

System Dependency Analysis Supporting Common Cause Analyses of Complex Aircraft Systems

Klaus Fritz

Copyright © 2009 SAE International

ABSTRACT

The system dependency analysis for complex aircraft systems is a model-based methodology and tool for analyzing availability and minimum acceptable control requirements for failures or event scenarios to support the aircraft and system safety analyses (SAE ARP4761) required to show compliance to 14CFR/CS §25.1309, §25.671 and others. Aspects of the system such as functional interaction and dependencies to supply systems, physical items (equipment, wiring and tubing) and installation aspects are included in the analysis. The SAE paper "System Dependency Analysis for Complex Aircraft Systems" (2007-01-3852) describes the modeling approach and the analysis of system dependencies supporting the aircraft and system safety analyses.

This paper provides examples for using the system dependency analysis to support the common cause analyses (SAE ARP4761) for complex aircraft systems. Each element of a common cause analysis – the particular risk analysis (PRA), the zonal safety analysis (ZSA) as well as the common mode analysis (CMA) – can gain advantage of the system dependency analysis with the integrated system model to show the failure propagation causing a system and aircraft level effect for various analyses and cases using the same system model and analysis database.

An example of a quad-redundant flight controls system for a regional jet aircraft serves to show the process, the system model, analysis management and the results including the definition of integration and installation requirements.

INTRODUCTION

SYSTEM DEPENDENCY ANALYSIS – The system dependency analysis provides a model-based systematic approach to determine fault propagation within supply systems and sub-systems up to the main system functions. It is based on the general principle to detect erroneous behavior near the failure source with subsequent fail-safe reaction deactivating the affected function. Deactivation may occur on any functional level depending on severity of the fault leading to a "loss of function". The function loss either propagates through the system, e.g. loss of an electric power supply leads to loss of a control function, or does not propagate if redundancy is available, e.g. a dual redundant power input prevents loss of a control function after loss of one power input.

For aircraft level analyses, the system model needs to consider end-to-end functionality, e.g. from the system sensors to the effective control actuation, as well as the integration with supply systems needs to consider source-to-end, i.e. from the power generation to the supply of power to control and actuation. All functions and the links between the functions are being considered. In addition, the system model includes the physical representation of the functions and links, such as equipment, wiring, hydraulic tubing or mechanical parts as well as their specific installation into the aircraft. To allow determination of main function availability with failures present, performance criteria (minimum acceptable control criteria or MACC) are also integrated into the system model. A performance criterion may, for example, determine the capability of continued safe flight and landing of the aircraft after occurrence of a failure condition.

The inclusion of the integration aspects (supply systems/functions), the physical implementation and the installation aspects into the system model allows not only to support the single and multiple failure analyses, but also provides capability to analyze event scenarios to be analyzed for the common cause analyses (e.g. PRA, ZSA and CMA) as per SAE ARP4761. Those typically create event scenarios to be analyzed for their functional effect, i.e. multiple failures of physical items, such as equipment, wiring bundles, hydraulic tubing or mechanical parts, of the system itself, but also of the supply systems. This paper provides examples for using the system dependency analysis especially for the common cause analyses.

MODELING TECHNIQUE – The system model for the system dependency analysis integrates all model items, representing functions, sub-functions, function links, performance criteria (MACC) and all physical items including their installation aspects equally into a database structure independent of their hierarchical level. The model for each item consists of a list of the associated dependencies and an analysis failure injection. The model result function combines the status of all dependencies and the fault injection, i.e. a model function is available, if all inputs to the function are available and if it is not set failed itself. The fault injection is used to set failure conditions for the analyses performed on the system model. The positive-fail logic uses "1" or "TRUE" representing a function "failed" and uses "0" or "FALSE" representing a function "ok" or "available". The result function may include a logic "AND"-function to represent redundancies. The logic "OR"-function is used to list dependencies leading directly to loss of the function. By integrating the model items into a system model, the database structure using lookup functions automatically connects the items to an overall system function "network" enabling visualization of the failure propagation.

The main aspects include, but are not limited to, the functional, the physical implementation and the installation levels (see figure 1). The modeling technique allows introduction of as many hierarchical levels and sub-levels as required to perform the analyses and to ensure a structured modeling approach. This technique also allows grouping of physical items and installation aspects for analysis purposes.

