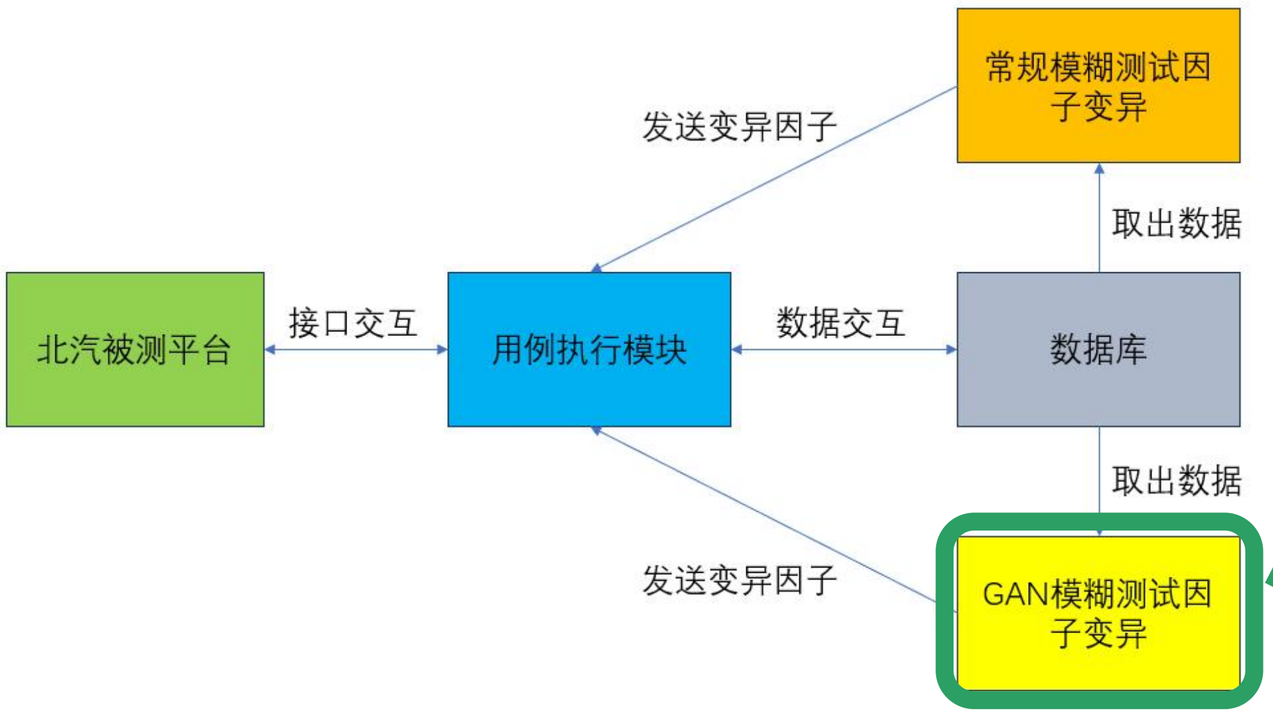
基于GAN的VCU休眠唤醒智能测试方案

Presenter:胡宝怡

项目架构与接口关系



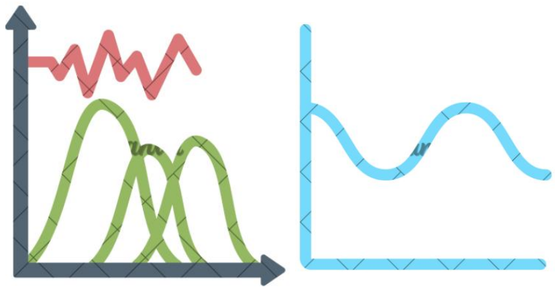
做单独的GAN服务，用接口与现有模糊测试相连

输入：

- 团队已积累的测试数据库
- 包含正常和异常的测试用例

输出：

- 针对性测试数据
- 高概率触发状态卡死的信号组合



项目整体流程

传统测试→经验积累 →模式学习 （我们的核心任务）→智能生成→效果验证→持续优化

历史测试数据

- 包含已发现的"状态卡死或失效"测试用例
- 包含正常工作的测试用例
- 包含各种边界条件的测试数据

GAN训练引擎

- 学习信号格式
- 学习故障特征
- 学习各种信号组合

智能测试序列生成

- 产生容易引发异常的连续数据组合

输入——每种信号特点与格式

- 五种唤醒信号

1、供电电压（9.0V-16.0V）

2、网络唤醒报文使能状态 （1）

3、CC2电压（4.0V-7.4V）← 当前重点

4、CP幅值（9.0V-13.0V）

5、CC电压值（0V-4.0V）

- 固定的休眠信号

1、供电电压（0V）

2、网络唤醒报文使能状态（0）

3、CC2电压（12V）

4、CP幅值（0V）

5、CC电压值（12V）

每次测试只使用一种唤醒信号，休眠是固定的一组值

数值型信号有明确范围和精度

测试流程：唤醒信号 → 休眠信号 → 循环测试

→

GAN模型学习每种信号的特点

便于生成更有效的输入信号

输入——已有输出信号与异常状态

· 关键状态指标：
整车State状态
总线报文发送标志位
PDCU唤醒原因
整车模式
功耗电流

· 三种目标状态：
output： 正常状态
error： 错误状态
stuck： 卡死状态

· 时序特征提取
时序模式特征：
- 短期模式（最近3次交互）
- 中期趋势（最近10次状态变化）
- 异常模式（历史异常序列）

状态转移特征：
- 状态稳定性
- 转移频率
- 异常跳变模式
- 恢复能力

· 当前测试输入信号对应的输出状态→有无异常？

· 当前测试的前序状态： 前N次休眠唤醒的结果

· 后续影响： 当前测试对后续状态的影响

→

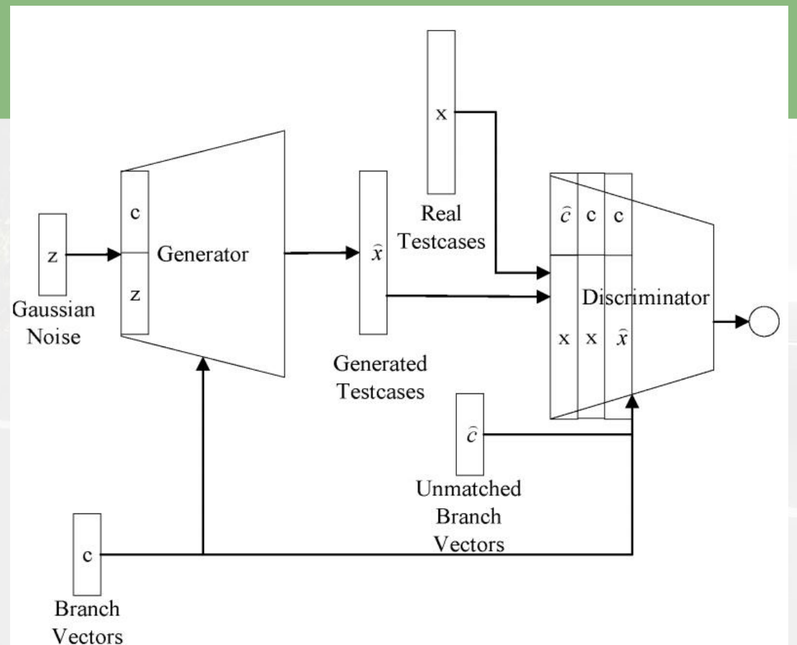
