CARIAD

Master Thesis: AI Usage in CI/CD/CT Pipelines for Compute Platforms in Automotives

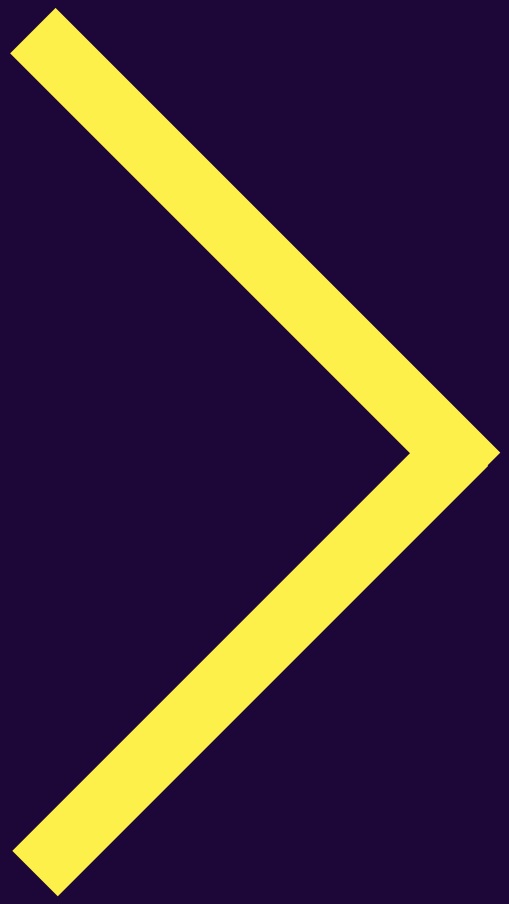
We transform automotive mobility

CARIAD
A VOLKSWAGEN GROUP COMPANY

Agenda

// Introduction
// Problem Statement
// Overview
// Research Objectives
// Key Differences
// Expected Outcomes
// Conlcusion

Introduction



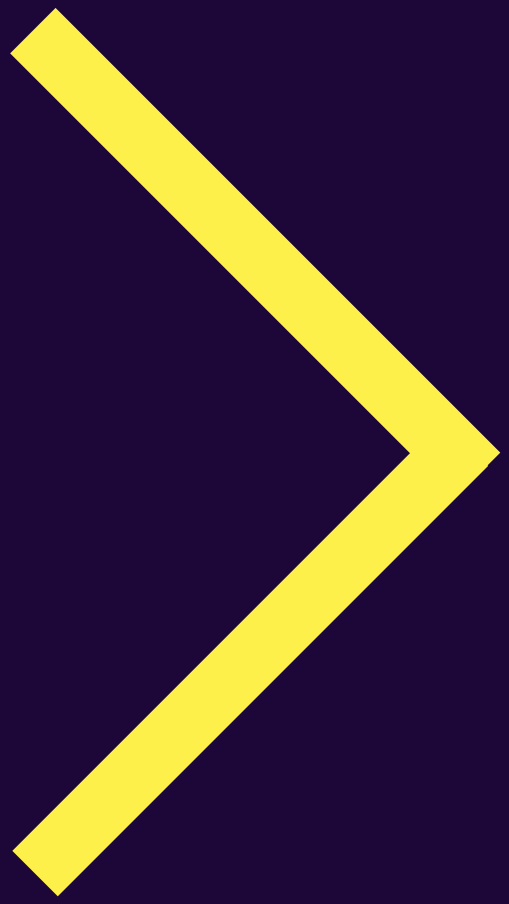
Introduction

- Rapidly growing software complexity & shorter release cycles
- Automotive ECUs are safety-critical—zero tolerance
- Traditional security tests cannot keep pace with CI/CD demand

Introduction

- Rapidly growing software complexity & shorter release cycles
- Automotive ECUs are safety-critical—zero tolerance

