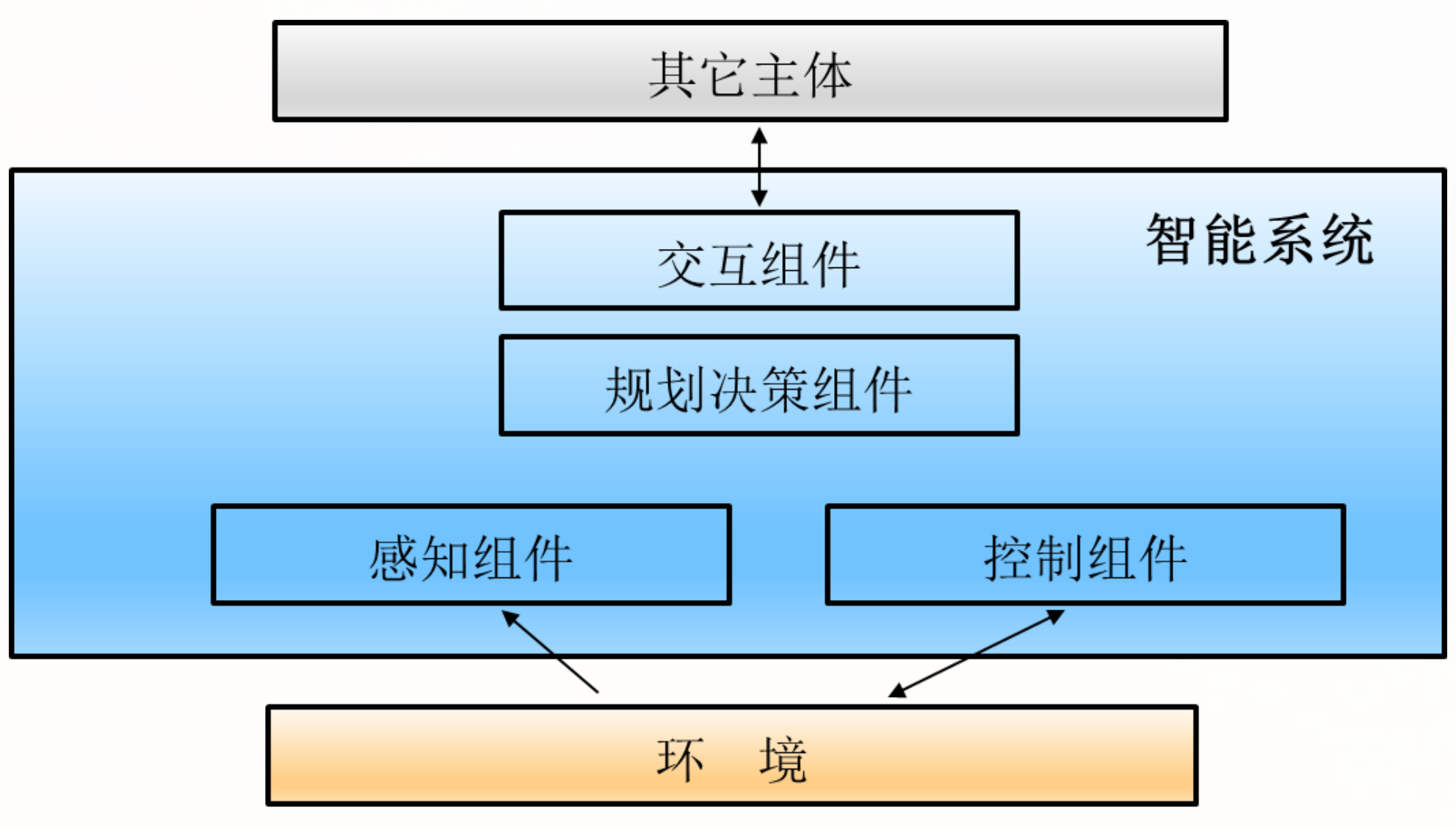
智能系统可靠性形式验证技术

张立军

联系方式：张立军，18610709769，zhanglj@ios.ac.cn

什么是智能系统？



智能系统是一种具有如下特征的计算机系统：

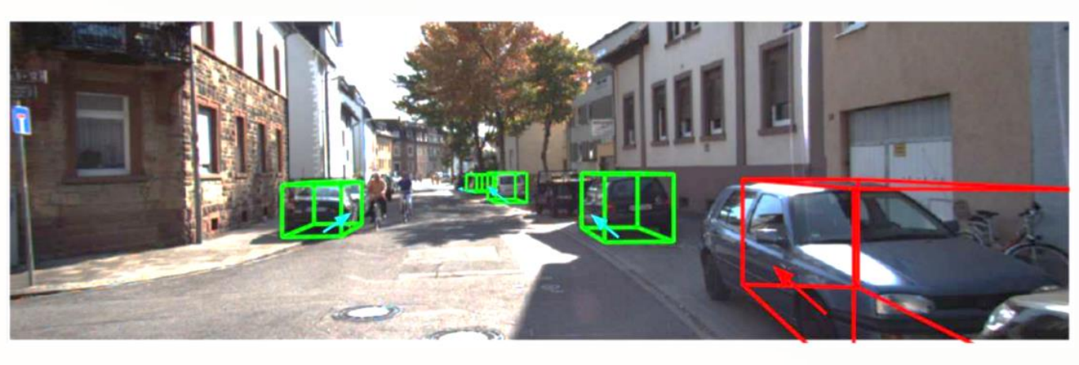
- 在复杂环境中自主运行；
- 拥有基本的认知能力：感知、行为控制、推理、语言使用；
- 展示复杂的智能行为：理性（利益最大化）、自适应、自省（强化学习，解释自身知识的运用的能力）