ANALYSIS TECHNIQUE – By extending the system model database with an analysis management connected to the model items failure injection, the system model can be subjected to various sets of failure conditions. The analysis management stores the fault injection for the individual analysis cases and scenarios and logs the associated results. The analysis management enables the use of a single system model for a wide variety of analyses and analysis cases. Storing the results allows documentation in order to support the traditional suite of safety analyses, but also enables determination of the impact of changes to system function, implementation, integration or installation without manually repeating all individual analyses.

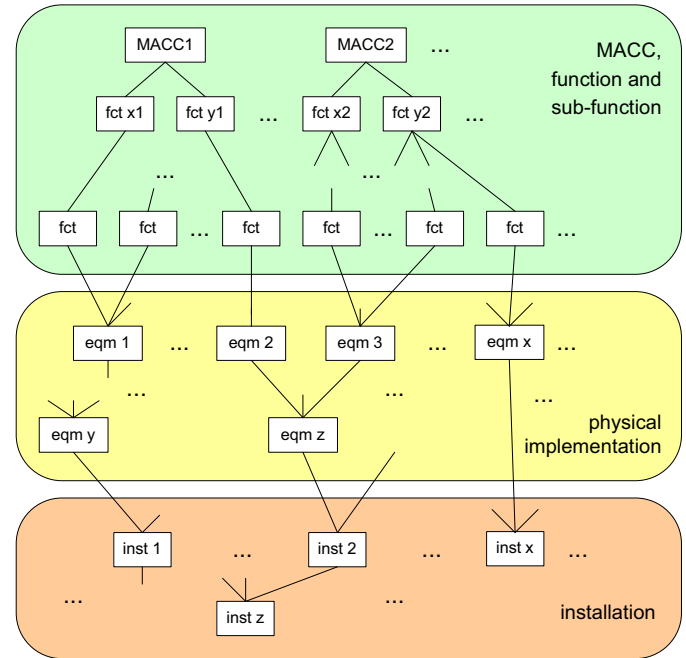


Figure 1: System Model Hierarchy

RESULT VISUALIZATION – The system dependency model and analysis database allows to visualize the failure propagation throughout the system up to the performance criteria. This is important not only for model generation, model debugging and verification, but most important to show analysis results at various level of detail. The visualization within the model items, the overall system model and optional visualization at aircraft system level allows to trace deficiencies and root causes in the system function architecture, and especially for integration and installation aspects including the supply systems.

Resolving these issues allows the creation of integration and installation concepts and requirements to ensure sufficient availability of system resources for all failure conditions or events.

EXAMPLE SYSTEM – A typical quad-redundant fly-by-wire flight control system to control the aircraft pitch axis is shown in figure 2. This simplified system will be used as a demonstration example for the system dependency model and analysis. The aircraft pitch axis is controlled by the flight crew operating the control columns installed on the flight deck. The movement of the columns is sensed by a position sensor package (SP). The pitch control computer (PCC) uses the position of the columns to control the elevator surface actuators (PA). Position sensors integral to the actuators allow closed loop control of the pitch actuator. The pitch control function is comprised of 4 redundant control channels, with 2 actuators in an active-active configuration moving each one of the two elevator surfaces (LH and RH ES). For this example, the minimum acceptable pitch control requirement for continued safe flight and landing is fulfilled, if at least one control channel is available to operate an elevator surface. The fly-by-wire computer

has a dual redundant electrical power supply. The surface actuator is hydraulically powered.

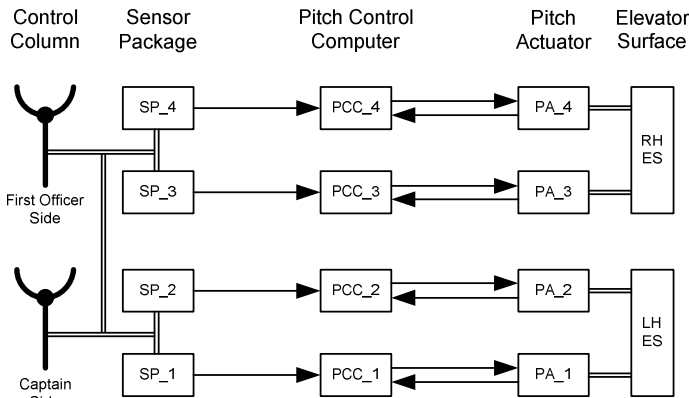


Figure 2: System block diagram of a quad-redundant pitch control function

The SAE paper "System Dependency Analysis for Complex Aircraft Systems" (2007-01-3852) describes the modeling and analysis technique in detail. An example model and analysis database implementation uses the desktop computer software Microsoft Excel © on the example fly-by-wire flight control system.

