B-737 MAX AND THE CRASH OF THE REGULATORY SYSTEM

Tommaso Sgobba

International Association for the Advancement of Space Safety
Kapteynstraat 1 2201BB Noordwijk, The Netherlands
Email: iaass.president@gmail.com

INTRODUCTION

The Boeing B-737 MAX accidents represent a major failure of the aviation regulatory system established in December 1944 with the signature of the Chicago Convention that started the International Civil Aviation Organization (ICAO). The ICAO SARPs (Standards and Recommended Practices) on which national regulations are based, served well the purpose of promoting safety and international air transport, but although regularly updated they became progressively antiquated in their essence and inadequate for integrating new technologies. There have been calls to reform the system to allow more innovation and less bureaucracy, and studies warning about the deficient approach for certifying new computer-based systems [4].

Compliance enforcement by the national regulatory bodies has become also progressively less effective because of the ever-widening skill gap between regulators and industry. The B-737 MAX accidents have badly shaken trust and confidence of foreign regulators, on which mutual recognition of airworthiness certifications is based, thus making impossible to leave the stone of the current system reform unturned.

The key questions are: 1) should prescriptive requirements, on which rules-based certification is based, be abandoned in favor of performance requirements and risk-based certification? 2) are purely quantitative performance requirements meaningful? 3) how can aviation regulatory bodies acquire and maintain the support of most current technical and scientific skilled resources needed to move from rules-based certification to risk-based certification?

1.0 THE ACCIDENTS

Recently two brand new Boeing 737 MAX-8, one of Lion Air of Indonesia and the other of Ethiopian Airlines, crashed within months killing 346 people on board. In both accidents the airplane was gaining altitude shortly after take-off, and apparently the pilots tried persistently to maintain the angle of attack (AOA) (Fig.1) to gain altitude at the planned rate, whilst the on-board Maneuvering Characteristic Augmentation System (MCAS), i.e. an automatic stability enhancing system embedded in the plane's autopilot, forced the airplane to nose-dive to catastrophic crash.

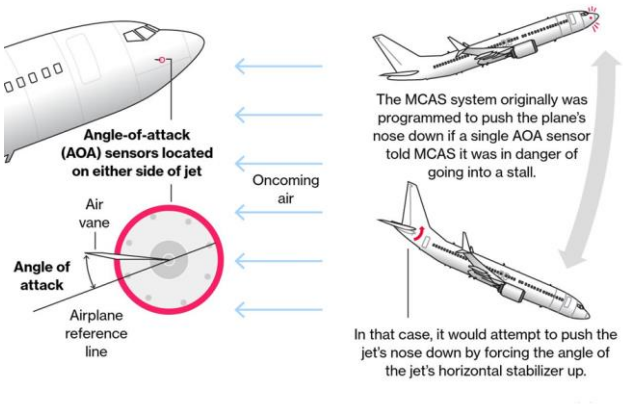

Fig. 1 Angle of Attack Sensors
Credit: Boeing/Mentourpilot

2.0 WHY A MCAS ON B-737 MAX?

On the B-737 MAX there are two AOA sensors, but only one feeds data into the MCAS. In both accidents this sensor seems to have malfunctioned driving the software to command the nose-down maneuver that the pilots were unable to override.

Although described by Boeing as a stability enhancing system, the MCAS ultimate function is to prevent "stall", one of the most dangerous phenomena in aviation. Stall is a loss of lift of the wing either due to very low speed or by exceeding a critical angle of attack of the wing relative to the airflow (Fig.2). The lift of a wing is driven by the aerodynamic lift coefficient of the airfoil (the shape of the wing cross-section) which varies with the angle of attack and drops when the

airfoil's critical angle of attack is exceeded. The engines of the Boeing 737 MAX-8 have a better fuel consumption than previous 737 versions, but a larger cross section and they are heavier.

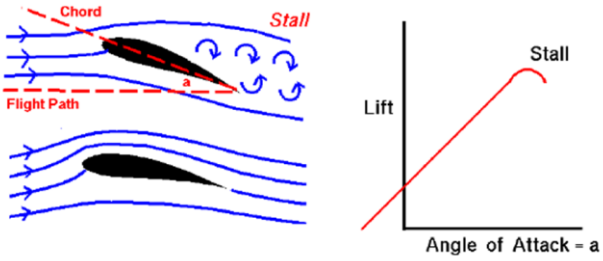

Fig.2 Angle of Attack and Stall
Source: adapted from NASA

It seems that during development to limit the modifications, Boeing decided to accommodate such larger and heavier engines a bit higher and a more in front of the wing than previous 737 versions. As the Center of Gravity (CG) of the airplane was moved forward, the nose-down moment (wing pitching moment) increased.