什么是智能系统的可靠性？

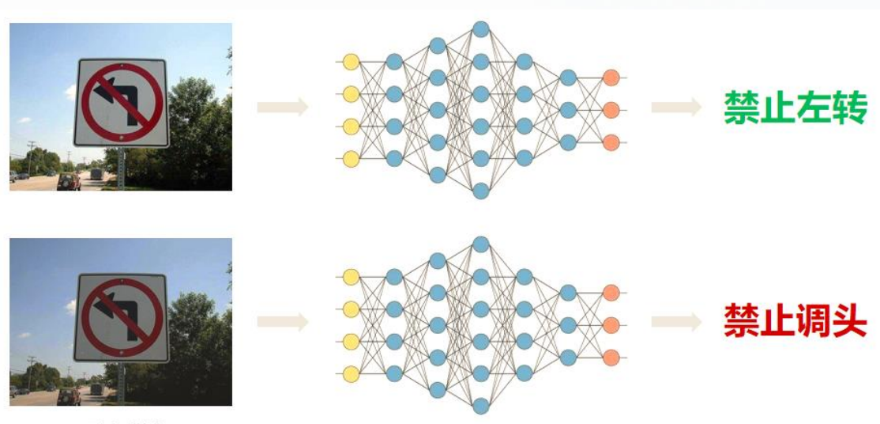
智能系统

可靠性？

可靠性：智能系统在给定的条件下完成规定的功能，不失效的能力



漏检车辆



误识标志

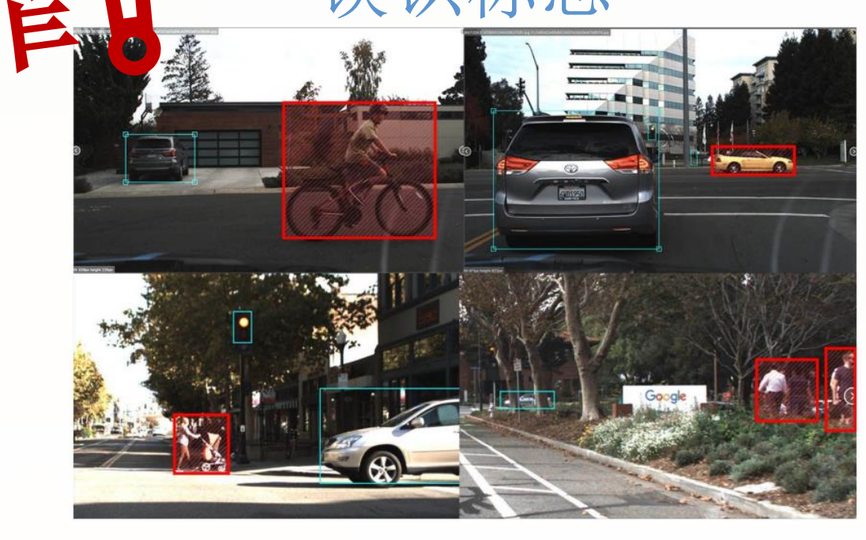
US investigates Autopilot after 11 Teslas crashed into emergency vehicles

Regulator worried Autopilot can't spot parked vehicles or keep driver engaged.

