Multiresolution Platform to Verify and Validate Cooperative Driving Automation Functionalities in Contested Environments

Arman Sargolzaei, PhD

Director of Resilient, Autonomous, Networked Control Systems Lab

Assistant Professor of Mechanical Engineering

Tennessee Technological University

asargolzaei@tntech.edu

www.rancs-lab.com

Introduction

- **Education:**
  - MSc: Aerospace Engineering, University of Florida, 2019
  - PhD: Mechanical Engineering, University of Florida, 2020
  - BSc, MSc, PhD: Electrical Engineering-control systems, 2010, 2012, 2015
- **Current position:**

  Assistant Professor of Mechanical Engineering
- **Research Interests:**

  Security of Networked Control Systems; Testing and verification of Connected and Autonomous Vehicles; Security of Multi-agent Systems
- **Previous positions:**
  - Assistant Professor of Electrical and Computer Engineering, Florida Polytechnic University
  - Director of Advance Mobility Institute, Florida Polytechnic University
  - Research Assistant Professor, Florida International University
  - System Development Engineer, PLC International Inc

RANCS Team

Dr. Arman Sargolzaei **Dr. Shirin Noei**

Cindy Escobar

James Holland

Jonas Cunningham-Rush

Miguel Fuentes

Nathan Gardner

Nathan Gardner

Introduction

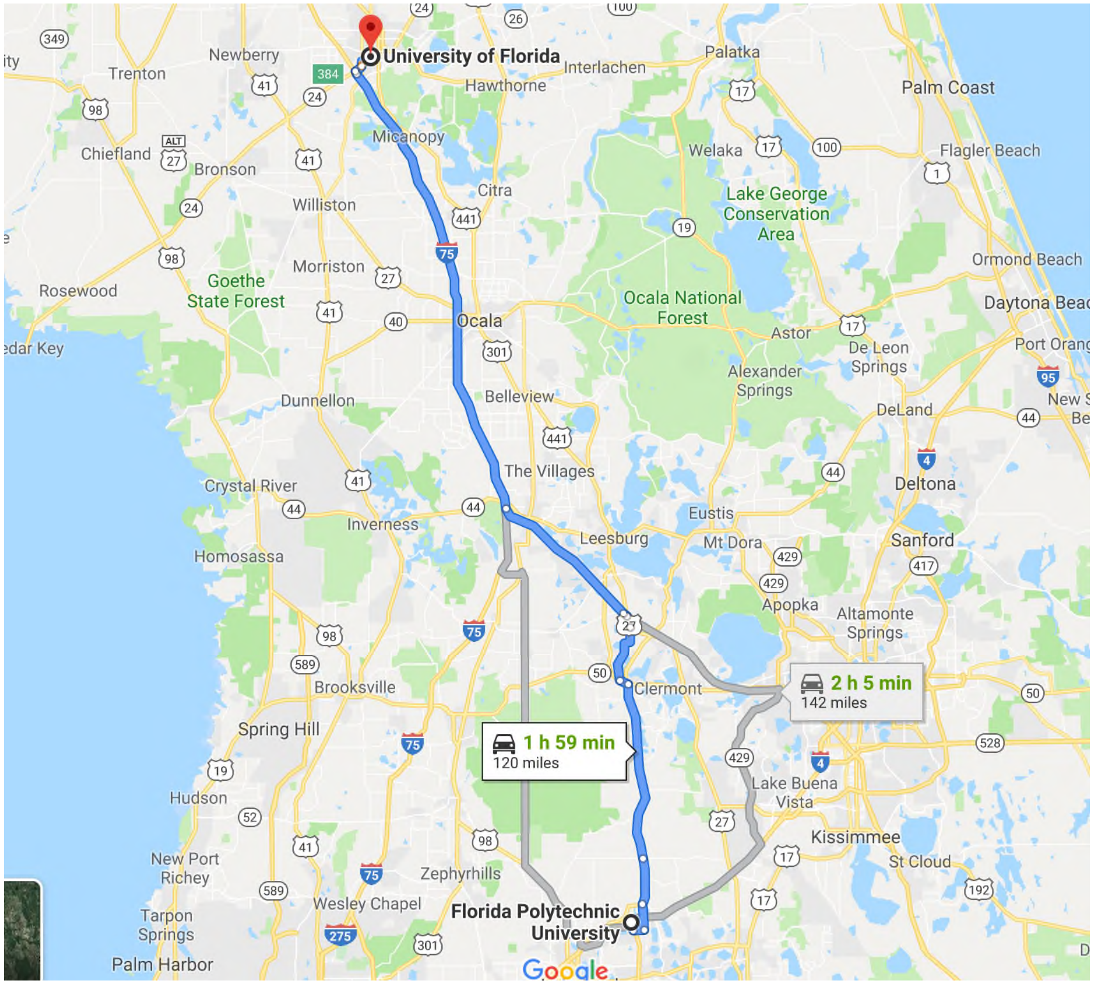
- According to a report of the National Highway Traffic Safety Administration (NHTSA), **94 percent of the 37,461** traffic fatalities in 2016 were due to human error.
- Autonomous Vehicles (AVs), including marine and robots, have the potential to add great value, but to be effective, they must be shown to be **safe and secure**.

