Undergraduate Thesis Prospectus

Discovering Physically Ill-Defined Operations in Cyber-Physical Systems

(technical research project in Computer Science)

A Public-Private Partnership Disaster: The Boeing 737 MAX

(sociotechnical research project)

by

Charlie Houghton

November 2, 2020

technical project collaborators:

Ben Ascoli

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.
Charlie Houghton

Technical advisor: Kevin J. Sullivan, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can dependability in cyber-physical systems (CPSs) be strengthened?

Cyber-physical systems, such as autonomous vehicles and aerospace guidance, interface software with the physical world. CPSs are "frequently deployed in safety-critical domains, such as nuclear or aerospace", and thus "require a stronger form of verification" (Luckcuck, 2019). The dependability of CPSs is partially derived from formal verification that they are safe, secure, and reliable. The presence of software errors compromises dependability. One such type of errors, *physical semantics* errors, occur when an operation a CPS program seeks to perform is computable, but becomes either incorrect or impossible when attaching physical types and meaning to the operation (or *semantics*). If errors in CPSs are found, the authority of the CPS's domain (e.g. FAA for aerospace systems) must ensure that those errors are resolved, otherwise, dependability would remain compromised.

Discovering Physically Ill-Defined Operations in Cyber-Physical Systems

How can CPS engineers discover mixed-frame physical semantics errors in their programs?

CPSs are systems that interact with the physical world, but they are not necessarily constrained by the physical domain in which they operate. For example, suppose a CPS program erroneously adds the distances 2 feet and 3 meters together. In a CPS program devoid of physical meaning, this would be a computable and valid operation, however, when the operation's physical domains are considered, this operation becomes physically meaningless, as the real result is neither 5 feet nor 5 meters. Any operation where a CPS performs a computable but physically incorrect operation is called a *physical semantics* error. Sullivan (2019) concludes that

"major systems malfunctions have occurred due to the machine-permitted evaluation of expressions that have no well defined physical meanings," one such example being NASA's 1999 Mars Climate Orbiter which was unsuccessful due to a failure to "convert from English to metric" before launch (Hotz, 1999).

Physical semantics errors encompass more than just unit inconsistencies, which is itself a solved problem. Among other tools, Microsoft's programming language F# has a system called "Units of Measure" that detects unit inconsistencies (Microsoft, 2020). To explain why detecting unit inconsistencies is insufficient, a notion of an *affine frame* is necessary. An affine frame is a collection of an origin point and basis vectors, creating a space in which definitions of other points and vectors is possible.

In December 2019, NASA launched Boeing's CST-100 Starliner spacecraft that planned to dock with the International Space Station but was ultimately not successful due to a misconfigured clock resulting in the Starliner's autonomous instructions being offset by 11 hours (Chang, 2019). What occurred was precisely a physical semantics error due to both CPSs performing operations in different affine frames, as their time origins differed. This incident highlights why same-frame verification is a more complete model for CPS formalisms than same-unit verification.

I will be partnering with Ben Ascoli, an independent research undergraduate, and we will be working with Professor Kevin Sullivan in the Computer Science department. Our primary goal is to extend the existing same-frame verification system, called Peirce, by integrating physical units as a means to define affine frames. We will be using a proof assistant called Lean for most of the project. When a CPS program is given to Peirce for the purpose of physical semantics verification, Lean code will be auto-generated based on the operations performed in

that program and the user-provided physical domains of each operation. If the CPS performs any mixed-unit or mixed-frame operations, the generated Lean code will fail to compile. Our extension to Peirce will be successful if mixed-unit operations, which create mixed-frame operations, are identified by Peirce. If successful, the next step would be to implement in-code Peirce unit annotations, allowing for more seamless integration with Peirce.

A Public-Private Partnership Disaster: The Boeing 737 MAX

How have U.S. airplane manufacturers, airlines, and U.S. aviation governing bodies organized to improve commercial aviation safety in response to the 737 MAX 8 incidents?

