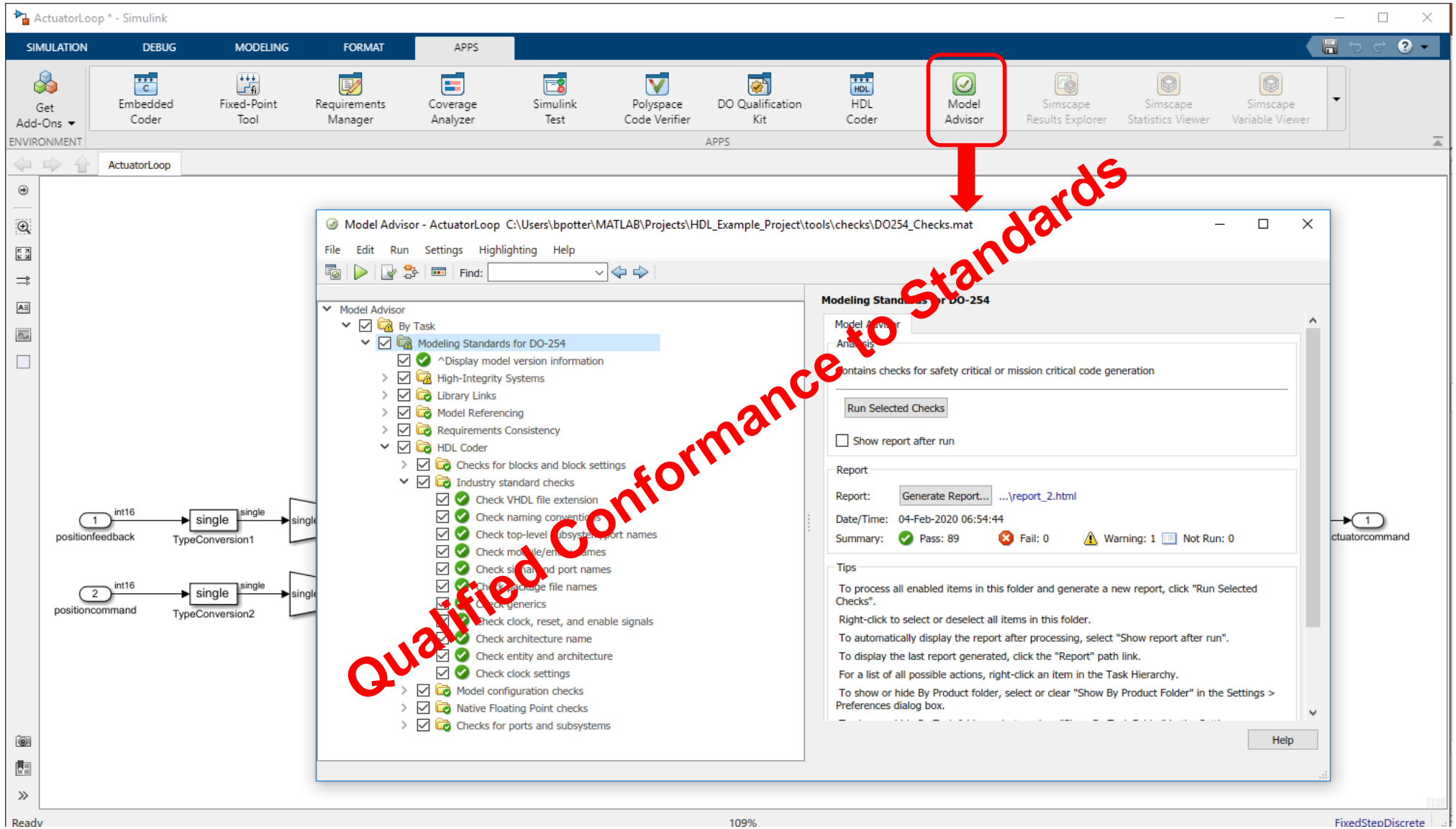
DO-178 and DO-254 Processes Using Models