Source: https://www.texastribune.org/2015/07/07/google-testing-self-driving-vehicles-austin/

Autonomous Vehicles

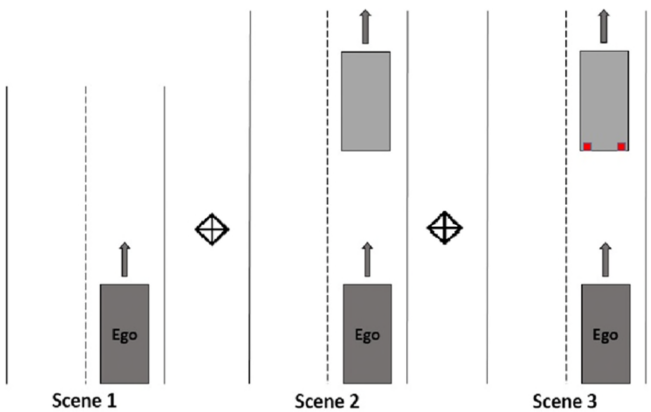
- Despite all of AV's advantages, the major barrier for wide-scale adoption of AVs is **the test and verification** regime to safety and security.

- To address this barrier, a process, which builds an *engineering argument* for assuring **safety and security**, must be developed.



Challenges

- **Scenario Testing and Verification**
  - How to generate interesting edge cases?
  - Do we need to test for all possible cases?
  - Can we eliminate similar scenarios using equivalent classes theory?
  - Can we do the coverage analysis?



- **Developed a language of factors that define a scene**
- **Factors translated into parameters for formulation**
- **Formulation enables pseudo-random test generation**

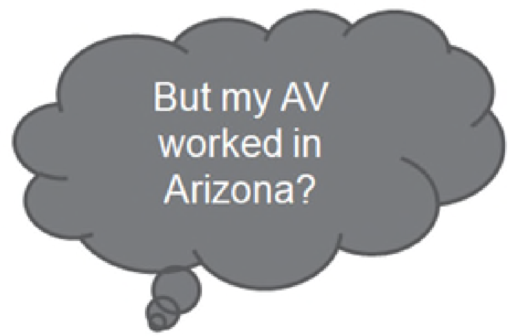
$$\left(\begin{bmatrix}0&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\\0&0&0&1&0\\0&0&0&0&0\end{bmatrix}\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\\0&0&0&1&0\\0&0&0&0&0\end{bmatrix}\right)\begin{bmatrix}d_{rlong}\\V_{rel}\\d_{rlat}\\d_{long}\\d_{lat}\end{bmatrix}=\begin{cases}pass\ if\begin{cases}d_{rlong}\geq 0\\V_{rel}>0\\d_{long}>0\end{cases}\\fail\quad Otherwise\end{cases}$$

Challenges

- **Scenario Testing and Verification**
  - How can we systematically learn from real-world crashes?
  - Can we test future CAVs based on real-world crashes?