Soon after the Boeing 737 MAX series was introduced into commercial air travel in 2017, two of the planes crashed, killing 346 people: a Lion Air flight in 2018, and an Ethiopian Airlines flight in 2019. FAA grounded all 737 MAX planes in March 2019. Recently, Bloomberg (2020) interviewed the executive director of the European Union Aviation Safety Agency (EASA), Patrick Ky. During the interview he indicated that the EASA deems the updated 737 MAX sufficiently safe and estimated that it could be back in service before the end of 2020 (Philip, 2020). In the U.S., the Federal Aviation Administration (FAA) review of the 737 MAX remains incomplete (Levin, 2020). Yet American Airlines is poised to bring the 737 MAX back into service in December, though it will "remain in contact" with FAA and "continue to update its plans based on when the aircraft is certified" (Goodwin, 2020). Boeing, like the EASA, FAA, and American Airlines, is confident in the return of the 737 MAX, stating that upon its return, it will be "one of the most thoroughly scrutinized aircraft in history" (Boeing Communications, 2020).

FAA regulates the manufacture, operation, and maintenance of U.S aircraft (USDOT, 2018) to "provide the safest, most efficient aerospace system in the world" (FAA, 2019). FAA shares information with the National Travel Safety Board (NTSB) (FAA, 2012). The U.S. Department of Transportation (USDOT) oversees FAA, and its primary objective is to ensure the U.S. "has the safest ... modern transportation system in the world" (USDOT, 2020). In 2020, USDOT found inadequate regulation enforcement by FAA, which put "17.2 million [Southwest Airlines] passengers at risk" (USDOT OIG, 2020). The House Committee on Transportation and Infrastructure (Transportation Committee), of which aviation is in its jurisdiction, also noted inconsistencies: the second of the two 737 MAX incidents occurred "just two years and two days after FAA had certified the new 737 derivative aircraft as safe to fly. Clearly it was not" (Transportation Committee, 2020a).

During the approval process of the 737 MAX, FAA "shifted more authority ... to the manufacturer itself, even allowing Boeing to choose many of the personnel who oversee tests and vouch for safety," creating an environment where FAA employees would face "retaliation for speaking up" (Robinson et. al, 2019). The Transportation Committee (2020) identified that this, as well as other "numerous oversight lapses" by FAA, "played a significant role" in the 737 MAX crashes. Fang (2020) suggests that a stricter approval process could also have geo-political implications: "It is imperative that FAA and Boeing implement stricter regulations for the 737 MAX and future aircraft" otherwise they risk "Chinese and Russian aircraft become alternative global standards of aviation."

NTSB, whose primary objectives include "making transportation safer by conducting independent accident investigations" (NTSB, 2017), found that both 737 MAX incidents were the result of "unintended MCAS operation" (NTSB, 2019). If the 737 MAX maintained a steep

angle-of-attack (AoA) during flight, the MCAS system would engage and correct it by pitching down (fig. 1). NTSB (2019) found that, while the MCAS system functioned correctly, "erroneous AoA input," in conjunction with an ill-equipped crew who did not know how to disengage the MCAS system, was the primary cause for both accidents.