Trace Models to Requirements

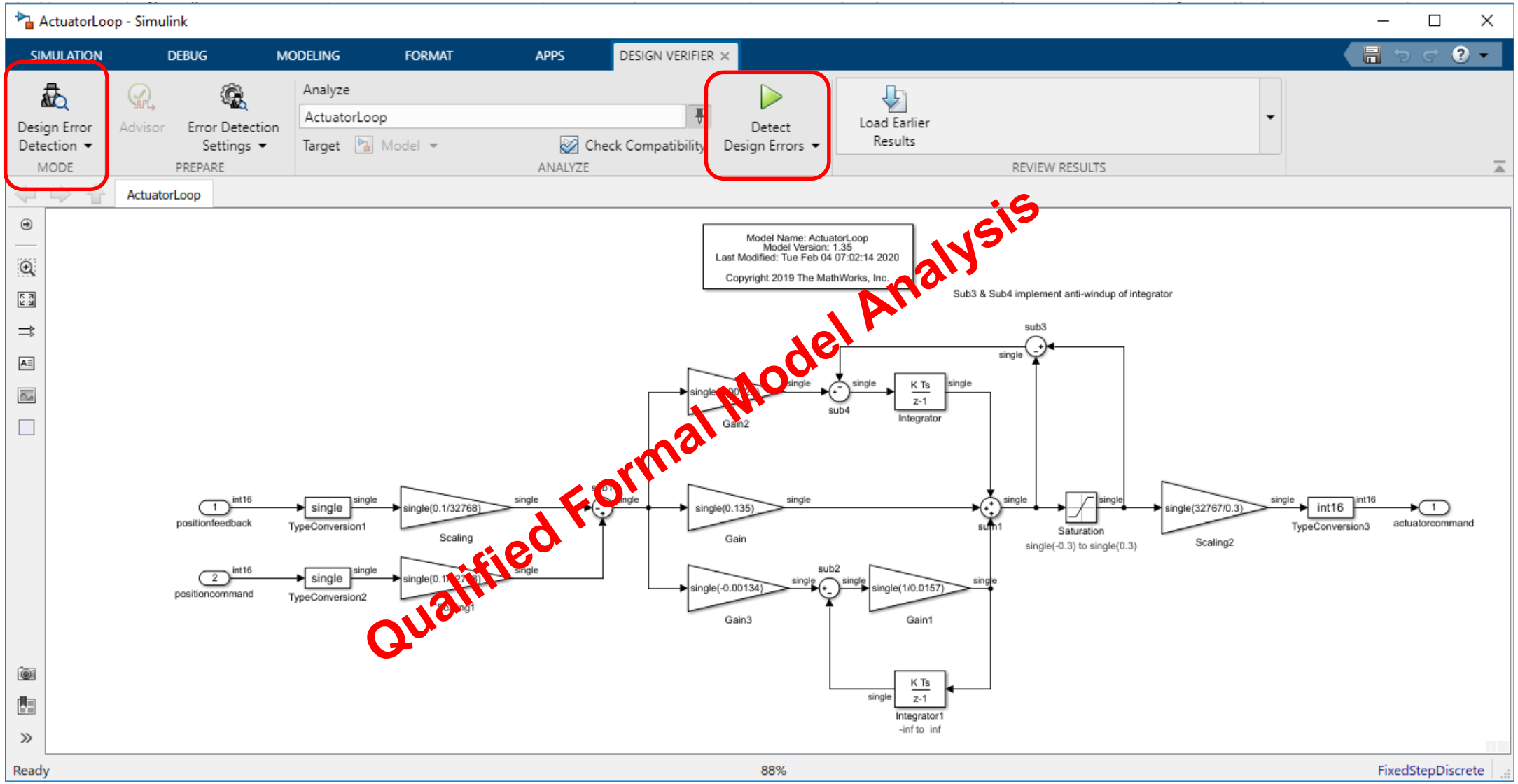


Verify Conformance to Model Standards

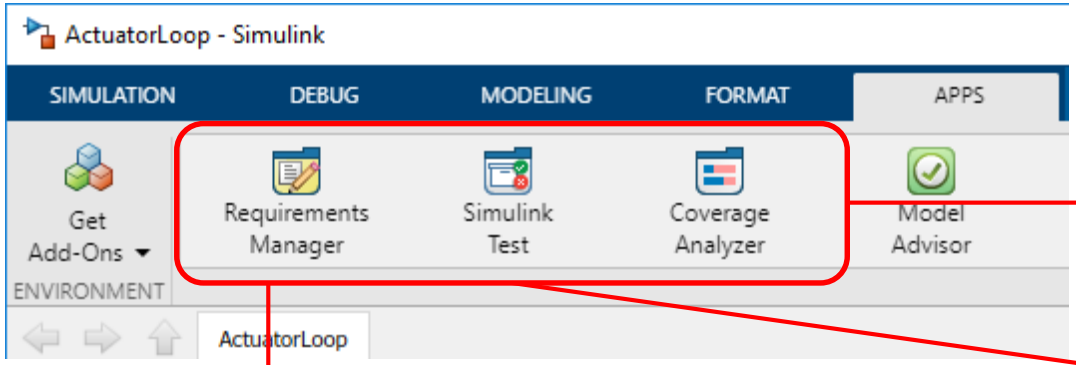


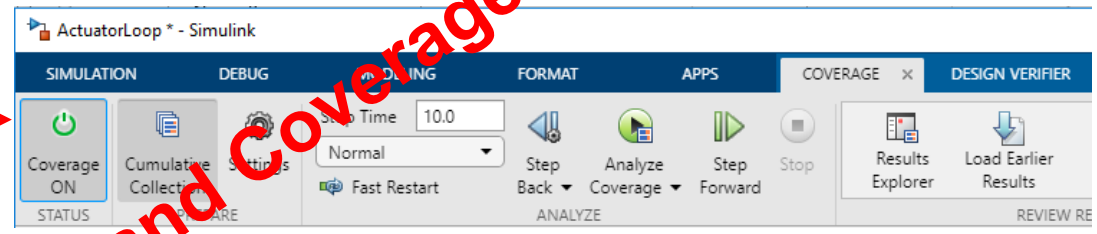
Qualified Conformance to Standards

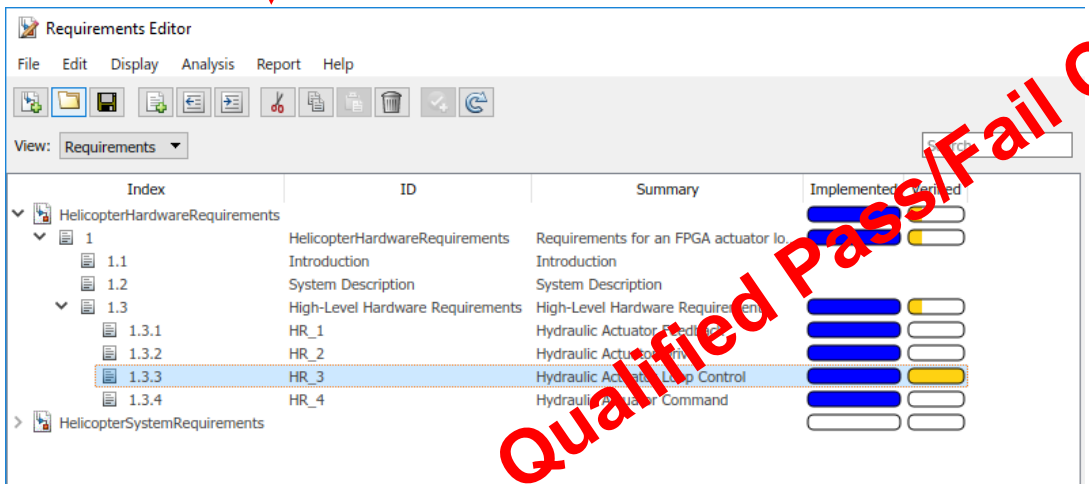
Perform Formal Analysis on Models



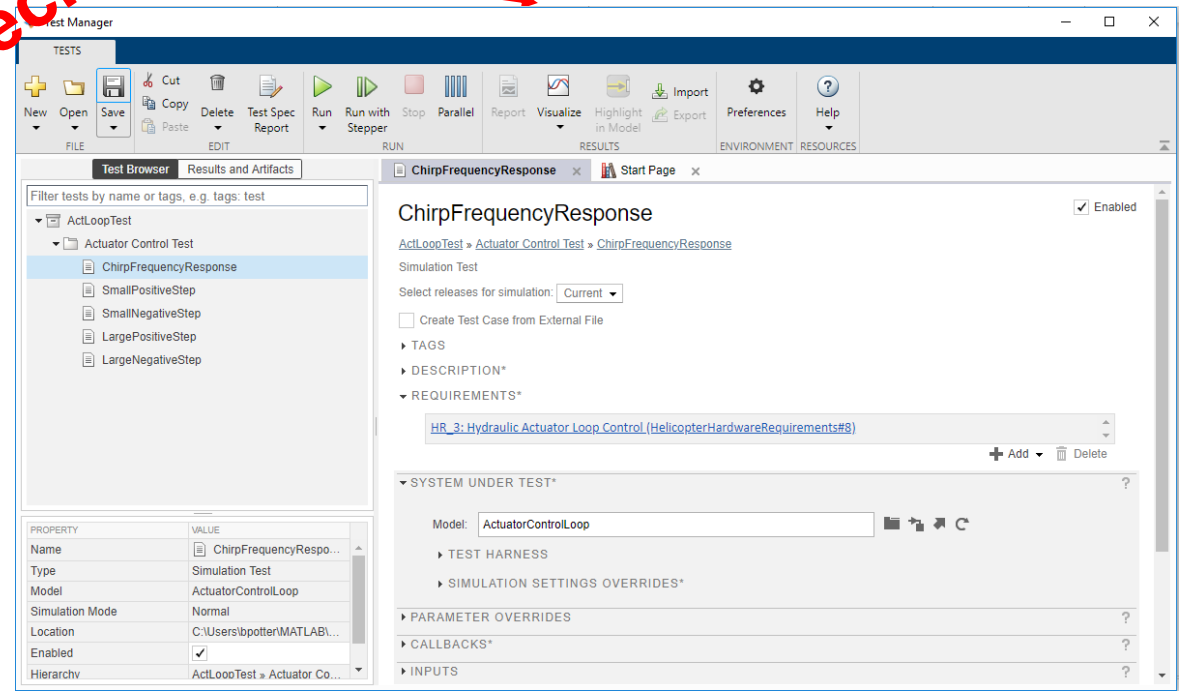
Integrated Requirements, Simulation & Model Coverage Analysis