TIM DE CHANT - 8/16/2021, 11:47 PM

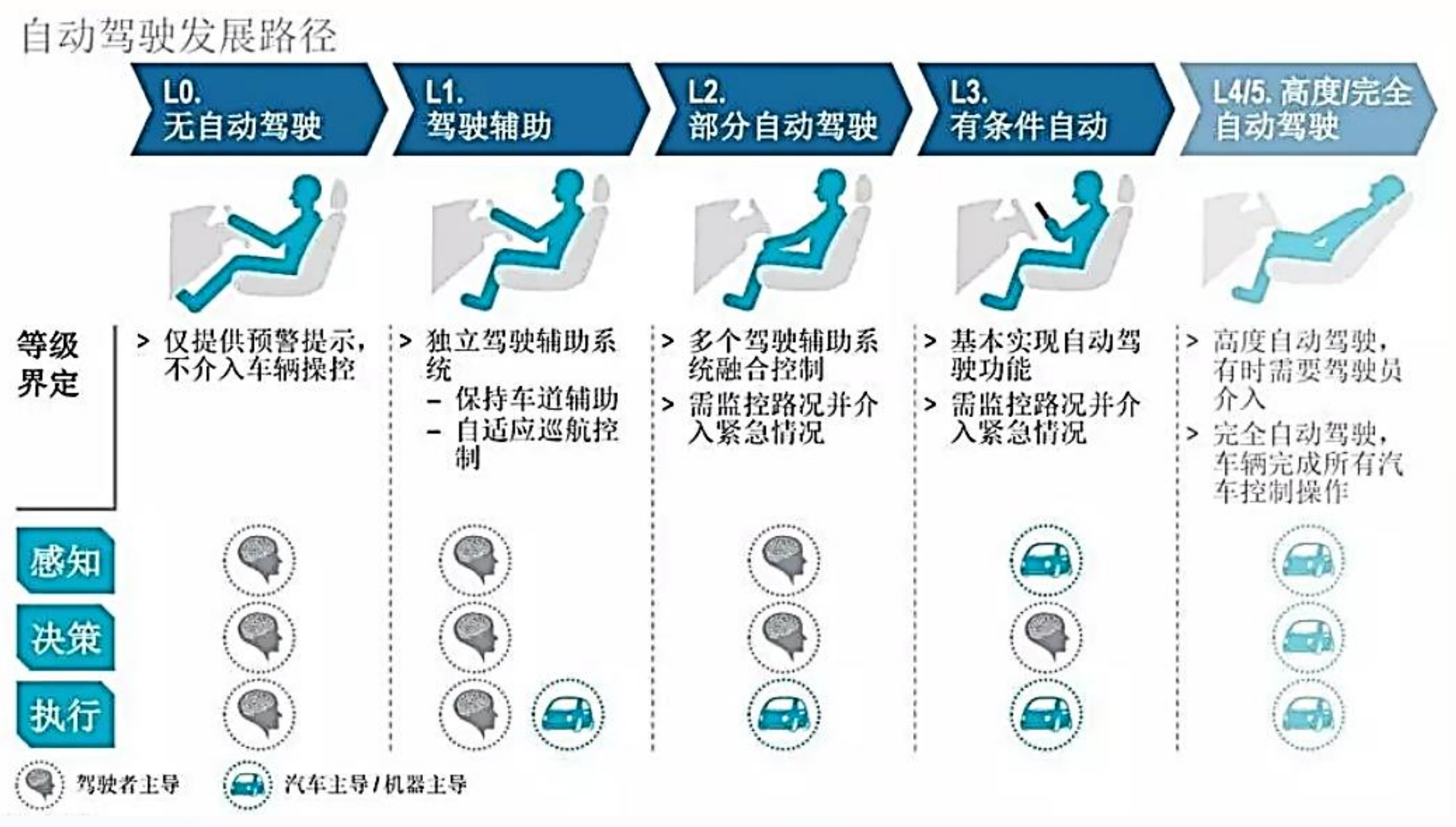
碰撞事故

不可靠！



