

# Leveraging Simulation and Automation for STPA

Pat Canny  
MathWorks

## Quick Disclaimer

- MathWorks and our customers are early in our “STPA journey”
- This brief talk will cover *some* of what we’ve been working on
- We are a software tool vendor, **not** expert STPA practitioners
- We are looking to engage! Reach out: [patcanny@mathworks.com](mailto:patcanny@mathworks.com)



## Key Takeaways

1. **Simulation** and **visualization** provide insights when identifying Loss Scenarios
2. Leverage traceability data to **automate analysis** and measure **impact of changes** on analysis



## Example: A New “Level Cruise Mode”

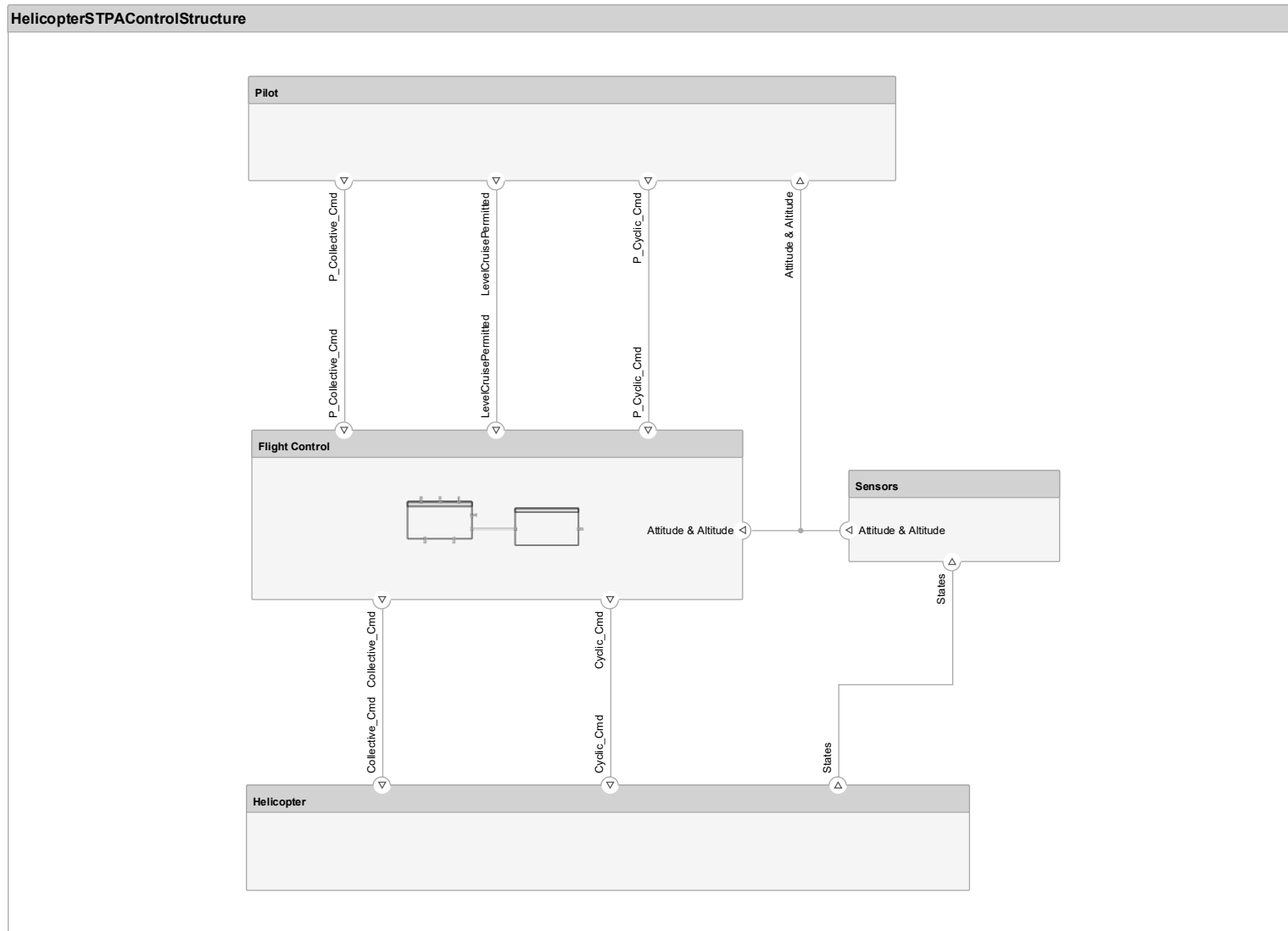
Newly proposed “Level Cruise Mode” which limits cyclic rate for “smoother” ride and improved part life