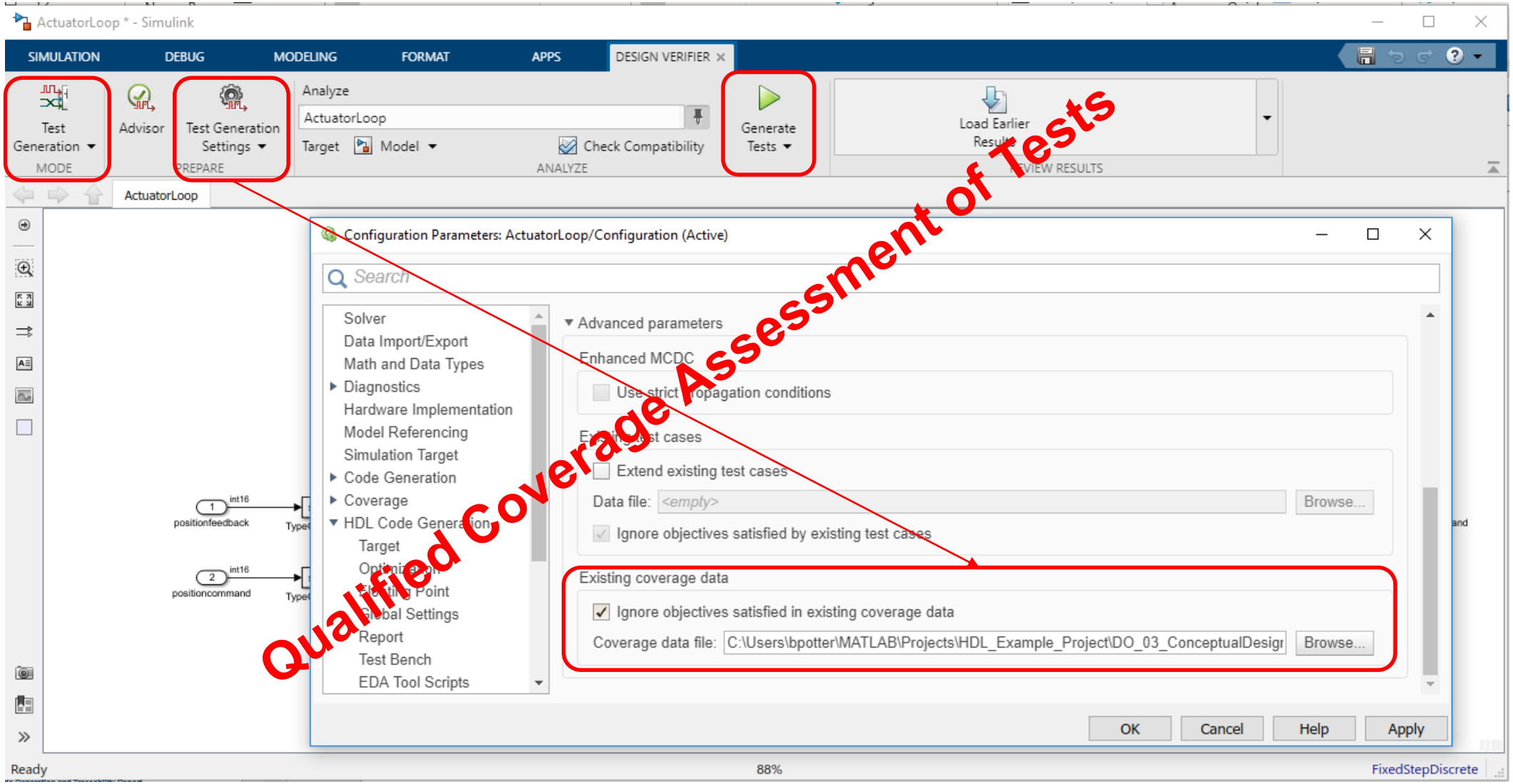




Qualified Pass/Fail Checking and Coverage

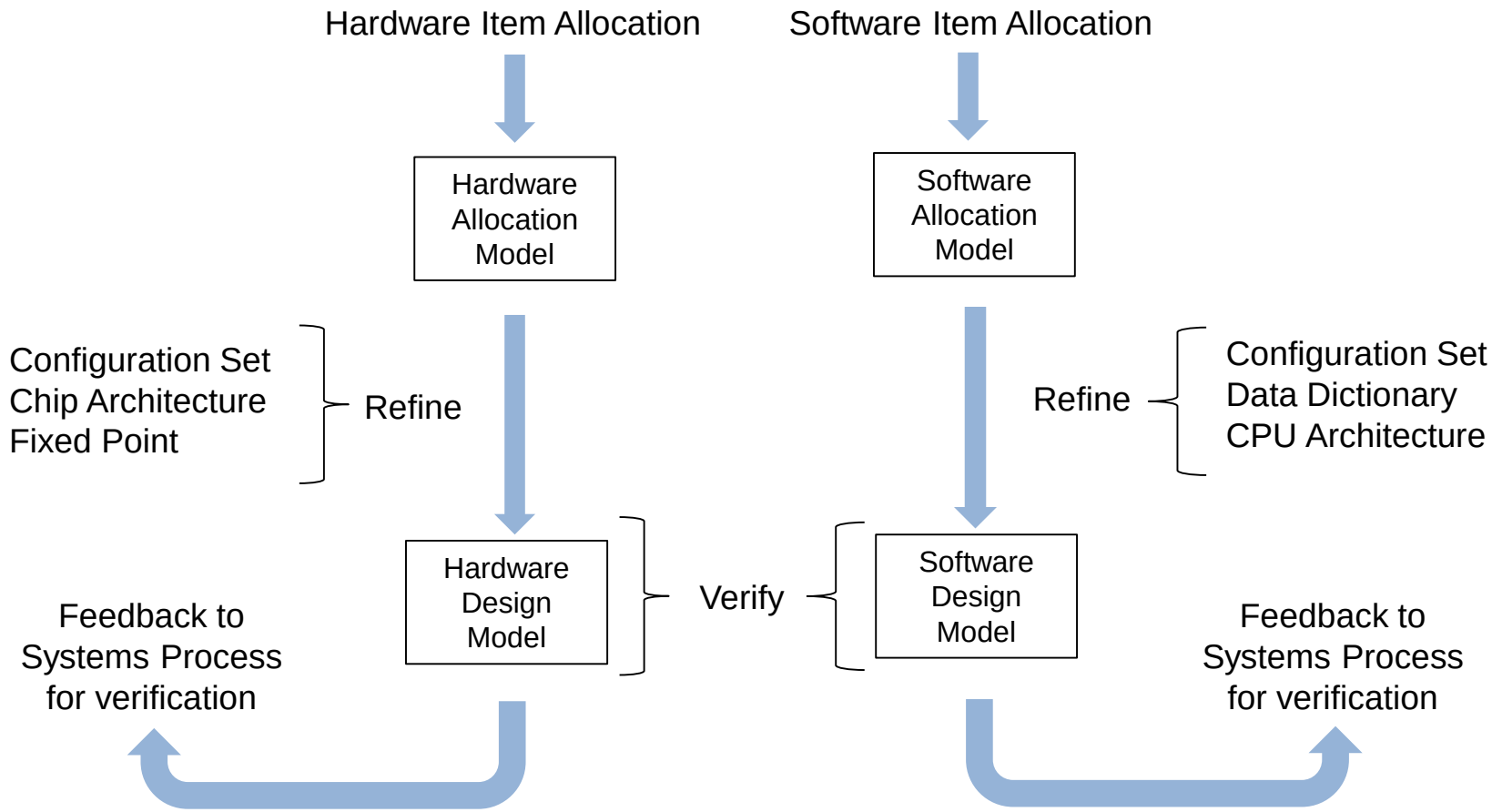


Test Generation for Missing Coverage



System Level Simulation

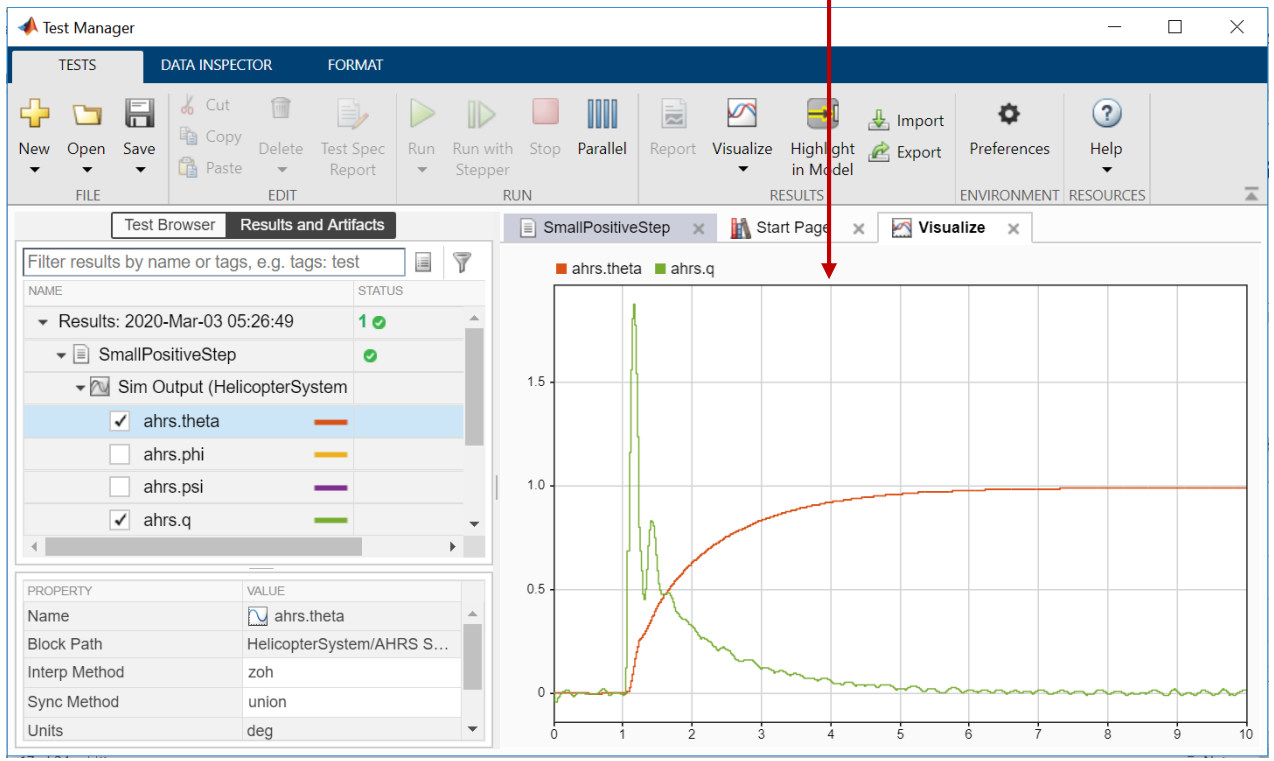
Provide Verified Models from Software (DO-178C) and Hardware (DO-254) Processes back to Systems (ARP 4754)

