Is our current certification process a threat to safety innovation?

Huijbrechts, Erik-Jan A. M.; van Paassen, M.M.

Publication date
2021

Document Version
Final published version

Published in
21st International Symposium on Aviation Psychology

Citation (APA)
Huijbrechts, E-J. A. M., & van Paassen, M. M. (2021). Is our current certification process a threat to safety innovation? In *21st International Symposium on Aviation Psychology* (pp. 358-363)

IS OUR CURRENT CERTIFICATION PROCESS A THREAT TO SAFETY INNOVATION?

Erik-Jan A.M. Huijbrechts
Airline Pilot and Independent Aviation Safety Researcher
Sassenheim, the Netherlands
M.M. (René) van Paassen
Associate Professor Delft University of Technology
Delft, the Netherlands

Certification is an important process in the aviation industry. The certified status of aircraft, aircraft equipment and procedures is often regarded as a guarantee for safety. However, if shortcomings emerge during operation, this certified status can prevent improvement of the design. In addition, to develop and certify new equipment, it is often easier to modify existing, certified equipment than have a full certification of a new system. Doing so, safety problems may be overlooked. In this paper, a link is made between the certification process and organizational safety of both manufacturers of aircraft or aircraft equipment and airline companies.

To guarantee safety in aviation, equipment and procedures are certified by aviation authorities. In this process, the manufacturer needs to demonstrate that the equipment and procedures fulfil the prescribed airworthiness regulations and/or achieve the required safety level. Due to the cost and effort associated with certification, manufacturers choose to re-use previous certification efforts rather than seek new approval when developing newer versions of aircraft. At this point, the certification process can become a barrier to safety innovation. While the aircraft is modernized to meet new demands, its equipment, systems and procedures will be largely remain based on legacy versions, with only incremental improvement. New automation is introduced piecewise on the flight deck, which can result in situations where isolated systems provide counteracting inputs. When new systems are introduced it may be profitable to consider them as just a modification on an already certified system.
Pilots and other operational personnel may recognize the possible dangers in systems and procedures. They may ask for improvement, however, in general, company management is reluctant to deviate from prescribed procedures for liability reasons. Furthermore, manufacturers are wary of proposed changes and will try to maintain the certified status of existing equipment and procedures. This paper identifies situations where the certified status of equipment and procedures or the certification process has hindered potential safety improvements, and invites ideas for improvement of the certification process.

Influence of Certification on Systems and Procedures

Systems and procedures that have passed the certification stage tend to remain unchanged over time, even when shortcomings may become known. The certified status of a system or procedure is often used as an excuse not to correct imperfections or even known safety hazards. This applies also when new variants or aircraft types are developed and certified on the basis of older models. Examples can be found that have lasted for decades. Sometimes guidance of authorities is required in order to correct an unsafe situation. Gradual introduction of new automation may result in unexpected safety problems that are overlooked in the certification

process. Economic pressures during the design process may shift the design goal from developing a new and safe system to, a development process where re-utilization of existing certified systems and components is maximized. This inevitably leads to compromises, as an already certified system is squeezed into fulfilling a new purpose.

Certified Systems

Systems that have passed the certification stage are often used in newer variants or types of aircraft without improvement on known deficiencies. The fuel crossfeed indication wiring in Fokker 70/100 and B737 aircraft can serve as an example.

The fuel crossfeed indication wiring. Both in the Fokker 70/100 and the Boeing 737 PG/NG, the fuel crossfeed indication light is wired over the Circuit Breaker (CB) that protects the Fuel Crossfeed valve. This design may cause confusion to pilots when a crossfeed operation is in place and the CB trips with the crossfeed valve not closed. In that case, the fuel transfer between tanks continues, while the indication light is extinguished suggesting that the crossfeed valve is closed. As a result, pilots have diverted their flights assuming there was a fuel leak. Manufacturers did not inform pilots about this in their Flight Crew Operations Manual (FCOM). Procedures for handling crossfeed problems were not suitable to cope with this situation either. Furthermore, the wiring design was not included in maintenance training manuals for technicians; it is only incorporated in wiring schematics. When Fokker was alerted to this safety related issue, they put some engineering effort into the design, however, this did not result in a modification as at that time the factory had already stopped the build of new aircraft. After alerting Boeing that the procedure was not correct, a change was made to the procedure, better clarifying the state of the system to pilots. Only in the B737 MAX, a separate CB for indication is installed, entirely solving the problem.

