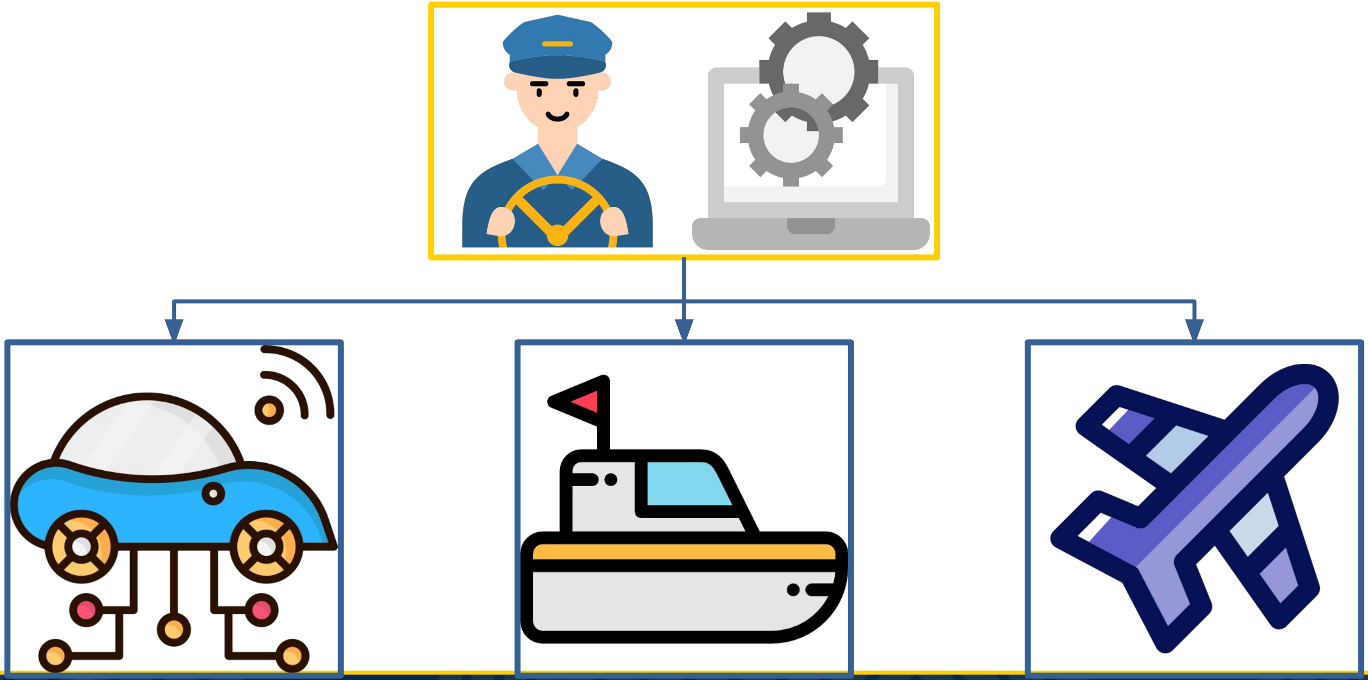
Analysis and Prevention of MCAS-Induced Crashes

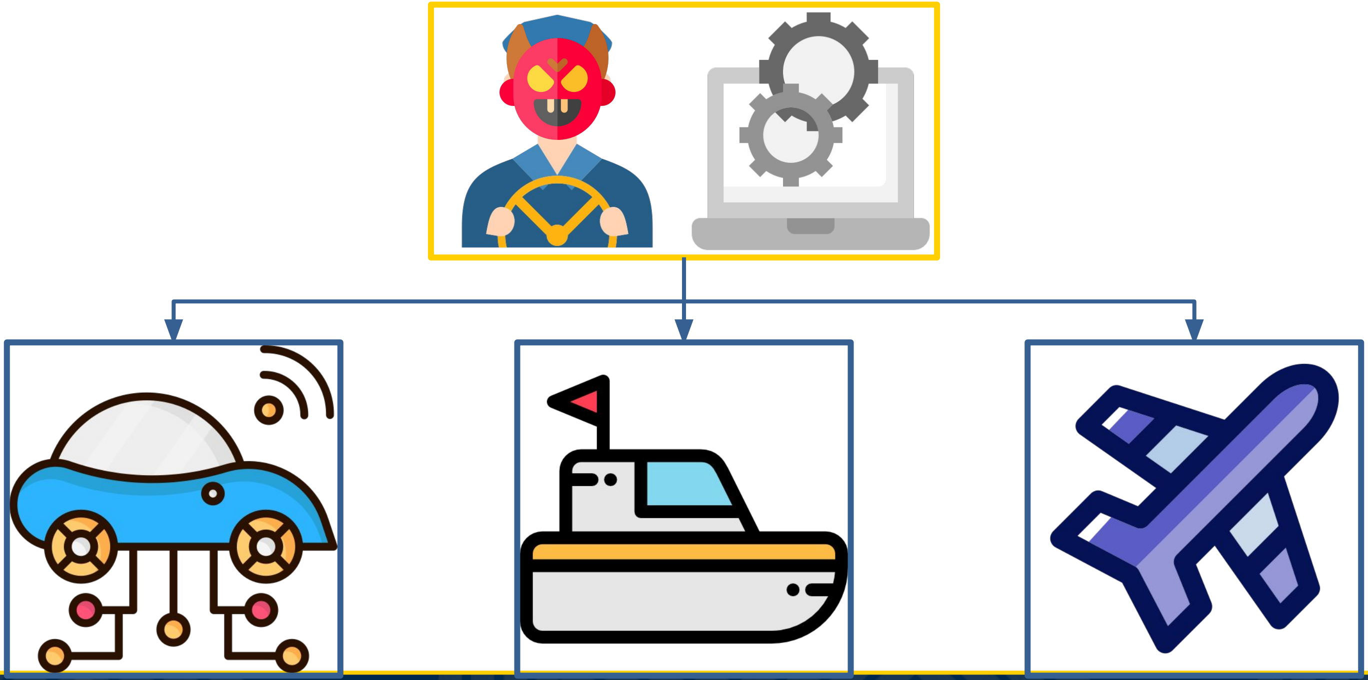
Noah T. Curran, Thomas W. Kennings, Kang G. Shin
Computer Science and Engineering, University of Michigan

2024 ACM SIGBED International Conference on Embedded Software (EMSOFT ‘24)
Raleigh, NC, USA
9/30/24

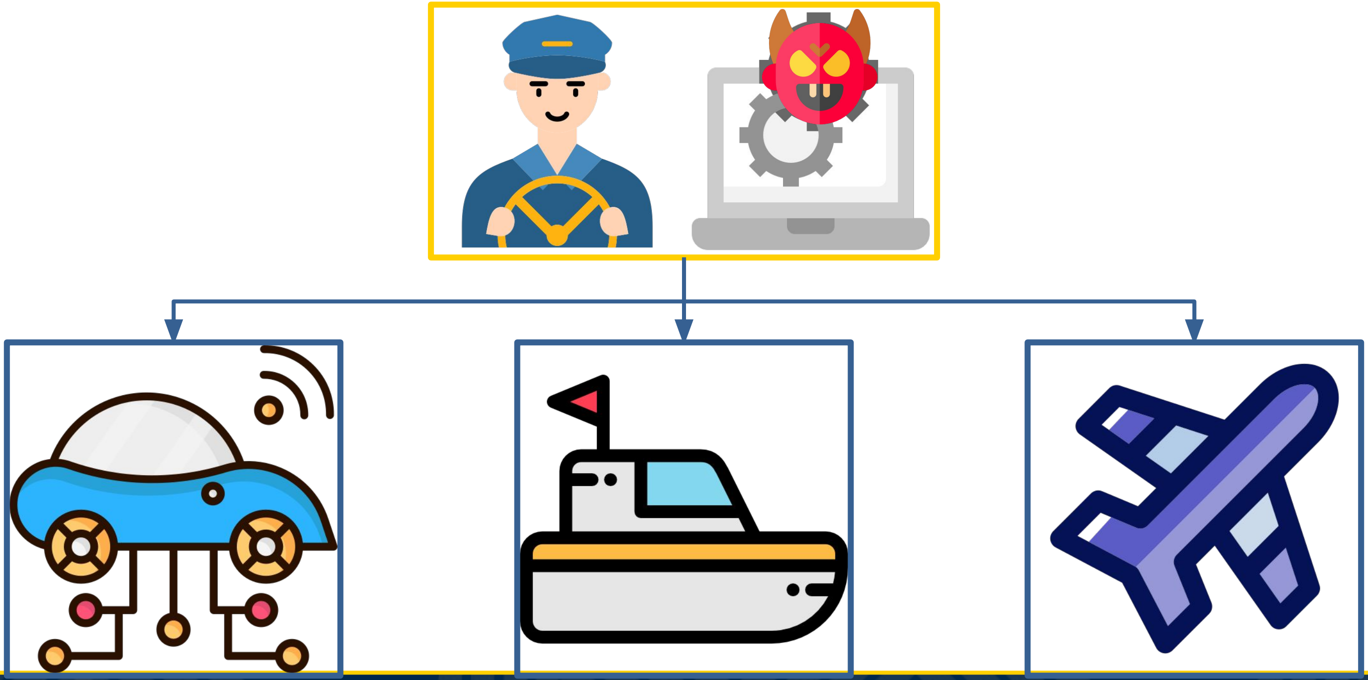
Semi-Autonomous Vehicles (SAVs)



Semi-Autonomous Vehicles (SAVs)

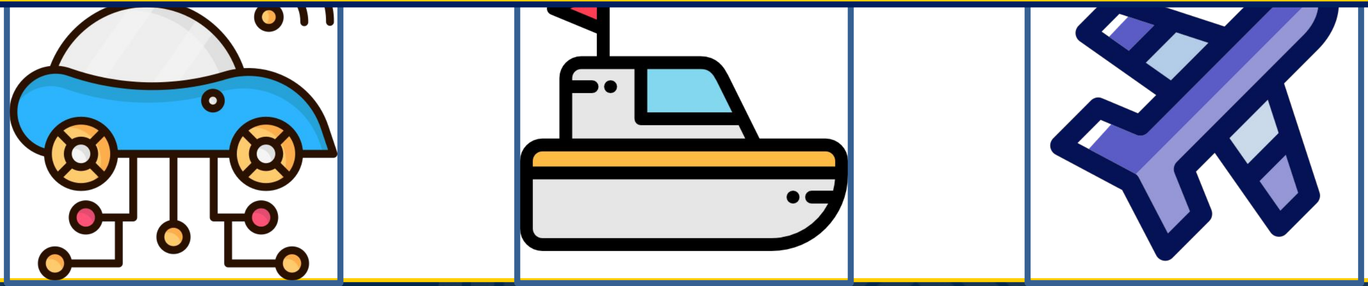


Semi-Autonomous Vehicles (SAVs)



Semi-Autonomous Vehicles (SAVs)

Semi-autonomous systems should not default control to the manual operator or the autonomous controller!