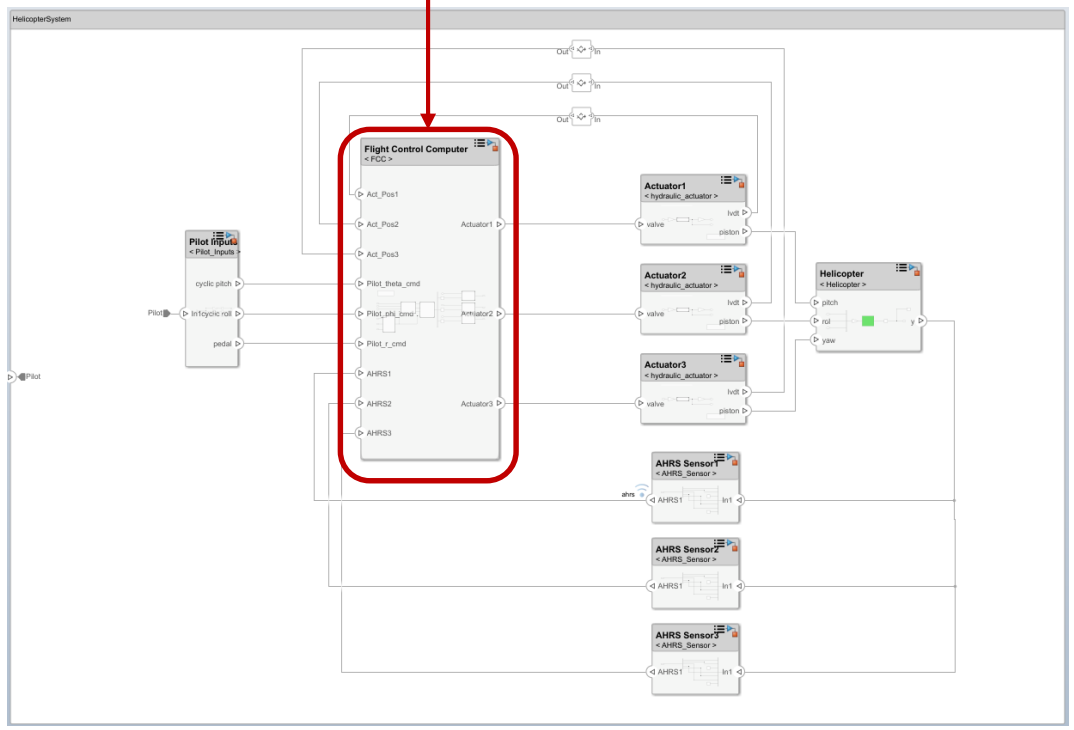


System Simulation using Design Models

System Response

Software and Hardware Design Models



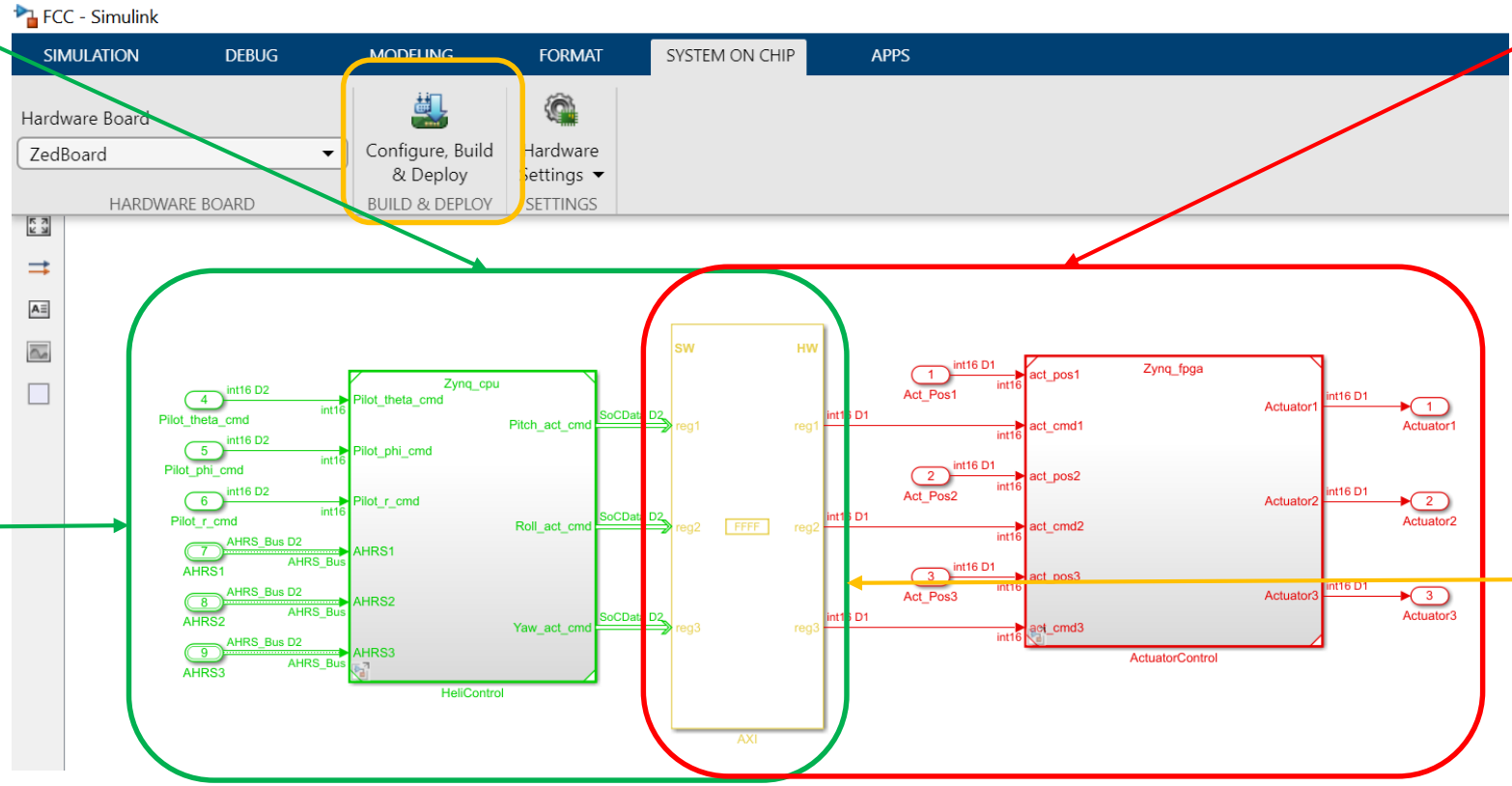


Software and Hardware Implementation

Generate C and VHDL Code and Deploy to SoC

C code