**[DISCLAIMER: entirely fictional!]**

Level Cruise Mode is entered when

1. “Level Flight” achieved (based on existing algorithm) for a short duration
2. Pilot then “Permits” mode, followed by brief delay

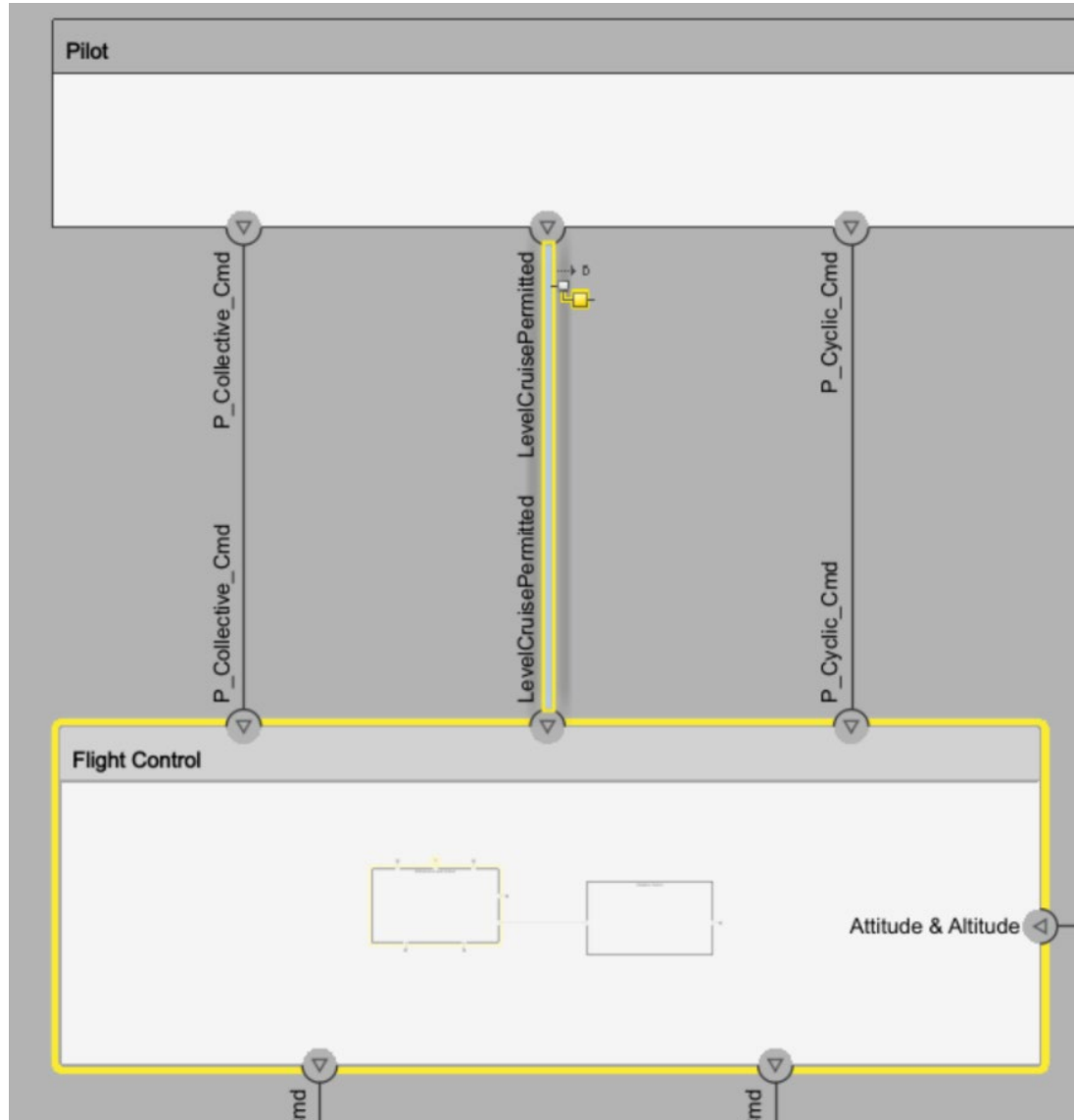




(Preliminary) Control Structure modeled in System Composer™

**Note: this is not for simulation!**

# “Permit Level Cruise Mode” Control Action



# Identify UCAs and establish traceability between artifacts

Safety Analysis Manager

HOME

New  
 Open  
 Save  
 Import  
 FILE

Paste  
 Cut  
 Copy  
 Delete  
 EDIT

Add Row  
 Add Column  
 Add Reference  
 Refresh Values  
 View Columns  
 SPREADSHEET