Semi-Autonomous Vehicles (SAVs)

Timeline of Boeing 737-MAX Crashes

2016

Changes During Flight Testing

- Pre-2016: Boeing decides to include MCAS to offset upward pitch due to heavier engines
- March/April 2016: Flight-test pilots discover issue with flight control during low-speed flight conditions
- Sometime after: Boeing gives ~4x greater authority to MCAS… FAA agreed not to notify pilots of the change to MCAS

2017

Aircraft Certification

- March 2017: FAA, EASA certified MAX for flight
- May 2017: First delivery completed

2018

First Crash

- October 2018: Lion Air Flight 610 crashed into the Java Sea

2019

Second Crash and Grounded Aircraft

- March 10, 2019: Ethiopian Airlines Flight 302 crashed into a farm field near Bishoftu, Ethiopia
- March 11-13, 2019: All major countries ground all MAX flights

2020

Return to Service

- January 2020: Issue found with the MCAS system, subsequently fixed
- November 2020: FAA cleared the MAX to return to service
- December 2020: Following repairs, airlines resume passenger service of the MAX

2021

Boeing Settlement and Aftermath

- Early-January 2021: USDOJ charged Boeing with fraud, settled for $2.5B
- Late-January 2021: EASA and Transport Canada cleared MAX with additional requirements
- December 2021: China becomes one of last major countries clear the MAX

Timeline of Boei

Changes During Flight Testing

- Pre-2016: Boeing decides to include MCAS to of upward pitch due to heavier engines
- March/April 2016: Flight-test pilots discover issu with flight control during low-speed flight condit
- Sometime after: Boeing gives ~4x greater autho MCAS… FAA agreed not to notify pilots of the ch to MCAS

Changes During Flight Test

- **Pre-2016**: include MCAS
- **March/April 2016**: Flight-test pilots discover issue with flight control
- **Sometime after**: Boeing gives ~4x greater authority to MCAS… FAA agrees not to notify pilots of the change to MCAS

ervice

- 20: Issue found with the MCAS bsequently fixed
- 2020: FAA cleared the MAX to ervice
- 2020: Following repairs, airlines ssenger service of the MAX

2016

2017

2021

Aircraft Certifi

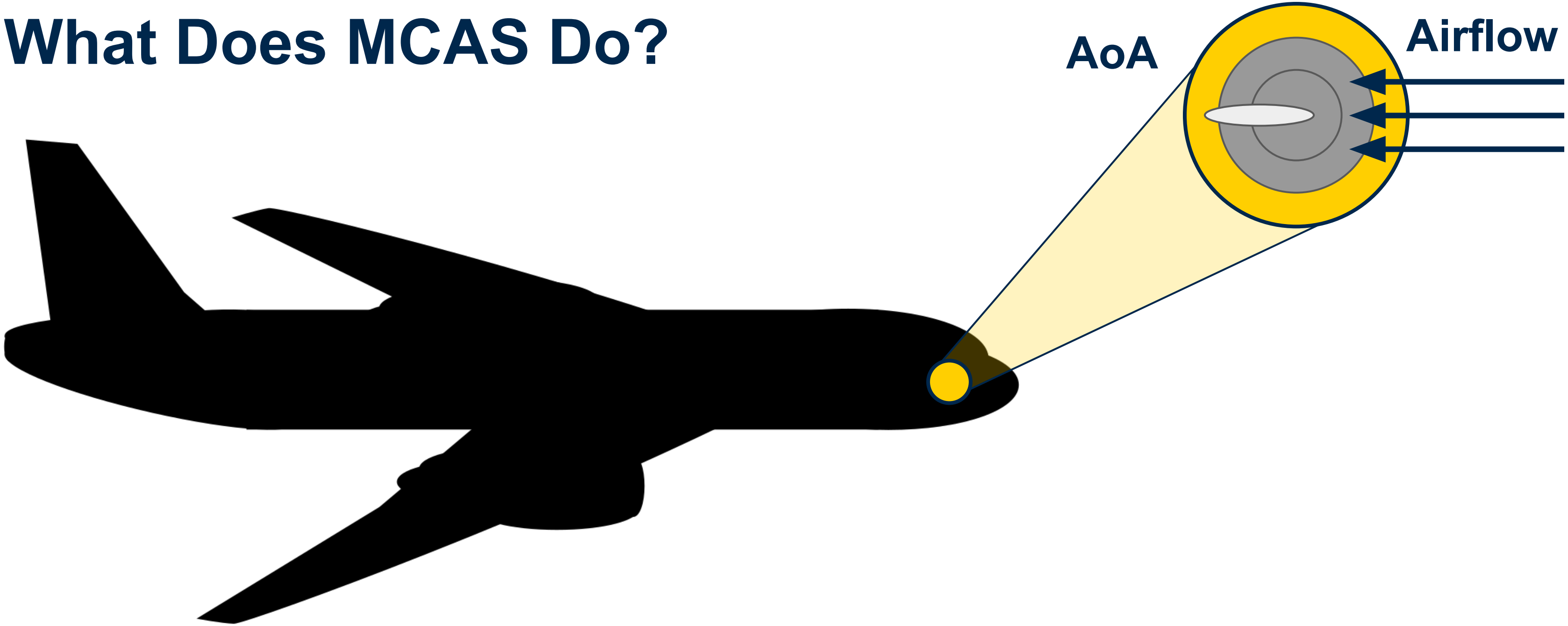
- March 2017: FAA, EASA certified MAX for flight
- May 2017: First delivery completed

- March 10, 2019: Ethiopian Airlines Flight 302 crashed into a farm field near Bishoftu, Ethiopia
- March 11-13, 2019: All major countries ground all MAX flights

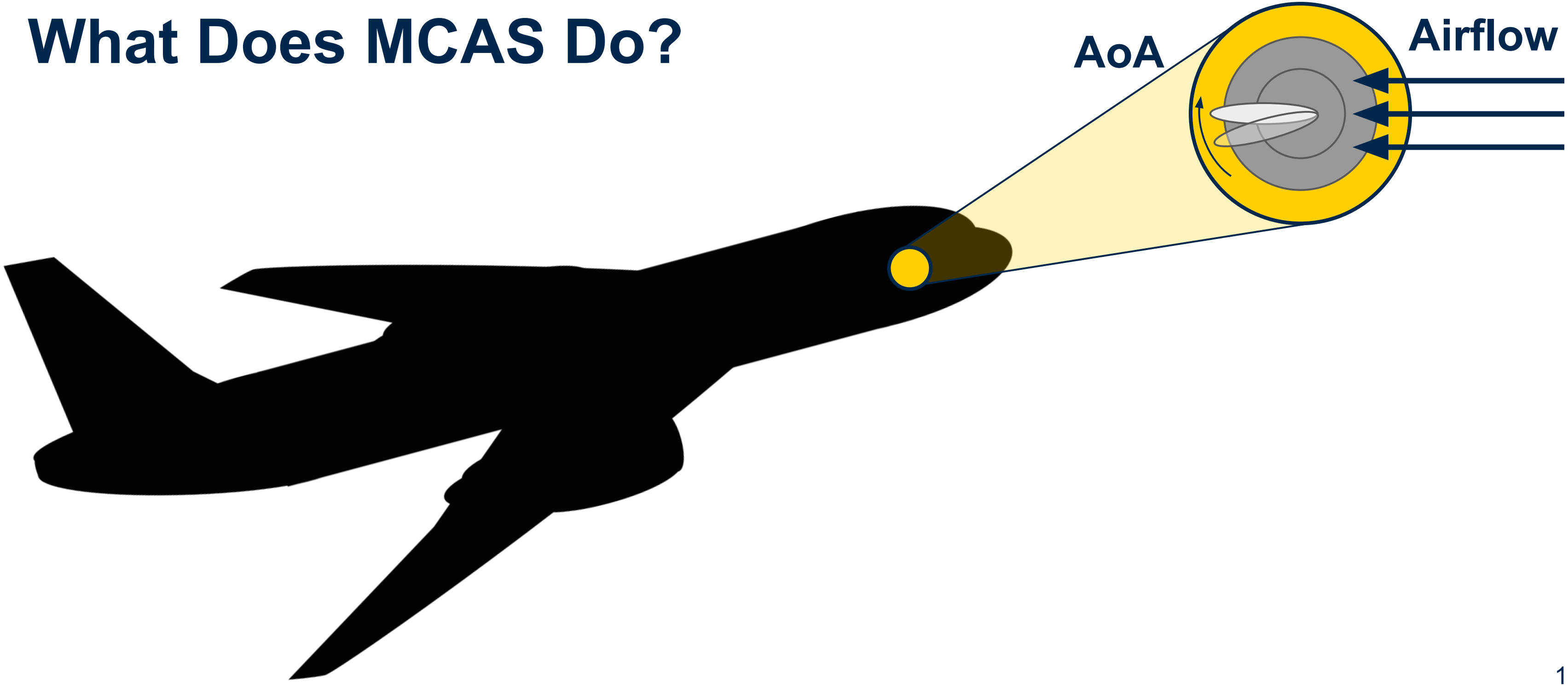
Boeing Settlement and Aftermath

- Early-January 2021: USDOJ charged Boeing with fraud, settled for $2.5B
- Late-January 2021: EASA and Transport Canada cleared MAX with additional requirements
- December 2021: China becomes one of last major countries clear the MAX

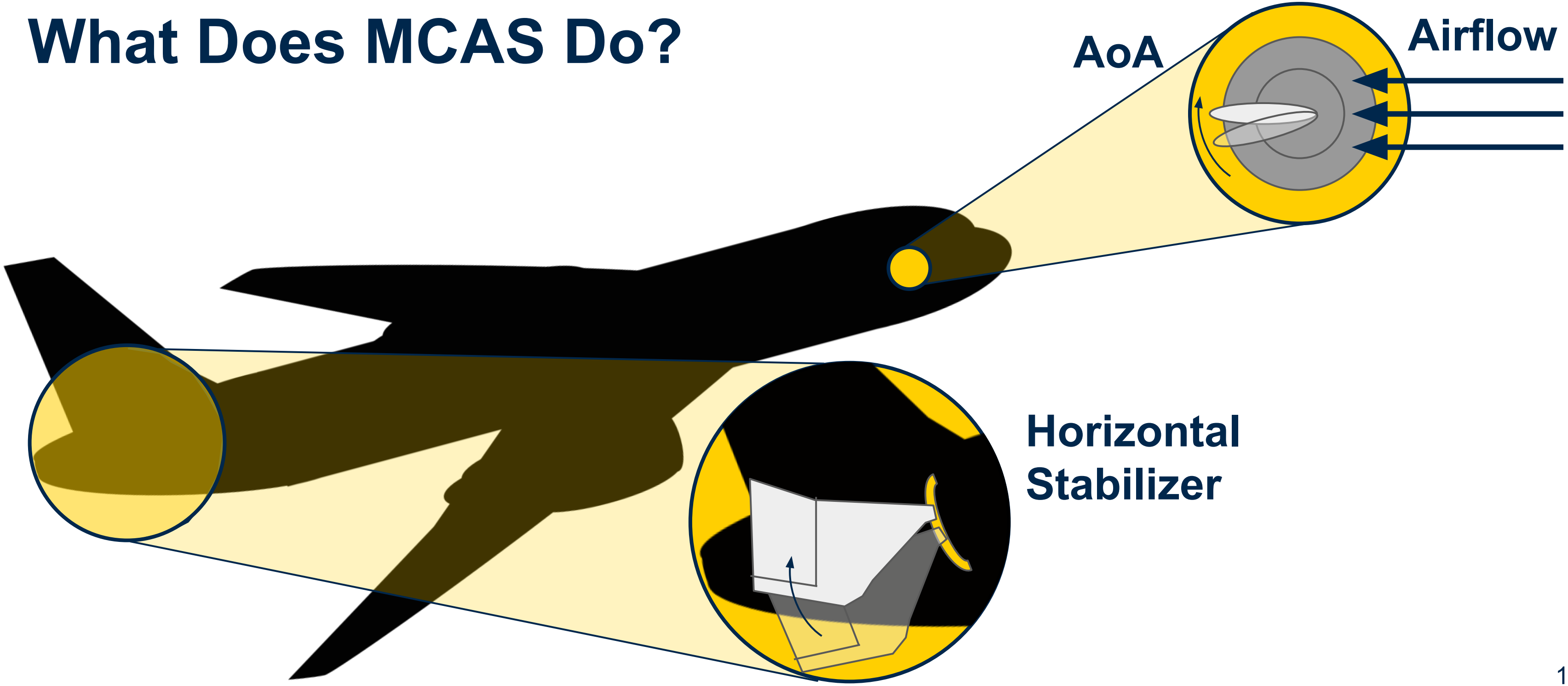
What Does MCAS Do?