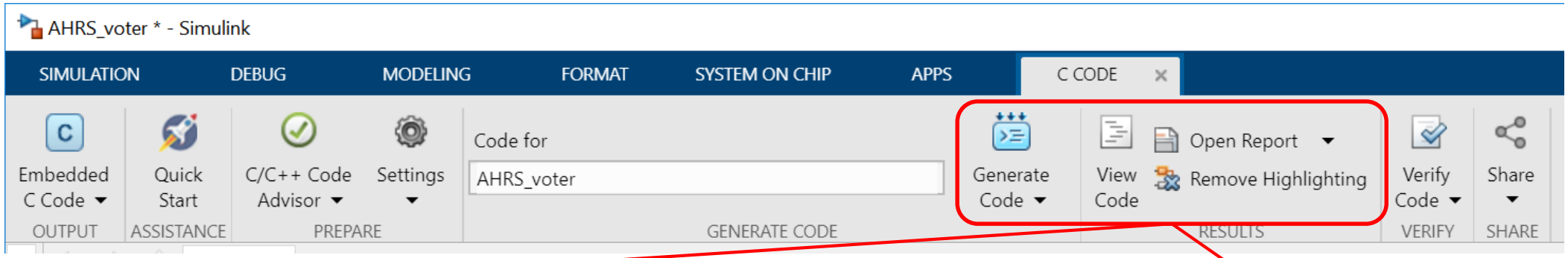
VHDL code

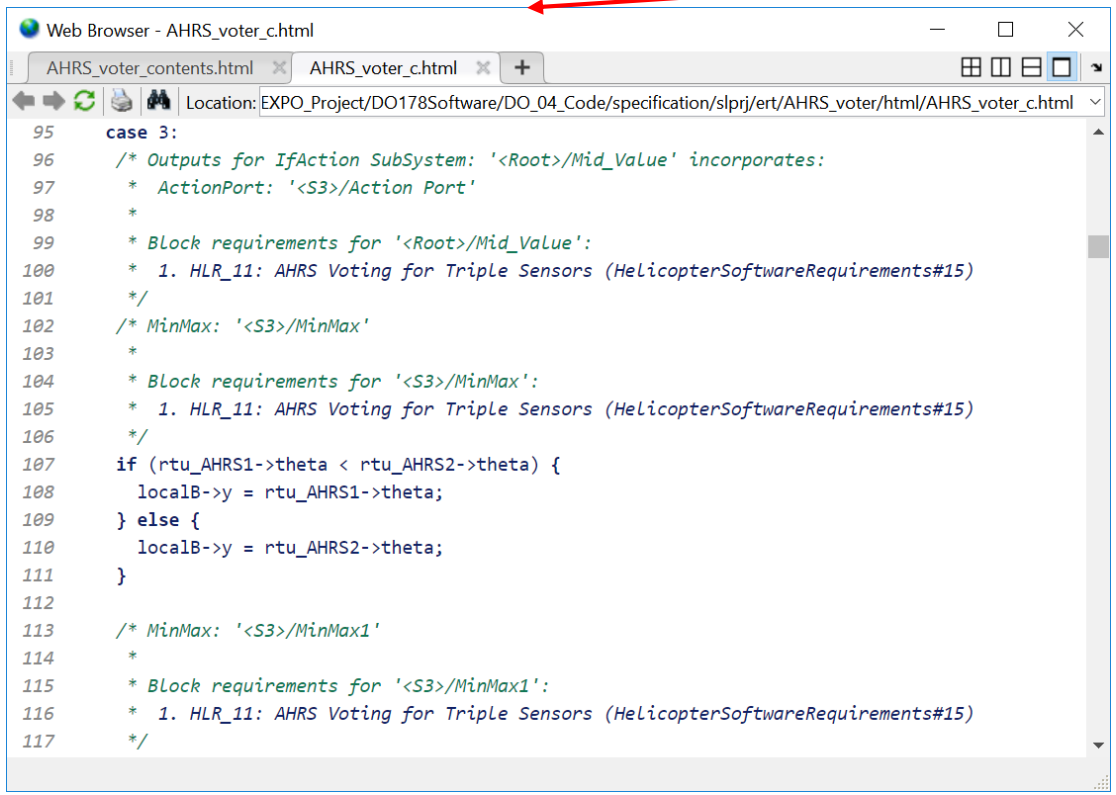


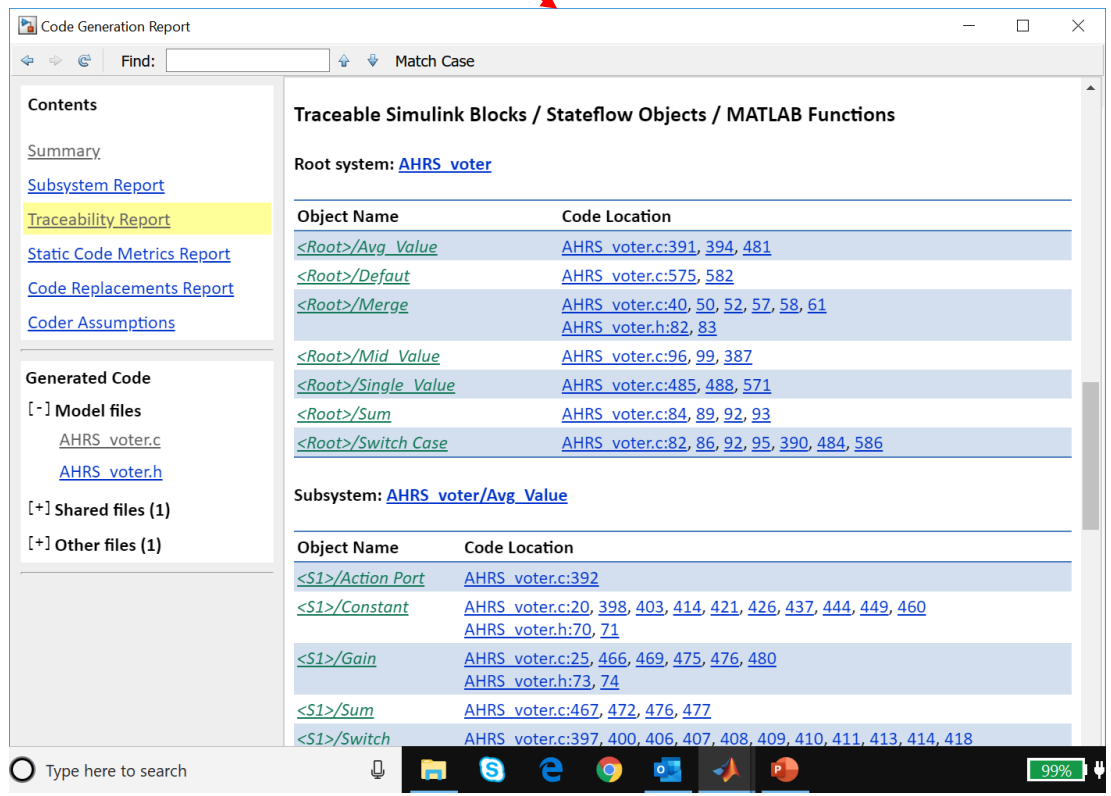
Generate for multi-core

Glue code C and VHDL

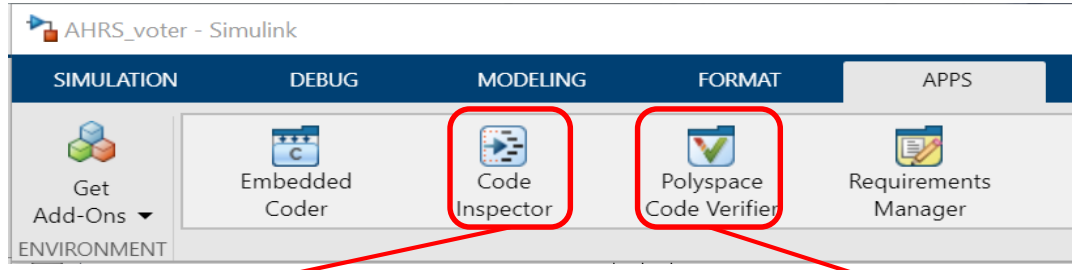
C Code Generation and Traceability Report

