Integrating Cybersecurity Concerns in Functional Safety Assurance of AI-Based Automotive Systems

03/11/2022

Francesco Merola
Università di Pisa – ISTI/CNR

INTRODUCTION

Vehicle-to-Network
(V2N)

Vehicle-to-Infrastructure
(V2I)

Vehicle-to-Vehicle
(V2V)

Vehicle-to-device
(V2D)

Vehicle-to-Pedestrian
(V2P)
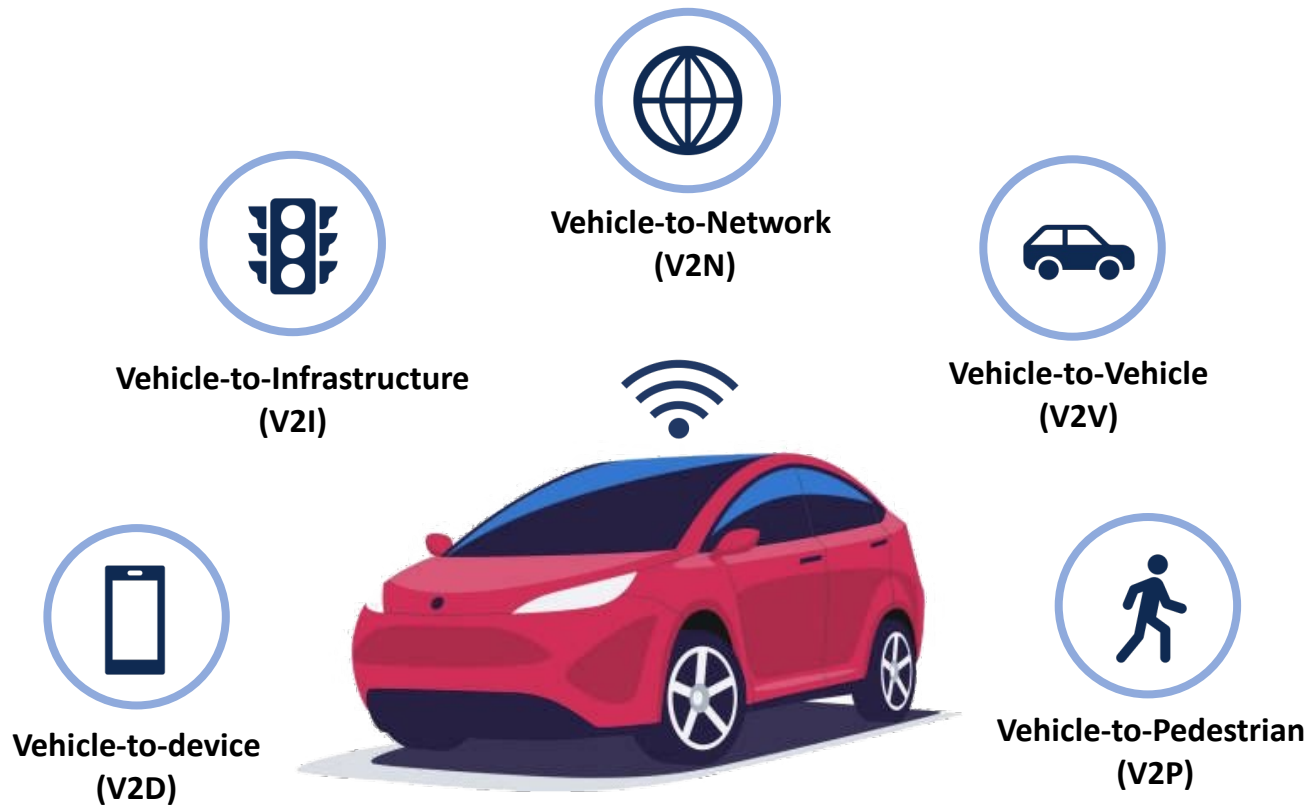
Connected and autonomous vehicles:

- Use of **Artifical Intelligence (AI)** based autonomous functionalities

- Increased connectivity beyond vehicle boundaries

- Significant increase in **risks related to cyber-security**

- Validation approaches need to evolve to account for these new functions

DISTANCE VS SCENARIO BASED VALIDATION

- Distance-based validation is a commonly used technique

- **Distance-based validation is infeasible** for complex autonomous driving functions
  - The number of km of test drives required would be too high

