Models of Human-Automation Systems: Initial Analysis of the Boeing 737MAX Design

Immanuel Barshi[1], Asaf Degani[2], Robert Mauro[3] & Randall J. Mumaw[4]

[1]Human Systems Integration Division, NASA Ames Research Center; [2]GM Advanced Technology Center; [3]Decision Research and University of Oregon; [4]San Jose State University Research Foundation.

We describe a formal approach to identifying human factors design vulnerabilities and usability concerns in the context of automated control systems. We present an initial analysis of the design of the B737MAX that has suffered two fatal accidents. We highlight two main design vulnerabilities and one usability concern. Key formal generic properties used to identify these vulnerabilities and usability concerns are defined. These generic properties, and others referenced in the paper, can be applied to the analysis of any human-automation system.

Every human-machine system can be characterized by a set of “models” (Degani, Shmueli, & Bnaya, 2022). A “machine model” can be used to characterize how the system’s technology is operated. An “information/interface model” can be used to represent the information available to human operators that guides their interaction with the system. Based on this information, as well as training and experience, operators develop a “user model” that represents their conceptualization of how the human-machine system works. Whereas the first two models are static, the user model is dynamic in the sense that it constantly evolves: people forget and re-acquire information, develop a different understanding of system behavior with experience, or completely revamp their understanding based on what others tell them (Gentner & Stevens, 1983).

A comparison of the three models can help highlight potential design vulnerabilities and usability concerns. For example, operators may believe that they have control over a process when in fact that control is conditional. Similarly, a system that is controllable at one point may become uncontrollable and unsafe when a certain threshold is crossed. Each of these vulnerabilities and concerns has a generic form, called a *property*, which once captured and understood, is part of a “toolset” that can be applied to any design by searching for it in the system. Naturally, as the toolset grows, it becomes more likely that vulnerabilities and concerns will be detected and addressed. This detailed comparison of the three models relies on a formal description of the system.

Formal Methods

Formal methods utilize various languages and methodologies to describe technological systems and identify design problems. The choice of a formal method depends on the specific goal of the analysis, such as hardware integration or software analysis (c.f. the Therac-25 accident, Leveson & Turner, 1993; Toyota unintended acceleration, NASA, 2011). One common language used for formal methods is the “finite state machine” modeling language.

Figure 1 depicts a simple reading lamp to illustrate the modeling language. It has two states: OFF or ON, transition arcs between them, and the specific events that trigger these transitions. For example, to trigger a transition from the OFF state to the ON state, the lamp’s switch must be pressed.

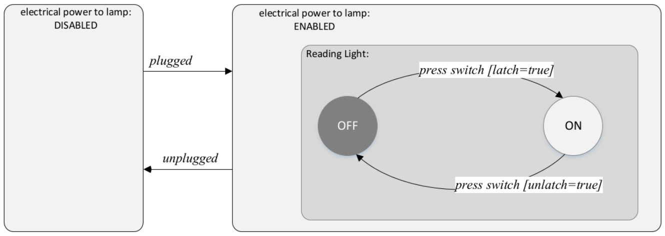
electrical power to lamp: DISABLED
electrical power to lamp: ENABLED
plugged
unplugged
Reading Light:
press switch [latch=true]
OFF
ON
press switch [unlatch=true]

Figure 1. Machine model of a reading lamp.

If the switch does not latch, the current will not flow and there will be no light. The model indicates this condition on the switch press event (latch=true). The user, however, is not privy to whether the solenoid is true or false and, hence, cannot reliably determine, a priori, if the transition to ON will take place or not. This situation is called “non-determinism” and is elaborated below.

To enable the lamp to work at all, light bulb and solenoid latch included, the electrical power must first be enabled by plugging in the lamp. These features of the reading lamp system can be depicted in the machine model. Note however, that the formal model says nothing about the size of the lamp, the materials it is made of, its color, or the luminosity of its bulb—or anything about the switch's shape and ergonomics.

This model and approach enable the designer to identify aspects of the design that could lead to operator confusion (see, e.g., Degani, Shmueli, & Bnaya, 2022). For example, if the switch is pressed and the light fails to turn on, the user does not know a priori whether the solenoid latch did not occur, electrical power was not enabled, or the lightbulb was burned out. Below, we illustrate this finite state machine modeling methodology to identify potential design vulnerabilities and usability concerns using an initial analysis of the Boeing 737 pitch trim system (Barshi, et al., 2023).