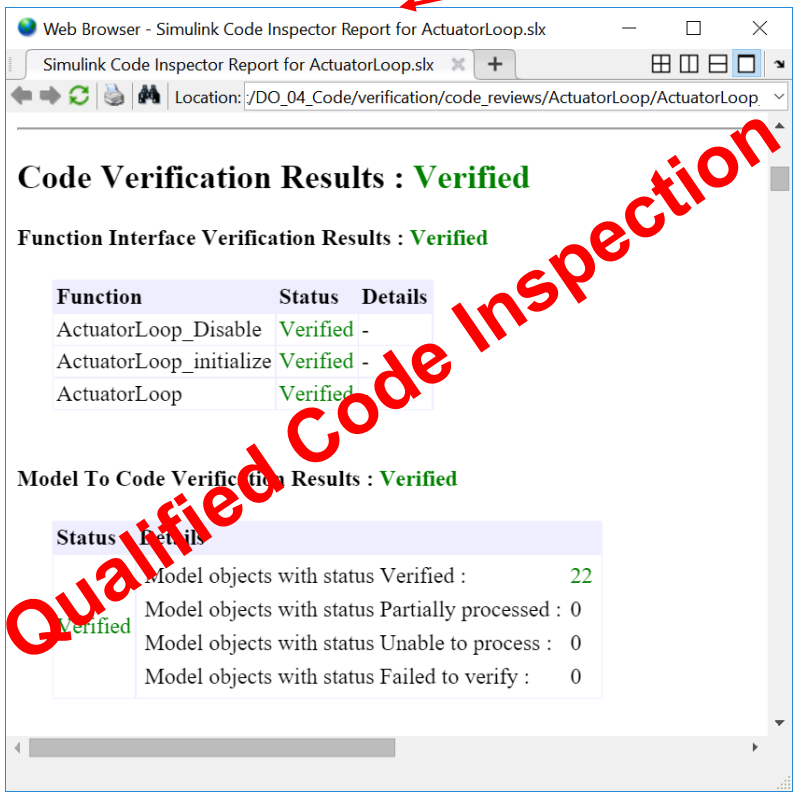




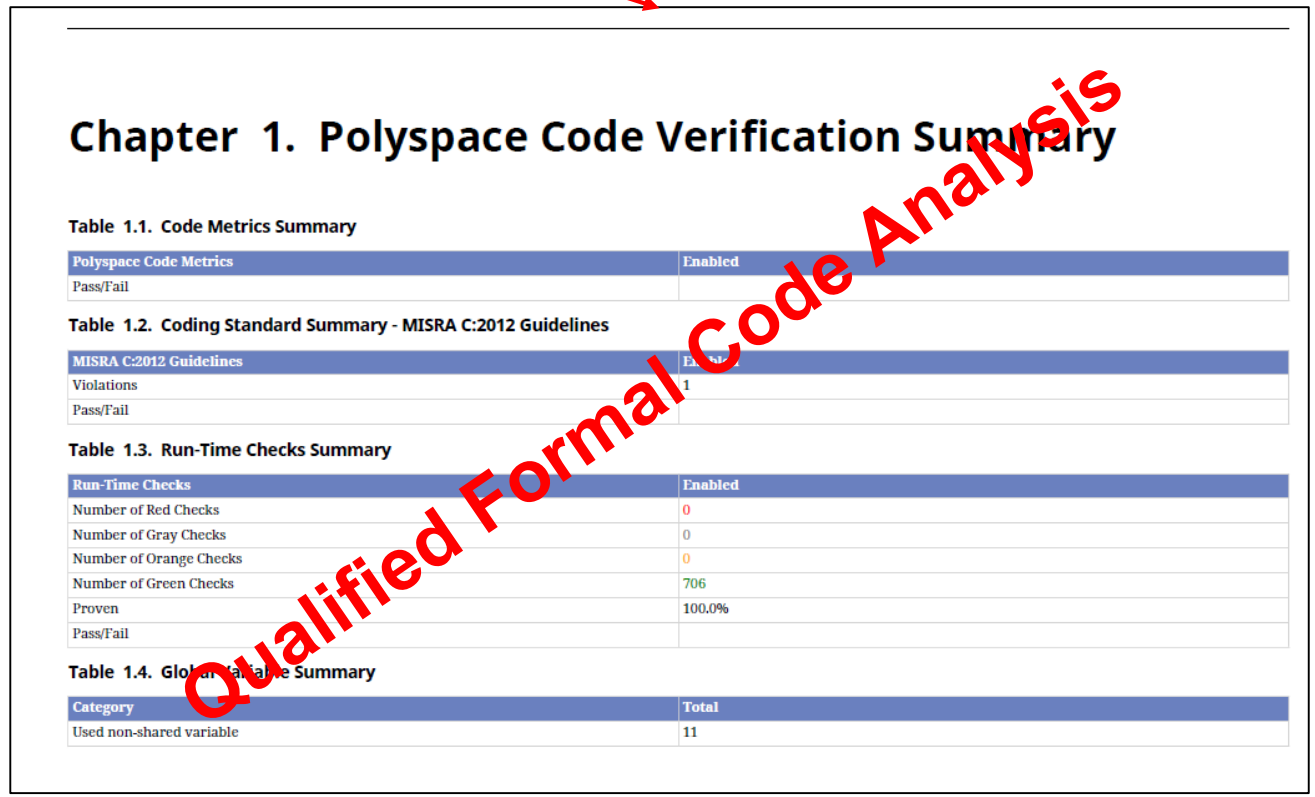


C Code Inspection and Formal Analysis



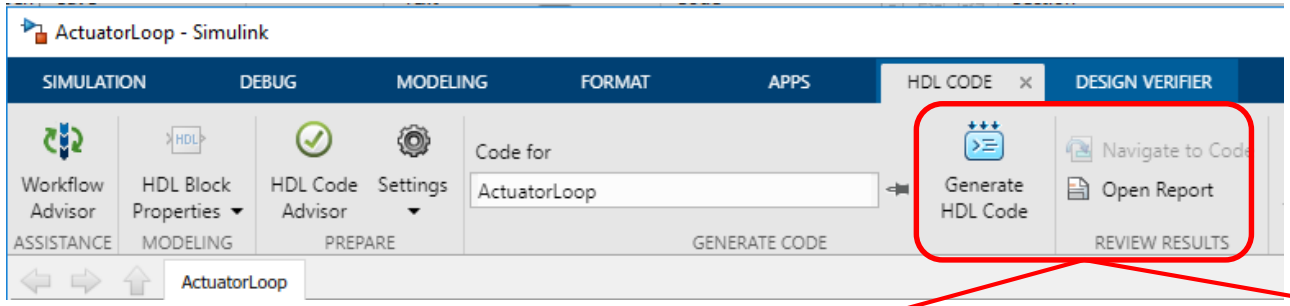


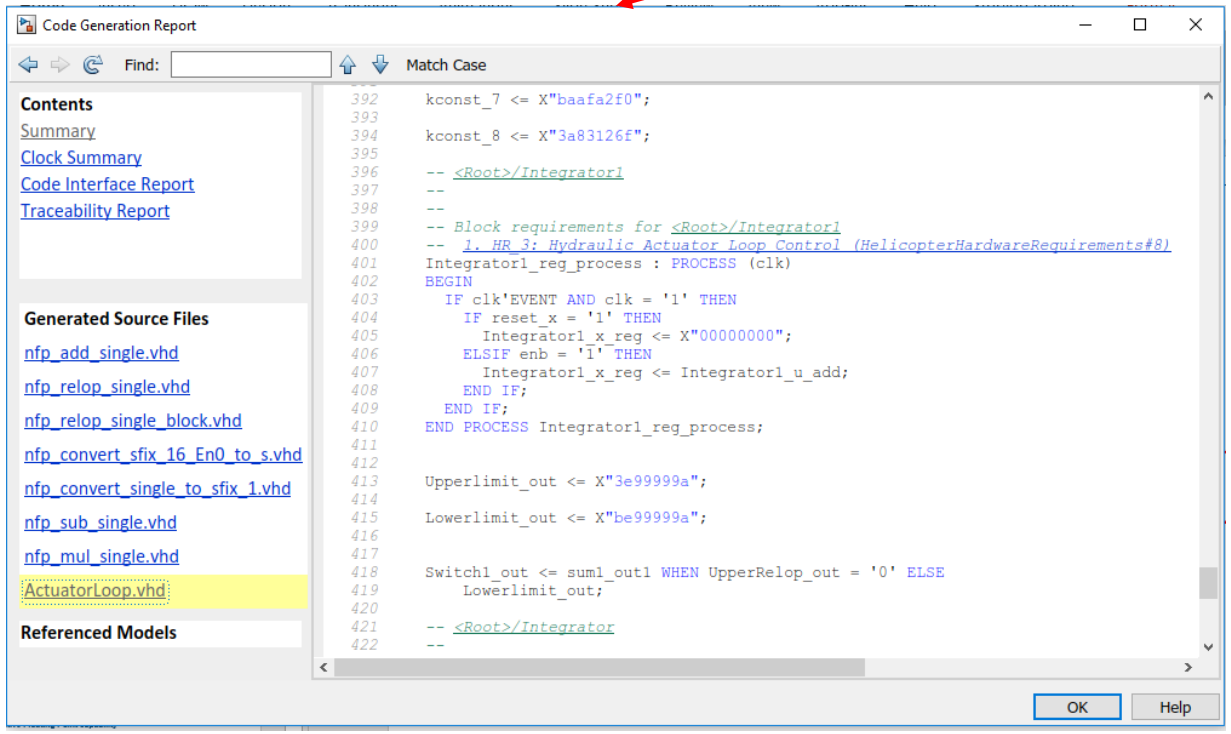
Qualified Code Inspection

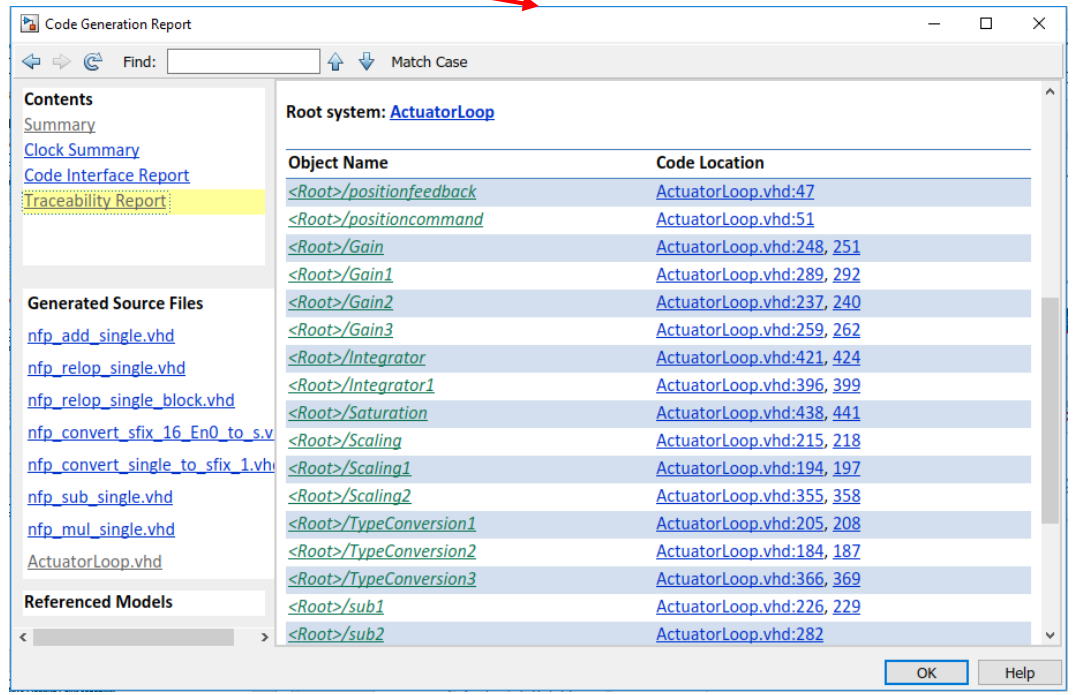


Qualified Formal Code Analysis

VHDL Code Generation and Traceability Report