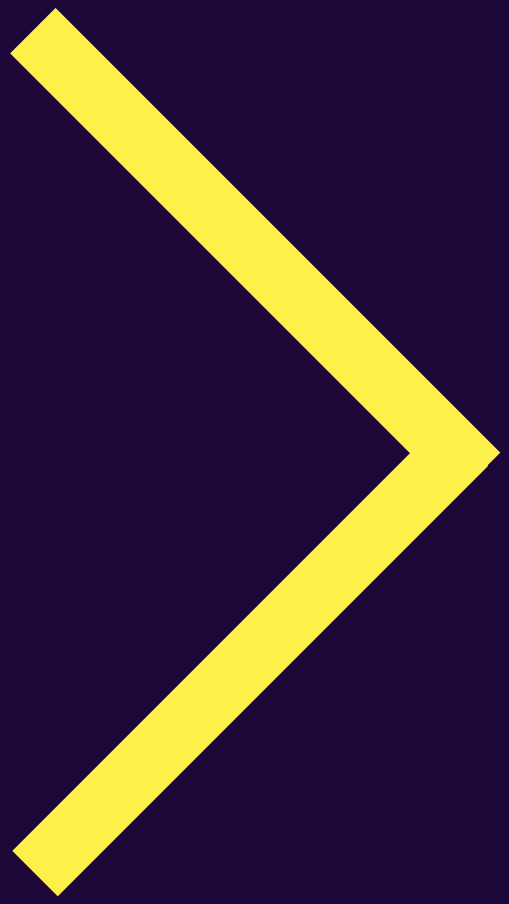
Problem Statement



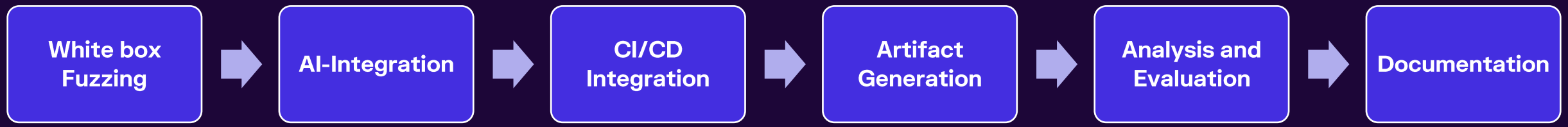
Problem Statement

- Current white-box fuzzing & testing are manual or slow to scale
- Vulnerabilities may slip through nightly CI due to time limits
- Need an AI-guided approach integrated into CI/CD/CT to
  - boost path coverage and
  - auto-generate actionable test artifacts

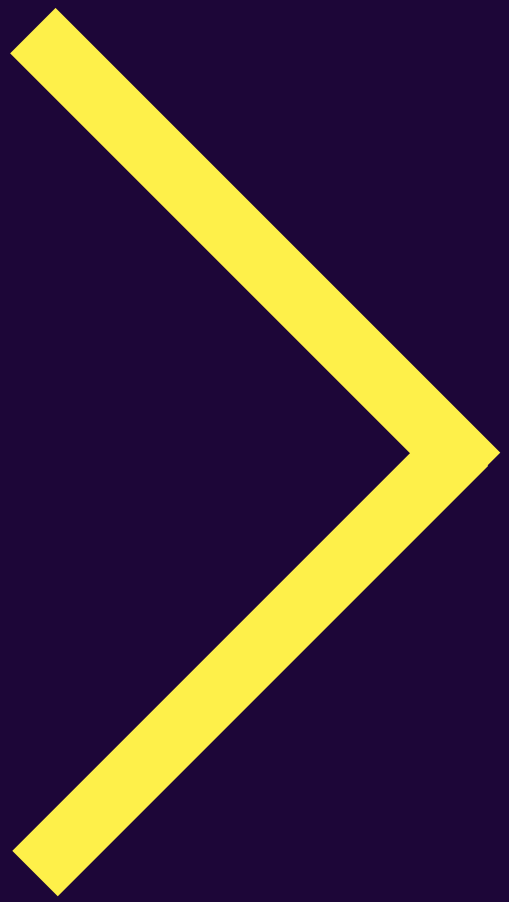
Overview



Overview


White box Fuzzing
AI-Integration
CI/CD Integration
Artifact Generation
Analysis and Evaluation
Documentation