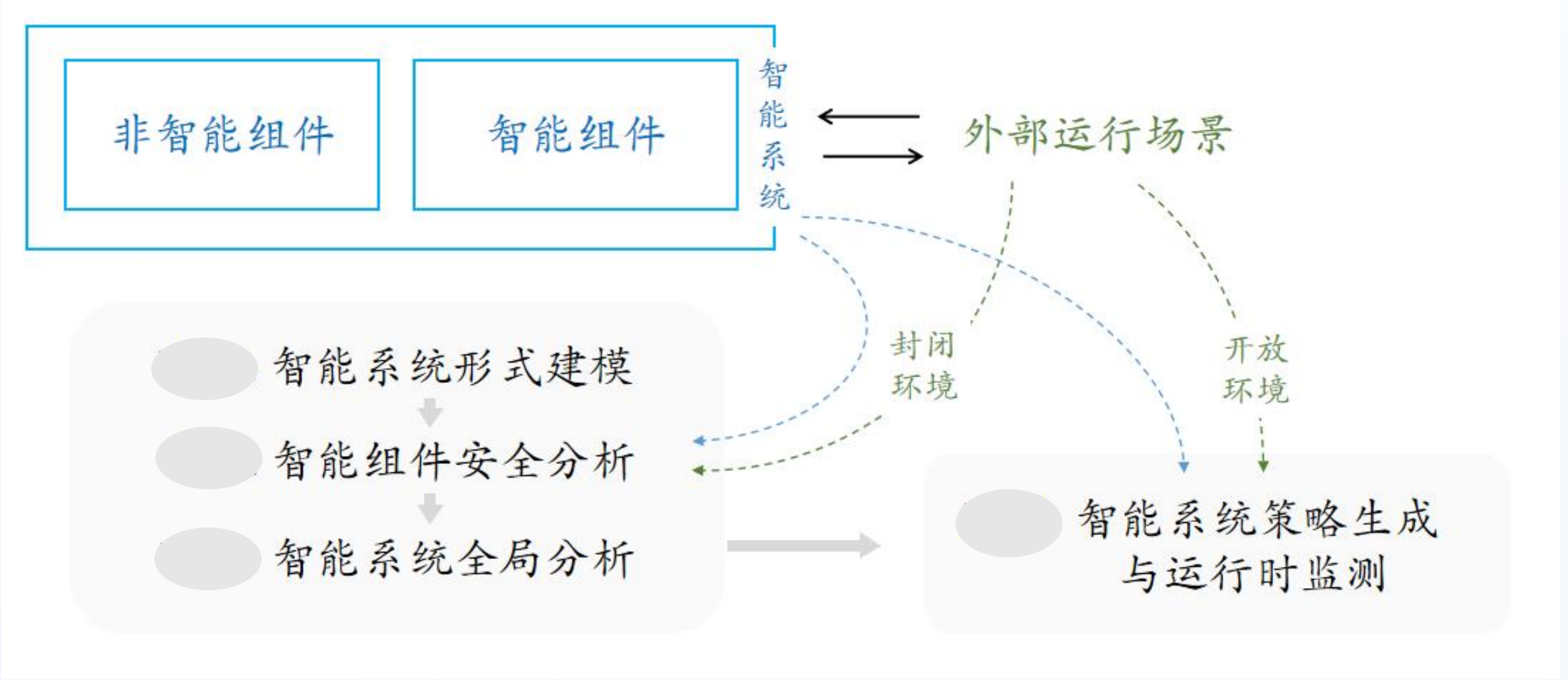
漏检行人

保证智能系统可靠性，为什么这么难？

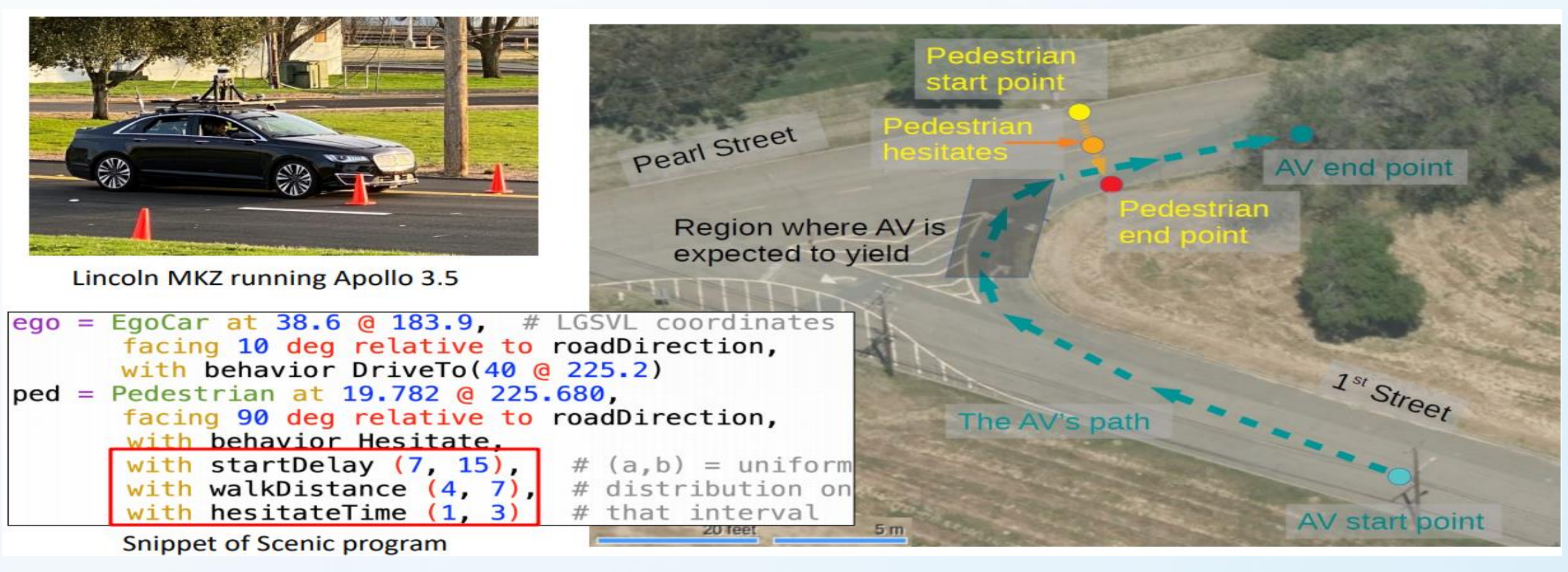


- 如果想让一辆Level 5级别的自动驾驶车辆上路，需要经过多少里程的测试？110亿英里！
- ≈100辆测试车的自动驾驶车队，7 × 24小时一刻不停歇地测试，完成110亿英里的测试里程也需要花费大约500年的时间！