BOEING 737NG AND 737MAX

The Boeing 737 is the most widely used airliner model in the history of aviation. At any given time, there are more B737s in the air than any other transport aircraft. The two fatal B737MAX-8 accidents—one in Indonesia in October of 2018 (NTSC, 2019) and one in Ethiopia in March of 2019 (EAAIB, 2022)—shook the aviation industry and led to the unprecedented global grounding of the MAX fleet.

Pitch/trim system

In both accidents, the pilots failed to overcome the inputs of the Maneuvering Characteristics Augmentation System (MCAS) to the horizontal stabilizer. The stabilizer is a large surface on the airplane's tail that can be moved up or down. The airplane's pitch trim system utilizes the aerodynamic impact of these movements to relieve pressure from the flight controls when the aircraft is maneuvered along its pitch axis (nose up or nose down) and to maximize aerodynamic efficiency. Moving the stabilizer to relieve control pressure is called "trimming." For instance, when pilots want to decrease airspeed while maintaining their altitude, they reduce power and gradually increase airplane pitch attitude to produce the lift needed to hold altitude. Instead of continuously holding back pressure on the control column, the pilot can trim the horizontal stabilizer to a position that will maintain the desired pitch attitude, removing the need for continual manual force on the control column.

In the B737, the pilots can directly trim the stabilizer in two ways: either by manually rotating the large trim wheels, located on the center pedestal between the pilots, or by pressing a pair of two thumb switches located on the control yoke that activate an electric motor that moves the trim wheels and the stabilizer itself. The autopilot of the B737 also uses the electric trim when it controls the aircraft, as well as the speed trim system, that is standard in all B737 models, and MCAS, which is a subcomponent of this speed trim system and is unique to the B737MAX.

The B737MAX is a derivative of the B737NG (Next Generation); that is, the design and the regulatory certification of the MAX were based on the certified and widely used B737NG model. The MAX was designed to be minimally different from the NG to reduce certification changes and training requirements. The major change from the NG to the MAX was new engines that are more efficient, quieter, and less polluting. Although the pitch trim systems on the two aircraft models only differ slightly, this difference was significant in these accidents.

Pitch trim system of the B737NG

The design of the pitch trim system involves several subsystems and multiple components. We focus on a single element: the transition of the electric trim motor from the engaged state to the disengaged state, which is related to the introduction of MCAS. There are two cardinal states: electric trim disabled, and electric trim enabled (Figure 2). The electric trim is normally enabled by default; that is, extra steps are required to disable it.

Once enabled and during flight, the electric motor is either disengaged (when no electric trim activation is required by the pilot or the automation) or engaged (when the pilot, autopilot, or the speed trim system demand activation). The activation can either be *nose down* or *nose up*.

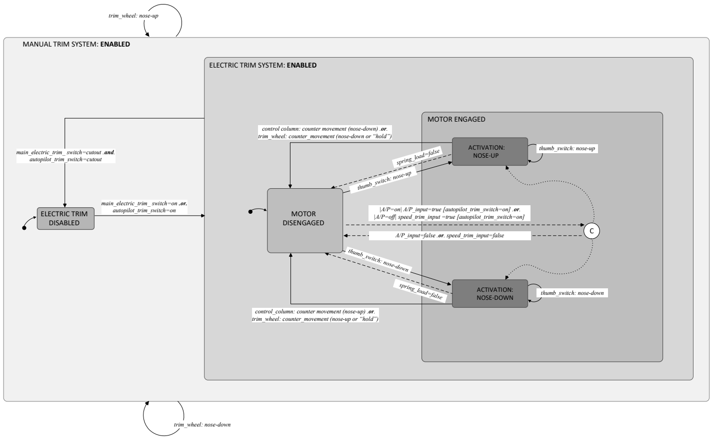
trim_wheel: nose-up
MANUAL TRIM SYSTEM: ENABLED
ELECTRIC TRIM SYSTEM: ENABLED
main_electric_trim_ switch=cutout .and.
autopilot_trim_switch=cutout
ELECTRIC TRIM DISABLED
main_electric_trim_ switch=on .or.
autopilot_trim_switch=on
control column: counter movement (nose-down) .or.
trim_wheel: counter_movement (nose-down or "hold")
MOTOR ENGAGED
ACTIVATION: NOSE-UP
thumb_switch: nose-up
spring_load=false
thumb_switch: nose-up
MOTOR DISENGAGED
|A/P=on| A/P_input=true [autopilot_trim_switch=on] .or.
|A/P=off| speed_trim_input =true [autopilot_trim_switch=on]
A/P_input=false .or. speed_trim_input=false
C
thumb_switch: nose-down
spring_load=false
ACTIVATION: NOSE-DOWN
thumb_switch: nose-down
control_column: counter movement (nose-up) .or.
trim_wheel: counter_movement (nose-up or "hold")
trim_wheel: nose-down