Add Link  
 Refresh Links  
 LINKS

Find  
 SEARCH

Analyze Spreadsheet  
 Edit Callbacks  
 Clear Flags  
 ANALYZE

Detect  
 Accept All  
 ANALYZE CHANGES

Export  
 SHARE

System-level Hazards ×

| ID    | Description  |
|-------|--|
| 1<br> | H-1<br>Unsafe attitude (excessive turbulence or pitch/roll/yaw.) |

Pilot UCAs ×

| Pilot Action (Role) | Not providing causes hazard   | Providing causes hazard  | Too early, too late, out of order | Stopped too soon, applied too long |
|---------------------|-------------------------------|--|-----------------------------------|------------------------------------|
| 1<br>               | Permit Level Cruise Mode.<br> | Providing causes hazard<br>Pilot provides Permit Level Cruise Mode when the aircraft is not in level flight.<br> |                                   |                                    |

**Note:** for simplicity, only one UCA shown

# Modeling a hazard for simulation

## ASSESSMENT

### ▼ At any point of time ...

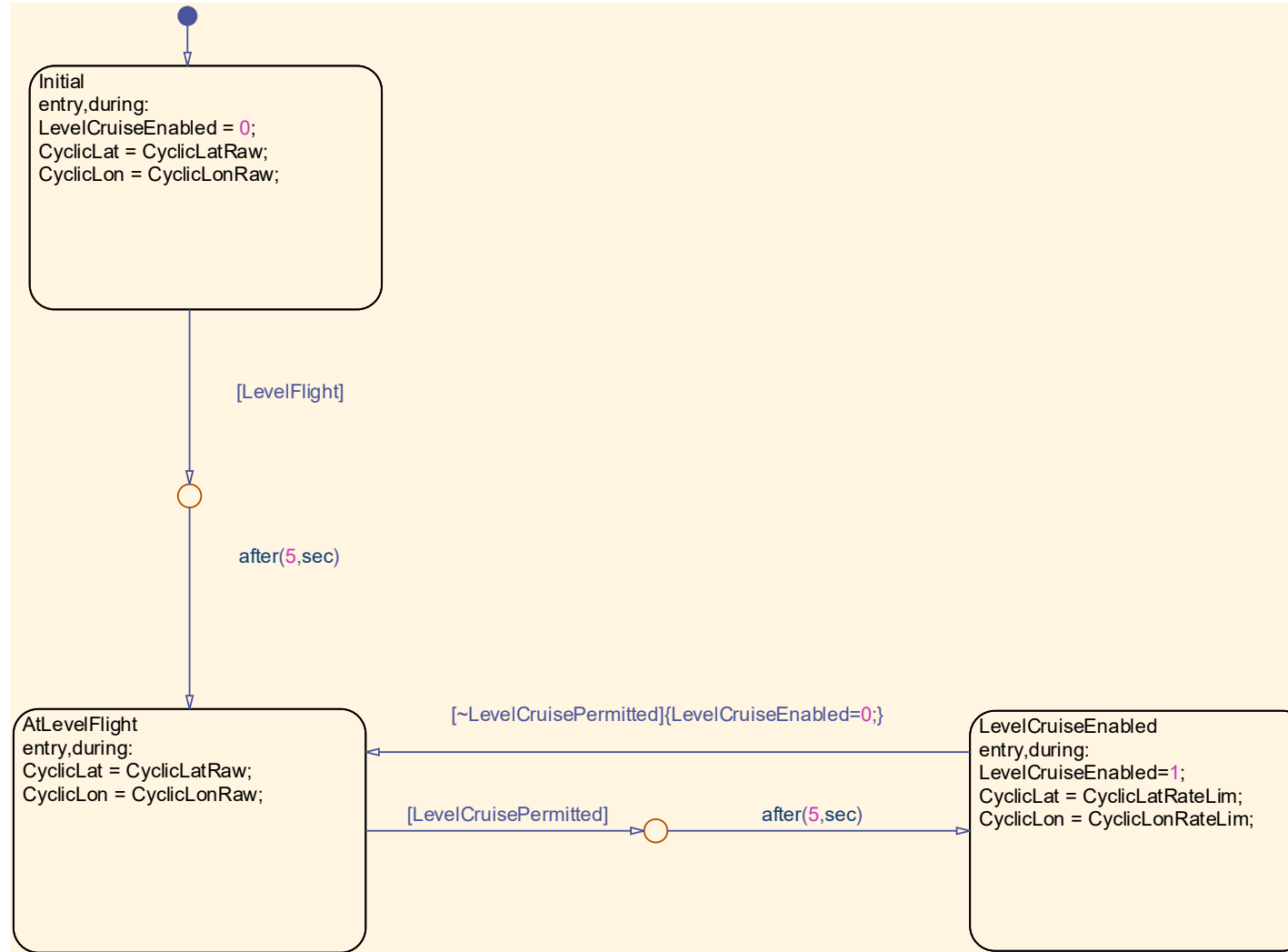
▶ trigger: whenever `LevelCruiseEnabled > 0` is true then ...