- **Scenario-based validation** is recently gaining popularity
  - Allows to only focus on **meaningful test-cases**
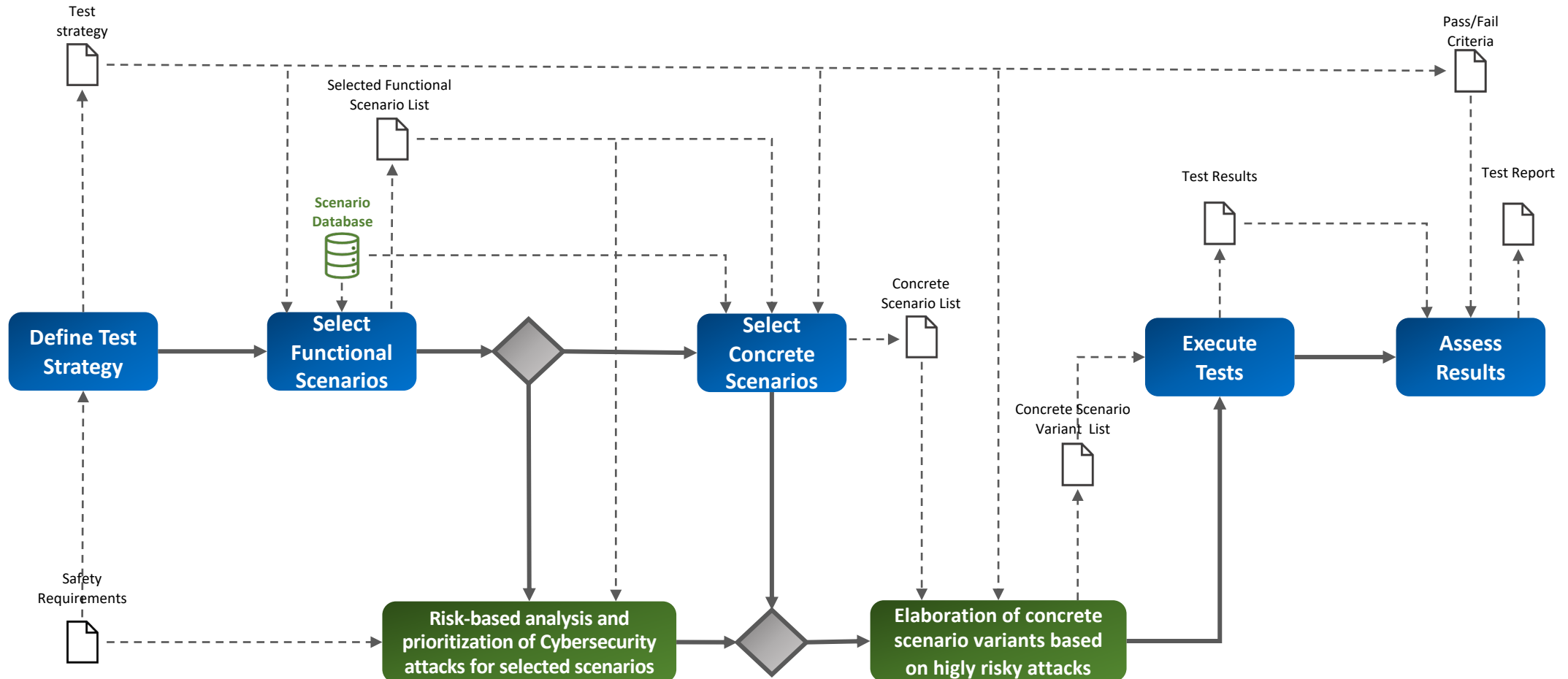 - Significantly reduces the required effort

