



Introduction

The **Safety Argument** component of the Safety Assurance Framework (SAF) evaluates test results to assess CCAM safety through 4 blocks: Coverage, Test Evaluate, Safety Case and Decide.

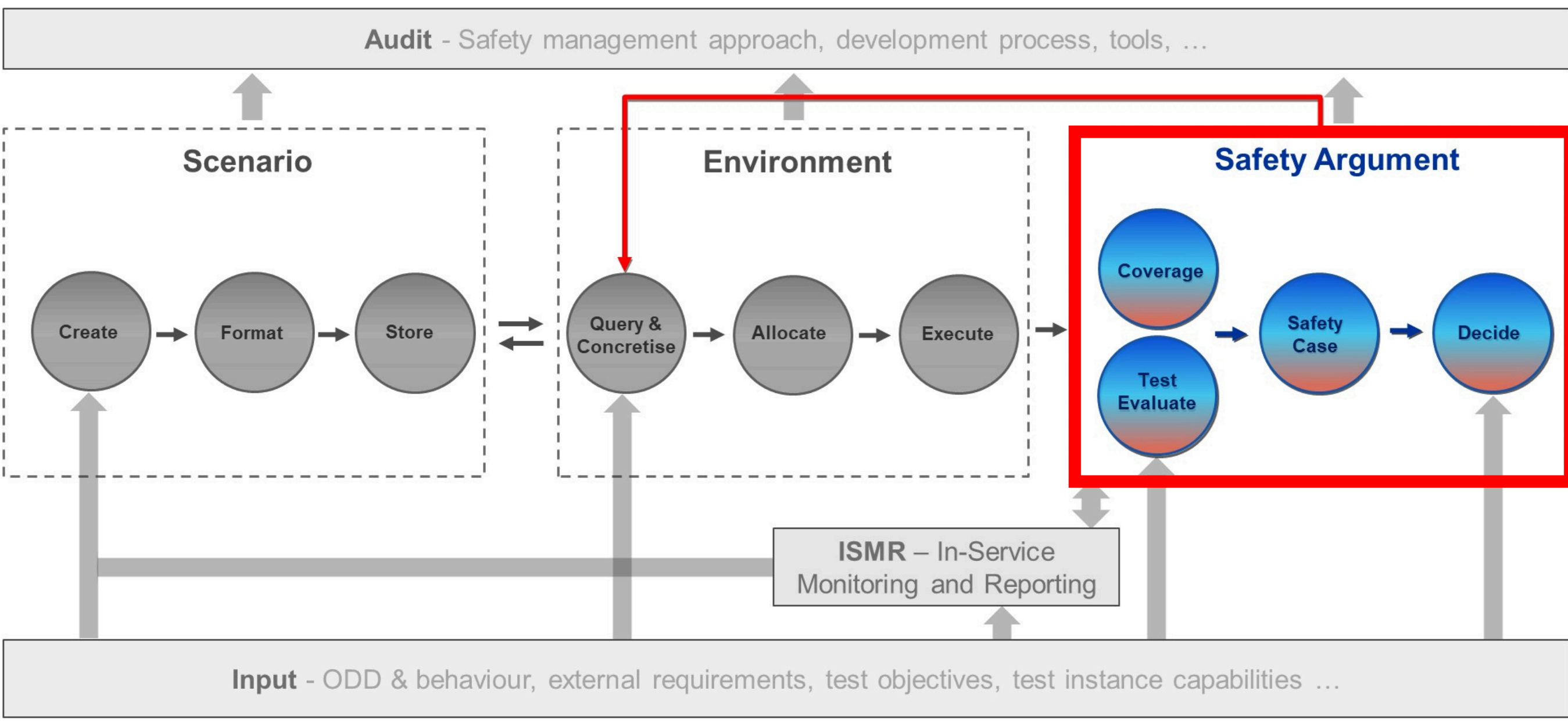


Figure 1. Safety Argument component of the Safety Assurance Framework

Coverage examines test coverage from multiple perspectives, including parameter ranges and boundaries of the Operational Design Domain (ODD).

Test Evaluate assesses test results to determine whether the system meets the safety requirements from the Input block.

Safety Case supports manufacturers in demonstrating that a CCAM system meets legal safety requirements by compiling structured evidence.

Decide combines all results from previous blocks into the overall safety assurance outcome of the CCAM system.

Coverage metrics

The term **Coverage** is defined as follows:

Definition Coverage:
Extent to which a set of scenarios cover the relevant aspects of an ODD.

“**set of scenarios**” could refer to:

- A set of test scenarios used for the safety assurance of a CCAM system.
- A set of scenarios observed in a (test) drive.

“**relevant**” depends on the context, e.g.:

- All relevant environmental conditions.
- A particular parameter space.

A good coverage metric...

- can be represented as a percentage.
- allows 100% coverage under realistic conditions.

Test validation metric

Test instances used in the Execute Block might contain models and tools that deliver unreliable results. Results are therefore validated by correlating against results of a higher test instance.

By clustering regions of the scenario parameter space by using results of the evaluation metric for the concrete scenarios, representative samples can be selected from these clusters.

These samples are then allocated to a higher fidelity test instance, using the SUNRISE allocation approach.

Dynamic allocation

The dynamic allocation process, allows for a reallocation of test cases to another test instance, if the test validation has failed.

If the validation shows a low correlation between results, an expert assessment has to be conducted. If sufficient evidence can be found to alter the functional test case requirements, the tests can be reallocated using the SUNRISE allocation approach.

Safety Case

A Safety Case is a set of documents with argumentation and evidence that a CCAM system meets legal safety requirements.

A Safety Case contains at least:

1. A **test matrix** per specific requirement, with test results and references (pass/fail).
2. **Convincing argumentation** to answer general requirements. For ex.: “The CCAM system shall not cause any collisions that are reasonably foreseeable and preventable”.
3. **Description of the response** of the CCAM system to scenarios relevant for soft requirements.

SUNRISE results include a document with principles and considerations regarding setting up a Safety Case, showing how the SAF is used to substantiate the Safety Case.

Partners



For more information, please contact:

erwin.degelder@tno.nl, jobst.beckmann@ika.rwth-aachen.de, olaf.opdenkamp@tno.nl