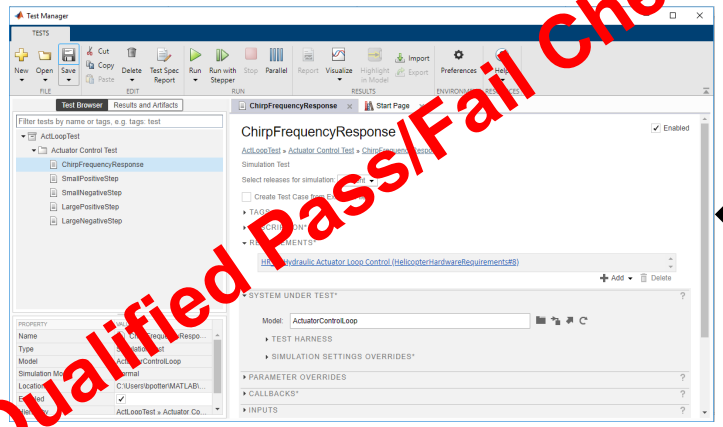


Hardware and Software Testing

Host-Based Software In-The-Loop and Co-Simulation Testing

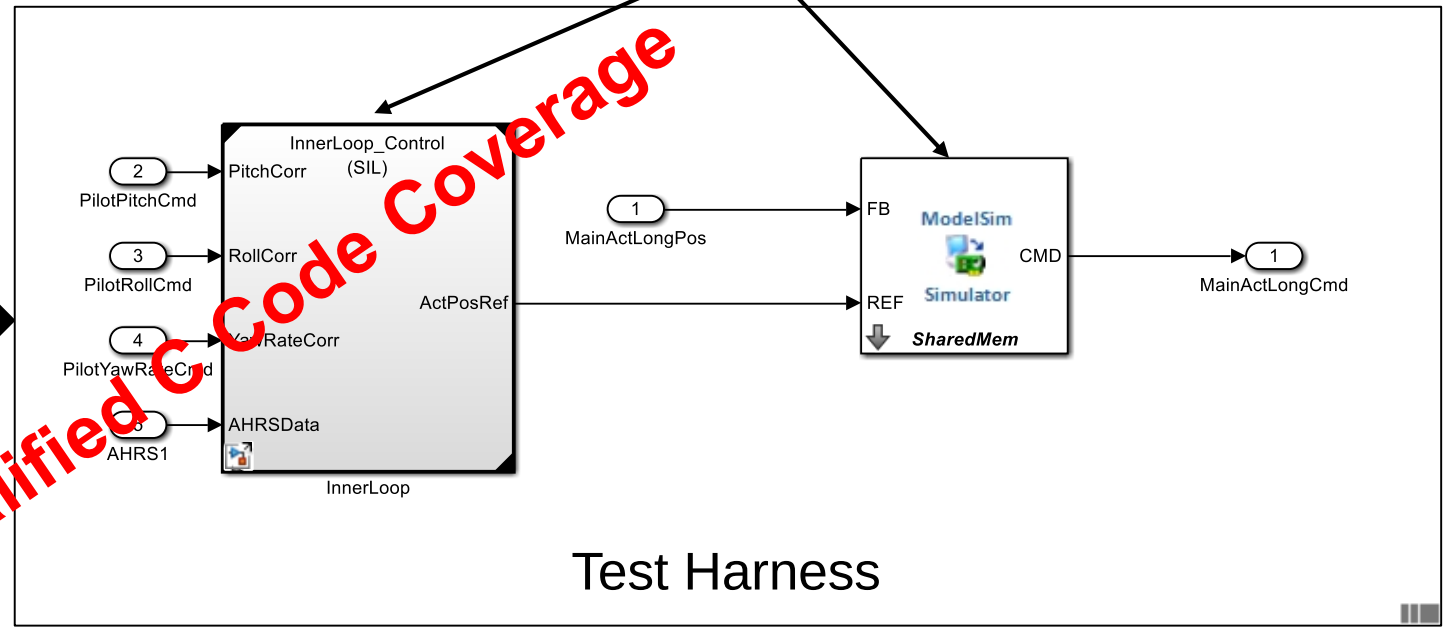
Code Coverage Analysis

Test Manager



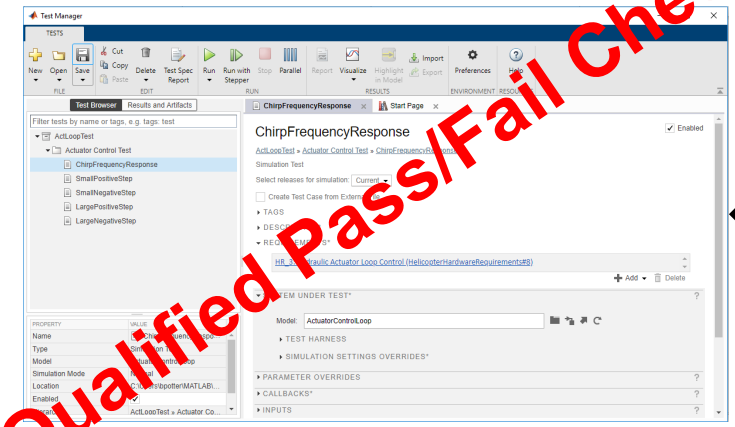
Qualified Pass/Fail Checking

Qualified C Code Coverage



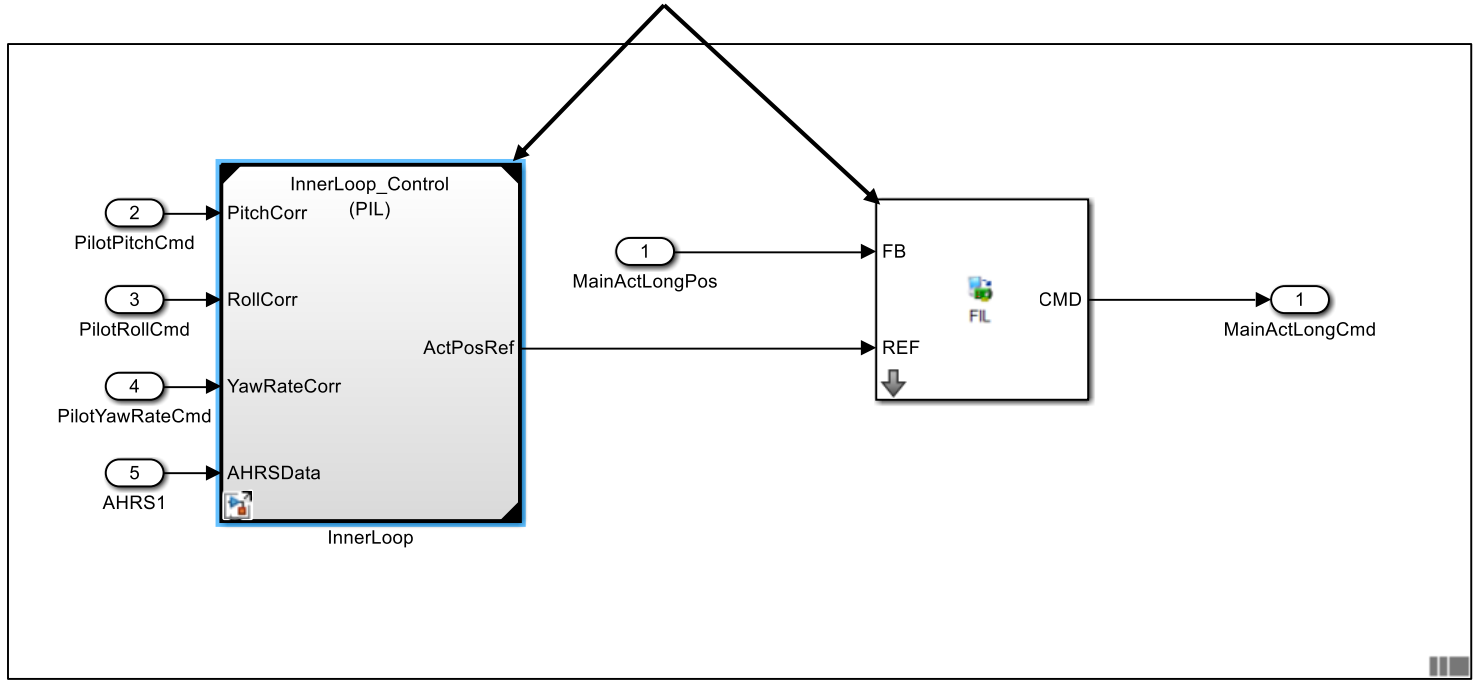
Target-Based Processor and FPGA In-The-Loop Testing