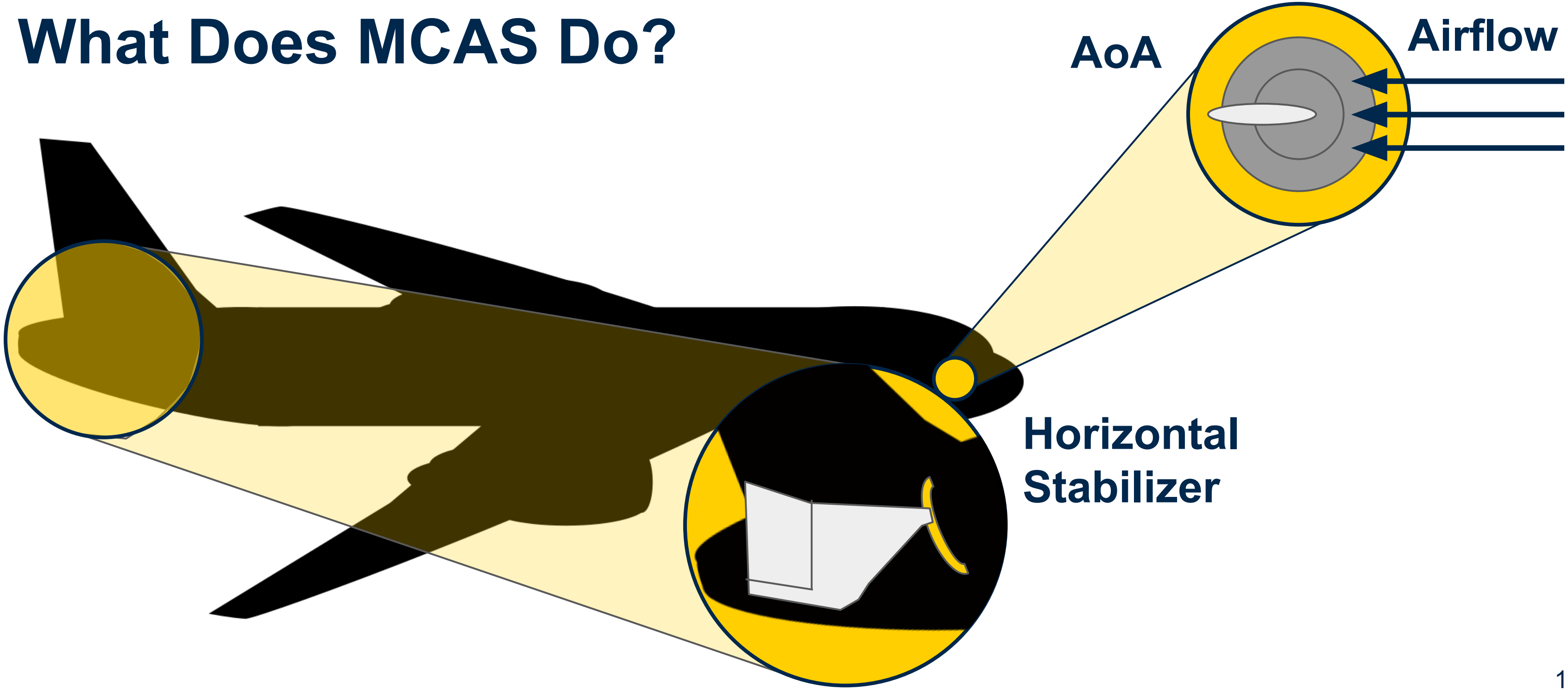
What Does MCAS Do?



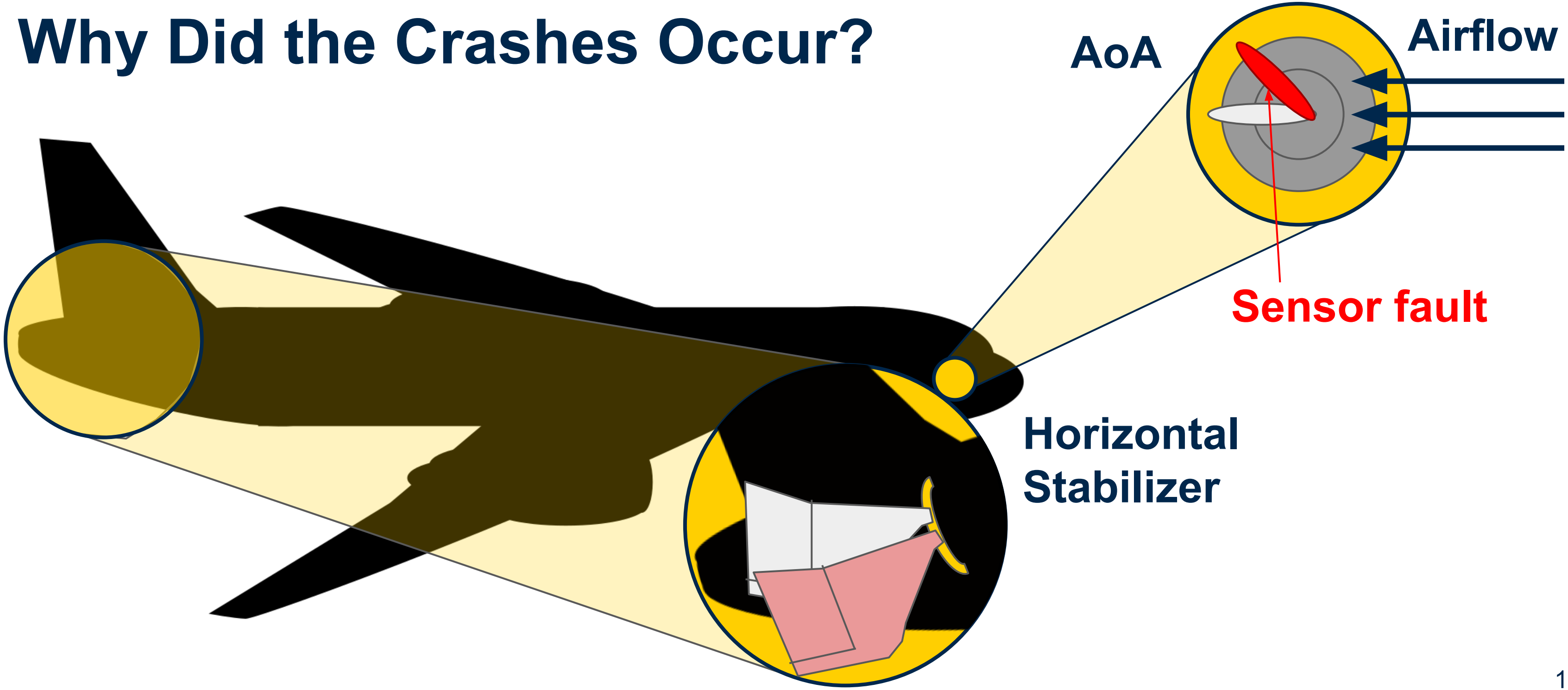
What Does MCAS Do?



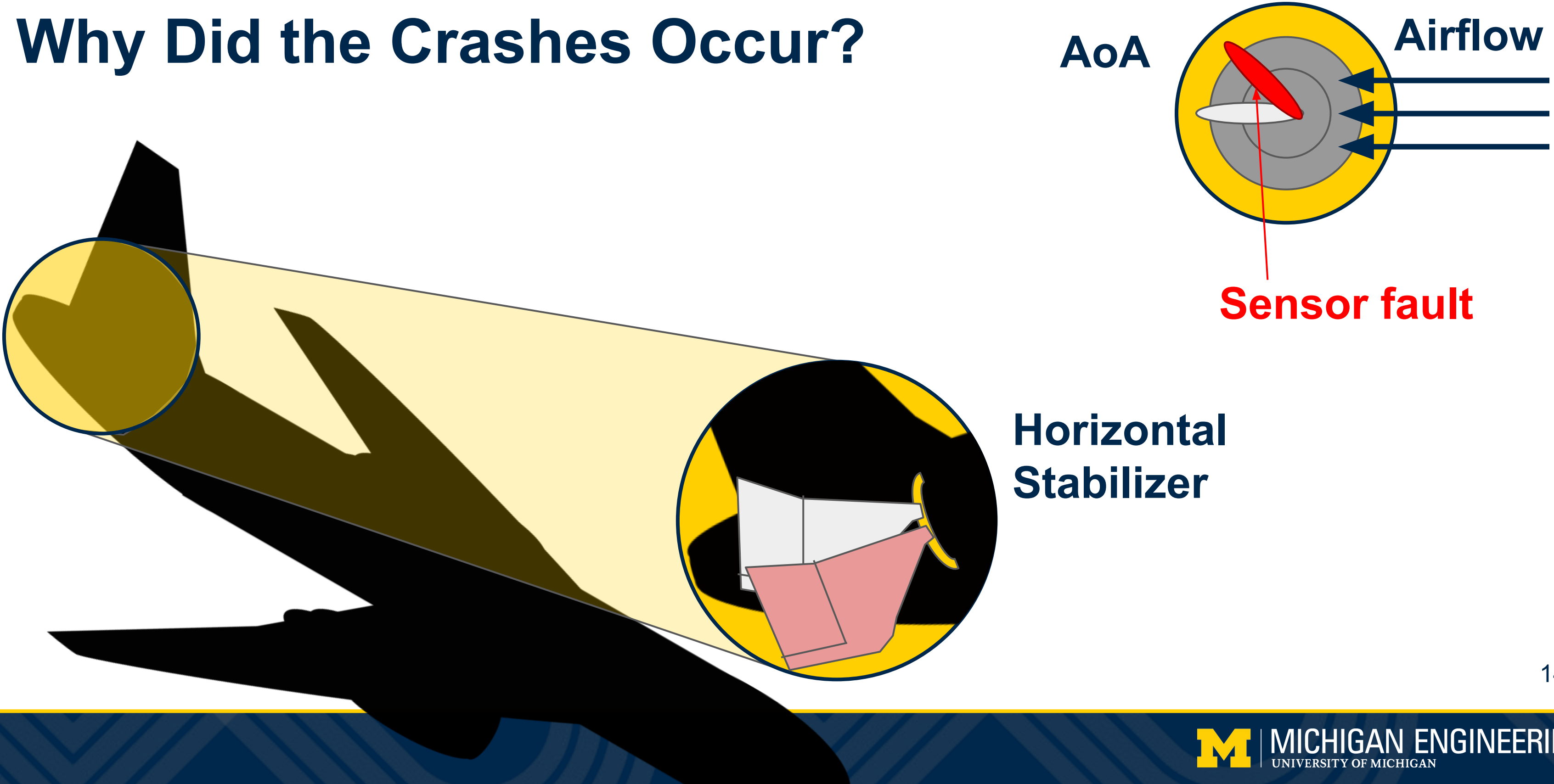
What Does MCAS Do?