Besides many different possible applications of the system dependency analysis supporting the suite of system and aircraft safety analyses, the following sections describe how it can be used specifically in the field of common cause analyses (SAE ARP4761), i.e. the particular risk analysis, the zonal safety analysis and the common cause analysis.

PARTICULAR RISK ANALYSIS

ANALYSIS VARIANTS - The particular risk analysis (PRA) is defined in SAE ARP4761 based on the certification paragraph for "equipment, systems and installation" (14CFR/CS §25.1309) which requires a system to function "under all foreseeable conditions". These foreseeable conditions identified for a system can be failure conditions caused by events or influences which are outside of the system or even outside of the aircraft. Those particular risks may include fire (e.g. cargo bay fire or equipment bay overheat), high energy devices (e.g. engine rotor burst), leaking fluids (e.g. toilet water tanks or hydraulic tubing failures), weather conditions, bird strike, tire failures (e.g. flailing tires or rim release), etc.

Occurrence of these particular risks may lead to single or multiple failures in the system or supply systems with failures propagating affecting continued safe flight and landing of the aircraft. The objective of the PRA is either to eliminate the safety related effects by generating requirements for appropriate mitigation or to show the risk to be acceptable. The certification paragraph and the associated acceptable means of compliance guidance (AMJ/AMC §25.1309) specifically includes the supply systems into the analysis considerations. Due to the

character of the particular risk analysis, the installation aspects of the physical items (equipment, wiring, hydraulic tubing etc.) of the system and supply systems are the focus of the analysis for determination of the aircraft level effects.

In general, the PRA is performed based on a specific risk assumption for one or more specific aircraft installation areas. The PRA for each risk assumption may include various cases of damage scenarios and associated failure conditions. A specific set of failure conditions on the physical items of system and supply systems considering the installation is determined for each analysis case. The failure effects of these conditions on physical items of the system function is evaluated concerning the aircraft minimum acceptable control criterion using the system dependency analysis.

The system dependency analysis provides the capability to analyze the system functional dependencies in combination with the installation aspects based on a single model for all cases. The functional model of the system (end-to-end) and the supply system (source-to-end) ensure consideration of failure propagation through the system and all dependencies up to the main system function and the associated MACC.

The following example for the pitch control function uses the system dependency analysis to perform a main engine rotor burst analysis, which is one type of analysis out of the suite of safety analyses which can be supported using a single system model.

EXAMPLE – Performance of a main engine rotor burst analysis is required by the 14CFR/CS E for engine certification. The guidance for the development of the damage scenario cases and determination of the affected system items is provided by AC/AMC-20-128A, and in the system context within 14CFR/CS §25.1309. The practice for system effect analysis and the associated PRA (high energy devices) is recommended by SAE ARP4761.

A main engine rotor burst analysis determines the aircraft level effects concerning continued safe flight and landing on an uncontained rotor burst of the aircraft main engines. The particular risk assumption includes various different cases including analysis of small fragments as well as a failure of the main rotor disk separating a 1/3 disc fragment with very high kinetic energy.

This simplified PRA example develops relevant cases for a main rotor disc failure limited to the LH main engine of a regional jet airliner showing the effect on the pitch control function of the flight control system including the associated supply systems.

To determine the relevant cases for this system all potential trajectories of the 1/3 disc fragment are analyzed and affected system and supply system equipment identified. The outline for all trajectories considers all translational release angles, i.e. the 360

degree ejection around the rotational axis of the engine (see figure 3) in combination with a spread angle, i.e. the ejection along the longitudinal axis of the engine (see figure 4). Following a worst-case analysis approach of AC/AMC-20-128A, it is assumed that the 1/3 disc fragment rotates around the center of gravity with sufficient kinetic energy to cut through all aircraft structures without deflections.

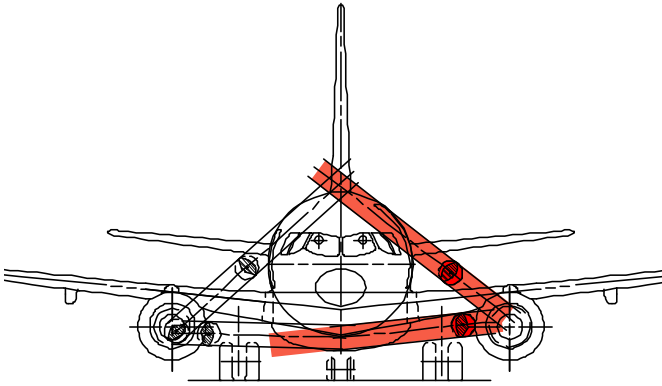


Figure 3: Two example trajectories affecting the fuselage for LH engine rotor burst – 1/3 disc, front view

All those trajectories are considered relevant risk angles, where physical items of the pitch control function (e.g. control computers, sensors, actuators, electrical signal wiring, etc.) or items of the supply systems (electric or hydraulic power supply) are affected. Each single trajectory is analyzed to identify affected items and evaluated for the analysis cases (includes generation of worst-case-scenarios and summarization of effects).