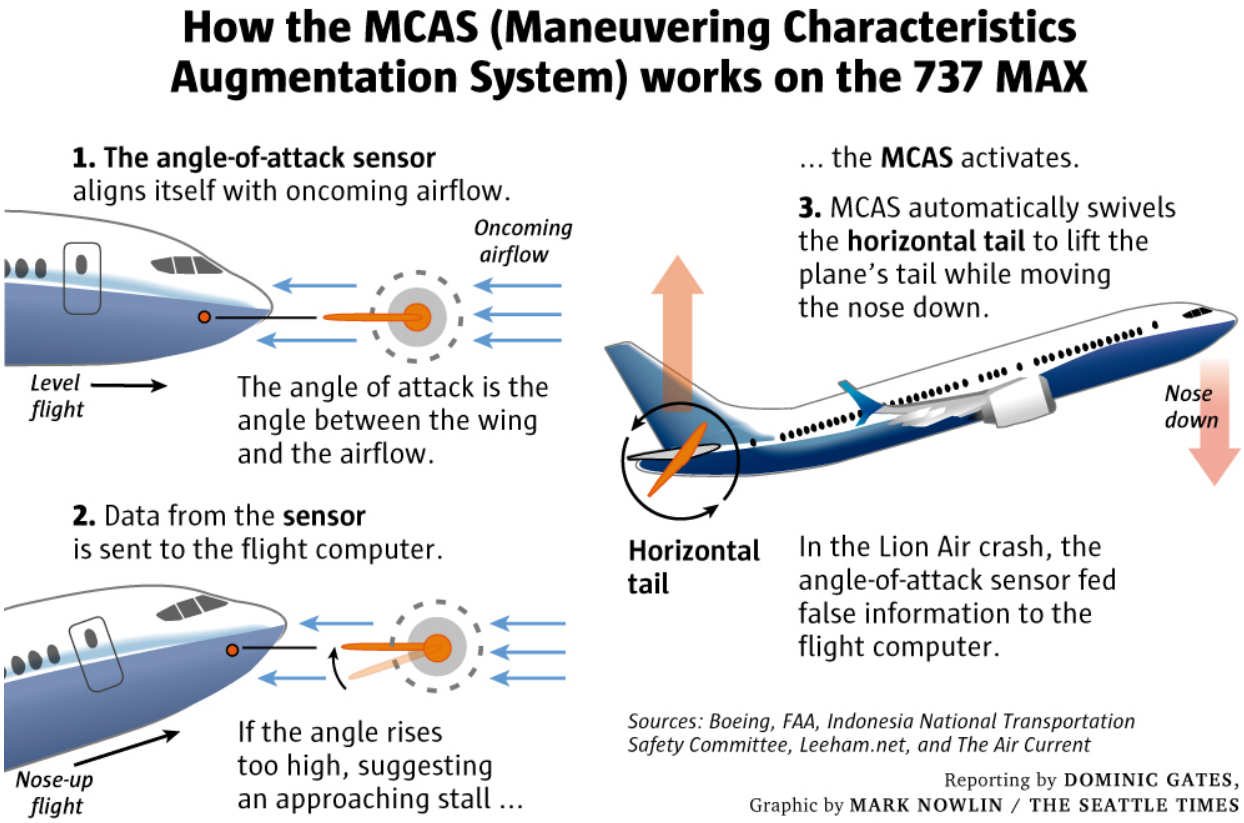

Figure 1. How the MCAS works on the 737 MAX (Nowlin, 2019)

Boeing is the second-largest airplane manufacturer in the world by market share. As a publicly-traded corporation, Boeing has a legal obligation to seek profit. Following the two 2018 and 2019 737 MAX accidents, Boeing's market share suffered, allowing Airbus and "non-Western manufacturers to fill the gap," demonstrating how safety is a prerequisite for profit (Fang, 2020). Some of the 737 MAX missteps can be attributed to Boeing's rushed production of the airplane to compete with Airbus's A320neo, which resulted in "extensive efforts to cut costs,

maintain the 737 MAX program schedule, and avoid slowing the 737 MAX production line" (Transportation Committee, 2020b). In that effort, Boeing promoted the plane as being similar to the existing Next-Generation 737 model "minimizing MAX pilot transition training," which "was an important cost saving for Boeing's airline customers" and "a key selling point for the jet" leading to more than 5,000 orders (Gates, 2019).

Airlines, including privately owned Lion Air and state-owned Ethiopian Airlines, are also primarily driven by profit. Airlines adopted the 737 MAX into their fleets because they were "better, lighter, and cheaper to fuel and maintain" than previous models (Topham, 2019). Profit-seeking behavior may also come in the form of safety assurances. One such example comes from Lion Air in 2017, when they asked Boeing for additional training resources for the 737 MAX, to which Boeing employees internally rebuked seeing the request as unnecessary (Gelles, 2020). Following the accidents and the tarnished safety record of the 737 MAX, deliveries halted and net orders decreased. 387 orders were nevertheless fulfilled and are sitting dormant, waiting to fly again (Boeing, 2020).

References

Boeing (2020, June). *737 Model Commercial Orders Summary.* http://active.boeing.com/commercial/orders/displaystandardreport.cfm?cboCurrentModel=737&optReportType=AllModels&cboAllModel=737

Boeing Communications. (2020, Sept. 16). *Boeing Statement on the House T&I Committee Report on 737 MAX* [Press release]. https://boeing.mediaroom.com/news-releases-statements?item=130735

Chang, K. (2020, March 6). Boeing Starliner Lands in New Mexico After Clock Error Prompts Early Return. *The New York Times.* https://www.nytimes.com/2019/12/22/science/boeing-starliner-landing.html