delay: with no delay ...

▶ response: `roll_pitch_rate < 4.2` must stay true for at least 5 seconds

“Undesirable Handling Qualities”

# Proposed Design



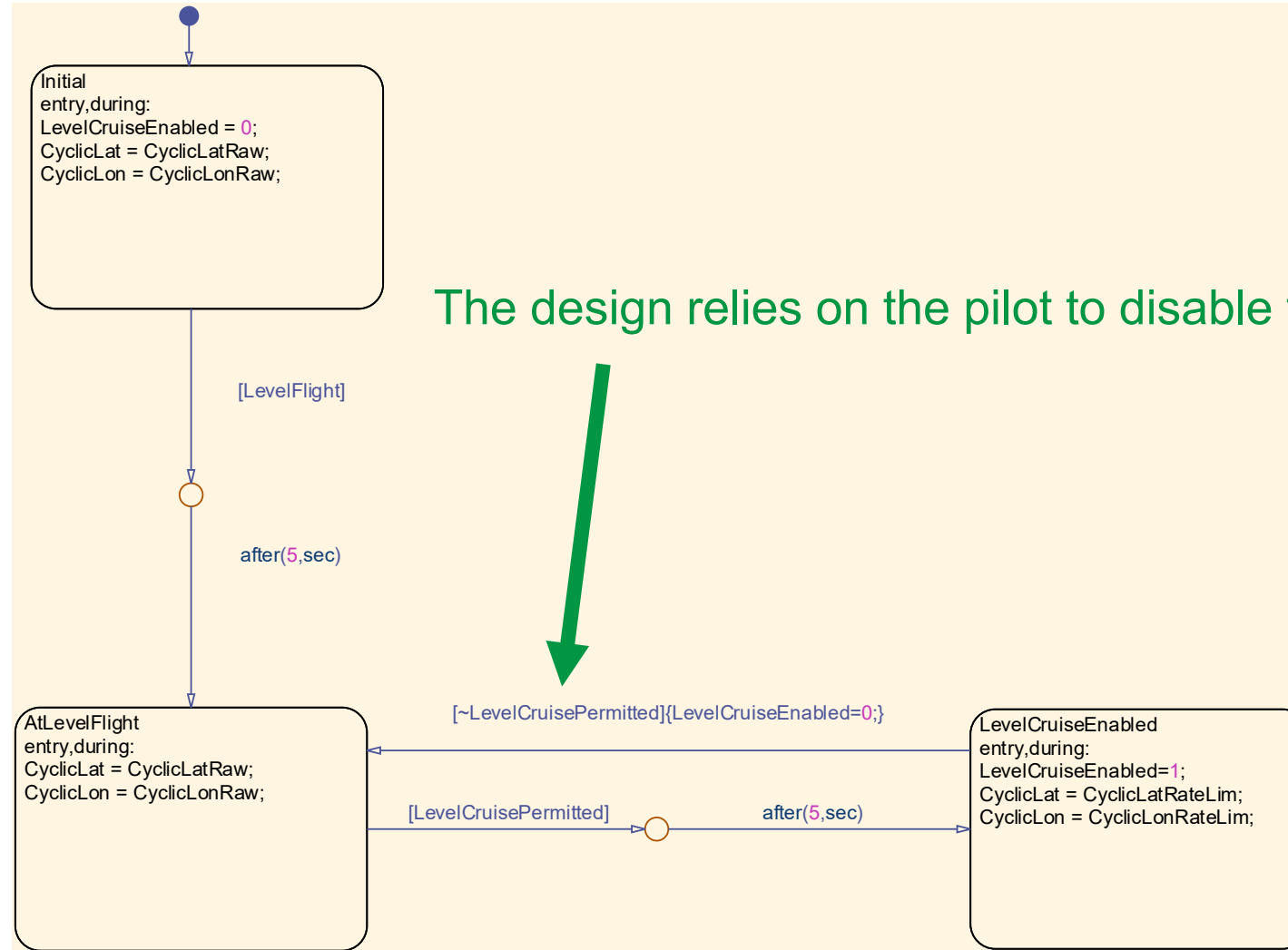
“Level Cruise Mode” Algorithm

Why would a pilot permit Level Cruise Mode when the aircraft is not in level flight?!

