



**HAL**  
open science

# Approach for Early Validation of System Requirements Application to software architecture of autonomous vehicles

Yasmine Assioua, Rabea Ameer-Boulifa, Patricia Guitton-Ouhamou, Renaud Pacalet

► **To cite this version:**

Yasmine Assioua, Rabea Ameer-Boulifa, Patricia Guitton-Ouhamou, Renaud Pacalet. Approach for Early Validation of System Requirements Application to software architecture of autonomous vehicles. Séminaire Doctoral, Rencontres Académie -Industrie AFIS, Dec 2022, Toulouse, France. hal-04341749

**HAL Id: hal-04341749**

**<https://hal.science/hal-04341749>**

Submitted on 13 Dec 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

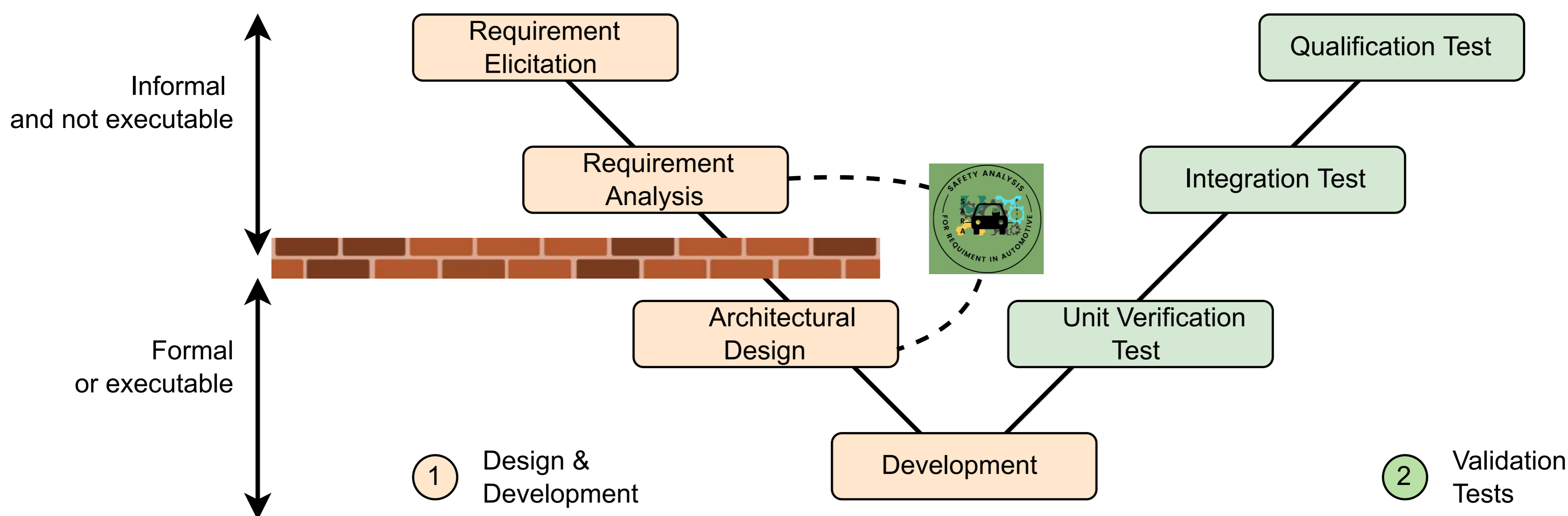


# Approach for Early Validation of System Requirements

Application to software architecture of autonomous vehicles

The standard software development process used in the automotive industry is the V-cycle. The left side is the part of requirement analysis, function design, and software development. While the right concentrates on verification and validation activities.

► We aim to help engineers to develop correct-by-construction systems. We aim to shift the verification above the informal and not executable limit by offering a method for early validation of systems under design that we called SARA.

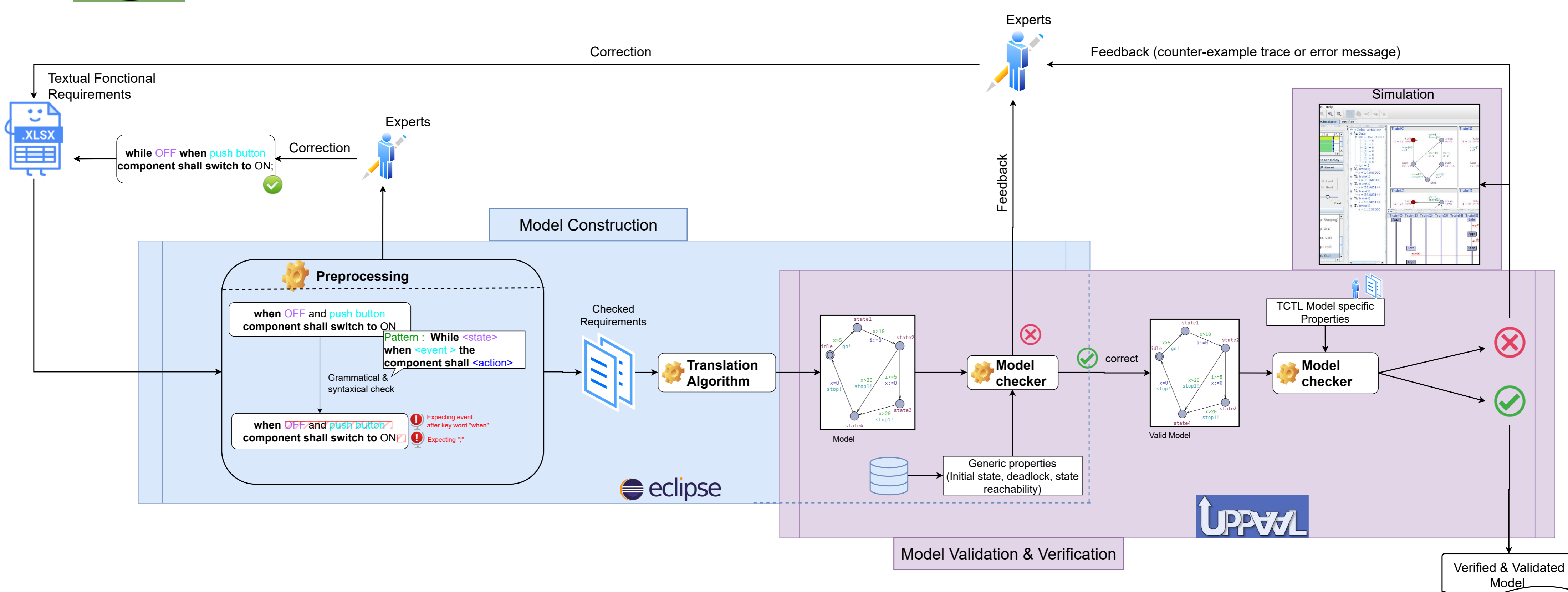


## Benefits:

- ✓ Reduce the need for validation testing and corrective measures at late development stages
- ✓ Push the validation limit
- ✓ Reduce time to market and costs



**SARA (Safety Analysis for Requirement in Automotive)** is a platform for early validation of (automotive) requirements through formal methods.



### 1 Model construction

- Pre-processing of requirements consists on grammatical and syntactical checking.
- Automatic generation of a formal model from textual requirements.

### 2 Model validation and verification

- Automatic verification of the model using model checking tool.
- Evolution of the early design model through iterative corrections/verifications until convergence to a correct model.