Fang, Y. (2020). The 737 Max and the Future of Commerical Aviation. *Harvard International Review, 41*(2), 33-39. doi:10.2307/26917300

FAA. (2019, Nov. 6). Federal Aviation Administration. *Safety: The Foundation of Everything We Do*. https://www.faa.gov/about/safety_efficiency/

FAA. (2012, Nov. 8). Federal Aviation Administration. *U.S. Aviation Industry, FAA Share Safety Information with NTSB to Help Prevent Accidents* [Press release]. https://www.faa.gov/news/press_releases/news_story.cfm?newsId=14053

Gates, D. (2019, March 21). Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system. *The Seattle Times.* https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lion-air-crash/

Gelles, D. (2020, Jan. 10). 'I Honestly Don't Trust Many People at Boeing': A Broken Culture Exposed. *The New York Times.* https://www.nytimes.com/2020/01/10/business/boeing-737-employees-messages.html

Goodwin, J. (2020, Oct. 18). American Airlines plans to return the 737 Max to service in December. *CNN.* https://www.cnn.com/2020/10/18/business/boeing-737-max-american-airlines/index.html

Hotz, R. (1999, Oct. 1). Mars Probe Lost Due to Simple Math Error. *Los Angeles Times.* https://www.latimes.com/archives/la-xpm-1999-oct-01-mn-17288-story.html

Levin, A. (2020, Sept. 30). FAA Chief Likes Revised 737 After Flight, But Review Continues. Bloomberg. https://www.bloomberg.com/news/articles/2020-09-30/faa-chief-calls-test-flight-of-737-productive-but-work-remains

Luckcuck, M., et al. (2019, Sept.). Formal Specification and Verification of Autonomous Robotic Systems: A Survey. https://doi.org/10.1145/3342355

Microsoft. (2020, Aug. 15). Units of Measure. *Microsoft Documentation.* https://docs.microsoft.com/en-us/dotnet/fsharp/language-reference/units-of-measure

NTSB (2019, Sept. 19). National Travel Safety Board. *Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance.* https://www.ntsb.gov/investigations/AccidentReports/Reports/ASR1901.pdf

NTSB (2017, Dec.). National Travel Safety Board. *National Transportation Safety Board FY 2018–2022 Strategic Plan.* https://ntsb.gov/about/reports/Documents/FY2018-2022strategicPlan.pdf

Philip, S. (2020, Oct. 16). Boeing Max Judged Safe to Fly by Europe's Aviation Regulator. *Bloomberg.* https://www.bloomberg.com/news/articles/2020-10-16/boeing-max-declared-safe-to-fly-by-europe-s-aviation-regulator

Robinson, P., et al. (2019, March 18). Boeing Drops as Role in Vetting Its Own Jets Comes Under Fire. Fortune. https://fortune.com/2019/03/18/boeing-safety-vetting-faa/

Sullivan, K. (2019, Aug.). *Explicating and Exploiting the Physical Semantics of Code*. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1909414

Topham, G. (2019, March 12). Boeing's 737 Max wooed airlines with its cost-saving fuel economy. The Guardian. https://www.theguardian.com/business/2019/mar/12/boeings-737-max-wooed-airlines-cost-saving-fuel-economy

Transportation Committee a. (2020, Sept.). Final Committee Report on the Design, Development & Certification of the Boeing 737 MAX. https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf

Transportation Committee b. (2020, Sept. 16). After 18-Month Investigation, Chairs DeFazio and Larsen Release Final Committee Report on Boeing 737 MAX [Press release]. https://transportation.house.gov/news/press-releases/after-18-month-investigation-chairs-defazio-and-larsen-release-final-committee-report-on-boeing-737-max

USDOT, OIG. (2020, Feb. 11). United States Department of Transportation, Office of Inspector General. *FAA Has Not Effectively Overseen Southwest Airlines' Systems for Managing Safety Risks.* https://www.oig.dot.gov/sites/default/files/FAA%20Oversight%20of%20Southwest%20Airlines%20Final%20Report%5E02.11.2020.pdf

USDOT. (2020, Jan. 29). United States Department of Transportation. *About DOT*. https://www.transportation.gov/about

USDOT. (2018, May 2). United States Department of Transportation. *Federal Aviation Administration*. https://www.transportation.gov/briefing-room/safetyfirst/federal-aviation-administration