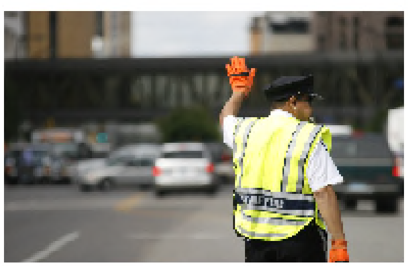
Challenges

- **Environmental and sensor testing**
  - How the perception of CAV performs under electromagnetic interferences?
  - How to test CAVs and their perception under different weather conditions?



Challenges

- **Language of Driving**
- Do we have a language for driving?
- How human in the loop can be tested?
- How ethical are CAVs?




Security Challenges

- Cyber-physical attack
  - How to test the security of CAVs in critical situations?
  - How to test the stability of CAVs under faults, failures, and cyber-physical attacks?

Challenges:

- Cost of redesign and collaboration problem
- Random attacks
- Resource constraints
- Communication protocols are not well designed
- Intelligent attacks

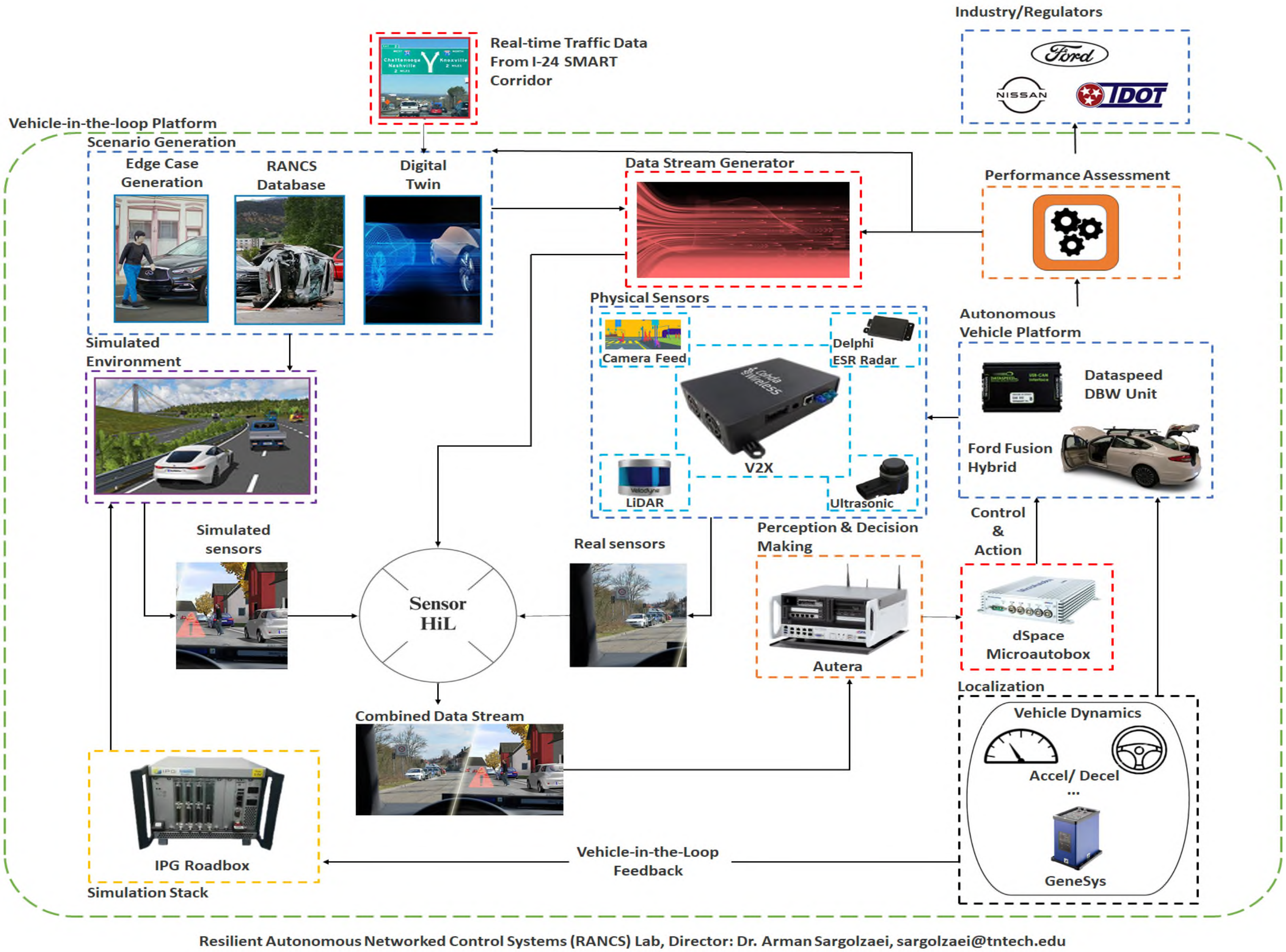
Testing Environments

Offline testing
- Software-in-the-loop

Real-time testing
- Software-in-the-loop
- Hardware-in-the-loop

Real-time testing
- Vehicle-in-the-loop
- Real-world

Mixed Reality Platform



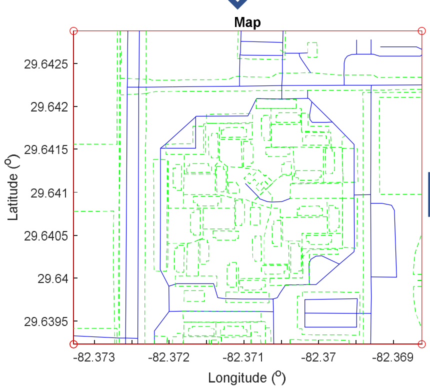
Modes of operation:

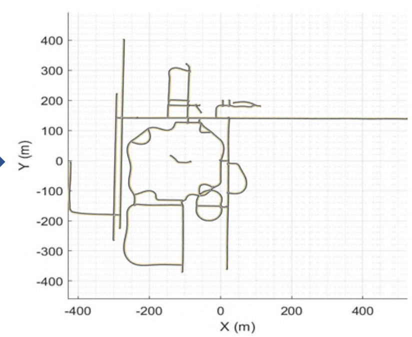
- Manual
- ViL
- Automated
- Autonomous Level 3+

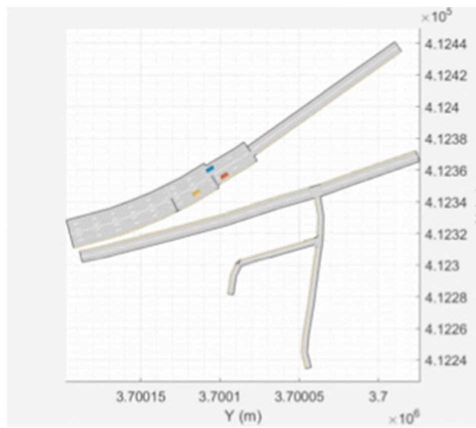

RANCS LAB

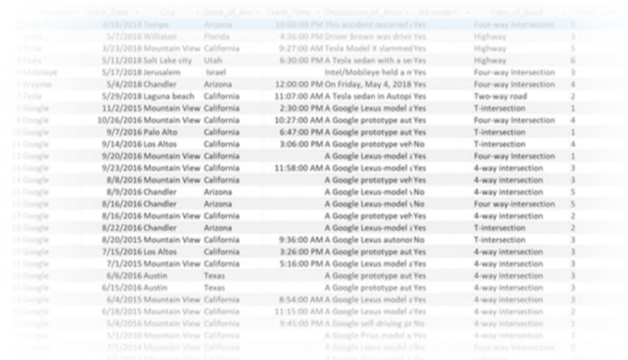
Scenario Generation

- Game engines and random scenario generation (coverage and equivalent Classes)
- Scenario abstraction from real life
- Digital Twin Environment