The PRA for the catastrophic failure conditions of the pitch control function analyzes all cases where physical items of the pitch control function (end-to-end) or of all supply functions (source-to-end) are affected.

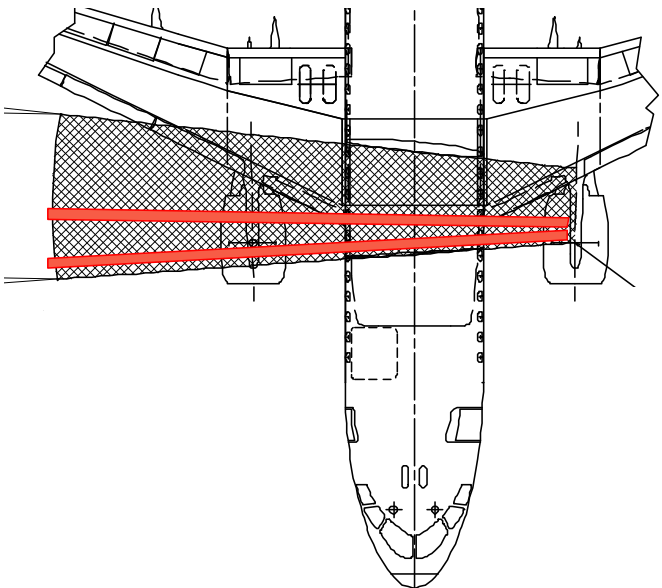


Figure 4: Two example trajectories affecting the fuselage for LH engine rotor burst – 1/3 disc, top view

Power Sources Affected by the Rotor Burst – Following a conservative worst-case safety analysis approach in combination with the characteristics of the example aircraft, it is assumed that the failure of the LH engine results in a loss of electric and hydraulic power in the associated systems.

For the hydraulic system, it is assumed that the nominal power demand for the flight controls cannot be provided by the electric motor pump (EMP) after loss of power to the engine driven pump (EDP), wing or engine hydraulic tubing is affected or that the disintegrated engine has caused a total loss of hydraulic pressure in hydraulic system 1 (leak).

The engine driven generator of the electric system 1 is not powered after the engine failure or failed due to the rotor burst damage. The APU as an additional source of electric power is not considered and not modeled for this example since it is a MMEL item and therefore assumed not available as a worst-case scenario. Additionally, the power cross feed between the electric systems is assumed to be not available since it is not tested before flight or is a MMEL item.

Equipment in the Rotor-Burst Zone – All potential trajectories for a 1/3 disc fragment following failure of the LH engine do not affect the aircraft equipment bays, therefore no equipment (controllers, electric power supply equipment, etc.) of the system and supply system. Various cases affect wiring of the pitch control function as well as power supply wiring and tubing of the hydraulic system installed in the rotor burst zone (see figure 4 hatched area).

Wiring Installation in the Rotor Burst Zone – In the rotor burst zone, the wiring bundles of the example are installed in 4 dedicated wiring areas (see figure 5). Those include the signal wiring as well as the wiring of the electric system. Although flight controls signaling and electric power wires are segregated into separate bundles, those bundles may be installed in the same wiring area. Following a conservative worst-case approach, it is assumed that the wiring area fails at once when affected. The analysis of the trajectories shows that all wiring areas fail independently for all cases, except the "lower" areas, which can also fail together.

The characteristic of the wiring installation of the example regional aircraft considering the worst-case approach leads relevant analysis cases of very simple nature. Partial failures of the wiring zones are not considered due to condensation to worst-case effects. Different trajectories along the longitudinal axis of the rotor burst zone do not lead to additional cases due to characteristics of the wiring installation. Wing leading edge installation areas contain own engine wiring and tubing only. Failure of these areas is considered within the worst-case assumptions for the engine failures.

An interface or wiring FMEA (refer to SAE ARP4761) has shown that a bundle failure leads to a fail safe state of