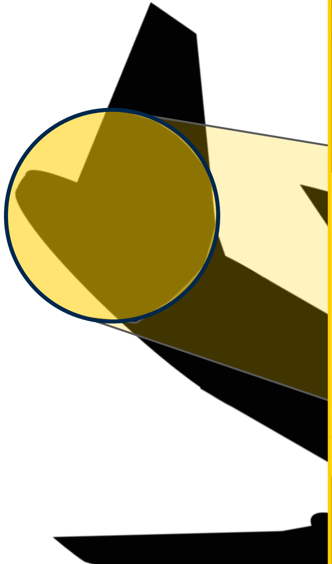
Why Did the Crashes Occur?

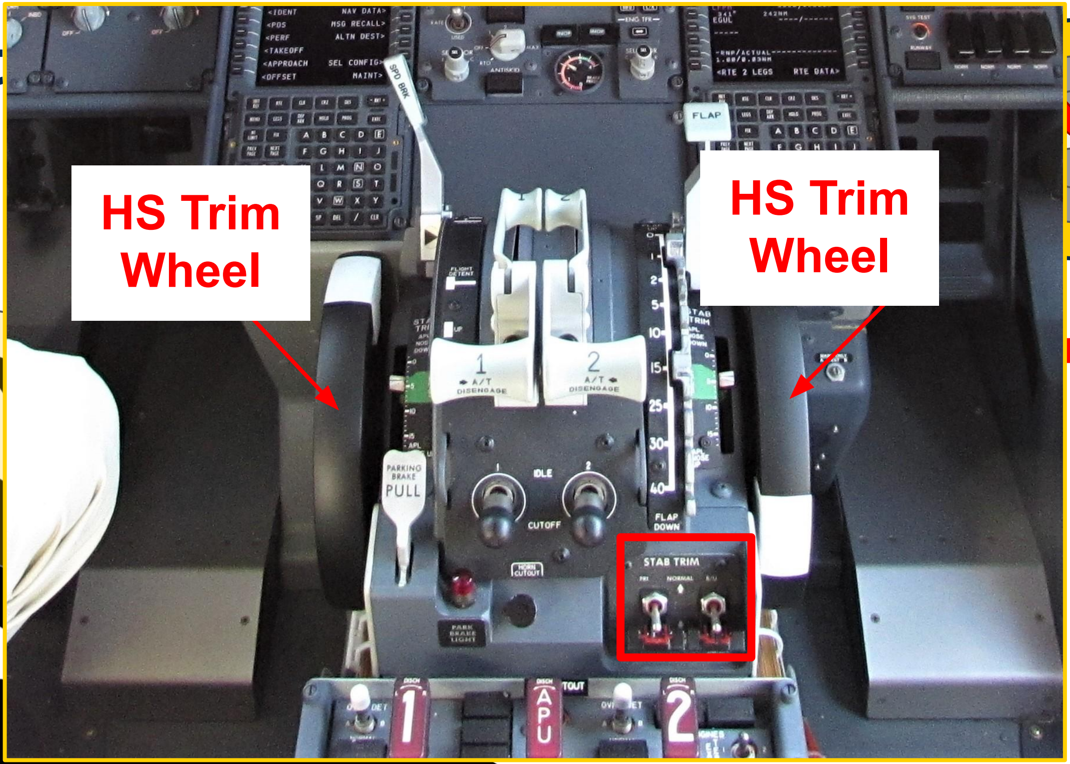


Why Did the Crashes Occur?



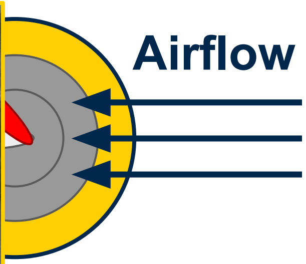
Why Did t





HS Trim Wheel

HS Trim Wheel



nsor fault

New MCAS Requirements

1. Check if all available AoA sensors exceed 17°
   - ↪ They also cannot disagree more than 5.5°

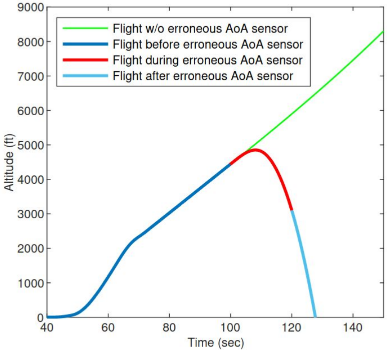
2. Using Mid-Value Select (MVS), activate MCAS only once until MVS “resets”
   - ↪ Meant to prevent runaway stabilizer problem

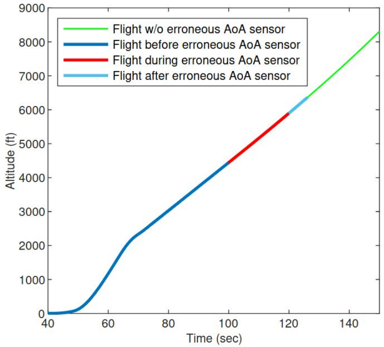
3. Pilots can manually disengage MCAS
   - ↪ Possible before, but now pilots trained to switch off *electric stabilizer trim*

Analysis of Old/New MCAS Requirements

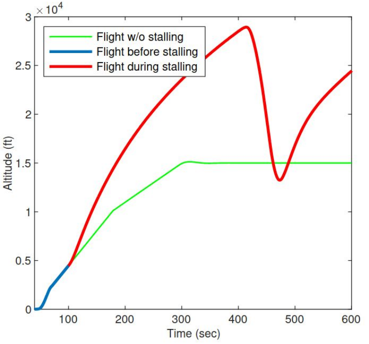
$MCAS_{old}$ ***$MCAS_{new}$***

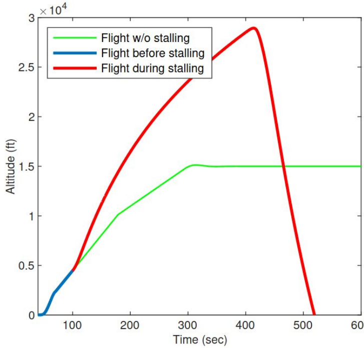
AoA Fault





Pilot Stall

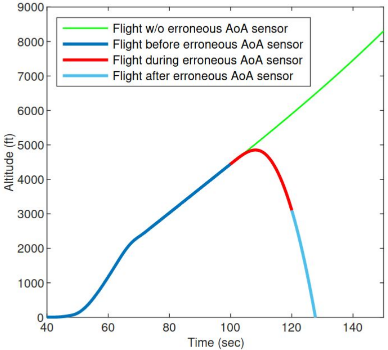


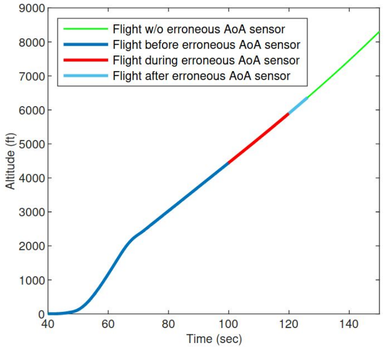


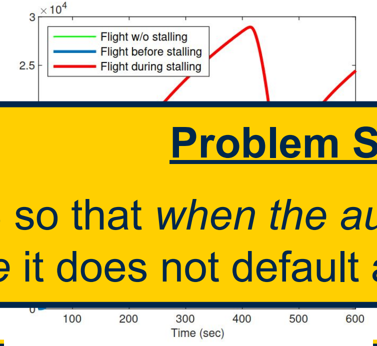
Analysis of Old/New MCAS Requirements

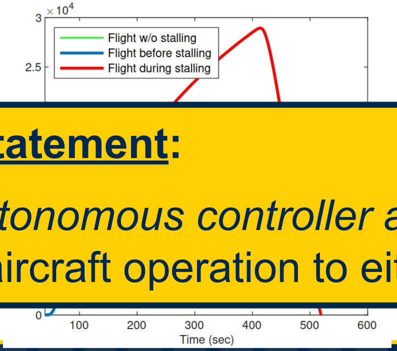
$MCAS_{old}$ **$MCAS_{new}$**

AoA Fault





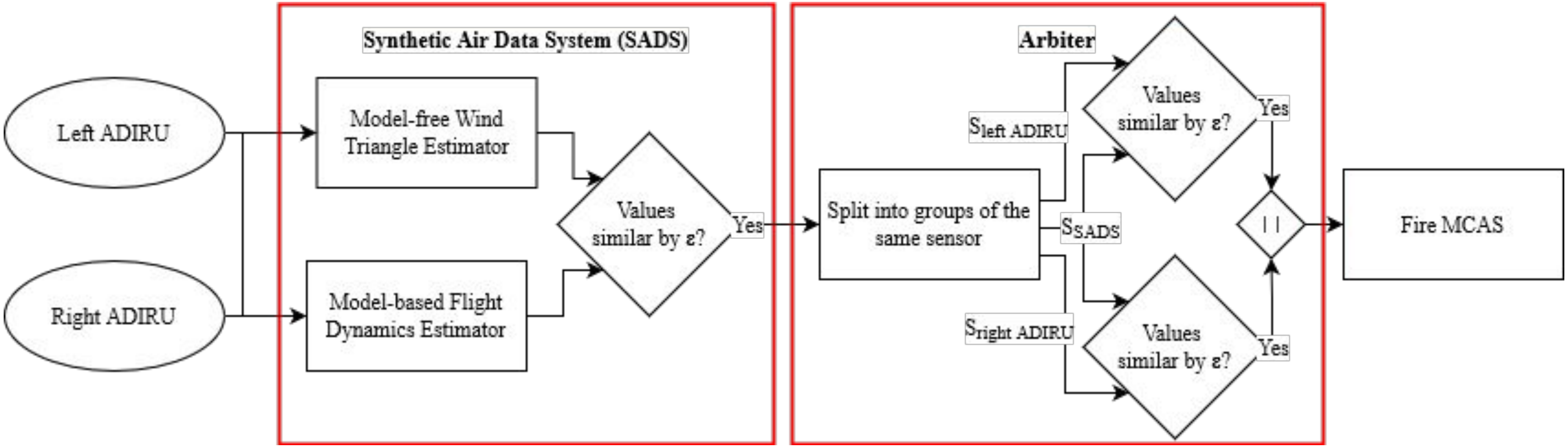




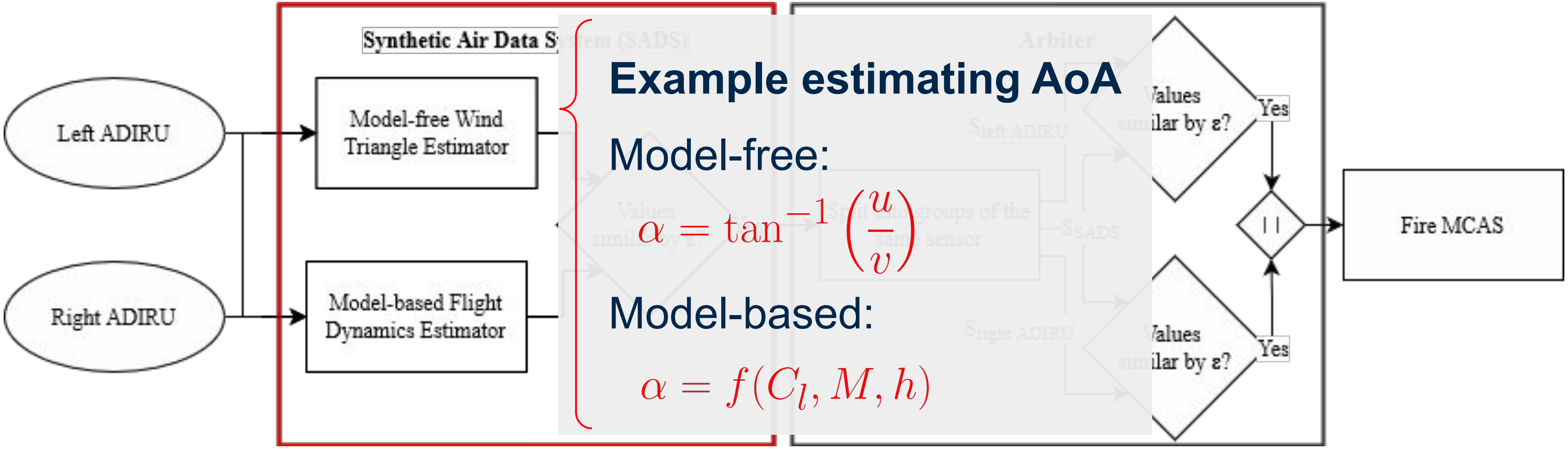
Problem Statement:

Can we design MCAS so that *when the autonomous controller and the manual pilot input disagree* it does not default aircraft operation to either agent?