如何验证智能系统可靠性？



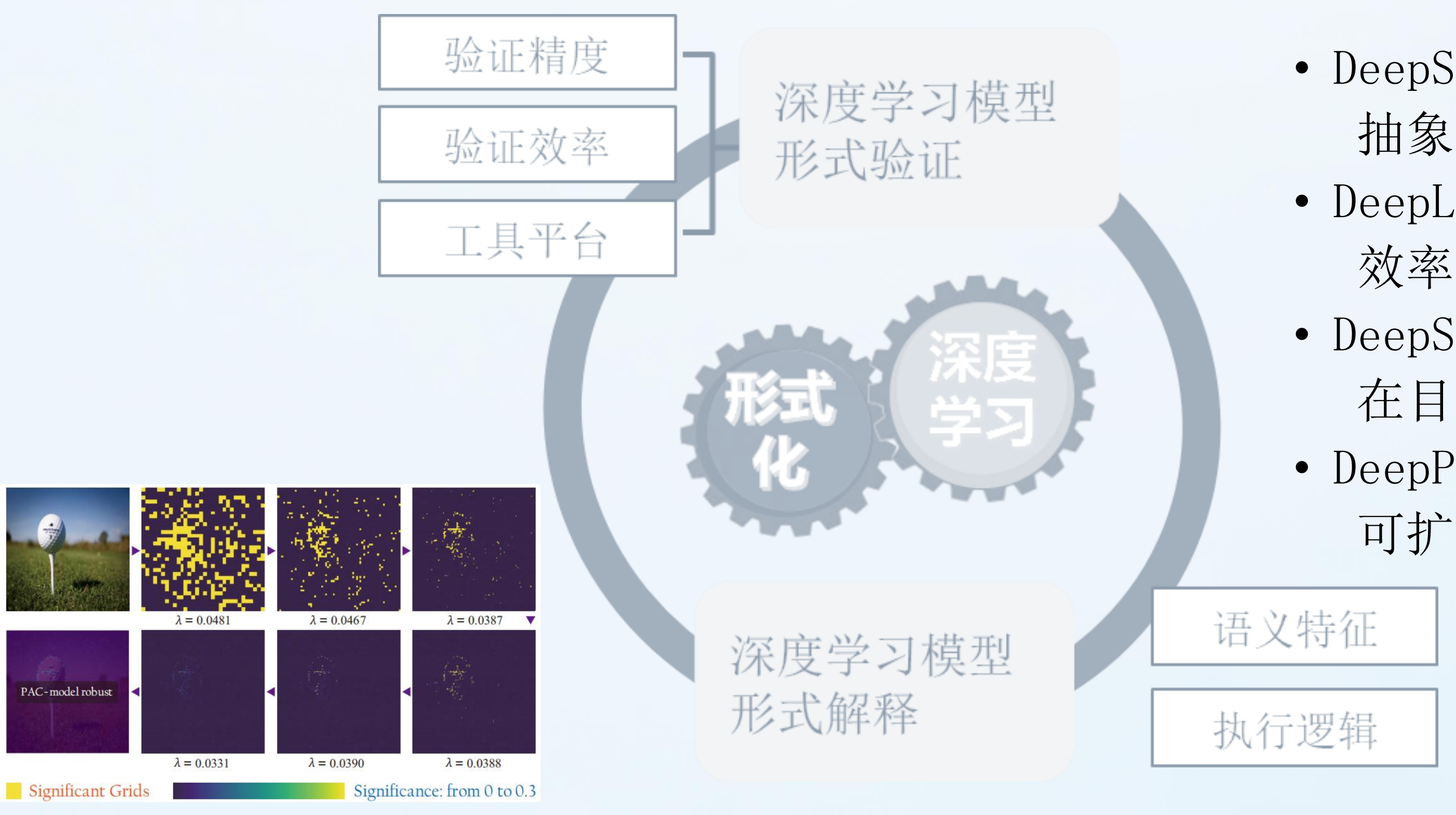
- **智能系统形式建模**



```
ego = EgoCar at 38.6 @ 183.9,   # LGSVL coordinates
      facing 10 deg relative to roadDirection,
      with behavior DriveTo(40 @ 225.2)
ped = Pedestrian at 19.782 @ 225.680,
      facing 90 deg relative to roadDirection,
      with behavior Hesitate,
      with startDelay (7, 15),    # (a,b) = uniform
      with walkDistance (4, 7),   # distribution on
      with hesitateTime (1, 3)    # that interval
```