# Use Visualization Tools to Help Identify Loss Scenarios

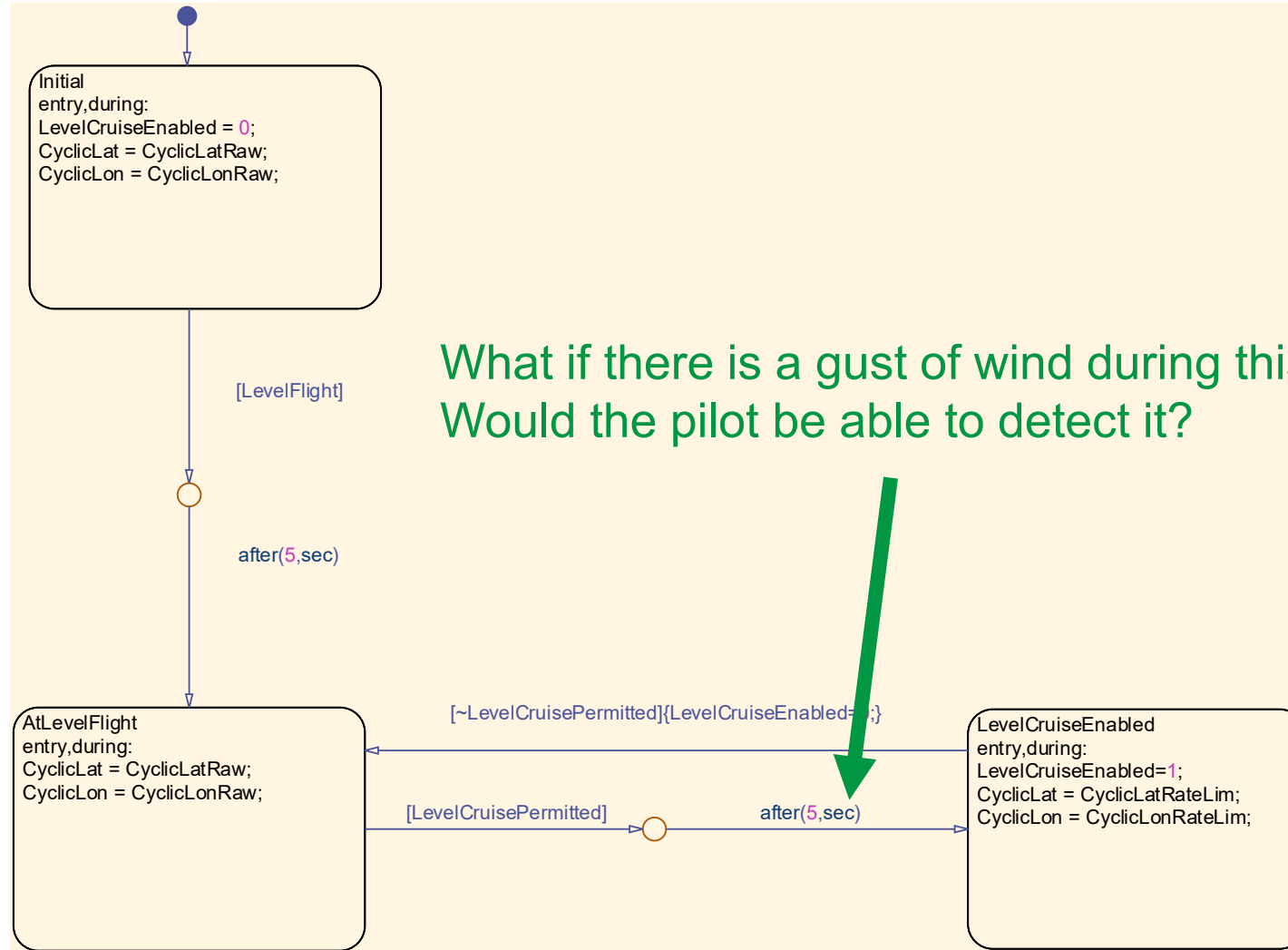


# What is the pilot's role?



“Level Cruise Mode” Algorithm

# Bad timing



“Level Cruise Mode” Algorithm

# WARNING!

You are about to see the term “test case.”

