Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

STPA-Based Safety Analysis Of Pitch Control Actuator Integration For Subsonic Military Jet Aircraft

Pšenička Milan, Fukalová Michaela

AERO Vodochody AEROSPACE a.s., U Letišť 374, Odolena Voda, Czech Republic.

Keywords: STPA, functional safety, aircraft, actuator, control system, aviation, military

For the subsonic military training jet aircraft L-39NG the primary control surfaces (ailerons, rudder and elevator) are mechanically controlled from both cockpits using a classic system of centrally located control levers and foot pedals. Currently, the Roll Control Actuator (RCA) is located in the route of roll control. The Pitch Control Actuator (PCA) for longitudinal control of the aircraft is also being developed. The purpose of this actuator is to reduce the forces in the longitudinal control, which arise here due to aerodynamic forces.

The architecture of the PCA includes an electronic part consisting of an ECU (electronic control unit) and a mechanical part containing a motor with a gearbox, a clutch and relevant sensors. The ECU is an electronic unit used to collect the necessary data (such as load, data from sensors) and for their subsequent use in the calculation of the appropriate power to be generated by the PCA motor. Based on this, the ECU controls the mechanical part of the PCA, i.e. the electric motor and the clutch.

For the PCA unit, its parallel connection to the control path is considered. Thus, if necessary, the pilot can directly control the elevator without using the PCA. Connecting the PCA to the control path will be enabled for the pilot using switches in the aircraft cockpit.

Given the fact the PCA is in the development phase, it is desirable to identify potential risks already at this stage, as well as the safety requirements for this system. Its involvement in the flight control route makes it a relatively critical system from the safety point of view, especially considering control in the longitudinal direction, where certain failure modes of the PCA could have catastrophic consequences, particularly in lower flight levels.

Traditional safety methods such as Functional Hazard Assessment (FHA) and Failure Mode, Effects and Criticality Analysis (FMECA) were used for System Safety Assessment (SSA) of PCA system even during design phase, but the overall complexity and potential criticality made us consider also System-Theoretic Process Analysis (STPA)-like safety analysis to be applied. Within the individual steps of STPA, the structure of the system is clarified and it is possible to identify and assess possible loss scenarios, which in the worst case could lead to undesirable control actions or system losses (Leveson, 2012, 2018). In addition to the fact that STPA appears to be suitable for hazard analysis, system requirements can subsequently be generated based on the steps taken within this analysis (Albrecht et al., 2016; Horney, 2017).

The whole STPA methodology is based on System-Theoretic Accident Model and Process (STAMP) model (Leveson and Thomas, 2018) where the essential point is the creation of a control structure diagram. Specifically, in the case of the PCA system, it was not only about examining its separate control structure, but mostly about integrating the PCA directly into the flight control system, where it interacts not only with the relevant control surface, i.e. the elevator, but also with the pilot as a human controller. In addition, there are a number of surrounding elements or aircraft systems or sensors that have a direct influence on the final functioning of the PCA.

In order to describe all possible connections of analyzed system with all other related aircraft systems we have slightly modified classical STPA control structure diagrams. The modification is mainly focused on incorporation

signaling/indication of defined failure modes to pilots and its connection to overall PCA functionalities. This allow us more options to distinguish indicated / not-indicated failure modes and its different severities and therefore different Risk Assessment Code (RAC) classifications in terms of safety certification requirements according to for example MIL-STD-882 military standard (DoD, 2012). Usual workflow is to start with original STPA methodology and create the basic control structure diagram that is iteratively updated in previously mentioned way during design phase. The process of continuously developed control structure diagram for PCA system is displayed on Figure 1.

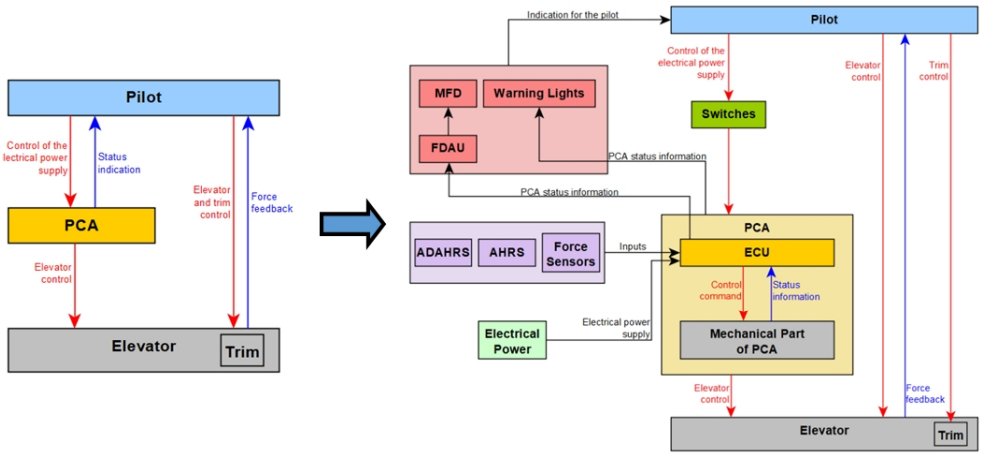

Fig. 1. Description of modified control structure diagram for PCA system of L-39NG aircraft.

Another rather small modification is based on explicit introduction of all inputs (sensors, power source, data etc.) into the control structure diagram in order to keep all possible information about PCA connectivity to other aircraft systems efficiently.

After definition of the purpose of the analysis and creation of the model of the control structure STPA methodology assumes identification of Unsafe Control Actions (UCA) and identification of Loss Scenarios. All of those steps focus on qualitative description of functional safety of the studied system and this is exactly what is needed during the design phase of PCA development. In order to use the STPA or modified STPA-like approach for certification purposes, it will need some quantitative output supplement as we have discussed in (Pšenička et al., 2023). The quantitative addition in form of for example Reliability Block Diagrams (RBD) or Fault Tree Analysis (FTA) can be directly connected with hazards and losses from the first STPA step.

The direct incorporation of information about indicated / not-indicated failure modes into STPA methodology does not change the classification of the failure condition, nor the occurrence probabilities, but may result in the reduction of the Development Assurance Level (DAL) of PCA system related components and thus results in lower development and certification costs, which should ultimately result in lower costs to install safety enhancing equipment on the aircraft.

References

DoD. 2012. MIL-STD-882E, Department of Defense Standard Practice: System Safety. Standard, Department of Defense (DoD).

Leveson, N. 2012. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.

Leveson, N. 2018. Safety Analysis in Early Concept Development and Requirements Generation. Paper presented at the 28th annual INCOSE international symposium.

Leveson, N., & J. Thomas 2018. STPA Handbook. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Abrecht, B. et al. 2016. A New Approach to Hazard Analysis for Rotorcraft. American Helicopter Society International.

Horney, D. C. 2017. Systems-theoretic process analysis and safety-guided design of military systems. Massachusetts Institute of Technology, Department of Aeronautics and Astronautics.

Pšenička, M., Fukalová M., & Lališ A. 2023. Implementation of STPA Methodology Into Military Jet Aircraft Certification Process According to EMAR Certification Criteria for Safety. Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023).