This document is a merged deliverable on the work done to cover the task "Implementation of methods and database into a tool" (Task 3.3.4, TUHH, INSAT, TEKNIKER) and the task “Tool case application” (Task 3.3.5, TUHH, INSAT, TEKNIKER) of work package WP3.3. The method described in D33.3 is implemented into a tool by developing an appropriate algorithm. The tool is validated with the results yielded by a model-based reliability analysis performed on a reference system.
# Table of Contents

1. **Glossary** .......................................................... 4
2. **Executive summary** ........................................... 5
3. **Introduction** .................................................. 6
4. **Cut-Set Identification Algorithm** .......................... 7
   4.1. **Description of Algorithm Functions** .......................... 7
   4.1.1. **CSIA_System_States** ........................................ 7
   4.1.2. **CSIA_System_States_Reduction** ............................ 8
   4.1.3. **CSIA_Simulation** ........................................... 9
   4.1.4. **CSIA_Top_Event_Identification** .......................... 9
   4.1.5. Implementation of uncertainties for reliability analysis .......................... 10
   4.1.6. Implementation of component failures ........................... 11
5. **Flight Control System Description** .......................... 12
   5.1. **Model of an Aileron Flight Control System** ...................... 12
   5.1.1. Description of the MATLAB/SIMULINK/SIMSCAPE model .............. 12
6. **System Inputs and Failures** ...................................... 16
   6.1. **Load profiles** ............................................... 16
   6.2. **Position command profiles** .................................... 16
   6.3. **Component failure modes** .................................... 16
   6.3.1. Failure modes for logical components ........................ 17
   6.3.2. Failure modes for physical components ........................... 18
7. **Tool case application** ........................................... 22
   7.1. **System extension and Top Event Definition** ...................... 22
   7.1.1. **Top Event implementation** ................................... 22
   7.1.2. Considerations on automated faults/failures analysis ............... 24
   7.1.3. **Reliability Analysis and Validation** ........................... 24
   7.1.4. Evaluation of the CSIA algorithm .................................. 30
8. **Conclusions and Outlook** ....................................... 32
9. **References** .................................................... 33
Table of figures

Figure 1. Steps of the method developed for model-based reliability analysis .............................................. 7
Figure 2. Example of system state matrix of order one ....................................................................................... 8
Figure 3. Composition of system_states-structure .............................................................................................. 8
Figure 4. Composition of simdata-structure ......................................................................................................... 9
Figure 5. Composition of cut_sets-structure ......................................................................................................... 10
Figure 6. Failure rates input as interval values in component masks ................................................................. 10
Figure 7. Permanent Actuation Flight Control System with EMAs ................................................................. 12
Figure 8. Aileron actuation system model ........................................................................................................... 13
Figure 9. Single EMA model - Logical system (SIMULINK) and Physical system (SIMSCAPE) ......................... 13
Figure 10. EMA CMM-COM Module .................................................................................................................. 14
Figure 11. EMA mode management module ......................................................................................................... 15
Figure 12. High-speed load profile ....................................................................................................................... 16
Figure 13. Threshold definition for jamming Top Event ...................................................................................... 23
Figure 14. Threshold definition for runaway Top Event ..................................................................................... 23
Figure 15. RBD for Top Event “Jamming” ........................................................................................................... 25
Figure 16. RBD for Top Event “control surface runaway” .................................................................................... 28
Figure 17. RBD for Top Event “loss of load limitation/critical overload” ............................................................. 30

List of tables

Table 1. Failures modes of CMM-COM .................................................................................................................. 17
Table 2. Failure modes of PCM ............................................................................................................................ 17
Table 3. Failure modes of planetary gearbox ....................................................................................................... 18
Table 4. Failure modes of two-stage gearbox ....................................................................................................... 19
Table 5. Failure modes of screw .......................................................................................................................... 19
Table 6. Failure modes of bearing – rod-end ......................................................................................................... 20
Table 7. Failure modes of PMSM .......................................................................................................................... 20
Table 8. Failure modes of force sensors ................................................................................................................ 21
Table 9. Failure modes of position sensors .......................................................................................................... 21
Table 10. Analyzed Top Events and their required failure rate ........................................................................... 22
Table 11. Order-one failures for Top Event “actuator jamming” ....................................................................... 25
Table 12. Order-one failures for Top Event “control surface runaway” ............................................................ 26
1. Glossary

