

Pre-processing phase



**Supervisory
Software**



PLC Device

**Functionality
analysis**

**Proprietary
protocol
analysis**

State Book

**Protocol
Knowledge**

Fuzzing phase

Crashes

Crash Monitor

Data Feeding

Input Generation

**State
Selection**