Snippet of Scenic program

- **智能组件安全分析**



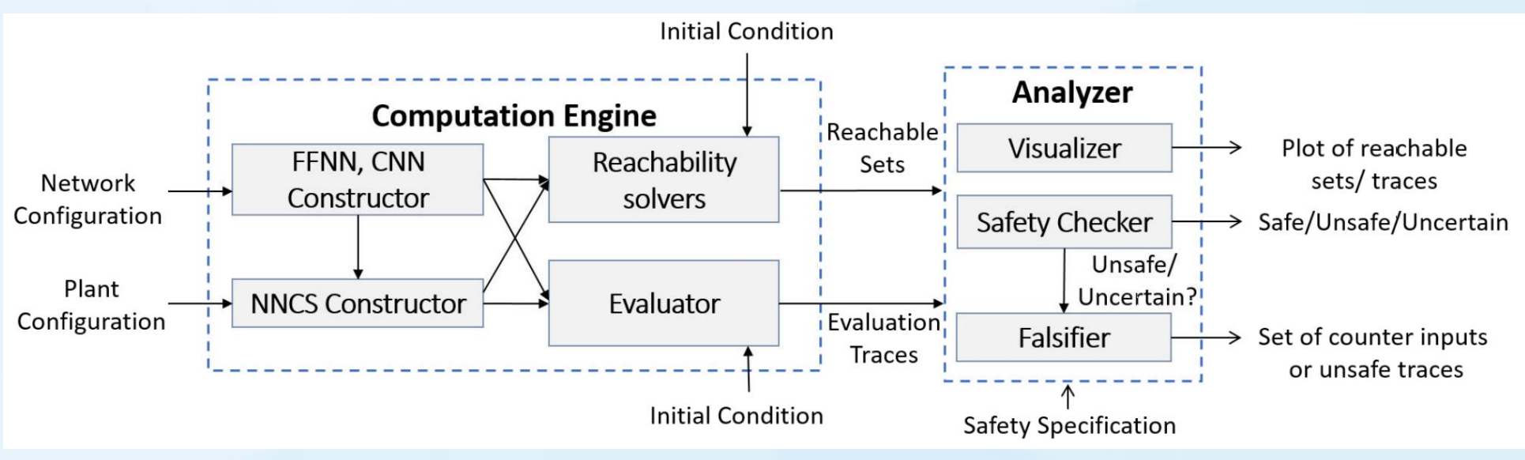
- DeepSymbol
  抽象解释方法中具有较高的可扩展性，适用于任何抽象域
- DeepLip
  效率极高，可以在分钟级别内验证百万个鲁棒性质
- DeepSRGR
  在目前所有的可靠但不完备的方法中，精度水平最高
- DeepPAC
  可扩展性远远好于严格可靠的方法，在概率方法中有着最好的验证精度