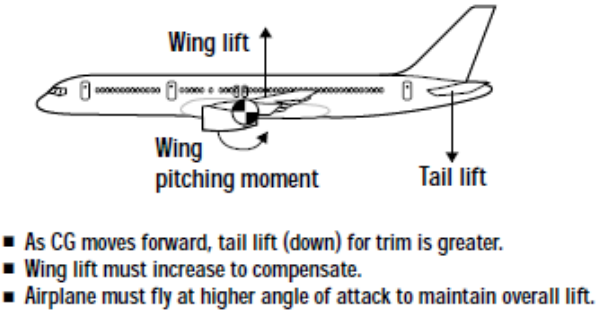

Fig.3 Wing Pitching Moment, Wing Lift and Tail Lift
Credit: Boeing [2]

The downforce on the horizontal tail required to trim (i.e. put the airplane in equilibrium: airplane total pitching moment = zero) is increased (Fig. 3). This means that the wing must provide enough lift to compensate for the download on the tail in addition to the weight of the airplane. Therefore, the airplane must fly at a higher angle of attack, but this is a stable condition [1]. There are two other conditions, which in accordance to the press were the main reasons for Boeing to include the MCAS, respectively a wing pitch-up moment at very lights weights and full aft CG, and wing pitch-up moment in steep turns, both concurrently with higher vertical component of the thrust (additional lift) generated by the new engines[3][5].

3.0 THE UNNOTICED REVOLUTION

The external appearance of an airliner except for larger engines and winglets has not changed very much in the last 50 years. Airplanes like Boeing 737 and 747, which first flew in the late sixties, look still very much the same but inside the cockpit and in many places out of passenger's view a big revolution took place. On a modern airliner there are hundreds of computers disseminated everywhere that interact with each other without the pilot being aware of this interaction. However, the way a civil aircraft is certified, which means the rules it must follow and how compliance with such rules is verified by the aviation authority have not changed very much over the last 70 years. It is exactly in such obsolete regulatory environment that some of the root causes of the B-737 MAX accidents lay.

Civil aircraft airworthiness certification is based on two tenets: use of prescriptive safety standards in design, and regulatory inspection and testing to ascertain compliance with rules. It is an axiom that prescriptive safety standards are based on experience and therefore do not anticipate technological progress. In other words, safety design rules in aviation are established reactively, and not proactively.

The aeronautical industry has been always very cautious in adopting new unproven technologies. This approach worked well for decades until size, complexity, crew workload and costs started demanding the ever-increasing use of electronics and computers on board. First fly-by-wire, then electronic engine control, digital autopilot/autothrottle, flight director, and many more automated systems. How did industry cope with safety? Essentially through abundant redundancies and back-ups. What did the regulators do on their side in terms of safety requirements not having anything to refer to? They established and "equivalent safety" policy principle consisting in treating those novel systems on a case-by-case basis, so-called "special conditions", and replacing (unavailable) prescriptive design rules with quantitative performance requirements to represent the overall acceptable level of risk. Such level was defined depending on the functional safety criticality of the system (e.g. $1x10^{-9}$ for catastrophic consequences in case of failure). The logic that was followed to define the acceptable levels of safety is very simple and ultimately linked to reliability. It is explained as follows: "*Taking into consideration the accident rate in commercial (occidental) aviation in the 10-year period from 1970 to 1980 a rate of catastrophic accidents a little less than 1x10-6 flight hours was detected…about 10 percent of the catastrophic accidents could be*

attributed to system failures. Hence the portion of catastrophic accidents attributed to systems was of the order of 1x10-7 flight hours. Starting from the arbitrary hypothesis that a commercial large aircraft could present 100 hazards (potential failure conditions) leading to a catastrophic effect, it follows that, for each system, the acceptable probability of catastrophic failure is less than 10-9 flight hours" [2].