SCENARIO-BASED VALIDATION
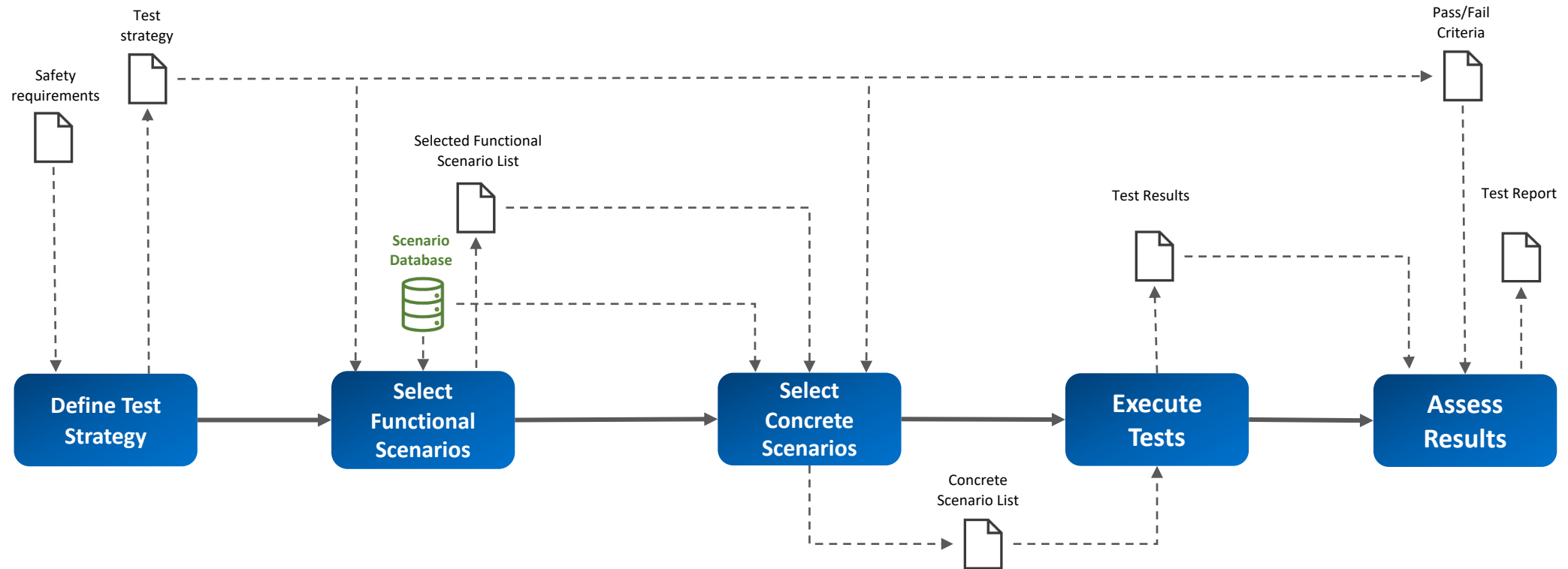
FUZZY LOGIC SECURITY RISK ASSESSMENT
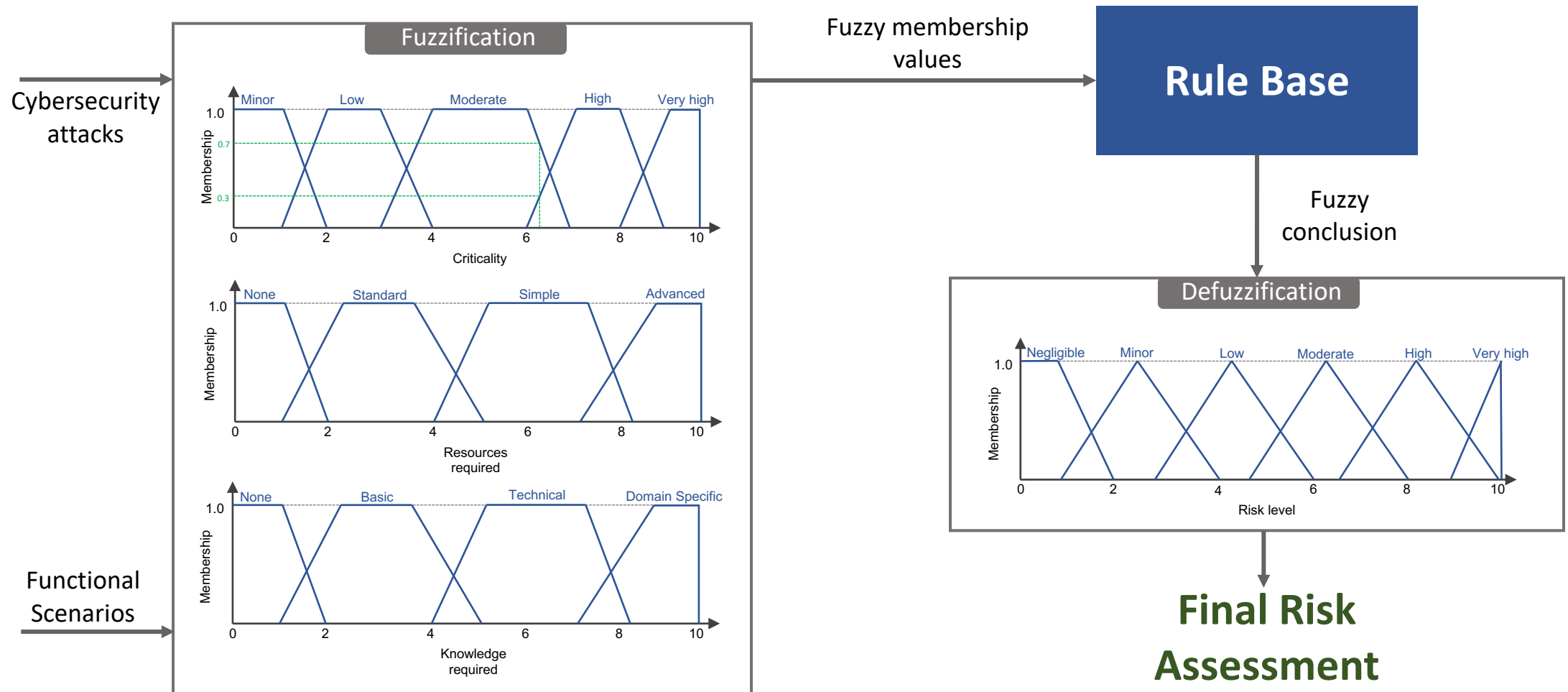
ISCA APPROACH

CONCLUSION & OPEN QUESTIONS

- A comprehensive validation methodology for higly autonomous vehicles (SAE Level ≥ 3) is still missing

- **Scenario-based validation** is a promising approach

- The **ISCA** variant that we propose extends the scope allowing for systematic consideration of **cybersecurity concerns**

- Some **open questions** remain:

  - How can we transition from a microscopic assessment (single scenario) to a macroscopic assessment of safety?
  - How can scenario-based methodologies be combined with other assessment methods?

THANK YOU

francesco.merola@isti.cnr.it