Figure 2. Machine model of the B737NG trim system.

If, however, an erroneous input is made to the electric trim motor, the aircraft can transgress into a potentially dangerous pitch attitude. This pitch attitude can be either too high, potentially leading to an aerodynamic stall, or too low, leading to a dive. The pilot may be able to momentarily hold the controls to prevent the aircraft from reaching an undesirable pitch attitude. However, stabilizer aerodynamic forces at the extreme deflection are very powerful and difficult to overcome; they may exceed the pilot's ability to manually counter the pitch movement generated by the stabilizer.

This extreme deflection, when it occurs automatically by erroneous inputs, is referred to as a "runaway trim" in aviation lingo. To limit the degree of possible pitch mis-trim, a mechanism is installed under the cockpit floor (referred to as the "floor switch") that automatically disengages the electric trim motor when the pilot moves the control column in a direction opposite to the trim input. For instance, if the speed trim system erroneously commands continuous nose-up trim, the pilot, to maintain the desired flight path, would respond by pushing the control column forward. When the floor switch threshold is reached, the trim motor is stopped. This stops the trim motor from moving the stabilizer any further. The control column countermovement is represented in the model as one of the two events that can trigger the trim motor to transition from an ENGAGED to a DISENGAGED state.

On the B737NG, moving the control column in the opposite direction to the movement of the stabilizer stops the movement regardless of whether the electric trim motion is commanded by the pilot's electric thumb switch or by the automation (autopilot and speed trim system). The same logic applies for aircraft nose down and aircraft nose up movements.

Pitch trim system of the B737MAX

Note, the discussion below is focused on the original design of the pitch trim system on the B737MAX (NTSB, 2019). Significant changes to that design were made following the accidents and the grounding of the MAX fleet.

The introduction of new engines on the B737MAX led to major changes in the aircraft's aerodynamics. To counter the aircraft's tendency toward nose up, the MCAS was designed to create forward pressure on the control column during manual flight (i.e., when the autopilot is not engaged), with flaps retracted, at a high angle of attack approaching a stall condition (NTSB, 2019). This forward pressure is induced by commanding the horizontal stabilizer on the aircraft's tail to be trimmed *nose down*. Because the MCAS is designed to produce forward pressure on the control column when the pilot is pulling the control column back, this counter action should not cause a trim motor disengagement. To address this issue, the MAX's floor switch is disabled when MCAS is moving the horizontal stabilizer in the *nose down* direction, thus allowing *nose down* stabilizer movement against pilot counter action (NTSB, 2019). The modification of the floor switch only applies to MCAS *nose down* activation; it does not apply to MCAS *nose up* activation.

ANALYSIS OF THE TRIM/PITCH SYSTEM

The model of the pitch trim system of the B737MAX depicts this specific modification as well as all the other changes from the B737NG model (see Figure 3). The control column countermovement is depicted as an event triggering a transition from the ENGAGED state to the DISENGAGED state in the case of stabilizer *nose down* or *nose up* activation. But when the MCAS is commanding horizontal stabilizer nose down activation, the transition back to the MOTOR DISENGAGED state is disabled and is indicated by a self-loop. The self-loop indicates that despite the counter movement of the control column, the nose down activation will continue undisturbed and no transition to

MOTOR DISENGAGED will take place (as long as MCAS is active and sends inputs).