Semi-Autonomous MCAS (SA-MCAS)



Synthetic Air Data System (SADS)



Example estimating AoA

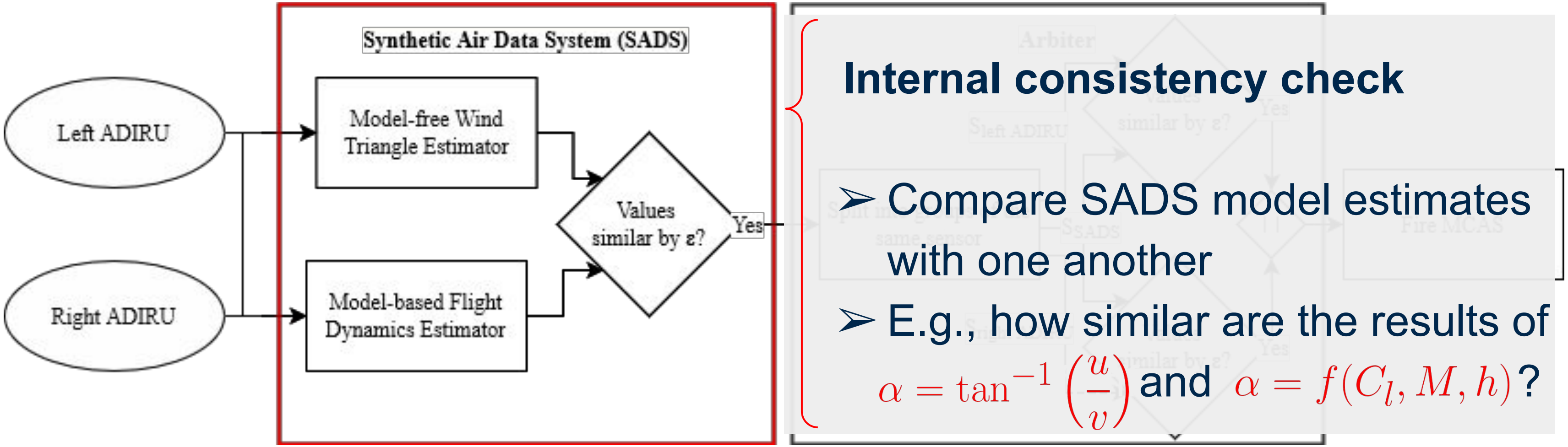
Model-free:

$$\alpha = \tan^{-1}\left(\frac{u}{v}\right)$$

Model-based:

$$\alpha = f(C_l, M, h)$$

Synthetic Air Data System (SADS)



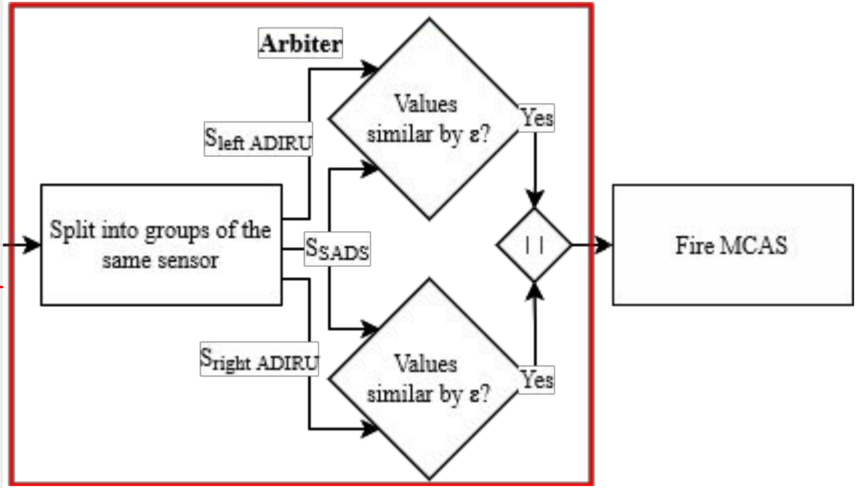
Internal consistency check

- ➢ Compare SADS model estimates with one another
- ➢ E.g., how similar are the results of $\alpha = \tan^{-1}\left(\frac{u}{v}\right)$ and $\alpha = f(C_l, M, h)$?

SA-MCAS Arbiter

External consistency check

- ➢ Compare left and right ADIRU sensor outputs with one another
- ➢ E.g., how similar are α_l and α_r to the results of the SADS model?



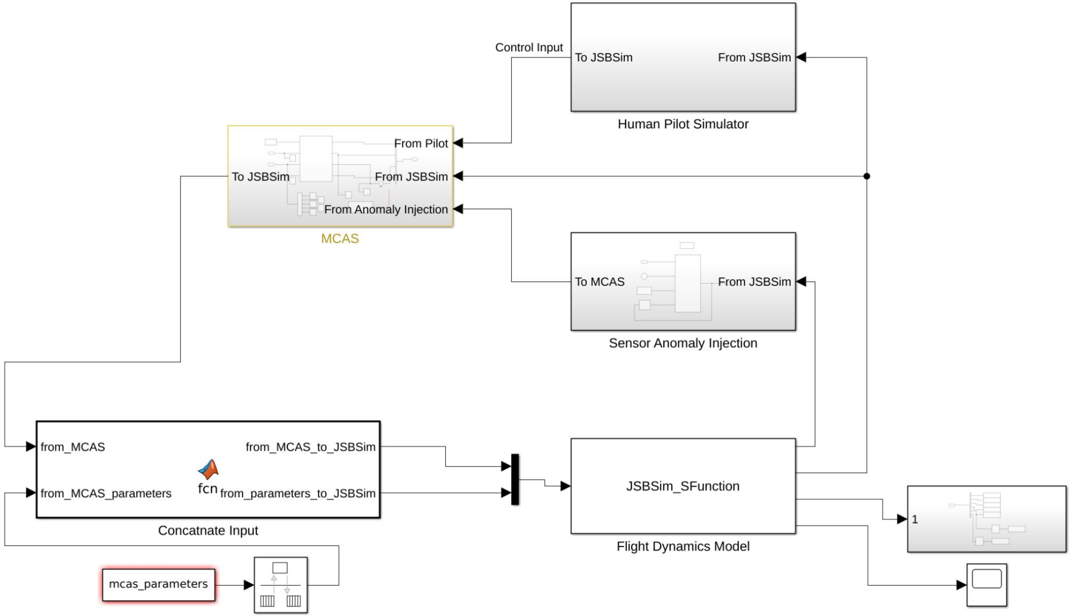
Research Challenges

➊ How to streamline the design and evaluation of MCAS without a physical aircraft?

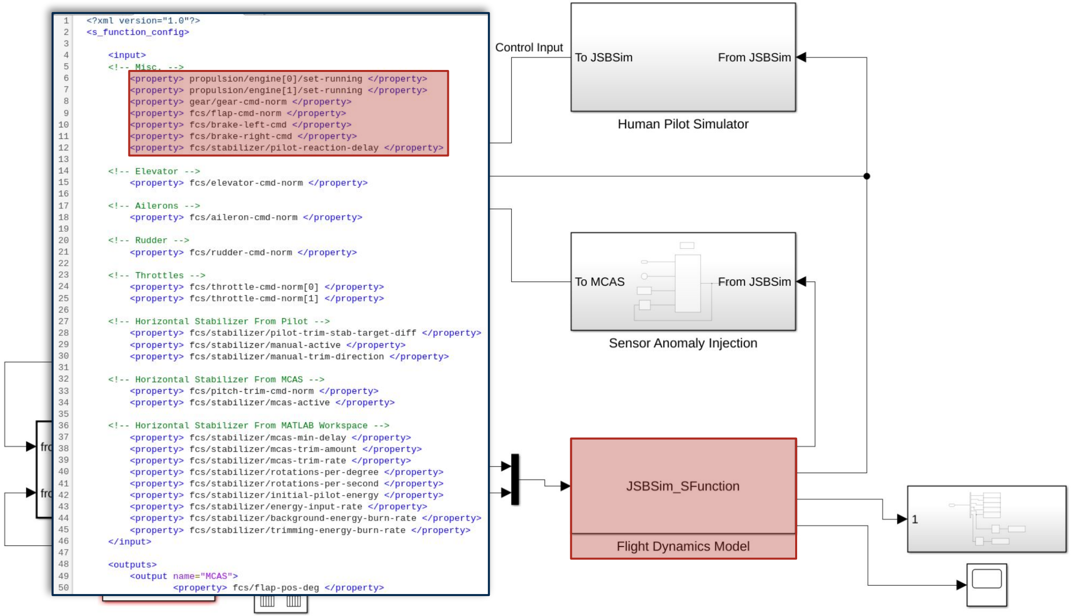
➋ Which control from MCAS and the human pilot threaten the safety of the aircraft?

➌ Does SA-MCAS mitigate the issues present in $MCAS_{old}$ and $MCAS_{new}$?