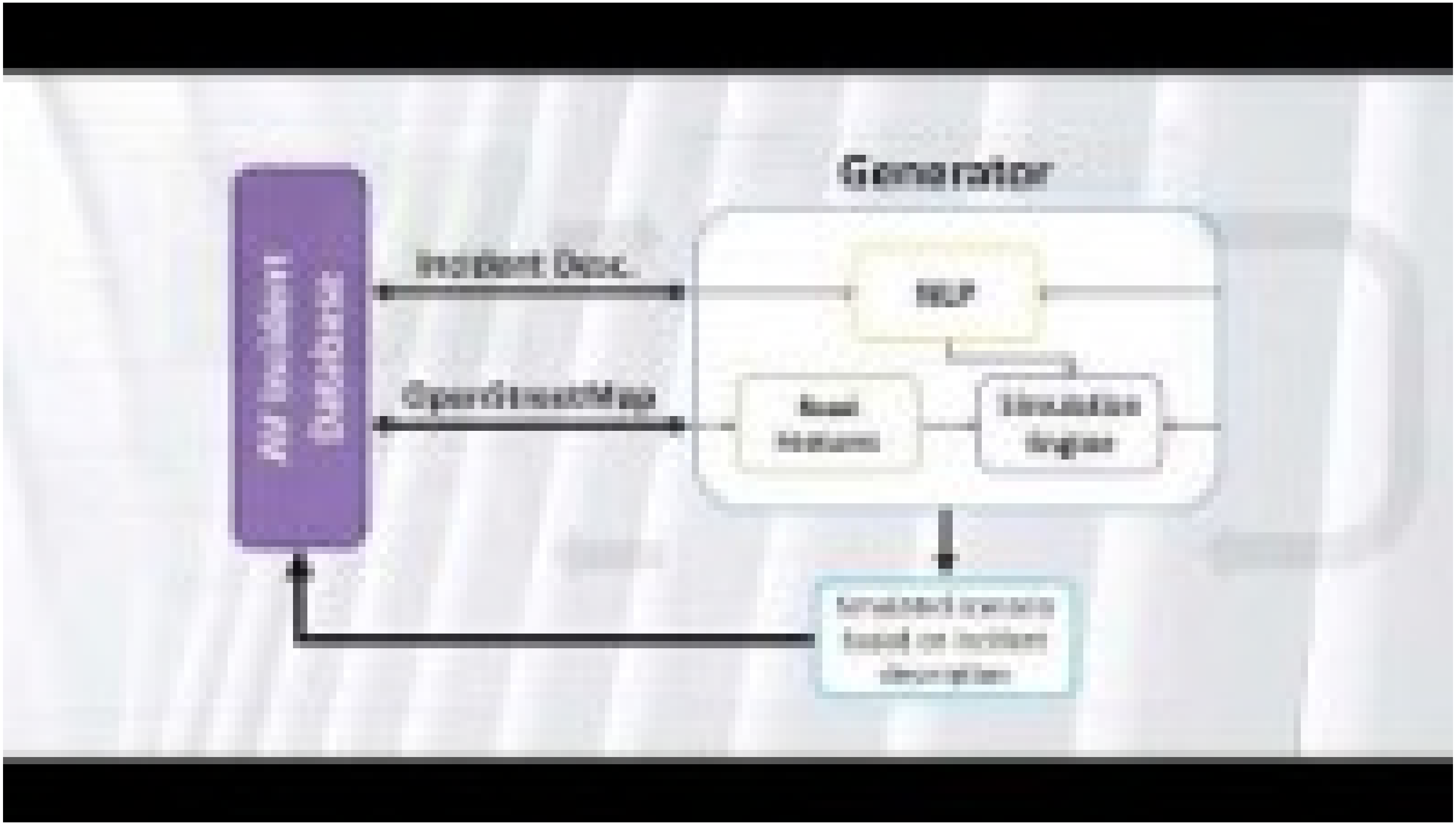




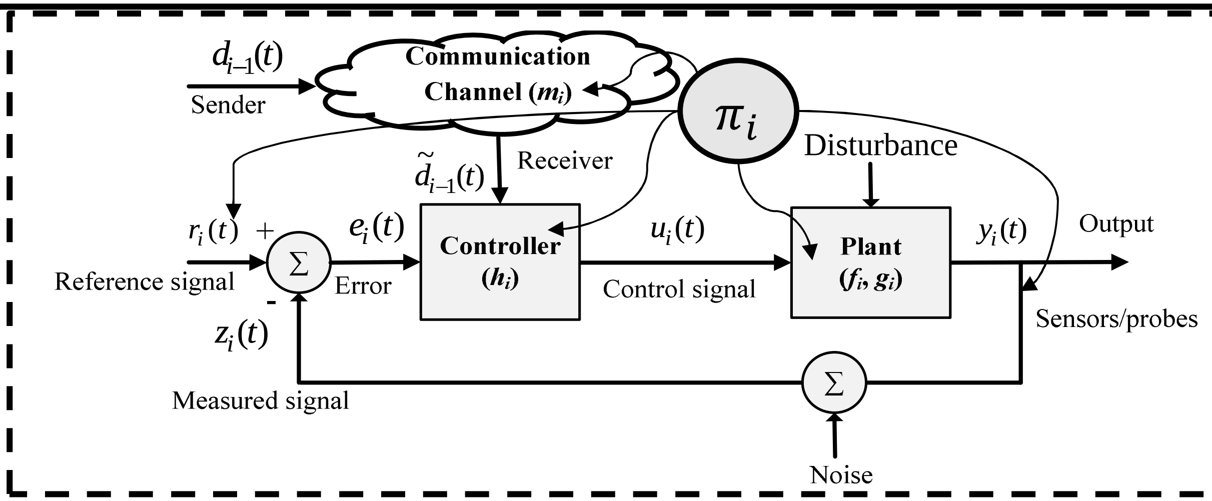




Scenario abstraction from real crashes