**Do not be alarmed.**

# Simulation-Based Loss Scenario Identification Using a “Test Case”

Sudden Gust - Proposed Design

- SYSTEM UNDER TEST\*
  - Model: HelicopterSTPA
    - TEST HARNESS
    - SIMULATION SETTINGS AND RELEASE OVERRIDES
  - PARAMETER OVERRIDES
  - CALLBACKS
  - INPUTS
  - SIMULATION OUTPUTS
  - CONFIGURATION SETTINGS OVERRIDES
- FAULT SETTINGS\*
 

| FAULT SET / MODEL ELEMENT  | FAULT NAME |
|--|------------|
| <input checked="" type="checkbox"/> Fault Set 1                          |            |
| <input checked="" type="checkbox"/> HelicopterSTPA/Sensor/Bias/Outport/1 | suddenGust |
- SEQUENCE DIAGRAM ASSESSMENT
- ITERATIONS
- LOGICAL AND TEMPORAL ASSESSMENTS\*
  - ASSESSMENT CALLBACK
    - Extend Result




| EN...                               | NAME        | ASSESSMENT   | REQUIREMENTS |
|-------------------------------------|-------------|--|--------------|
| <input checked="" type="checkbox"/> | Assessment1 | At any point of time, whenever LevelCruiseEnabled > 0 is true then, with no delay, roll_pitch_rate < 4.2 must stay true for at least 5 seconds | None         |


Gust of wind


The beginnings of a Loss Scenario?

Hazard

# Link “test case” to analysis artifacts for traceability and automation

| Pilot UCAs ×  |   |                               |   |   |
|---|---|-------------------------------|---|---|
|   | ⋮ Pilot Action (Role)   | ⋮ Not providing causes hazard | ⋮ Providing causes hazard   | ⋮ |
| 1   | Permit Level Cruise Mode.   |                               | Pilot provides Permit Level Cruise Mode when the aircraft is not in level flight.   |   |
|  |  |                               |  |   |

 → Related to:

 [Sudden Gust - Proposed Design](#)

# Link “test case” to analysis artifacts for traceability and automation

**Callbacks Editor**

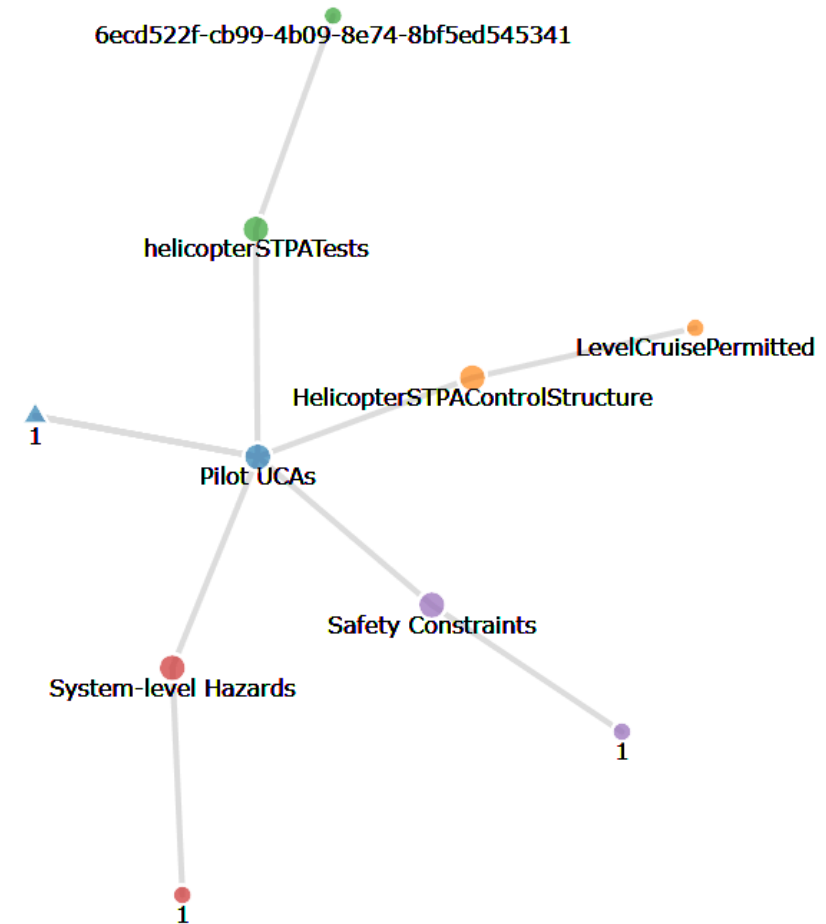
- PreLoadFcn
- PostLoadFcn
- ▼ AnalyzeFcn\*
- Default**
- validateWithTests
- PreSaveFcn\*
- PostSaveFcn
- CloseFcn