❶ Simulation of MCAS: Overview of Simulator

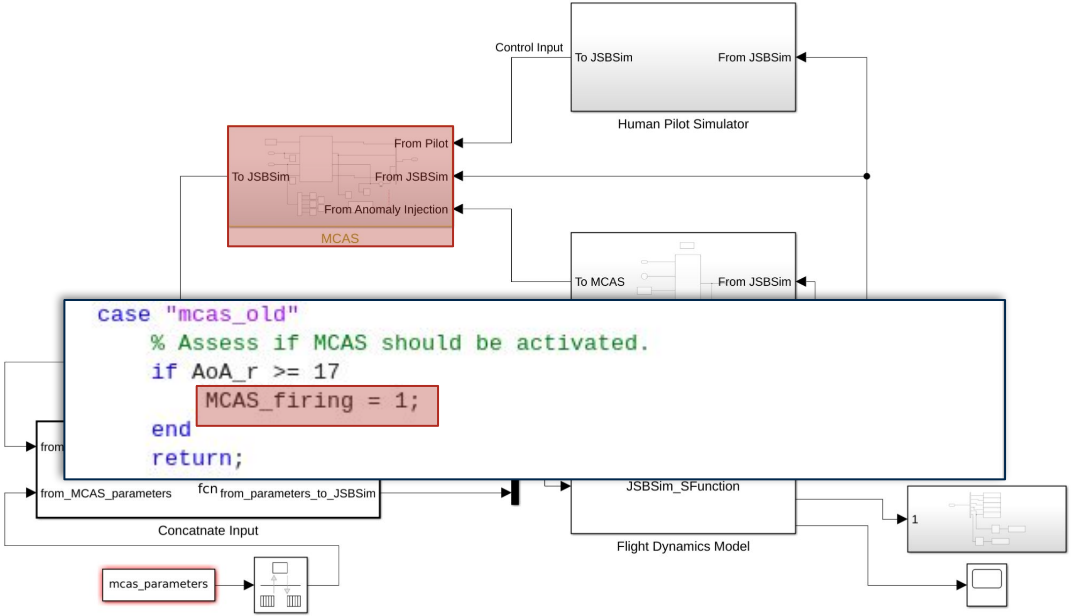


❶ Simulation of MCAS: Configuring Sensors



```xml
<?xml version="1.0"?>
<s_function_config>

    <input>
    <!-- Misc. -->
        <property> propulsion/engine[0]/set-running </property>
        <property> propulsion/engine[1]/set-running </property>
        <property> gear/gear-cmd-norm </property>
        <property> fcs/flap-cmd-norm </property>
        <property> fcs/brake-left-cmd </property>
        <property> fcs/brake-right-cmd </property>
        <property> fcs/stabilizer/pilot-reaction-delay </property>

    <!-- Elevator -->
        <property> fcs/elevator-cmd-norm </property>

    <!-- Ailerons -->
        <property> fcs/aileron-cmd-norm </property>

    <!-- Rudder -->
        <property> fcs/rudder-cmd-norm </property>

    <!-- Throttles -->
        <property> fcs/throttle-cmd-norm[0] </property>
        <property> fcs/throttle-cmd-norm[1] </property>

    <!-- Horizontal Stabilizer From Pilot -->
        <property> fcs/stabilizer/pilot-trim-stab-target-diff </property>
        <property> fcs/stabilizer/manual-active </property>
        <property> fcs/stabilizer/manual-trim-direction </property>

    <!-- Horizontal Stabilizer From MCAS -->
        <property> fcs/pitch-trim-cmd-norm </property>
        <property> fcs/stabilizer/mcas-active </property>

    <!-- Horizontal Stabilizer From MATLAB Workspace -->
        <property> fcs/stabilizer/mcas-min-delay </property>
        <property> fcs/stabilizer/mcas-trim-amount </property>
        <property> fcs/stabilizer/mcas-trim-rate </property>
        <property> fcs/stabilizer/rotations-per-degree </property>
        <property> fcs/stabilizer/rotations-per-second </property>
        <property> fcs/stabilizer/initial-pilot-energy </property>
        <property> fcs/stabilizer/energy-input-rate </property>
        <property> fcs/stabilizer/background-energy-burn-rate </property>
        <property> fcs/stabilizer/trimming-energy-burn-rate </property>
    </input>

    <outputs>
        <output name="MCAS">
            <property> fcs/flap-pos-deg </property>
```

❶ Simulation of MCAS: Building MCAS Module



```
case "mcas_old"
    % Assess if MCAS should be activated.
    if AoA_r >= 17
        MCAS_firing = 1;
    end
    return;
```

❶ Simulation of MCAS: Model Sensor Failures

Definition of sensor errors:

1. Sudden error
   - ➢ $\bar{\mathbf{x}}_s(t) = \delta$
2. Delta error
   - ➢ $\bar{\mathbf{x}}_s(t) = \mathbf{x}_s(t) + \delta$
3. Gradual error
   - ➢ $\bar{\mathbf{x}}_s(t) = \mathbf{x}_s(t_0) + f(t)$

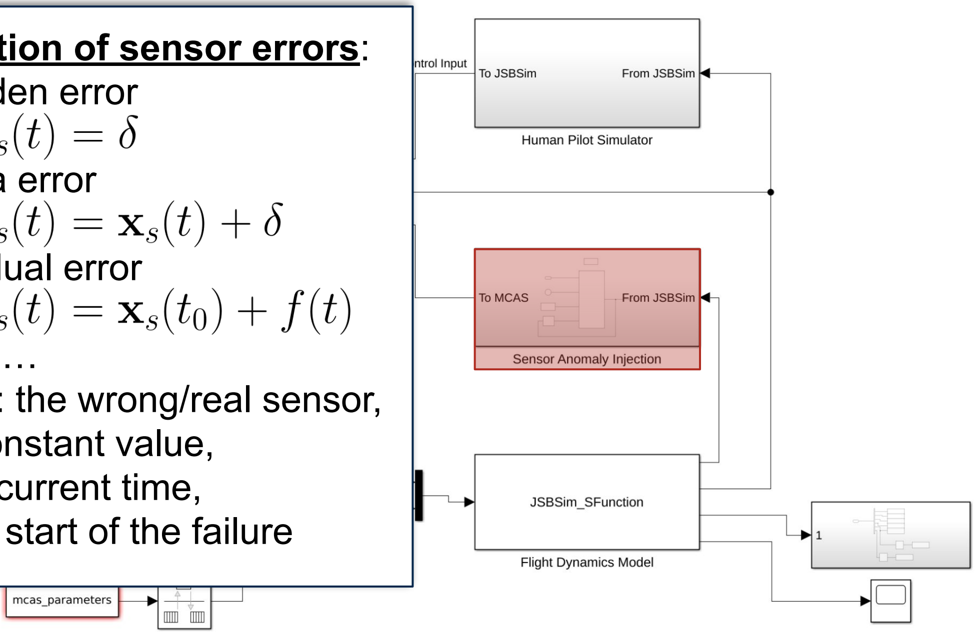
Where…

$\bar{\mathbf{x}}_s$ / $\mathbf{x}_s$: the wrong/real sensor,

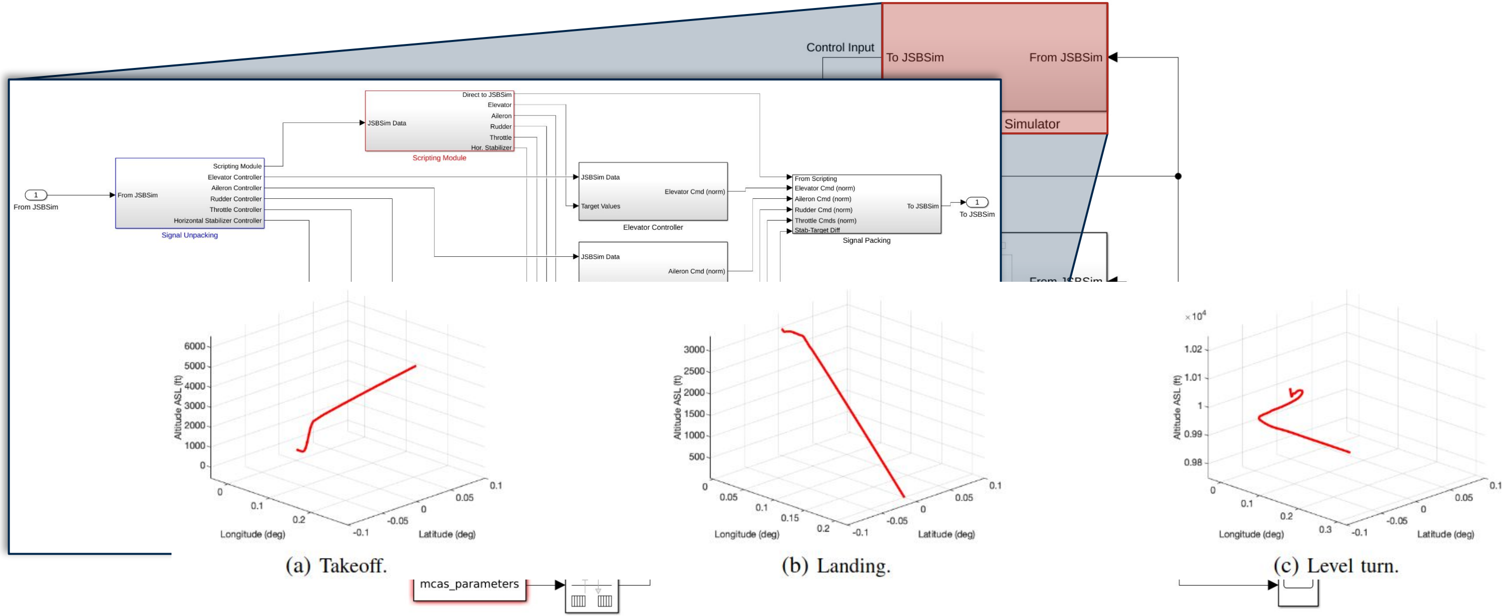
δ: a constant value,

t: the current time,

t_0: the start of the failure



❶ Simulation of MCAS: Model Pilot Control



(a) Takeoff.

(b) Landing.

(c) Level turn.

Research Challenges

❶ **How to streamline the design and evaluation of MCAS without a physical aircraft?**

- We provide an open-source toolkit built on JSBSim.
- We validate the correctness and usefulness of the simulations and include guidelines for using this toolkit.

❷ **Which control from MCAS and the human pilot threaten the safety of the aircraft?**

❸ **Does SA-MCAS mitigate the issues present in $MCAS_{old}$ and $MCAS_{new}$?**

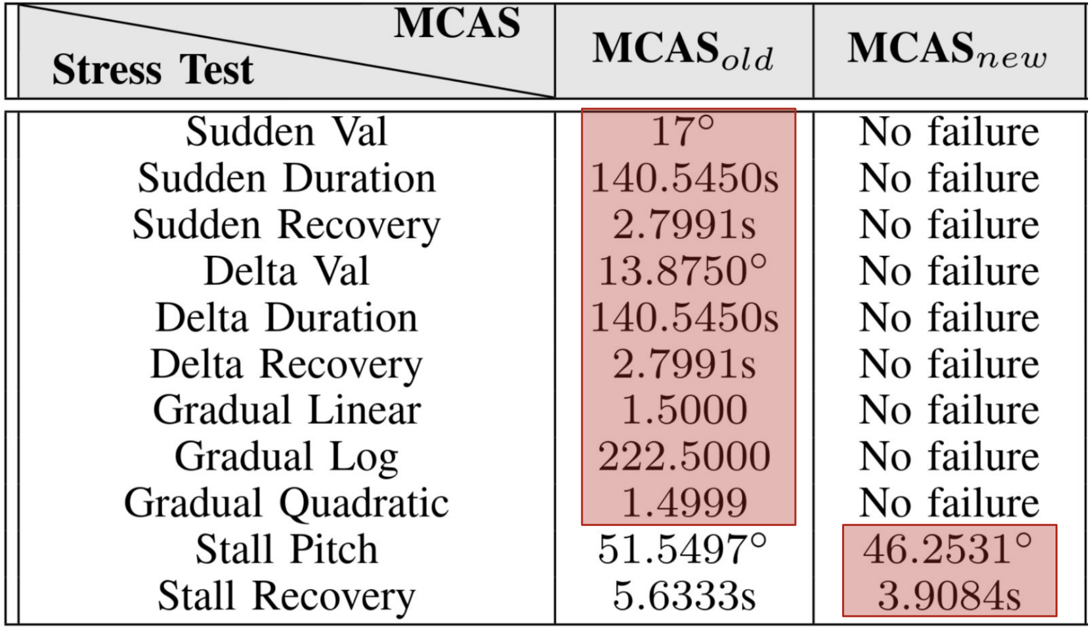
❷ Experiment Setup (Sensor Fault)

