

# RVFuzzer

---

## RVFuzzer两个关键组件

---

- the control-guided instability detector that monitors the vehicle's control state to detect controller malfunction
- the control-guided input mutator that generates control program inputs for efficient program testing

## Control-guided input mutator

---

软件测试系统需要明智地生成程序输入，以实现较高的错误覆盖率，同时减少主程序的测试运行次数——有足够的代表性。

### Control Parameter Mutation Space

- the list of dynamically adjustable control parameters
  - 从控制程序的规范和GCS命令中获得
- the range of all possible values for each parameter
  - 数据类型
  - 轮询控制程序（传入最大值/最小值来确定实际maximum/minimum，程序实现决定）
- the default value of each parameter

### Feedback-Driven Parameter Input Mutator

- the control parameter mutation space
- the result of the Control Instability Detector from the previous run of the control program

检测所有可能的输入值不可行——对参数进行一维突变和多维突变。

假定：参数的变化将引起稳定性的单调变化。因此，参数的不合法区域为一个范围。

一维突变：二分查找。

多维突变：设定一个target参数，其余参数只取三个值：最大、最小和默认值。递归所有其他参数可能的组合，二分target参数可能的范围。