Zooming out and zooming in: Synthesising and analysing human-machine interaction in the cockpit

Don Harris

Coventry University

Overview

- Design Induced Error
- The Regulation
- Acceptable Means of Compliance
- Predicting Error

DESIGN INDUCED ERROR

Or, someone else's lack of thought becomes my problem…

Design Induced Error

- Typically, these are errors induced by poor interface designs that:
  - Encourage you to do the wrong thing, or
  - Make doing the wrong thing easier than doing the right thing, or
  - Make it unclear what to do or what mode you are in

Encouraging You To Do The Wrong Thing

Pushing on a handle is required to open these doors when going in one direction

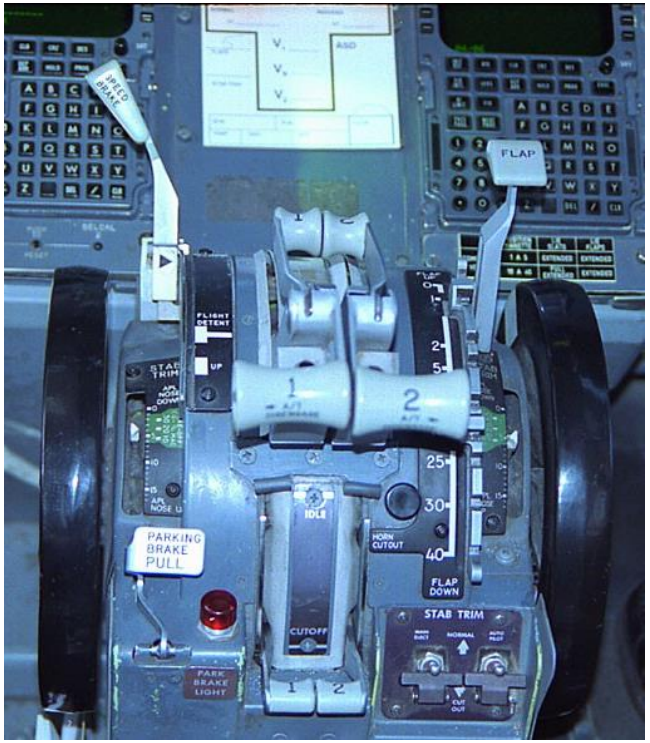
Encouraging You To Do The Wrong Thing

Encouraging you to set vertical speed when you meant to set flight path angle...

Make Doing The Wrong Thing Easier Than Doing The Right Thing!

To set the alarm on this kitchen timer for less than 15 minutes you need to turn it past 15 minutes and then turn it back otherwise it doesn't go off!

Make Doing The Wrong Thing Easier Than Doing The Right Thing!



Aborting a take-off under autothrust control at a ground speed of 40 kts or less in a Boeing 737-300/400…

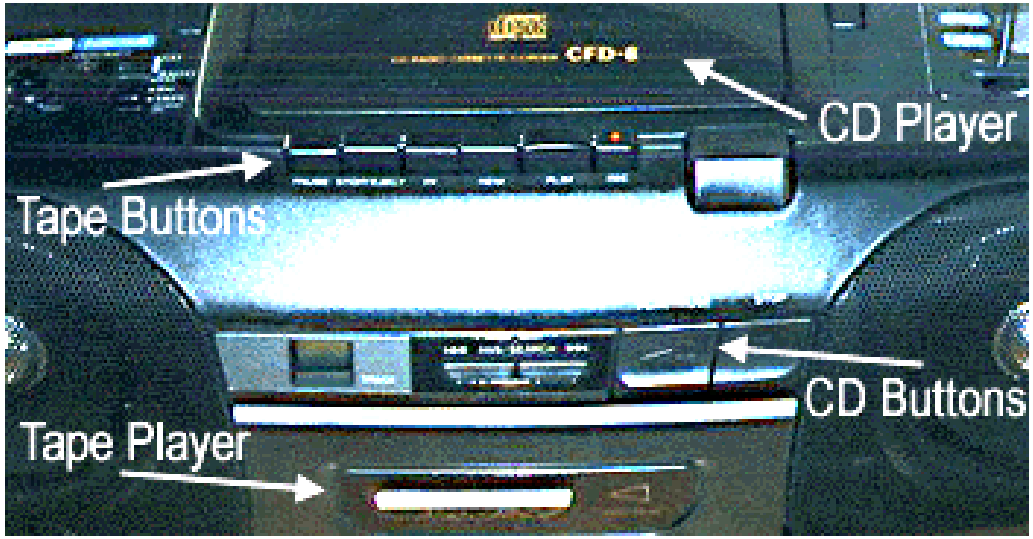
Throttles back, apply thrust reversers and brakes…

Won't work!

Make Doing The Wrong Thing Easier Than Doing The Right Thing!

Just retarding the throttles below 64 kts will have no effect. The autothrottles will only disconnect in this manner above 64 kts when the automatic system shifts to ‘throttle hold’ mode. Below this speed the autothrottles must be disconnected manually.