Test Manager



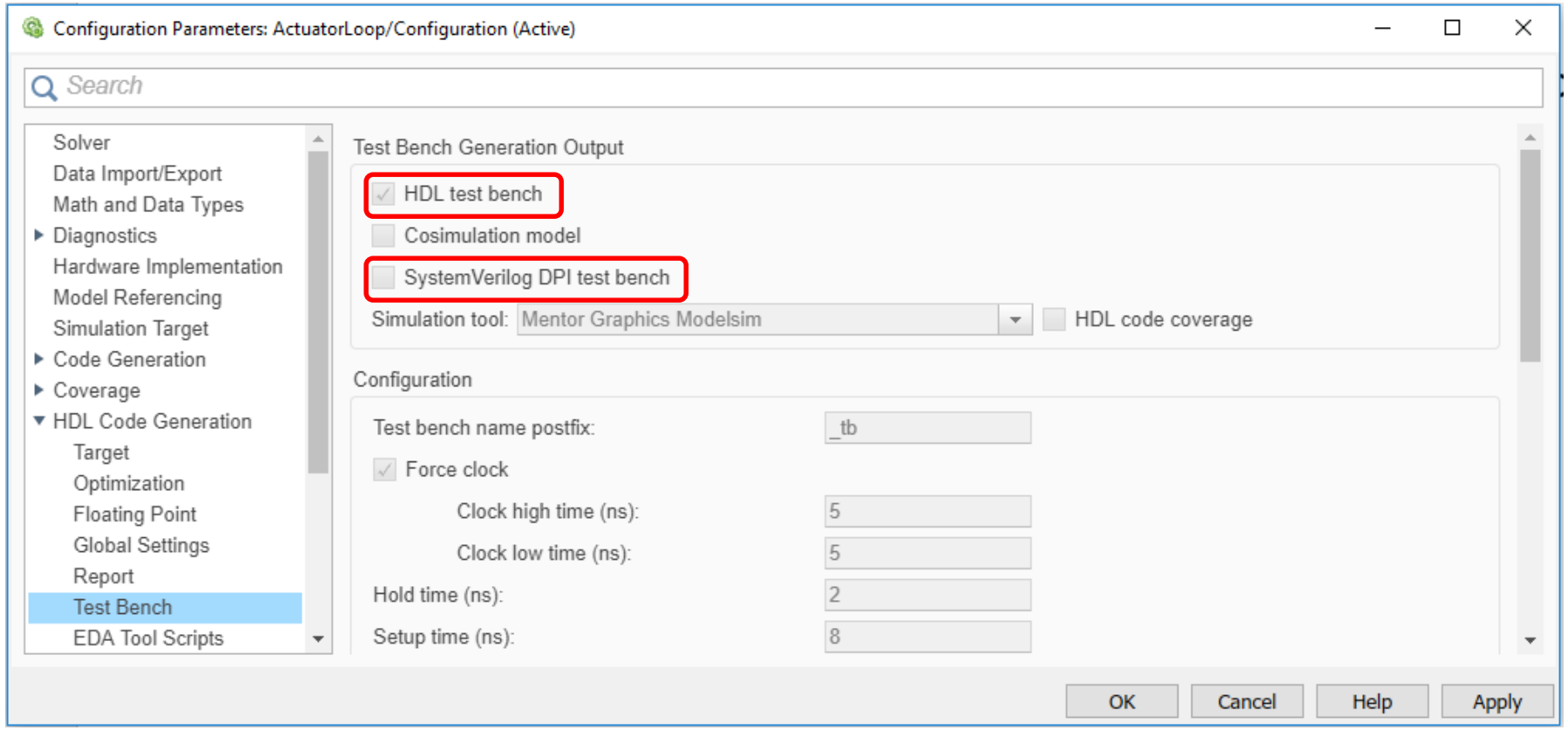
Qualified Pass/Fail Checking

Hardware-Software Integration Tests



Alternate Hardware Testing Methods Using Test Benches

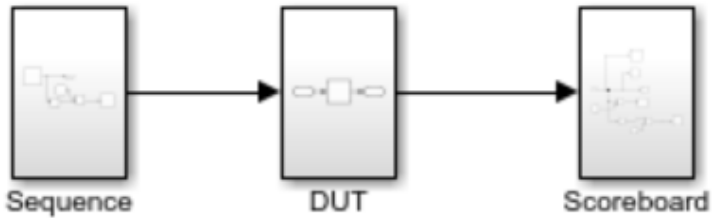
- Simulation cases and Simulink Design Verifier cases are exported to Test Benches



Alternate Hardware Testing Methods using Universal Verification Methodology (UVM)

- Simulation cases and Simulink Design Verifier cases are exported to UVM

```
open_system('hdlv_uvmbuild');
```



Generate UVM Test Bench

Generate a UVM test bench from this Simulink model, specifying the paths to the DUT, sequence, and scoreboard subsystems.

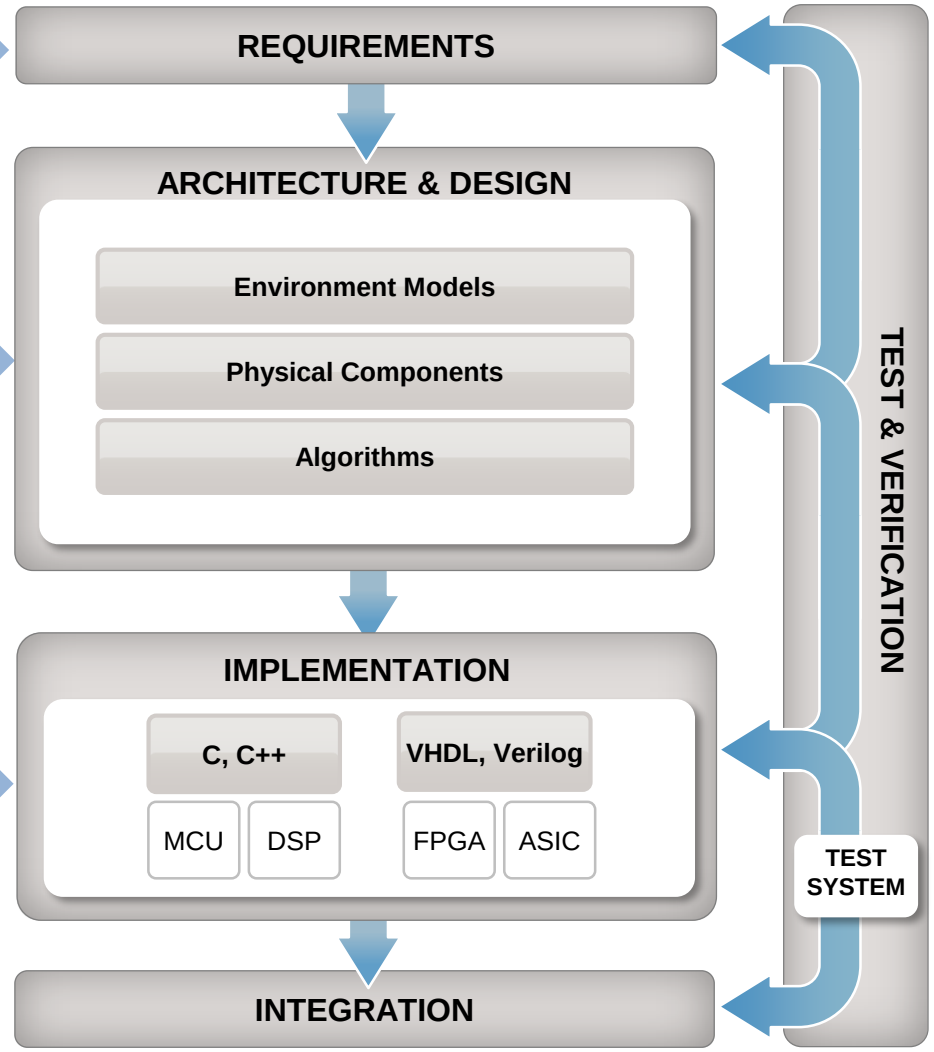
```
uvmbuild('hdlv_uvmbuild/DUT','hdlv_uvmbuild/Sequence','hdlv_uvmbuild/Scoreboard');
```

Qualified Tools ✓

- Simulink Requirements ✓

- System Composer
- Simulink
- Stateflow

- Embedded Coder
- HDL Coder



- Simulink Check ✓
- Simulink Test ✓
- Simulink Coverage ✓
- Simulink Design Verifier ✓
- Simulink Report Generator ✓

- Simulink Code Inspector ✓
- Polyspace Bug Finder ✓
- Polyspace Code Prover ✓
- HDL Verifier

User Stories and Examples

DO Qualification Kit (for DO-178) — Examples

Tool Qualification

DO-178C Simulink Project Template

Helicopter Flight Control: A Model-Based Design Example for DO-178C an…

Demonstrates the use of the DO-178C project template in a helicopter flight control project.

Airbus Develops Fuel Management System for the A380 Using Model-Based Design

Airbus A380, the world's largest commercial aircraft.

Challenge

Develop a controller for the Airbus A380 fuel management system

Solution

Use MATLAB, Simulink, and Stateflow for Model-Based Design to model and simulate the control logic, communicate the functional specification, and accelerate the development of simulators

Results

- Months of development time eliminated
- Models reused throughout development
- Additional complexity handled without staff increases

"The Simulink and Stateflow models enabled us to validate requirements early and communicate the functional specification to our suppliers, complementing the written requirements in conformance with ARP 4754."

Christopher Slack
Airbus

BAE Systems Delivers DO-178B Level A Flight Software on Schedule with Model-Based Design

Primary flight control computers from BAE Systems.

Challenge

Develop flight-critical software for a midsized business jet in compliance with DO-178B Level A standards

Solution

Use Model-Based Design to model the software and systems, run simulations with customer-provided test vectors, trace requirements to model elements, and generate 200,000 lines of certified code

Results

- Development efficiency doubled
- Certification schedule maintained
- Communication between teams facilitated

"When we generated code from our Simulink models with Embedded Coder, the team we handed it off to knew it was gold—that it was debugged and fully met the requirements—because we had run it through the Simulink test vectors supplied by our customer. That was a huge advantage on this program."

Maria Radecki
BAE Systems

Conclusion

- Model-Based Design increases productivity for development of certified systems
- A single development environment for System on a Chip
- Qualified tools that span ARP 4754A, DO-178C and DO-254

- Whether you are a systems engineer, software engineer or hardware engineer, you can deploy Model-Based Design on your certification project

Learn More

- ARP 4754 Solutions Page
  - https://www.mathworks.com/solutions/aerospace-defense/standards/arp-4754.html
- DO-178 Solutions Page
  - https://www.mathworks.com/solutions/aerospace-defense/standards/do-178.html
- DO-254 Solutions Page
  - https://www.mathworks.com/solutions/aerospace-defense/standards/do-254.html
- DO Qualification Kit
  - https://www.mathworks.com/products/do-178.html