Attack and Fault Generation



Effects of attack π_i can be modeled as

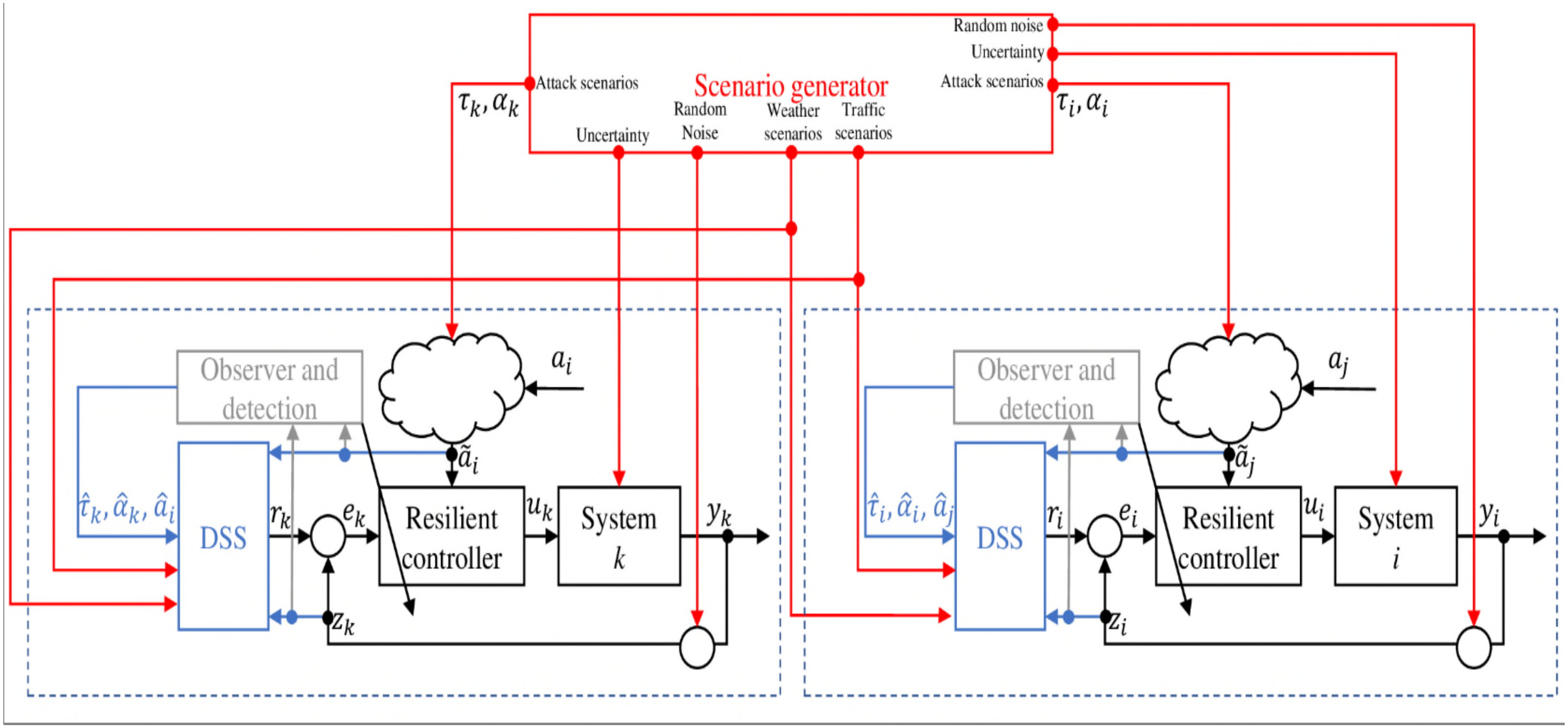
$$\tilde{\gamma}_i(t) = \pi_i(\gamma_i(t)) = \gamma_i(t - \tau_i(t)) + \beta_i(t)$$

where β_i and τ_i are random variables, γ is the signal/information under attack.