The level of failure tolerance and the detailed safety features of the design (i.e. redundancies and inhibits) are left to the manufacturer to decide. What he is required to do is to perform first a function criticality analysis, and then a reliability analysis to demonstrate that the system probability of failure is lower than the applicable quantitative risk level. The MCAS was classified by Boeing as criticality "hazardous" (which is one level below "catastrophic") with associated risk level of "extremely remote", i.e. 10-7 for a large airplane. A failure condition is classified as "hazardous" if it would *reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be: a) a large reduction in safety margins or functional capabilities; b) physical distress or higher workload such that the flight crew cannot be relied on to perform their tasks accurately or completely, or c) serious or fatal injury to a relatively small number of occupants* [2].

Demonstrating system safety to the regulatory authority for novel systems is essentially a hardware reliability computational task, which does not include neither software nor human interaction due to difficulties to model them from the reliability standpoint. There is also a qualitative assessment of how the design prevents that redundancies are defeated by common causes. Instead, for software a "fault-avoidance" approach was taken by requiring different levels of rigor in development and testing depending on criticality. Human interactions continued to be treated as a training issue. As a result, the hardware-software-liveware system unity was split to follow the logic of conventional aviation subsystems, as if the interaction between human and automatic system is the same of human and conventional mechanical or electrical instrument, and as if making a software "safe" is solely a matter of process quality control. Overall, the certification process administered by the regulators continues to be very much inspection and testing oriented, with the difference that for non-conventional systems like the MCAS it has shifted from hardware inspection to checking that the manufacturer has performed criticality and reliability analyses according to best-practices, i.e. paperwork inspection.

4.0 MOVING TO A GENUINE RISK-BASED CERTIFICATION SYSTEM

"*According to the FAA's own website, the aviation environment has reached a level of complexity where it cannot achieve further safety improvements by following a purely rule-based approach. Consequently, the FAA's stated desire to focus certification resources based on risk rather than solely box-check compliance against all rules. We applaud and encourage the FAA's movement to a risk-based certification analysis*" [6]

Moving from the current rules-based certification system (plus acceptable level of risk for "special conditions" discussed above), to a genuine risk-based certification system would unleash massive innovation in aviation and potential cost reductions, however it requires an upgrade of skills and organizational set-up which is not sustainable by current regulatory bodies. It would have also a major impact on ICAO, which relies on a policy of harmonization of prescriptive safety requirements for mutual recognition of airworthiness certificates. To understand the terms of the problem, the differences between designing and certification in one case and in the other (i.e. prescriptive vs. performance) needs to be explained.

The story of the Titanic accident helps to point out advantages and disadvantages of rules-based design. In the early hours of 15 April 1912, the RMS Titanic struck an iceberg on her maiden voyage from Southampton, England, to New York, and sank. A total of 1,517 people died in the disaster because there were not enough lifeboats available. During the Titanic construction Alexander Carlisle, one of the managing directors of the shipyard that built it had suggested using a new type of larger davit, which could handle more boats thus giving Titanic the potential for carrying 48 lifeboats providing more than enough seats for everybody on board. But in a cost cutting exercise, the customer (White Star Line) decided that only 20 lifeboats would be carried aboard thus providing capacity for only about 50% of the passengers on the maiden voyage. This may seem a carefree way to treat passengers and crew on-board, but as a matter of fact the Board of Trade regulations of the time stated that all British vessels over 10,000 tons had to carry 16 lifeboats. The (prescriptive) regulation had become obsolete within a short period of time when at the beginning of the 20th century ship tonnage raised up to Titanic's 46,000 tons. Furthermore, the RMS Titanic was believed to be unsinkable by design, therefore, why to worry about lifeboats?

4.1 Prescriptive Standard

A prescriptive standard specifies design requirements, such as materials to be used, how a requirement is to be achieved, or how an item is to be fabricated or constructed, such that the item can be considered safe. A prescriptive requirement is an explicitly required design solution for an implicit safety goal. Generally, prescriptive requirements are very useful at the bottom of the product tree (parts levels, bolts, nuts, etc., tanks, batteries, etc.). Prescriptive standards (also called design standards or rules-based standards) are easier for developers and operators to implement; easy to check compliance with for the safety authority; schedule efficient: just read and transpose into design; and there is no need (for industry) to think "is this good enough".