Certified Procedures

Procedures that have passed the certification stage and are incorporated in a manufacturer's Flight Crew Operations Manual (FCOM) or Aircraft flight Manual (AFM) remain unchanged over time, even if it may be clear to many operators (pilots) and the manufacturer that the procedure is not correct or optimal. Also when newer aircraft models are introduced, the procedure may remain unchanged. The Boeing stall recovery procedure can serve as an example.

The Boeing stall recovery procedure. The old Boeing recovery procedure for a stall or an approach to stall situation requires the operator (pilot) to first increase thrust and then reduce pitch attitude. When a stall is imminent, the stalled condition can be aggravated if the thrust on underwing mounted engines is increased. This is particularly prominent with the installation of new and large engines on later versions of the Boeing aircraft. Although the problem was recognized by Boeing, and a note to this effect was added in the Flight Crew Training Manual (FCTM), the procedure remained unchanged in the FCOM from the introduction of the first Boeing 737 models in 1968 until the Boeing 777. Only after several stall related crashes in 2009 and the issue of Advisory Circular 120-109 (Federal Aviation Administration, 2012), the procedure was corrected. The new stall recovery procedure for all Boeing aircraft models requires the operator (pilot) to decrease pitch attitude before increasing thrust.

Gradual introduction of new Systems

When new systems or automation is added to already certified equipment the combination may result in unexpected safety issues. The combination of actions of autothrottle and autopilot, that played a role in the Turkish Airlines crash at Amsterdam can serve as an example.

The Turkish airline crash. The crew of TK1951 was forced into a rushed approach. Through a defect of the radio altimeter, incompatible actions of the autothrottle and the autopilot systems lead to an aerodynamic stall and a thrust position that made it difficult to recover from this stalled condition (The Dutch Safety Board, May 2010). This crash also initiated a review of the stall recovery procedure.

Certification of new Systems and Procedures

When new systems are to be developed by a manufacturer, it is often easier to adapt an existing, certified system to serve a new purpose than to have a newly developed system certified. This is true for aircraft models, that are equipped with new engines and technology, to keep up with the demand for better efficiency and to comply with new regulations. It is also true for aircraft systems. Maintaining the current certification is often set as a constraint in the development of a system. This goal may invite for legal shortcuts rather than a thorough operational evaluation of the system. The recent safety problems with the Boeing 737 MAX MCAS (Maneuvering Characteristics Augmentation System) can serve as a good example.

The Boeing 737 MAX MCAS system. The Boeing 737 MCAS system was introduced on the B737 MAX to compensate for the additional pitch up effect that resulted from the modified placement of newer and larger engines on the 737 airframe. The system was supposed to make handling of the MAX aircraft similar to its predecessor, the B737 NG, and provide a safety catch in low speed situations when high thrust is delivered by the engines. To reduce efforts in the certification process, the MCAS was presented as a modification of the previously certified Speed Trim System (STS) in the B737 PG and NG variants. (DeFazio & Larsen, 2020) By using the previous system as a basis for certification, only a limited evaluation was needed, and a thorough evaluation of all safety aspects associated with a new system was avoided. Presenting the new MCAS as an incremental development of the STS also posed constraints on the design process, limiting the ways in which the two system could differ. Regarding procedures and pilot training, it was assumed that pilots would be able to compensate for possible malfunctions using the already established runaway stabilizer procedure also used in the older variants of the 737 airframe. (van Paassen et al., 2021) By stressing the similarity between the aircraft, the initial training requirements for transitioning to the new aircraft could be limited to computer-based instruction.

Influence of Certification on Organizational Safety

Companies in aviation, be they operators or manufacturers, generally have multiple stakeholders, and to each of these certification plays a different role. The management (blunt end) of an aviation related company is often focused on process and legal aspects, and to management the certified status of a system or procedure may be regarded as a guarantee for safety. The certified status may be used as an argument to quell concerns from actors at the sharp end (operators and designers) of the organization about safety. (Rantanen & Huijbrechts, 2021) There is a difference in how management attitude can affect organizational safety in manufacturing and airline companies.