将每次的输入信号对应的输出状态以及上下文状态转换成条件向量输入给模型学习

1、这些状态指标值为多少对应卡死/正常/失效
2、出现异常情况的上下文信号输入情况及输出状态

输入——训练模型的数据格式

・条件向量的组成

```
condition_correct = {
    "target_state": "stuck",          # 期望触发的目标状态
    "timing_pattern": "rapid_oscillation", # 期望的时序模式
    "context_features": {             # 上下文特征（不含当前输入）
        "previous_states": ["normal", "normal", "error"],
        "stability_score": 0.2,
        "transition_frequency": "high"
    }
}
```



・ 训练数据的基本结构

```
training_sample = {
    # 条件部分 （告诉模型要学习什么模式）
    "condition": {
        "target_state": "stuck",
        "timing_pattern": "rapid_oscillation",
        "context_features": {...}
    },

    # 真实数据部分 （模型要学习生成这个）
    "real_data": {
        "input_signals": [4.5, 7.0, 4.8, 6.8, 5.0],  # 真实的电压序列
        "actual_state_sequence": ["normal", "stuck", "normal", "stuck", "normal"]
    }
}
```

- 生成器： 根据条件生成假的电压序列
- 判别器： 判断(真实电压, 条件) vs (生成电压, 条件)

输出——容易引发异常的信号组合

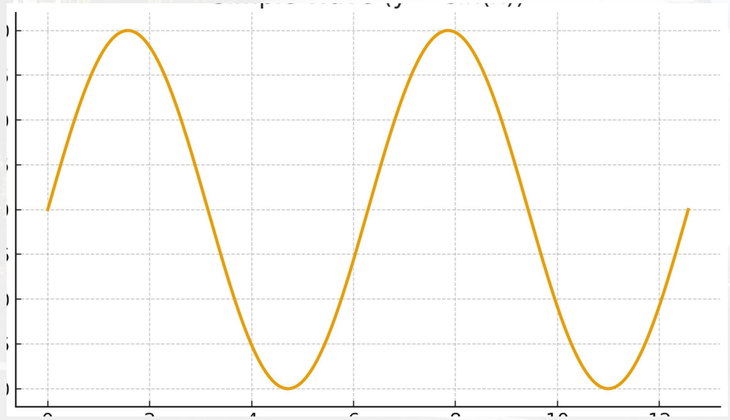
一些设想的智能信号组合：

边界振荡攻击"：
"在电压边界快速振荡，测试系统稳定性"

"渐进加压攻击"：
"逐步逼近临界值，测试系统容错"，

状态跳变攻击"：
"快速切换休眠唤醒，测试时序逻辑"