► **Help on callback predefined variables:**

```
1 |for i = 1: sfa_spreadsheet.Rows
2 |    runLinkedTests(getRow(sfa_spreadsheet,i));
3 |end
```

# Explore Traceability and Assess Impact of Changes

- STPA is iterative by nature
- Modeling allows you to “lock down” behavior for future use
- Verify previously identified Loss Scenarios are accounted for as design evolves



Traceability Graph

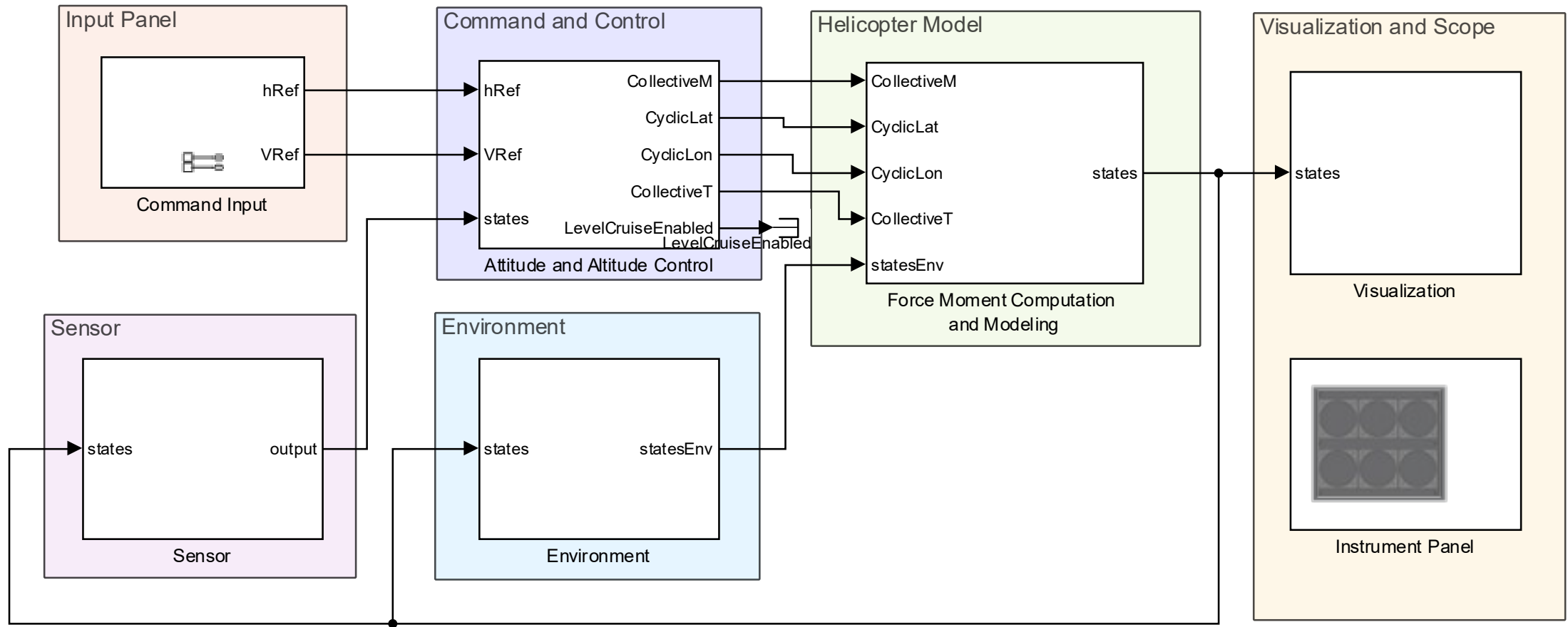
## Key Takeaways

1. **Simulation** and **visualization** provide insights when identifying Loss Scenarios
2. Leverage traceability data to **automate analysis** and measure **impact of changes** on analysis