Make It Unclear What To Do



CD player controls are next to the tape deck, and *vice versa*

Making it unclear what mode you are in

Automatic Mode Transitions - McDonnell Douglas MD 82

- If the ILS signal is lost during approach the aircraft will transition from approach mode to vertical speed mode at the same descent rate
- This should allow it to be in the correct position when the ILS signal is reacquired
- But, V/S mode will make the aircraft maintain a constant rate of descent until the crew intervenes
- Reversion to V/S mode may not cause the aircraft to be on the correct ILS glideslope profile

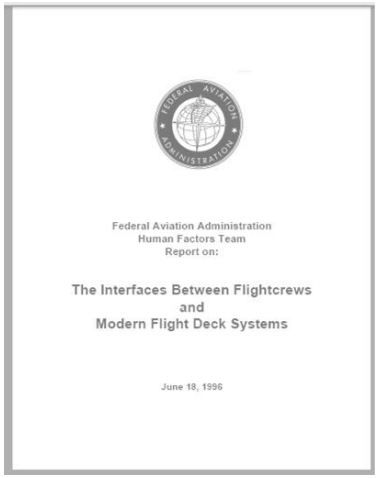
Making it unclear what mode you are in

China Northern Airlines MD-82 accident in Urumqi, China

- Autopilot disconnected during ILS approach resulting in mode transition to V/S mode at 800 feet/per minute
- Crew did not notice the mode transition
- Aircraft crashed short of the runway

FAA Human Factors Team Report (1996)

- 51 recommendations came out of the report, including (from a regulatory perspective)
  - 'The FAA should require the evaluation of flight deck designs for susceptibility to design-induced flightcrew errors and the consequences of those errors as part of the type certification process'
  - 'The FAA should establish regulatory and associated material to require the use of a flight deck certification review process that addresses human performance considerations'


Federal Aviation Administration
Human Factors Team
Report on:

The Interfaces Between Flightcrews
and
Modern Flight Deck Systems

June 18, 1996

THE REGULATION

Seven years of my life I will never get back…

Human Factors Certification on the Commercial Flight Deck

- EASA in 2007 (and FAA in 2011) introduced a new airworthiness requirement in Part 25:
- It was specifically aimed at reducing the incidence of design induced error on the flight deck
  - CS/FAR 25.1302: Installed systems and equipment for use by the flight crew

The Rule CS 25.1302

Installed systems and equipment for use by the flight crew

- This paragraph applies to installed equipment intended for flight-crew members' use in the operation of the aeroplane from their normally seated positions on the flight deck. This installed equipment must be shown, individually and in combination with other such equipment, to be designed so that qualified flight-crew members trained in its use can safely perform their tasks associated with its intended function by meeting the following requirements:

The Rule CS 25.1302

- (a) Flight deck controls must be installed to allow accomplishment of these tasks and information necessary to accomplish these tasks must be provided.
- (b) Flight deck controls and information intended for flight crew use must:
  - (1) Be presented in a clear and unambiguous form, at resolution and precision appropriate to the task.
  - (2) Be accessible and usable by the flight crew in a manner consistent with the urgency, frequency, and duration of their tasks, and
  - (3) Enable flight crew awareness, if awareness is required for safe operation, of the effects on the aeroplane or systems resulting from flight crew actions.

The Rule CS 25.1302

- (c) Operationally-relevant behaviour of the installed equipment must be:
  - (1) Predictable and unambiguous, and
  - (2) Designed to enable the flight crew to intervene in a manner appropriate to the task.
- (d) To the extent practicable, installed equipment must enable the flight crew to manage errors resulting from the kinds of flight crew interactions with the equipment that can be reasonably expected in service, assuming the flight crew is acting in good faith. This sub-paragraph (d) does not apply to skill-related errors associated with manual control of the aeroplane.

Unique aspects of this rule

- It is a task-based rule
- It still addresses the basic fabric of the aircraft
  - This is what part 25 is about
- It is designed to address pilot error of the flight deck resulting from poor interface design

Rationale for this task-based approach

- Activity on the flight deck proceeds on a task-by-task basis (as does human factors design itself)
- Pilots interact with several systems when performing a task, thus inconsistencies in interfaces are much more obvious them
- Many human factors problems lie not within an individual regulation but between regulations

The view of error in certification

- Certification is really aligned with the ‘old’ Safety I view
  - It is about avoiding error – constraining the system to avoid it lapsing into an unsafe state
  - It isn’t really about making things usable
    - In fact inserting safety barriers can make things frustrating and unusable!
- Safety II is about normal performance
  - This is where usability comes in

ACCEPTABLE MEANS OF COMPLIANCE

You will obey, resistance is futile

Barrier Analysis

- The approach implicit within the regulation effectively requires the trapping of predictable errors or their mitigation
- However, to insert barriers you need to know what you are trying to protect against
- A way of achieving this at the initial design stages is via formal error prediction techniques