"累积效应攻击"：
"重复特定模式，测试内存/状态累积"



比如：
输出序列 = {
"signals": [4.5, 7.0, 4.8, 6.8, 5.0]，# 大幅振荡的电压序列
"pattern": "正常→卡死→正常→卡死→正常"，# 预期状态转移
"context": "快速信号跳变导致状态不稳定"　# 异常机制

GAN模型调研概述

01

WGAN（Wasserstein GAN）

特点：便于训练模型，训练稳定

适用：需要针对性生成特定状态测试数据

02

GANFuzz（工业协议测试）

特点：RNN+CNN结构，专注协议格式学习

适用：复杂格式数据生成

03

CGRLfuzz（GAN+强化学习）

特点：结合强化学习优化生成策略

适用：需要动态调整生成策略的场景

下一步方案

1、模型选择与训练

- 根据CC2电压的测试结果训练模型

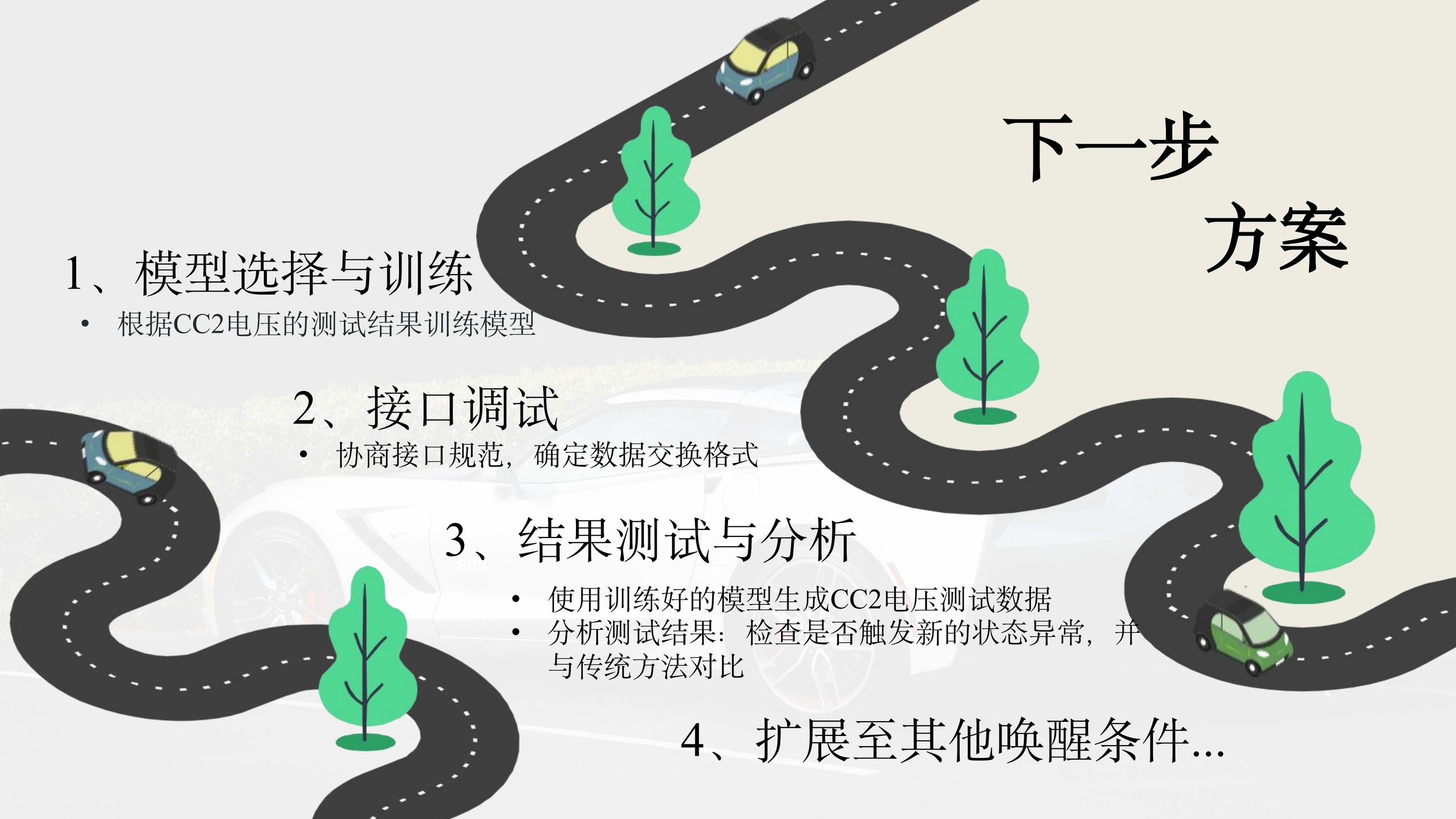
2、接口调试

- 协商接口规范，确定数据交换格式

3、结果测试与分析

- 使用训练好的模型生成CC2电压测试数据
- 分析测试结果：检查是否触发新的状态异常，并与传统方法对比

4、扩展至其他唤醒条件...



感谢您的聆听
恳请批评指正