<table>
<thead>
<tr>
<th>Abbreviation / acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMM</td>
<td>Control and monitoring module</td>
</tr>
<tr>
<td>CMM-COM</td>
<td>Control module</td>
</tr>
<tr>
<td>CMM-MON</td>
<td>Monitoring module</td>
</tr>
<tr>
<td>CSIA</td>
<td>Cut-set identification algorithm</td>
</tr>
<tr>
<td>EMA</td>
<td>Electromechanical Actuator</td>
</tr>
<tr>
<td>FFC</td>
<td>Force-fight compensation</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure modes and effects analysis</td>
</tr>
<tr>
<td>PCM</td>
<td>Power core module</td>
</tr>
<tr>
<td>PDE</td>
<td>Power drive electronics</td>
</tr>
<tr>
<td>RBD</td>
<td>Reliability block diagram</td>
</tr>
</tbody>
</table>
2. Executive summary

This document details the work done to cover the task "Implementation of methods and database into a tool" (Task 3.3.4, TUHH, INSAT, TEKNIKER) and the task "Tool case application" (Task 3.3.5, TUHH, INSAT, TEKNIKER) of work package WP33 "Reliability and Uncertainty Analysis". The objective of these tasks is to implement the method described in D33.3 – Report on safety and reliability assessment method including uncertain parameters into a tool by developing an appropriate algorithm and then validate the results yielded by a model-based reliability analysis performed on a reference system. The reliability parameters input to the tool include failure rates of actuator components in interval form to take into account uncertainties in reliability data, and thus output an interval failure rate at system level for relevant top-events. The flexibility that the developed tool offers in terms of model management, suggests it can be used for further case studies in the A2015 program where various different modelling approaches are being employed. A minimum adaptation of the models is necessary to meet the requirements of the algorithm and to make it work. Thanks to its generic implementation, it is suitable for performing reliability studies in any kind of system, and not strictly on electromechanical actuators. This makes it exploitable in further projects.

For convenience, deliverables D33.4 Report on Safety and Reliability Assessment Tool Including Uncertain Parameters (Chapters 4-5 of this document) and D33.5 Safety and Reliability Tool validation report (Chapters 6-7 of this document) have been merged in a single document because many cross references are needed among the two deliverables. Furthermore, the case study made for D33.5 Safety and Reliability Tool validation report is related to specific failure modes of the reference system described in the implementation part of D33.4 Report on Safety and Reliability Assessment Tool Including Uncertain Parameters.
3. Introduction

This document details the work done to cover the task "Implementation of methods and database into a tool" (Task 3.3.4, TUHH, INSAT, TEKNIKER) and the task “Tool case application” (Task 3.3.5, TUHH, INSAT, TEKNIKER) of work package WP33 "Reliability and Uncertainty Analysis". The objective of these tasks is to implement the method described in D33.3 into a tool by developing an appropriate algorithm and then validate the results yielded by the model-based reliability analysis performed on a reference system. Chapter 4 describes the implementation and functions of the developed algorithm, in Chapters 5 and 6 the reference model and the utilized inputs are presented, and in Chapter 7 a case study is developed using the reference model.

A systematic safety and reliability analysis constitutes a very important part of the design process; model-based methods aid in accomplishing such task. One precondition for performing reliability analyses based on simulation models is the introduction of known failure modes in every component of the flight control system. This permits simulating the system nominal and faulty behaviours under selected operating conditions. As a result, the effects of all failure modes on the system can be analysed. Furthermore, with the definition of thresholds to characterize the transition of a faulty system behavior into undesired top-events, minimal cut-sets and reliability block diagrams for the system can be derived.

With the help of the tool that has been developed for automatically simulating system failures and identifying the system minimal cut-sets, the reliability analysis of a primary flight control actuation system is performed. It is therefore the main objective of the tool to allow conducting a model-based reliability analysis for a reference system architecture. The resulting reliability values for system-level Top Events will be compared to the objectives of an aircraft roll control functional hazard assessment. For actuator-level Top Events, the reliability objectives are those stated in the A2015 requirements for an aileron/elevator actuator. It is worth mentioning that this tool could be used with the models of the Modelica Actuator Library developed in WP31. Only small additions have to be made to the models in order to make them compatible with it.
4. Cut-Set Identification Algorithm

The following section presents a summary of the implementation of the Cut-Set Identification Algorithm CSIA with the purpose of creating an understanding for the proposed model-based reliability process. It is important to understand the particular steps that divide the CSIA process (Figure 1), as for example the preparation of the model that has to be conducted in a specific way prior to automated faults and failures simulation. [3] introduces the overall reliability analysis method using the CSIA, and the process for model extension. In the following section, the implementation of the method will be presented in terms of the functions that characterize it.