Manufacturers

A manufacturer may use certification as a target in their design process of an aircraft or aircraft system. This invites shortcuts, like using the certified status of existing systems to facilitate the certification process of a new system. Effort in the design process must now be spent to re-use and adapt existing components and procedures, while at the same time the safety review is limited because existing certification efforts can be re-used. The cumulative effects of stepwise adaptation in multiple generations of aircraft on the operation can then easily be overlooked. Once certification is ensured, the accumulated safety record for older generations becomes part of the renewed airplane's reputation, making it difficult for concerns from technical and operational experts to gain traction.

Airline Companies

Airline companies may be adversely affected in their safety level when operating equipment and using procedures that were developed without a thorough safety screening during certification. Although flight deck procedures preferably must be tailor fit to the circumstances within which the airline company works (Barshi et al., 2016), many airline companies choose to trust and present manufacturers' procedures without adaptation to their operators (pilots). In smaller companies, the knowledge or assets to adapt procedures may not be available. In bigger companies, the fear for liability issues is often greater than the urge to improve safety by issuing company procedures. When a "process and legal" mindset is prominent in an airline company, the combination of unadapted procedures and a rigid procedure-oriented operation may impair organizational safety. (Rantanen & Huijbrechts, 2021)

Evaluation

Certification was intended to assure that systems and procedures fulfilled legal requirements and thus provided a certain safety level. In the past, the certified status of equipment and procedures has prevented improvement on the safety level. Clearly, the cost of certification and the effort invested in design of new procedures and systems must somehow be balanced with the yields from operation, both for manufacturers and operators. Re-using existing knowledge and certification is often key to profitability and ultimately success of the company. However, a means to identify and follow up on safety issues and prevent a slow drift into unsafety is important to long-term profitability. Indeed, as the saying goes, "if you think safety is expensive, try an accident…"[1]. With the practice of re-using designs, procedures and certification efforts, a means must be available to stop cumulation of small changes from resulting in real threats to safety. This drift is often first visible to the operators at the sharp end, but it is the responsibility of the operators at the blunt end, i.e., management, and certification authorities, to detect and amplify these alarms. When the management of a company is not product and operation oriented and instead focusses on processes and legal aspects, poor communication between sharp- and blunt end of the organization can have a detrimental effect on organizational safety (Rantanen & Huijbrechts, 2021). Hence, a mechanism must be found to convince management that the certified status does not relief a company from its responsibility for safety of a system, procedure or operation. This may require reviewing the certification process.

Conclusions

If a system or procedure is certified, it tends to remain unchanged although it is known that changes can improve the safety level. The certified status thus prevents safety improvement.

Gradual addition of new systems or automation to certified equipment may introduce new safety hazards that may remain concealed during the certification process. Attention must be given to signals from the operation when safety hazards emerge.

Certification can be used as a target in a design process. This goal invites for adaptation of the design process, possibly trading safety for a speedier and less costly certification.

The certified status of an aircraft, aircraft system or procedure does not absolve a manufacturer from its responsibility for safety of that aircraft, aircraft system or procedure.

Using certified manufacturers equipment and procedures does not absolve an airline company from its responsibility for a safe operation.

[1] Alternatively attributed to Stelios Haji-Ioannou or Trevor Kletz

Acknowledgements

I want to thank Esa Rantanen and Maartje Huijbrechts for critical reading, hints and tips. This report is not initiated by, nor does it reflect the views of my employer.

References

Barshi, I., Mauro, R., Degani, A., and Loukopoulou, L., *Designing Flightdeck Procedures,* NASA/TM-2016-219421, October 2016
§ 2.1 Step 1: Determining When Procedures Need to be Designed or Modified

DeFazio, P & Larsen, R, *Final Committee Report*
The design, Development & Certification of the Boeing 737 MAX, September 2020
Chapter 5 Maneuvering Characteristics Augmentation System (MCAS)

Federal Aviation Administration, *Stall and Stick Pusher Training,* Advisory Circular 120-109 (2012) (later replaced by:) *Stall Prevention and Recovery Training,* AC 120-109A (2015)

van Paassen, M.M. (René), Reitsma, J.R., Huijbrechts E-J.A.M., Borst, C. and Mulder, M.
The Skill Assumption – Over-Reliance on Perception In Error Analysis
Conference Paper, ISAP 21, may 2021

Rantanen, E. & Huijbrechts E-J.A.M., *Organizational Safety in Airline Operations*
Conference Paper, ISAP 21, may 2021

The Dutch Safety Board, *Crashed during approach, Boeing 737-800, near Amsterdam Schiphol airport, 25 February 2009*, May 2010 p.52