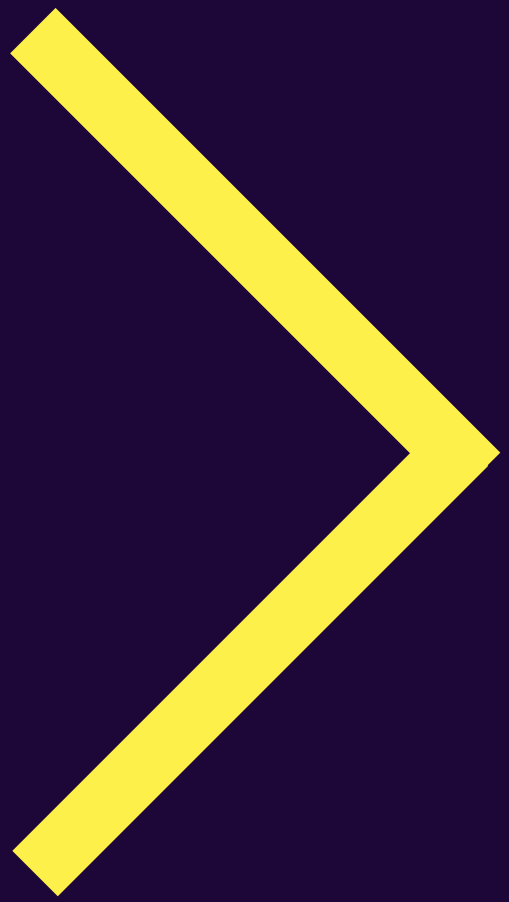
Key Differences



Key Differences

Normal Fuzzing	LLM Based Fuzzing
Random mutation of seed inputs	Content-aware, AI-driven input generation
Brute-force, random	Reinforcement learning, symbolic execution
Static, predefined input mutations	Dynamic, learns from previous tests (Continuous Fuzzing)

Research Objectives



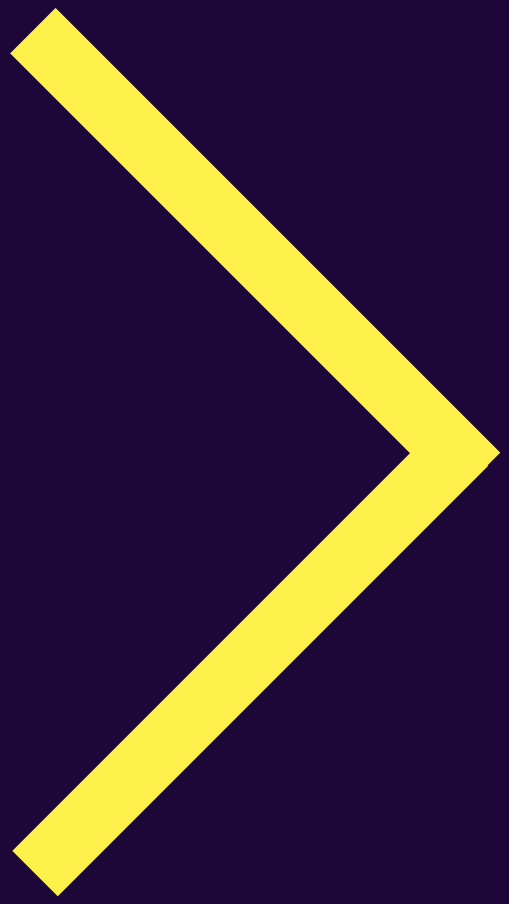
Research Objectives

Technique Design
- AI-assisted white-box fuzzing for automotive targets

Pipeline Integration
- Embed continuous fuzzing into existing CI/CD/CT

Artifact & Impact Automation
- Auto-generate test cases, reports, quality matrix
- Measure coverage, MTTV, and CI latency vs. baseline

Expected Outcomes



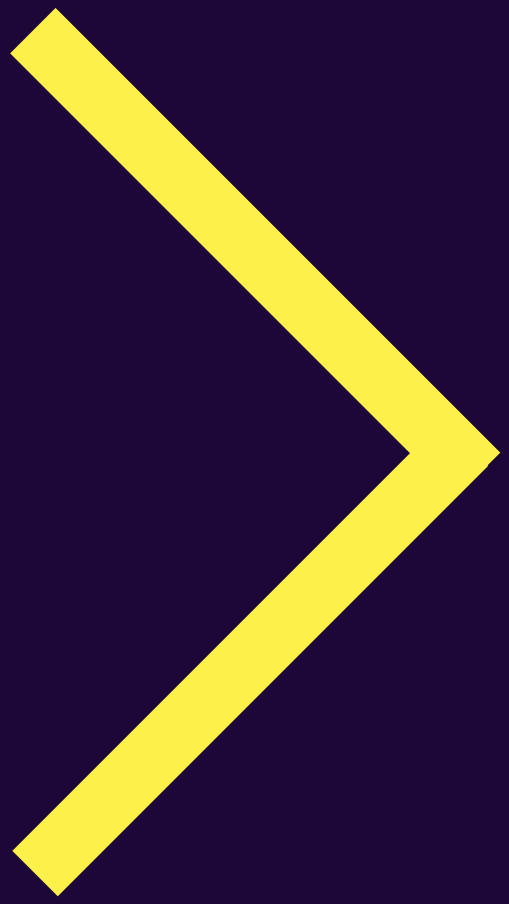
Expected Outcomes

AI-Driven Security Testing

Integration into the existing CI/CD Pipeline

Automation of test artifact generation

Conclusion



This thesis focuses on integrating AI and LLMs into CI/CD/CT pipelines to improve the security testing of automotive software

Thank you!