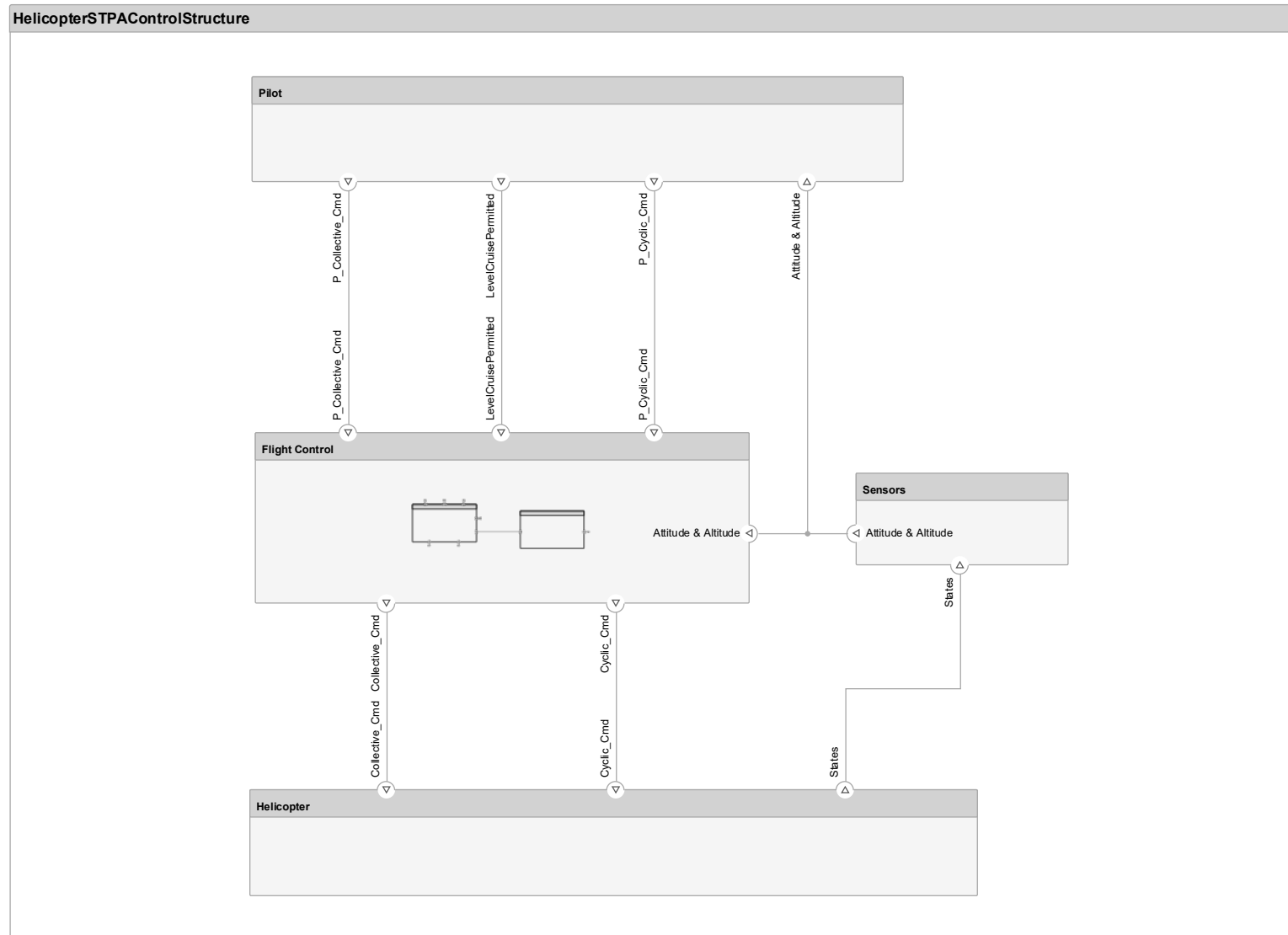
Next step: “extracting” data from legacy models?

# Many teams often have “legacy” behavior models



Copyright 2024-2025 The MathWorks, Inc.

# How (and should) they extract data for use in STPA?



Reach out! We are looking for your insights!

**Pat Canny**

[patcanny@mathworks.com](mailto:patcanny@mathworks.com)