Our analysis revealed that this modification produces a *design vulnerability* and *usability concern* that can lead to operator confusion. The first design vulnerability has to do with the pilot's inability to reliably predict the result of countermovement actions of the control column. Pulling back on the control column when the electric trim motor is moving the stabilizer *nose down* will disengage the motor when the movement is commanded by thumb switches, the autopilot, or the speed trim. However, when the *nose down* movement is commanded by MCAS, pulling back on the control column will NOT disengage the motor, and *nose down* activation will continue. Since the flight deck interfaces do not indicate which system is providing the trim input, it is impossible for the pilot to predict the outcome of a countermovement. From the pilot's perspective, the system is unpredictable in the sense that it behaves non-deterministically.

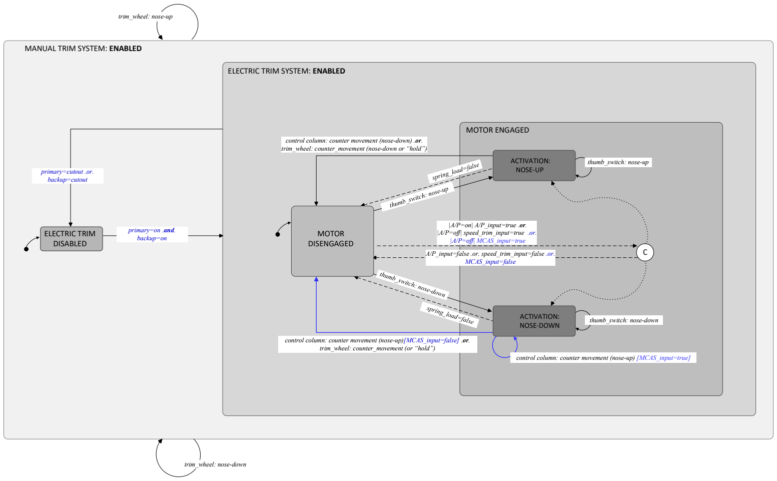
trim_wheel: nose-up
MANUAL TRIM SYSTEM: ENABLED
ELECTRIC TRIM SYSTEM: ENABLED
MOTOR ENGAGED
control column: counter movement (nose-down) .or.
trim_wheel: counter_movement (nose-down or "hold")
ACTIVATION: NOSE-UP
thumb_switch: nose-up
spring_load=false
thumb_switch: nose-up
primary=cutout .or.
backup=cutout
ELECTRIC TRIM DISABLED
primary=on .and.
backup=on
MOTOR DISENGAGED
|A/P=on| A/P_input=true .or.
|A/P=off| speed_trim_input=true .or.
|A/P=off| MCAS_input=true
C
A/P_input=false .or. speed_trim_input=false .or.
MCAS_input=false
thumb_switch: nose-down
spring_load=false
ACTIVATION: NOSE-DOWN
thumb_switch: nose-down
control column: counter movement (nose-up)[MCAS_input=false] .or.
trim_wheel: counter_movement (or "hold")
control column: counter movement (nose-up) [MCAS_input=true]
trim_wheel: nose-down

Figure 3. Machine model of the B737MAX trim system (superimposed on the same system of the B737NG; changes from the NG are marked in blue).

The second potential source of confusion results from the lack of symmetry between the motion of the electric trim motor in *nose down* versus *nose up* inputs. In the B737MAX, when the electric trim is moving the stabilizer *nose up*, the control column movements in a direction opposite to the stab movement will always disengage the motor regardless of which automated system (autopilot, speed trim, MCAS) is commanding the trim motor. However, when the motor is moving the stabilizer nose down, control column movements in the opposite direction to the stabilizer movement will disengage the electric motor in some cases (when the autopilot or speed trim provide input), but not in others (when the MCAS provides input). This lack of symmetrical consistency between the *nose up* and *nose down* movement of the stabilizer is confusing to the user because it breaks up the internal coherency of the design (Brunswik, 1943). It represents a usability concern that cannot be resolved even if MCAS inputs are made visible on the interface (See Nielsen, 1994, on "consistency" and Norman & Draper, 1986, on "symmetry" and "mapping").

A pilot transitioning from flying the B737NG to flying the B737MAX would expect that control column movements in either direction should stop stabilizer trim motion (either commanded by the yoke-mounted electric switch or by any automated system). By comparing the machine model to the user model (or in this case, by comparing the machine model of the B737NG and the machine model of the B737MAX), the discrepancy between the models highlights areas of vulnerability and usability concerns.