![Figure 1. Steps of the method developed for model-based reliability analysis](image)

4.1. Description of Algorithm Functions

In the following the functions for automated faults and failures simulation and for the cut-set identification algorithm CSIA are presented. It is paid special attention to the CSIA functions that need to be manually modified prior to analysis.

4.1.1. CSIA_System_States

The main task of the function CSIA_System_States is to determine all possible failure combinations of the order set for the analysis (first or second order). It identifies the number of implemented failures in each component, which are defined through the parameter failure_mode, and generates a system state matrix with the help of “for” loops. For failure combinations of order one a system state matrix might look like shown in Figure 2.
Figure 2. Example of system state matrix of order one

It consists of two components 1 and 2 (rows), with component 1 having three different failure modes (1, 2, 3) implemented and component 2 having two different failure modes (1, 2). Each combination is then determined through an iterative process by firstly separately setting failure modes of component 1 with component 2 in nominal behavior (left blue sub-frame), and secondly setting failure modes of component 2 with component 1 in nominal behavior (right blue sub-frame). Doing this not just for order one, but also for order two up to order n, generates a set of matrices that are saved in the variable `system_states` as seen in Figure 3.

Figure 3. Composition of system_states-structure

4.1.2. CSIA_System_States_Reduction

This function objective is to reduce system states that provide no information for the further analysis process. There are three different reduction principles that are to be distinguished. The first principle is to neglect system states whose probability of occurrence is lower than a threshold defined in the CSIA configuration settings. Especially for failure combinations of high order this function provides a very successive method.

A second principle is based on the definition of minimal cut-sets, which are defined as system states with a failure combination number as low as possible that lead to a specific Top Event. If for example a single component failure already leads to a specific Top Event, no further failure combinations of higher order are analyzed. These system states are deleted from the system state matrix.

Lastly, the third principle is based on system states that do not trigger any Top Event and therefore seem to be negligible. Before these system states are deleted from the system state matrix they are first combined with other failures of higher order to guarantee that Top Events are definitely not triggered at all.
4.1.3. **CSIA_Simulation**

With the help of this function all system states which have been determined in CSIA_System_States and further reduced by CSIA_System_States_Reduction are separately simulated and the simulation data collected by Simulink-simout blocks are stored in the structure “simdata” as a cell-array. These data are needed further down the process in order to compare the defined system Top Events to the simulation results. At first, CSIA_Simulation simulates the system nominal behavior which means that all component \textit{failure_mode} variables are set to “0”. This information is then stored in the structure \textit{correct_behaviour}. Afterwards all system states or failure combination of order 1 up to \( n \) are separately simulated and their simulation data stored in \textit{failure_behaviour} as seen in Figure 4.

![Figure 4. Composition of simdata-structure](image)

4.1.4. **CSIA_Top_Event_Identification**

The identification of system cut-sets is conducted with this function. It compares the simulation data stored for every system state to the thresholds that define the Top Events. These thresholds need to be defined manually before running the analysis. They must specifically characterize a Top Event by using the simulation data collected through Simulink-simouts for a particular variable or variables e.g. EMA output position or motor current. In order to do so the model behavior has to be studied well enough to know what effect the failures have on a simulation variable. When CSIA_Top_Event_Identification detects an exceeding of Top Event thresholds, the corresponding system state is added to the structure array “cut_sets”. This is iteratively done for each Top Event and first for failure combination order 1 up to \( n \), as seen in Figure 5.
4.1.5. Implementation of uncertainties for reliability analysis

In order to analyse the system with the use of interval failure rates to represent uncertainty in the reliability data assigned to each failure mode, the tool INTerval LABoratory INTLAB has been used. It was developed by Siegfried M. Rump (Institute for Informatics III at the Hamburg University of Technology) [7] and is realized in the MATLAB environment. For this reason the tool has proven to be convenient as an extension to the cut-set identification algorithm. The failures modes and effects analysis FMEA performed in [5] provides failure rate information for individual component failures with an uncertainty interval since different reliability data sources contain differing information. In this sense, it was desired to include minimum and maximum failure rates in order to obtain system-level reliability results with an uncertainty interval.