- **智能系统全局分析**

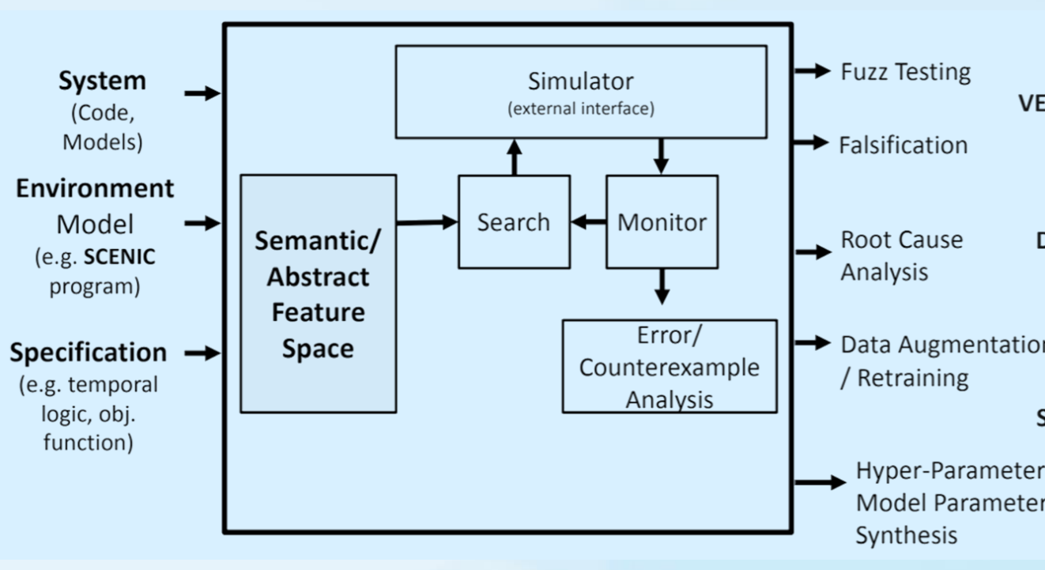
智能系统安全性质形式验证技术

智能系统测试技术

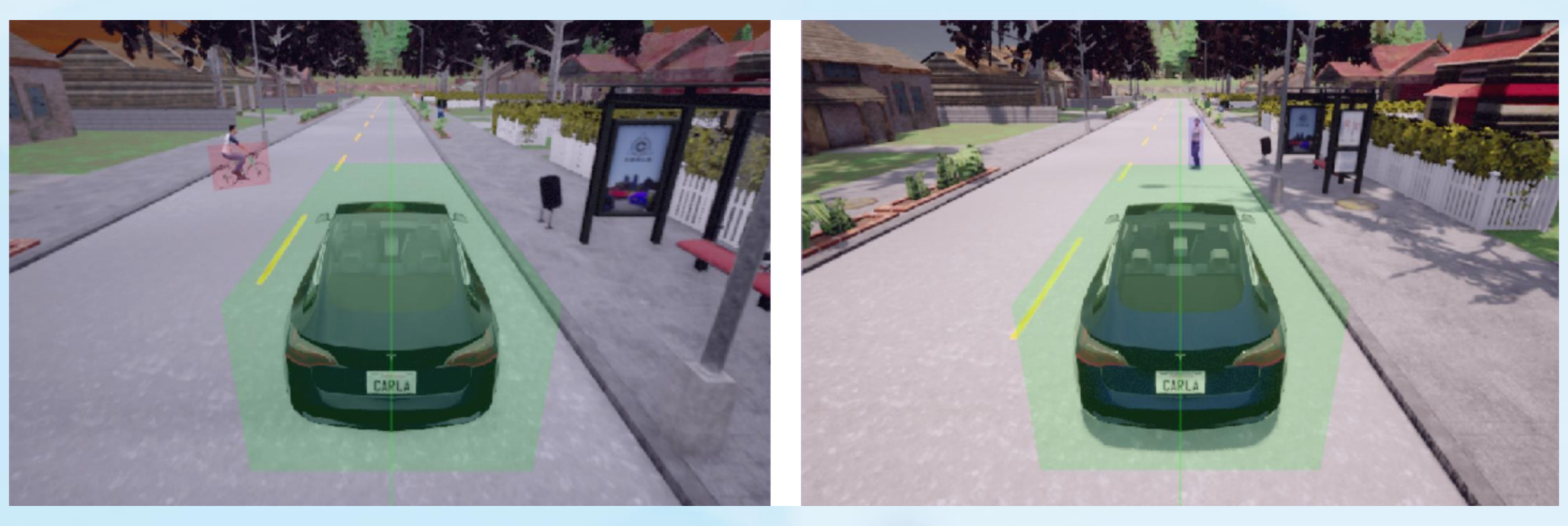
智能系统验证和模拟融合技术



NNV



VerifAI



Percemon运行时监测