The disadvantages of prescriptive standards is that they may be effective in some cases but not in other cases; may prove to be more costly than other equally effective solutions; can inhibit innovation or become obsolete; are reactive (reviewed and changed post mishap), may lead to over/under-engineering; and may nurture a compliance mindset rather than a safety mindset. The underlying motivation for prescriptive requirements is to prevent circumvention by avoiding any subjective interpretation in the implementation as well as in compliance verification. Violation of a requirement can be unequivocally determined by a simple inspection. Most safety standards in use in aviation and other "evolutionary" industries are the result of lessons learned from incidents and accidents, and slow technological advancement. In contrast, there are industries in which building by following past experiences is not possible, because the system is completely new, highly safety-critical (e.g. nuclear power plants) and/or extremely expensive.

4.2 Performance Standard

A performance standard specifies the outcome required (i.e. acceptable safety level) but leaves the concrete measures to achieve that outcome up to the discretion of the designer. How performance standards are designed and how they are implemented and enforced matters greatly

Performance standards could be *qualitative* and/or *quantitative* with reference to the acceptable safety level. *Quantitative* performance requirements can be distinguished between those for which compliance can be demonstrated by *prediction* (e.g. system failure), and those for which compliance can be demonstrated by *measurement* (e.g. actual measurement of air contaminants). *Qualitative* performance requirements are expressed in terms of level of fault/failure tolerance.

By focusing on outcomes, performance standards give to developers flexibility and make it possible to find lowest-cost means to achieve compliance. Performance standards can generally accommodate technological change and the emergence of new technology driven hazards in ways that prescriptive standards cannot. Performance standards can be imprecise when the requirements are too loosely specified or questionable when compliance will be assessed by quantitative predictions (e.g. reliability analysis). Sometimes uncertainty is willingly injected into a performance standard just because of the need to make it as generic as possible.

The correct implementation of safety performance standards requires training and familiarity of the project team such to avoid misinterpretations of the requirements (too loose, too tight), and requires the execution of hazard analyses at system level (hardware+software+liveware).

Sometimes, guidelines on requirements interpretation and accepted means of compliance can help the design team. In any case, the key concept in implementing a performance safety standard is that it cannot be used directly for design. It is through a risk-based design process (i.e. iterative hazard analyses) that detailed design features and operational procedures are selected. A risk-based design process is fundamentally different from the safety assessment required by the aviation regulations for non-conventional aviation systems [4]. Performance requirements are tailored through hazard analysis of the entire system in an integrated fashion, and modulated depending on consequence severity.

Verifying the conformity of a system with performance requirements is much more complex than for prescriptive requirements. Today's aviation regulatory bodies difficulties in terms of skilled resources will be multiplied with risk-based certification. While objective evidence of compliance with prescriptive requirements can be assessed by an inspector, assessing compliance with performance requirements necessitates an independent multi-disciplinary review team with design and operations skills and competences equal or even better than those of the project team. We can say that measures to evaluate and ensure conformity with performance standards are of as much or more significance than the standards themselves. Furthermore, the review team should have the authority to "own" the standard's uncertainties (provide interpretations) and to approve equivalencies.

For the certification of a system against a performance safety standard, unique skills and a well-

thought organizational set-up are required. The results of the hazard analyses, the description of the risk mitigation measures, and the verification of implementation of such measures would be documented in a report that it is submitted to what is basically an independent peer review. According to The UK Nuclear Industry Guide To Peer Review of Safety Cases:

"*A key benefit of Independent Peer Review is that it allows a competent team, free from project/production pressures, the time to read the safety submission and to think clearly and logically about the hazards and risks inherent in an activity and from this make a judgement on whether the safety submission has demonstrated that these hazards and risks are adequately controlled. Being independent from those responsible for the production of the safety submission allows the Peer Review process to bypass any 'group think' mentality and any pre-judgements on safety that may exist within production teams*."

"*The Peer Reviewer must have a comparable degree of technical competence and experience to the author of the safety submission. Peer Reviewers should therefore have appropriate academic, professional or vocational qualifications in the relevant subject matter. Peer Reviewers must also have an understanding of the principles and concepts in safety and safety management and of the safety regulatory framework, standards, guidelines and codes of practice pertaining to the subject of the submission*".