Figure 5. Composition of cut_sets-structure

Figure 6. Failure rates input as interval values in component masks
INTLAB offers interval arithmetic for real and complex data that include vectors and matrices as well as automatic differentiation, various standard functions and other arithmetic. Its main advantages are seen in its simplicity of application, its broad application spectrum and fast calculating time. For a more detailed overview about INTLAB functions, characteristics and its realization it is referred to [7]. For interval calculations INTLAB uses three different rounding modes that allow rounding upwards, downwards and to the nearest floating point that can be switched according to demand. The application of INTLAB is simple, interval values have to be defined with the MATLAB specifier \( \text{infsup}(\text{min}, \text{max}) \) and input this way to the CSIA code for further processing. Failure rates can thus be written in the components mask under “Failure Options” in the corresponding way with respect to minimum and maximum values as shown in Figure 6.

4.1.6. Implementation of component failures

Failure implementation is based on the principle that only one failure mode for each component can be active at a time. Its implementation follows the guidelines presented in [3] with an additional feature that has already been previously mentioned and concerns failure triggering time. It has been identified that failure effects caused by an active failure mode are more significant if they occur during the EMA extension or retraction process rather than if the failure is activated when the actuator is in steady state or reaches a commanded position. To realize this aspect, an additional parameter \( \text{time}_{\text{triggering}} \) is implemented that is used next to the parameter \( \text{failure}_{\text{mode}} \) variable to modify component equations. It can be set preliminary to simulation in the components’ mask. A failure mode can then only be active if the following condition is true, with \( \text{time} \) referring to the simulation time.

\[
\text{time} >= \text{time}_{\text{triggering}} . \tag{1}
\]
5. Flight Control System Description

5.1. Model of an Aileron Flight Control System

The model of the aileron flight control system that was employed to conduct the investigations presented in this document was in great part derived from the EMA model provided by GAS-F (now UTC Aerospace Systems) in [4]. While the same modeling approach for the EMA components was adopted, the complete EMA model was translated to the MATLAB/SIMULINK/SIMSCAPE modeling language. This was done in order to be able to represent some physical effects more closely and simplify the models with the use of object-oriented programmatic modeling. Additionally, the models are thus made compatible with those of the A2015 Modelica Actuator Library. The reference architecture for the aileron flight control system can be seen in Figure 7.

The components that were selected to integrate this architecture are all high-end industrial components. Therefore a closer approximation to the behaviour and performance of aerospace actuators can be achieved. Furthermore, the simulation and test results can be verified against requirements documents tailored for aerospace actuators. For a detailed list of the selected components along with their most important parameters refer to [2].

5.1.1. Description of the MATLAB/SIMULINK/SIMSCAPE model

Figure 8 displays the architecture of the reference system model, with two identical EMAs in parallel configuration marked with index 1 and 2, respectively. Both EMAs are modelled with logical and physical components representing each of the EMA functions. Figure 9 displays an excerpt of the model that shows the second EMA with its logical and physical components highlighted in the red frame (logical components) and green frame (physical components).
The logical system for one EMA comprises first a Primary Flight Controls Computer PFCC that in this case is simplified to a component which takes the pilot analogue commands and converts them into a digital signal. It integrates signal limiting functions for uncontrolled or illicit high pilot commands. The digital signal is then routed to Actuator Monitoring Module CMM-MON and Actuator Control Module CMM-COM computers. The monitoring module collects all the information concerning the EMA, such as load and position information, temperature information, EMA mode (active or off), power information and pilot commands and transfers them to the control module. There the information is used by the EMA Mode Management.

The logical system for one EMA comprises first a Primary Flight Controls Computer PFCC that in this case is simplified to a component which takes the pilot analogue commands and converts them into a digital signal. It integrates signal limiting functions for uncontrolled or illicit high pilot commands. The digital signal is then routed to Actuator Monitoring Module CMM-MON and Actuator Control Module CMM-COM computers. The monitoring module collects all the information concerning the EMA, such as load and position information, temperature information, EMA mode (active or off), power information and pilot commands and transfers them to the control module. There the information is used by the EMA Mode Management.

useful results out of the faults/failures analysis. At the Actuator Control Module (CMM-COM) all commands concerning the EMA are generated. These include electrical commands for the Power Core Module PCM. The CMM-COM collects information from the feedback sensors and realizes the cascaded control of the actuator.

A voltage command is transferred to the Power Core Module, where depending on the EMA mode (active or off), electrical power is either transferred to the motor or no power is transferred to it. The physical system consists of several components that can be divided in three different function categories: the motor, the mechanical transmission, and linkage/kinematic. The motor receives the
voltage signal from the Power Core Module (PCM), generating a torque and angular velocity that are then transferred to the gear transmission. The air load profile on the flight control surface is represented through a hinge moment which is connected to a kinematics block. It corresponds to A320 kinematics and both actuators are attached to it.