- Sudden and delta errors:
  1. $\boxed{\delta \in [0, 90]^\circ}$ $t \in [100, 150]s$ pilot react after 5s
  2. $\delta = 18^\circ$ $\boxed{t \in [100, t_{end}]s \quad t_{end} \in [110, 180]s}$ pilot react after 5s
  3. $\delta = 18^\circ$ $t \in [100, 150]s$ $\boxed{\text{pilot react after} \in [0, 10]s}$
- Gradual errors:
  - ○ $f(t) = at,$ $\boxed{a \in [0, 3]}$ $f(t) = a\log(t),$ $\boxed{a \in [0, 500]}$ $f(t) = at^2,$ $\boxed{a \in [0, 3]}$
  - ○ Pilot react after 5s
- If MCAS activates, pilot trims horizontal stabilizer at rate of 3.5 RPS

❷ Experiment Setup (Pilot Fault)

1. Pitch variation
    - Pilot pitches aircraft $\in \boxed{[20, 90]^\circ}$
    - If MCAS activates, pilot responds in 5s
2. Response variation
    - Pilot pitches aircraft 50°
    - If MCAS activates, pilot responds in $\in \boxed{[0, 10]s}$

❷ Analysis of MCAS$_{old}$ and MCAS$_{new}$ Summary



MCAS Stress Test	MCAS$_{old}$	MCAS$_{new}$
Sudden Val	17°	No failure
Sudden Duration	140.5450s	No failure
Sudden Recovery	2.7991s	No failure
Delta Val	13.8750°	No failure
Delta Duration	140.5450s	No failure
Delta Recovery	2.7991s	No failure
Gradual Linear	1.5000	No failure
Gradual Log	222.5000	No failure
Gradual Quadratic	1.4999	No failure
Stall Pitch	51.5497°	46.2531°
Stall Recovery	5.6333s	3.9084s

Research Challenges

❶ **How to streamline the design and evaluation of MCAS without a physical aircraft?**

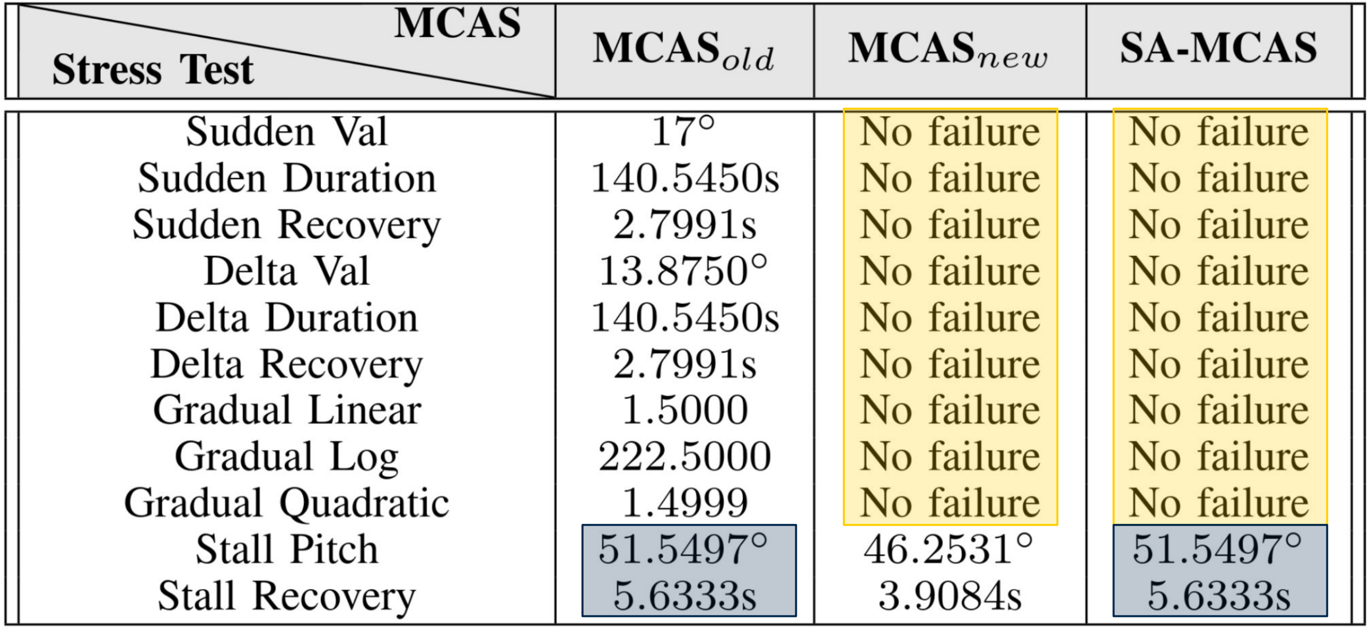
- We provide an open-source toolkit built on JSBSim flight.
- We validate the correctness and usefulness of the simulations and include guidelines for using this toolkit.

❷ **Which control from MCAS and the human pilot threaten the safety of the aircraft?**

- We demonstrate threats that show the new Boeing MCAS design is susceptible to dangerous control from the pilot.
- Our analysis unveils precise upper bounds for aircraft recoverability during erroneous MCAS events.

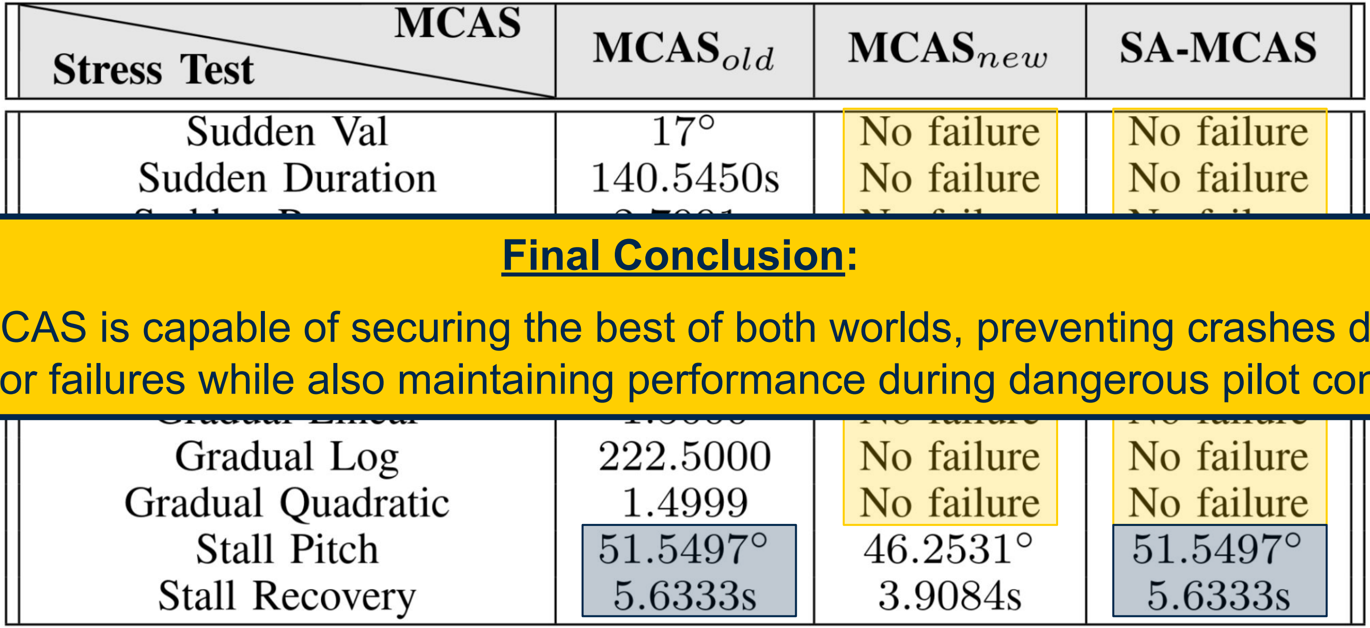
❸ **Does SA-MCAS mitigate the issues present in $MCAS_{old}$ and $MCAS_{new}$?**

❸ Analysis of SA-MCAS



MCAS **Stress Test**	**MCAS$_{old}$**	**MCAS$_{new}$**	**SA-MCAS**
Sudden Val	17°	No failure	No failure
Sudden Duration	140.5450s	No failure	No failure
Sudden Recovery	2.7991s	No failure	No failure
Delta Val	13.8750°	No failure	No failure
Delta Duration	140.5450s	No failure	No failure
Delta Recovery	2.7991s	No failure	No failure
Gradual Linear	1.5000	No failure	No failure
Gradual Log	222.5000	No failure	No failure
Gradual Quadratic	1.4999	No failure	No failure
Stall Pitch	51.5497°	46.2531°	51.5497°
Stall Recovery	5.6333s	3.9084s	5.6333s

❸ Evaluation of SA-MCAS



MCAS / Stress Test	**MCAS$_{old}$**	**MCAS$_{new}$**	**SA-MCAS**
Sudden Val	17°	No failure	No failure
Sudden Duration	140.5450s	No failure	No failure
Gradual Log	222.5000	No failure	No failure
Gradual Quadratic	1.4999	No failure	No failure
Stall Pitch	51.5497°	46.2531°	51.5497°
Stall Recovery	5.6333s	3.9084s	5.6333s

Final Conclusion:

SA-MCAS is capable of securing the best of both worlds, preventing crashes during sensor failures while also maintaining performance during dangerous pilot control.

Research Challenges

❶	**How to streamline the design and evaluation of MCAS without a physical aircraft?**	● We provide an open-source toolkit built on JSBSim flight. ● We validate the correctness and usefulness of the simulations and include guidelines for using this toolkit.
❷	**Which control from MCAS and the human pilot threaten the safety of the aircraft?**	● We demonstrate threats that show the new Boeing MCAS design is susceptible to dangerous control from the pilot. ● Our analysis unveils precise upper bounds for aircraft recoverability during erroneous MCAS events.
❸	**Does SA-MCAS mitigate the issues present in MCAS_{old} and MCAS_{new}?**	● We evaluate SA-MCAS, which is capable of resolving conflicts between the manual and automatic control. ● It is capable of performing the best of MCAS_{old} / MCAS_{new}

Discussion and Future Work

- Discussion
    - Passenger trust still needs to be regained
    - Limited ability to prevent dangerous pilot control

- Future Work
    - What do we do when neither the pilot nor the autonomous control is safe?
    - Currently do equal to better of autonomous/manual control, but can we do better?

Questions?

