Aerospace Europe Conference 2023
Joint 10th EUCASS – 9th CEAS Conference

Abstract #XXX *(to be filled by the organizers)*
Preferred Topics: FDGNCAV
Corresponding author: HÜBENER Dominik
e-mail of corresponding author: d.huebener@tu-berlin.de
Type: Oral
Status of corresponding author: Regular

Title
Concepts for Independent Monitoring of Flight Control Laws

Authors
Dominik HÜBENER [1], Robert Luckner [2], Guido Weber [3]*

** Corresponding author*
[1] TU Berlin, Institut für Luft und Raumfahrttechnik, 10587 BERLIN, Germany, d.huebener@tu-berlin.de
[2] TU Berlin, Institut für Luft und Raumfahrttechnik, 10587 BERLIN, Germany, robert.luckner@tu-berlin.de
[3] Liebherr-Aerospace Lindenberg GmbH, 88161 LINDENBERG, Germany, guido.weber@liebherr.com

Abstract
Electronic flight control systems (FCS) are safety critical systems requiring highest levels of integrity and availability. The embedded flight control laws (FCL) software undergoes rigorous verification. However, the complete absence of FCL development errors cannot be guaranteed. Usually, there is one set of FCL requirements, from which FCL software is developed. Undetected FCL requirement errors represent a single point of failure. As new actors push into the market, e.g. eVTOLs for Urban Air Mobility, and as new functions increase the complexity of FCL, the risk of latent FCL development errors rises. Means to mitigate the effects of such errors are becoming more and more important, as EASA's current investigation on FCL monitors [1] shows. This paper investigates possible concepts for an *Independent Monitor* of Flight Control Laws to detect and mitigate the effects of FCL requirement errors.

State of the art FCS architectures often compare the outputs of redundant lanes with similar FCL software and are therefore vulnerable to common mode (FCL development) errors. Typically, dissimilarity is implemented on code level to mitigate software coding errors. However, nearly all serious accidents in which software was involved are related to requirement flaws and not coding errors [2]. Commonly development assurance is used to mitigate the risk of development errors. However, the certification authorities state in a position paper that "development assurance alone is not necessarily sufficient to establish an acceptable level of safety" and that additional mitigation techniques i.e., fault tolerance, should be applied [3]. An Independent Monitor that detects faults is key to achieving fault tolerance against FCL requirement errors.

The FCL Monitor should be functionally independent from the FCL, to minimize the likelihood of common mode requirement errors. Potential independent FCL Monitors can be categorized by detection measure. Two concepts are considered: *Comparator* and *Acceptability Check*. In the first, the output of the nominal (Normal Mode) FCL is compared to the output of a simplified FCL to detect failures. The second concept uses predictions on the system state to determine if the output is acceptable for safe flight rather than correct. Figure 1 shows a simplified pilot aircraft control loop and three options for an independent FCL Monitor.

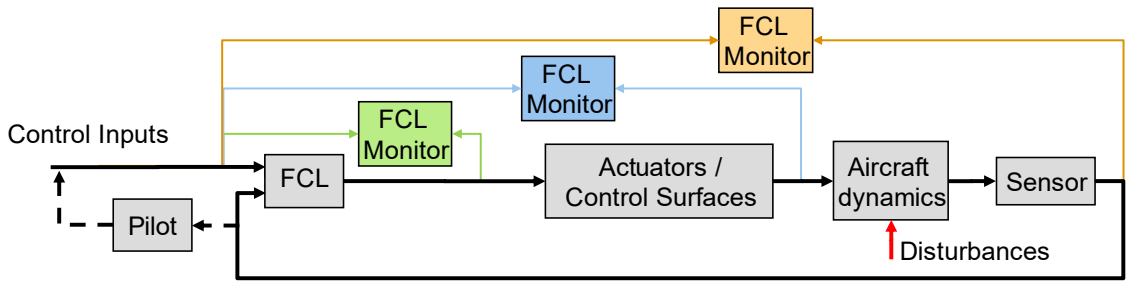

Figure 1: Options for an independent FCL Monitor

This paper describes state of the art FCS architectures and explains their vulnerability to common mode FCL errors. The scope of the independent FCL Monitor is discussed, and assumptions on the FCS are made. Possible concepts are categorized by fault detection measure. Finally, two concepts, *Comparator* and *Acceptability Check*, are described.

References

[1] "Monitoring of flight control laws," EASA, https://www.easa.europa.eu/en/research-projects/monitoring-flight-control-laws (accessed Feb. 14th 2023).

[2] N. G. Leveson, "*Engineering a Safer World: Systems Thinking Applied to Safety*," Cambridge, MA: MIT Press, 2011.

[3] "Reliance on Development Assurance Alone When Performing a Complex and Full-Time Critical Function", Position Paper CAST 24 of Certification Authorities Software Team, 2006.