View of Error

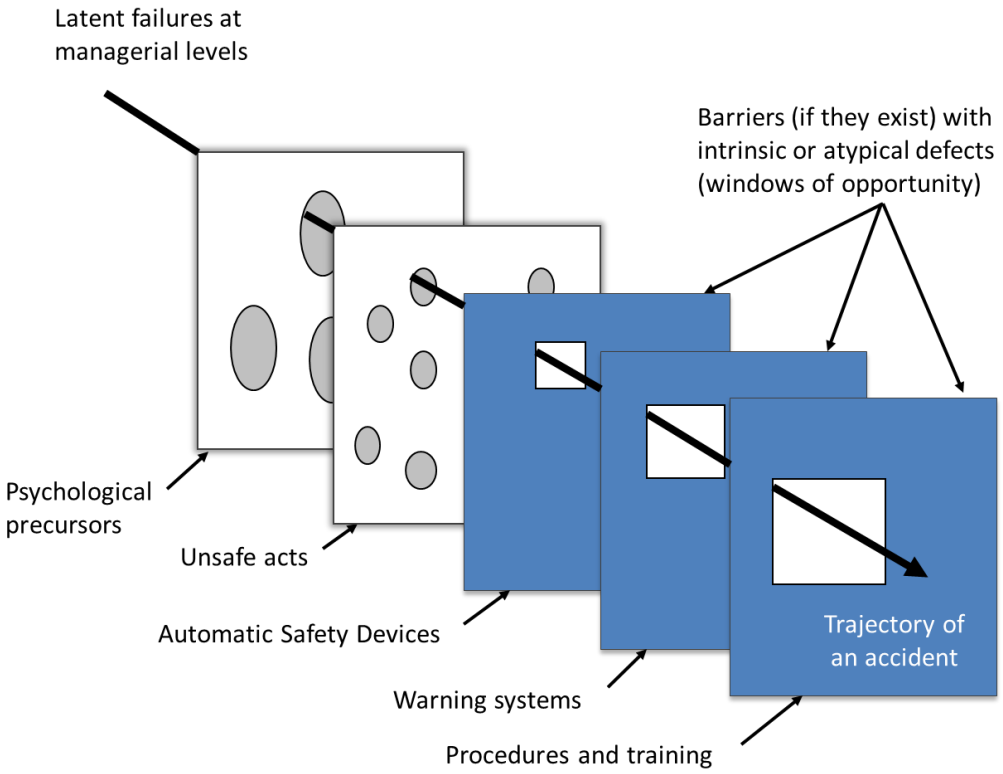
- Formal error analysis immediately implies that there are aspects of human performance that you want to avoid and you can predict
  - Aspects of human performance variability where it strays beyond acceptable system-defined bounds
- Defining human error as a judgement made in hindsight is not useful from the perspective of interface design

View of Error

- Within an interface design context this requires a (very) old definition of error
  - *Errare (Latin)* ‘To wander’ (from the path)
- A user’s route through an interface is a prescribed path of allowable actions to perform a task
  - You don’t want them to wander down unmarked paths…

Trajectory of an Accident (from Reason)

- Preventing design induced error is not about producing good performance: it is about avoiding bad performance



MIL-STD-882D

- *Design for minimum risk* – Eliminate the hazard from the system if possible: design the system to eliminate the particular failure mode
- *Incorporate safety devices* – Design into the system automatic devices which, when a specified hazard, prevent the system from entering a dangerous state
- *Provide warning devices* – These should activate early, leaving the operator time to stop a critical system state developing
- *Develop procedures and training* – Provide adequate training in procedures to operate in a safe manner

PREDICTING ERROR

When running fast it is always better to identify brick walls by sight rather than by touch…

My Father

A Forward Looking Approach

- Errors can be predicted using formal methods
  - but this approach is limited to aspects of error associated with design
    - Design of equipment
    - Design of procedures (including aspects of training)
- Organisational roots of error can't really be predicted in this way

The role of the Controller Interface

- The controller's interface is the main tool by which control and management of the airspace is exercised
  - It is the place where decisions are implemented
- It needs to facilitate these actions and (if possible) check them
- The interface also needs to promote awareness
  - Help avoid errors of omission!

Formal Methods

- Best used at design stages so that potential error modes can be removed
  - Can be used after equipment (interface) design has been finalised but only to modify procedures
- When used properly, equipment design and procedures are undertaken almost simultaneously
  - Driven from the initial requirements and task analysis

Formal Methods

- All start with a task analysis…
- Followed by an interface analysis in conjunction with the required tasks to identify potential weaknesses
- There are actually very few basic errors that can be made
  - All errors in this case refer to what is required by the system
    - NOT a cognitive approach to error

Design Implications

- *Avoiding* error via interface design immediately implies restricting performance in some way
- Then we face the 'Catch-22' issue in equipment design:
  - You can make things simple and easy to use with little error potential but reduce flexibility, or
  - You can increase flexibility, but also increase system complexity and the potential for error.

CONCLUSIONS

Nearly finished, just a few more minutes…

A Certification view of Error

- System Design and Certification adopt very much an older view of error
  - Something defined by the system; behaviours to be eliminated or constrained
- Error is a judgement made in foresight, not hindsight
- Not a total solution - operates in conjunction with other views
  - Complements Safety II – does not compete with it

Many Thanks for your Attention