"It is particularly important to be aware of the dangers of Peer Reviewers losing their independence and becoming part of the project team's decision-making process. Peer Reviewers should not advise projects on what decisions to make or what safety argument would be acceptable and must not provide verbatim text to be written into a safety submission. Nevertheless, in the interests of efficiency, if a Peer Reviewer is aware of a better way of doing things or something important has been missed, then they should point this out in clear and unambiguous terms whilst being careful not to compromise their independence when giving such advice to a Project". [7]

5.0 A NEW ORGANIZATIONAL SET-UP NEEDED

How can aviation regulatory bodies acquire and maintain the support of most current technical and scientific skilled resources needed to move from rules-based certification to risk-based certification? Our answer is that regulatory bodies should establish independent support organizations in which experts from industry, academy and from regulators themselves can evaluate within multidisciplinary teams the results of hazards analyses and the relevant design solutions. Apart from a small core team, such organization, we may call Aviation Safety Institute, would make use of temporary staff seconded from permanent mother organizations (manufacturers, operators, universities, etc.) for the duration of a specific project or certification activity. Examples of such kind of organization already exist in other safety-critical business fields like the INPO (Institute of Power Operations), established after the Three Mile Island accident of 1979, or the COS (Center of Offshore Safety) established after the Deepwater Horizon oil-rig disaster in the Gulf of Mexico of 2010.

	COMPANY	SAFETY INSTITUTE	REGULATORY BODY	INT. ORG
POLICIES	-	advise	develop	coordinate
STANDARDS	implement	develop	validate	-
CERTIFICATION	data	perform	oversight	-
PROCESSES	establish/execute	establish/execute	establish/execute	-
AUDITS	-	Company	Safety Institute	-
	COMPETENCE			
		INDEPENDENCE		
			AUTHORITY	

Fig. 4 Distribution of Roles and Responsibilities
Credit: IAASS

The Aviation Safety Institute (ASI) would be somehow a "middle-man" between the national regulatory body and aircraft manufacturers for the benefit of both parties. The ASI would provide standardization and safety certification services as a "recognized organization" approved by and operating under oversight of the regulatory entity. It would include:

1) Standardization secretariat: for planning and tracking of standardization activities.

2) Safety review panel(s): for reviewing certification data packages, approval of hazard controls/verifications, and providing recommendations to the regulatory body.

3) Safety programs auditing function: for periodically auditing companies' design organizations, design, processes, safety capabilities and performance, related to risk-based design.

6.0 CONCLUSIONS

The Boeing B-737 MAX accidents represent a major failure of the aviation regulatory system. Current

airworthiness standards are antiquated in their essence (mainly prescriptive) and inadequate for integrating new technologies. There have been calls to reform the system to allow more innovation and less bureaucracy, and studies warning about the deficient approach for certifying new computer-based systems. Compliance enforcement by the national regulatory bodies has become also progressively less effective because of the ever-widening skill gap between regulators and industry. The regulatory bodies should move from rules-based certification to risk-based certification. They should emphasize qualitative performance requirements (minimum failure/fault tolerance depending on consequence severity) and use of hazard analyses during design. Deemphasize quantitative performance requirements as "true" measure of safety but use them as design goal to support qualitative performance requirements. Finally, independent supporting organizations should be established by regulatory bodies to get access to current technical and scientific skilled resources at level equal (or better) of industry to perform system safety reviews.

7.0 REFERENCES

[1] J. E. Cashman, B. D. Kelly, N. Nield, Operational Use of Angle of Attack on Commercial Jet Airplanes, Boeing AERO Magazine, 2010

[2] Filippo De Florio, Airworthiness, An Introduction to Aircraft Certification, Elsevier, 2011

[3] F. George, Pilot Say MCAS Software Updates Prove Effective in Simulator Demo, Aviation Week & Space Technology, April 11, 2019

[4] N. Leveson, Ch. Wilkinson, C. Fleming, J. Thomas, I. Tracy, A Comparison of STPA and the ARP 4761 Safety Assessment Process, MIT PSAS Technical Report, Rev. 13, October 2014

[5] J. Ostrower, What is the Boeing 737 MAX Maneuvering Characteristics Augmentation System? – he Air Current, Nov. 13, 2018 https://theaircurrent.com/aviation-safety/what-is-the-boeing-737-max-maneuvering-characteristics-augmentation-system-mcas-jt610/

[6] Ken L. Statler, Streamline Certification, Aviation Week & Space Technology, November 13-26, 2017

[7] UK Nuclear Industry Guide to Peer Review of Safety Cases, August 2016