Takeaways:

- Semi-autonomous systems should not default control to manual operator or autonomous controller
- SA-MCAS provides dynamic control arbitration for 737-MAX

Contributors

Funding

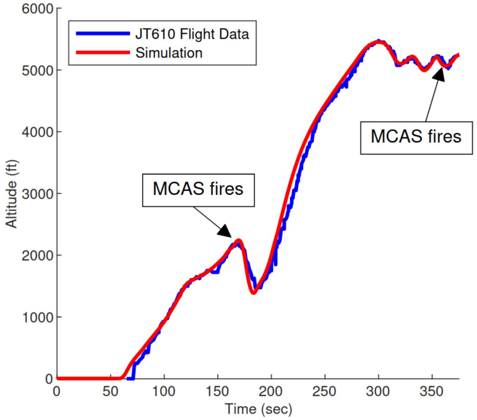
Office of Naval Research
ONR
Science & Technology

Paper URL

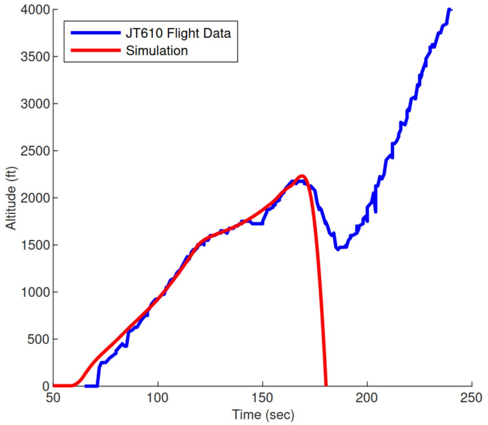
❶ Simulation of MCAS: Validation

JT610 Crash Simulation Using the Modeling Toolkit

Pilot Intervention



No Pilot Intervention

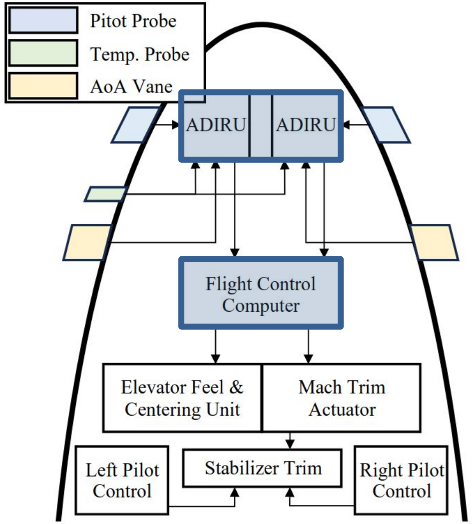


Why Did the 737-MAX Crashes Occur?

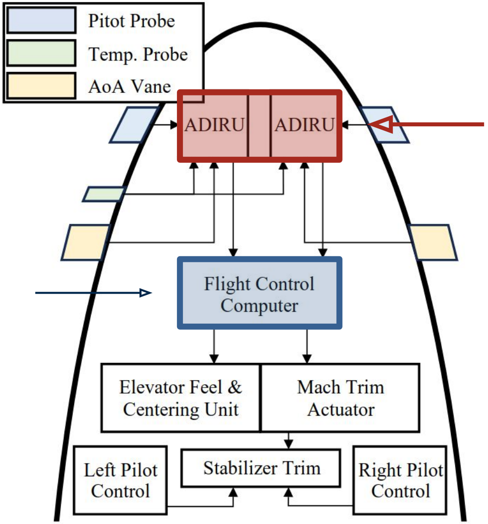
Sources: Boeing, Mentourpilot

Bloomberg

Boeing 737 Aircraft Network



Synthetic Air Data System (SADS)



SA-MCAS

SADS

Example estimating AoA

Model Free:

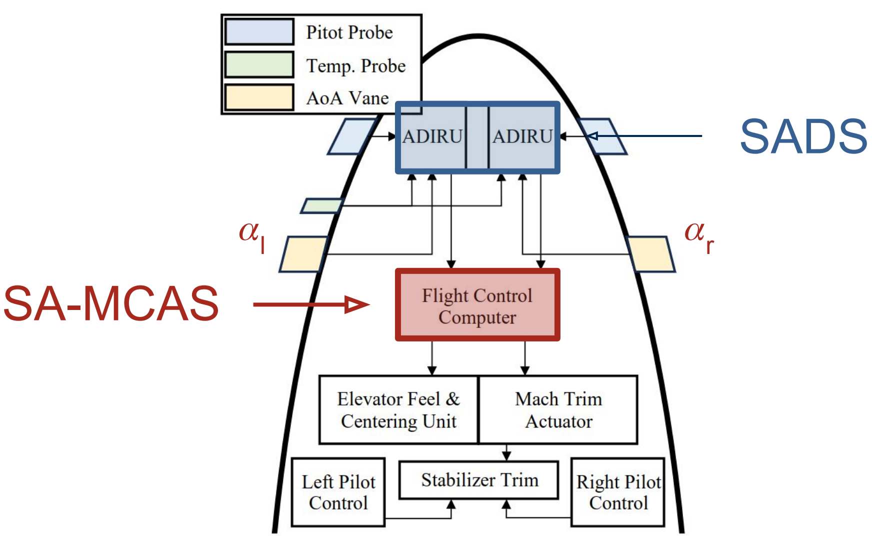
$$\alpha = \tan^{-1}\left(\frac{u}{v}\right)$$

Model Based:

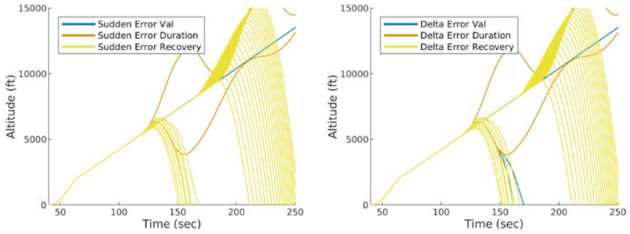
$$\alpha = f(C_l, M, h)$$

Semi-Autonomous MCAS (SA-MCAS)

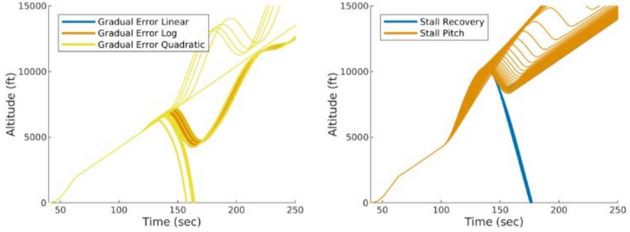
1. Internal consistency check
   - ➢ Compare SADS model estimates with one another
   - ➢ E.g., how similar are the results of $\alpha = \tan^{-1}\left(\frac{u}{v}\right)$ and $\alpha = f(C_l, M, h)$?
2. External consistency check
   - ➢ Compare left and right ADIRU sensor outputs with one another
   - ➢ E.g., how similar are α_l and α_r to the results of the SADS model?



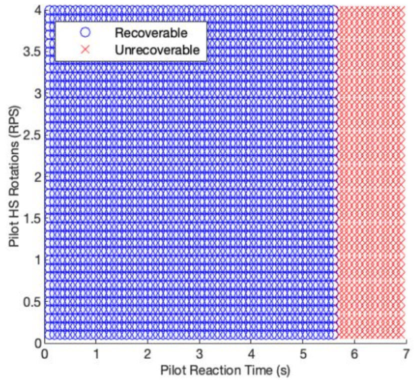
❷ How Does $MCAS_{old}$ Cause Dangerous Control?



(a) Sudden error flight paths. (b) Delta error flight paths.



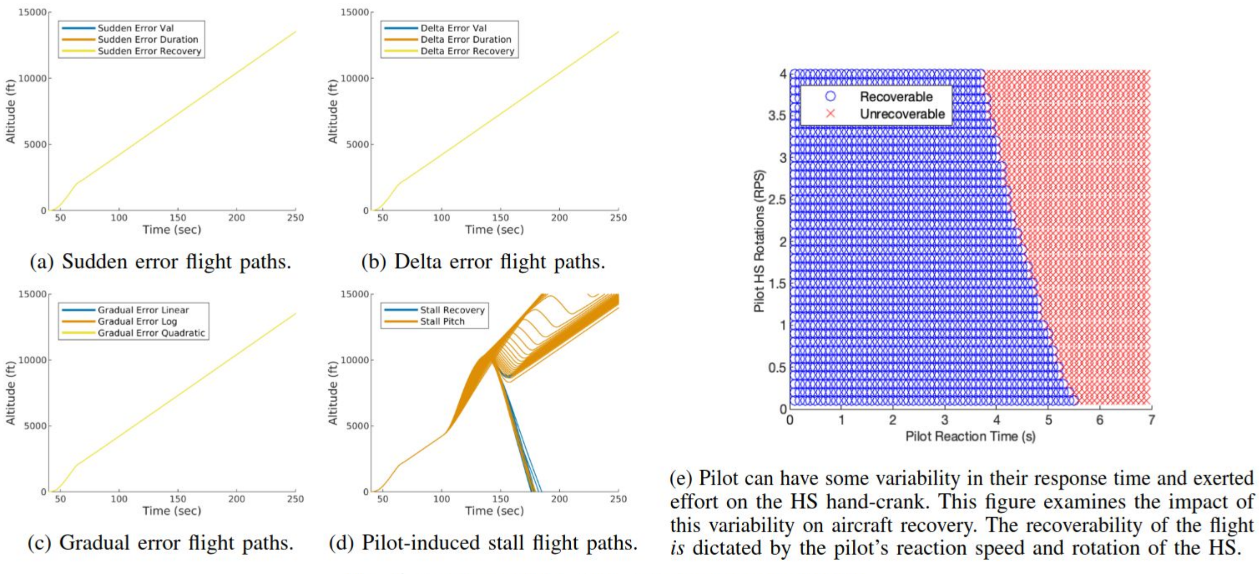
(c) Gradual error flight paths. (d) Pilot-induced stall flight paths.



(e) Pilot can have some variability in their response time and exerted effort on the HS hand-crank. This figure examines the impact of this variability on aircraft recovery. The recoverability of the flight *is not* dictated by the pilot's reaction speed and rotation of the HS.

Fig. 5: Summary of the stress test simulation for MCAS_{old}.

❷ How Does $MCAS_{new}$ Cause Dangerous Control?



(a) Sudden error flight paths.

(b) Delta error flight paths.

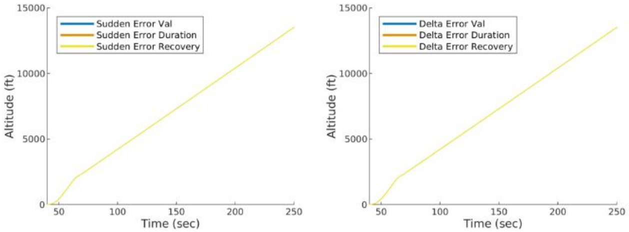
(c) Gradual error flight paths.

(d) Pilot-induced stall flight paths.

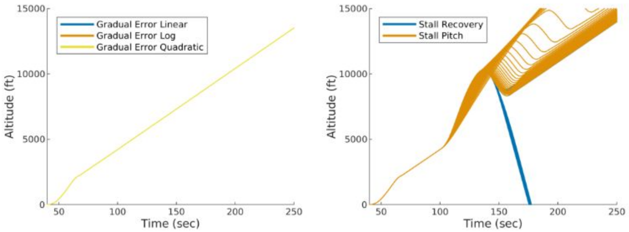
(e) Pilot can have some variability in their response time and exerted effort on the HS hand-crank. This figure examines the impact of this variability on aircraft recovery. The recoverability of the flight *is* dictated by the pilot's reaction speed and rotation of the HS.

Fig. 6: Summary of the stress test simulation for MCAS_{new}.

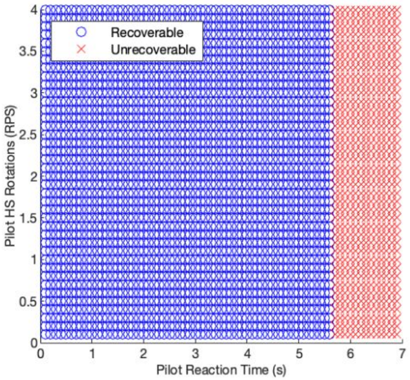
❸ Evaluation of SA-MCAS



(a) Sudden error flight paths. (b) Delta error flight paths.



(c) Gradual error flight paths. (d) Pilot-induced stall flight paths.



(e) Pilot can have some variability in their response time and exerted effort on the HS hand-crank. This figure examines the impact of this variability on aircraft recovery. The recoverability of the flight *is not* dictated by the pilot's reaction speed and rotation of the HS.

Fig. 7: Summary of the stress test simulation for SA-MCAS.