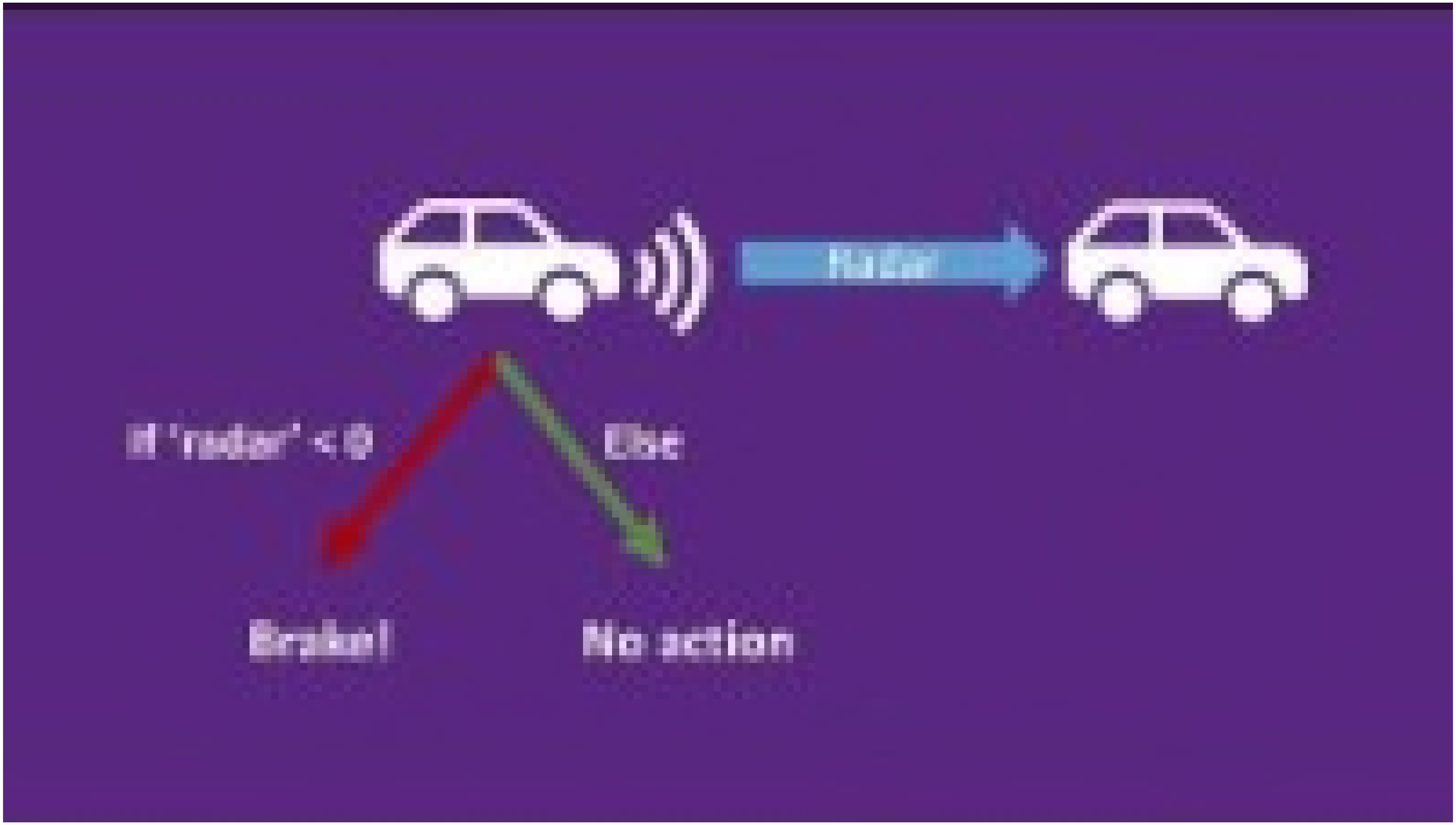
- **False Data Injection (FDI) Attack:** $\tau_i = 0$ and $\beta_i \neq 0$ for $t \geq 0$
- **Time-Delay Switch (TDS) Attack:** $\tau_i \geq 0$ and $\beta_i = 0$ for $t \geq 0$

The proposed model covers weather effects on sensors and vehicle communication.

Attack and Fault Generation



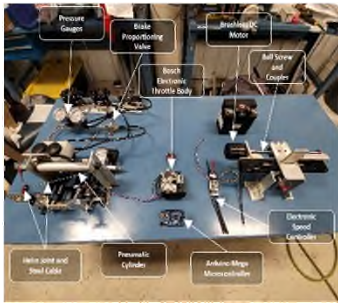
CAV under Attack



Autonomous Race Vehicle

Our Research:

- Testing and Verification of CAV
- Testing V2P interactions
- Testing and training human and CAV interactions
- Digital Twin and Mixed Reality Platform
- Drive by Wire Table for Racing Vehicle
- Autonomous Racing Vehicle
- Autonomous Golf Cart
- Vehicle Simulator



Towards Autonomoy

Q/A

Arman Sargolzaei, PhD

Assistant Professor of Mechanical Engineering

Tennessee Technological University

asargolzaei@tntech.edu

www.rancs-lab.com