MCAS CONTROL

MCAS, when enabled, monitors several aircraft parameters, including speed and angle of attack. The MCAS compares these parameters to respective threshold values. If the current aircraft parameters are within the normal range (i.e., below threshold), MCAS stays disengaged. However, when the parameters are above threshold, the MCAS engages and sends inputs to activate *nose down* stabilizer trim motions. These trim movement commands produce nose down inputs at a fixed rate of 0.27 degrees per second. After the target value has been achieved, the MCAS (as it worked in these accidents) stops activation of the electric trim motor for a period of 5 seconds (NTSB, 2019).

After the 5 second hold, if the parameters are still above threshold, another activation will take place, and so on. The original design of the MCAS control logic had no limits with respect to the number of activations (Note, this logic was changed in later designs.). These activations, if not arrested by the pilot, can accumulate to a stabilizer deflection region that may exceed the pilot's ability to manually counter the pitch movement generated by the stabilizer. The possibility and the unannounced nature of the transition between a "safe" control region where the pilot can recover from MCAS accumulation using manual force and transgression into an "unsafe" one where it exceeds the pilot's manual force is another vulnerability in the original MCAS design. Following the two accidents and the grounding of the MAX fleet, the control logic of the MCAS was changed such that only a single input is allowed. Thus, these accumulations, either within the pilot manual control region or beyond it, are no longer possible.

DISCUSSION

The analysis described here identified one design vulnerability and one usability concern related to the control column modification: non-deterministic behavior of the control column countermovement when the MCAS is active, and the lack of symmetry of control column responses between *nose up* and *nose down* while the MCAS is active.

A second design vulnerability concerns the control logic of the MCAS. Because the original MCAS control logic allowed for unlimited nose down activation, the lack of pilot correction in the form of nose up trim inputs was able to lead to an accumulation of stabilizer deflection. This accumulation could reach a point where aircraft pitch control enters into an unsafe region of operation. In this unsafe region, because of the large stabilizer deflection, pilots can no longer arrest the aircraft dive using the manual trim wheels or any manual control column movement (ECAA, 2019).

References

Brunswik, E. (1943). Organismic achievement and environmental probability. *Psychological Review, 50*, pp. 255–272.

Barshi, I., Degani, A., Mauro, R., & Mumaw, R.J., (2023). *Analysis of the Boeing 737MAX accidents: Formal models and psychological perspectives.* Presented at the 22nd International Symposium on Aviation Psychology, Rochester, NY.

Degani, A., Shmueli, Y. & Bnaya, Z. (2022). *Equilibrium of Control in Automated Vehicles: Driver Engagement Level and Automation Capability Levels*. Proceedings of the 4th IFAC Workshop on Cyber-Physical & Human-Systems. Houston, TX: IFAC.

EAAIB (2022). Investigation Report on Accident to the B737-MAX8 Reg. ET-AVJ Operated by Ethiopian Airlines, 10 March, 2019. Report No. AI-01/19.

ECAA (2019). Aircraft Accident Investigation Preliminary Report, Ethiopian Airlines Group, B737-8 (MAX) Registered ET-AVJ, 28 NM South-East of Addis Ababa, Bole International Airport, March 10, 2019. Addis Ababa: Ethiopian Civil Aviation Authority

Gentner, D. & Stevens A. (1983). *Mental models*. Hillsdale, NJ: Erlbaum.

Leveson, N.G., & Turner, C.S., (1993). An investigation of the Therac-25 accidents. *Computer, 26*, 7, pp. 18-41.

NASA (2011). *Technical support to the National Highway Traffic Safety Administration (NHTSA) on the reported Toyota Motor Corporation (TMC) unintended acceleration (UA) investigation*. National Aeronautics and Space Administration: Langley, VA.

Nielsen, J. (1994). Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods, John Wiley & Sons, New York, NY

Norman A. & Draper, S. (1986). User centered system design. Hillsdale, NJ: Lawrence Erlbaum Associates.

NTSB (2019). System Safety and Certification Specialist's Report. National Transportation Safety Board, NTSB ID No.: DCA19RA017. Washington, DC.

NTSC (2019). Final Report (Aviation Division). Boeing 737-8 (MAX); PK-LQP, Tanjung Karawang, West Java, 29 October 2018. PT. Lion Mentari Airlines. Jakarta, Indonesia: National Transportation Safety Committee.