**EMA control module CMM-COM**

Apart from standard cascaded position, velocity, and current controllers being implemented in each EMA control module, a force-fight compensation function is also included. The force-fight compensator collects load information from both EMA force sensors and generates a delta position command that is fed back to the position controller. Whenever a load difference between the two parallel EMAs occurs, the generated delta position command compensates the EMA loads by equalizing the position of both EMAs with respect to a common origin.

Additionally, a mode management module is embedded in the CMM-COM of each EMA. Its general architecture with inputs and outputs is shown in Figure 11. The correct function of the mode management is essential for EMA operation as it switches the actuator in different modes depending on undesired system states in order to mitigate system failures using dedicated protection functions and thus guarantee safe operation.
Figure 11. EMA mode management module

Four different modes are defined inside the EMA Mode Management: active-full mode, active-degraded mode, off-free mode and off-locked mode. The active-full mode allows all system functions to run normally, while active-degraded mode limits the EMA performance for reducing the inertial effects when the system needs to operate in active-damping mode or in a faulty state.

Off-free mode allows the actuator to be moved by the flight control surface and the adjacent actuator while applying only a damping force. Force-fight compensation is disabled in this mode. In contrast, the force-fight compensation is active in off-locked mode. Events which trigger a transition from active-full mode to any of the other three modes are categorized as undesired system states, for which thresholds are defined inside the state machine. For instance, these could be events such as overload, overheat, overcurrent, powered runaway, and unpowered runaway.
6. System Inputs and Failures

Demanding but realistic position and load profiles have to be defined as inputs to the flight control system. A small number of inputs must be able to cover as many operating scenarios as possible and sufficiently excite important system modes.

6.1. Load profiles

A profile for high speeds as seen in Figure 12 is considered where the maximum deflection is +/- 5°. In this case the maximum operating load is reached at 5° deflection.

![High-speed load profile](image)

Figure 12. High-speed load profile

6.2. Position command profiles

The position command profile is directly related to the load profile considered. It implies a ramp signal from 0° to a positive deflection of 7°, then to -7° and back to 0°. Although the maximum positive deflection in Figure 12 is +5° the actuator is driven up to over stroke in order to be able to trigger the failures at the maximum nominal load and capture the consequences of a further retraction of the actuators towards the over stroke area. The triggering time for the failure modes was selected by engineering judgment depending on the most critical moments at which the failures can occur along the surface deflection.

6.3. Component failure modes

Conducting a piece-part FMEA on the linear electromechanical actuator system model along the process guidelines, identifies important and realisable failure modes in all physical components as well as in two logical components: Power Core Module (PCM) and Actuator Control Module (CMM-COM). Failure modes for the logical components have further been determined through a functional FMEA. For reference concerning component failure rates the safety and reliability database for EMA components released by [5] has been utilized. The listed reliability information is separated in four different tables that refer to mechanical components, electrical components, power electronics and sensors. Failure rates have been determined for each component failure mode with some containing further failure rate distributions. Due to failure rate uncertainties that naturally appear during the process (caused by tests and the entirety of different references), component failure rates are defined through minimum and maximum values. In the following sections the reliability information for each component is presented, also naming other references that besides the A2015 database have been used to specify
individual failure rates. For structure reasons first all failure modes for the logical components are presented and then second all failure modes for the physical components. The tables are subdivided in failure mode number, failure mode, failure cause, failure effects, failure rates and last references. It shall be mentioned that the listed failure causes for each failure mode do not cover all processes that ultimately lead to the triggering of these – they rather represent important examples.

6.3.1. Failure modes for logical components

Existing data concerning failure rates for logical components, largely consisting of power electronic components, are usually listed for subparts. These include transistors, capacitors, inductors and others. If the specification of the model is detailed enough to be able to include these piece-part failure modes, failure rates can be determined. If not, empirical values often have to be utilized that are determined in functional FMEA.

**EMA control module CMM-COM**

Two failure modes have been identified that disable two important EMA safety functions: EMA Mode Management and Force Fight Compensation. Switch or bus faults can for instance cause these functional failure modes which result in a complete loss of such functions. A failure rate for these failure modes could not specifically be determined since bus systems and switches were not included in the references. Therefore the failure rates for the failures “EMA mode management disabled” and “force fight compensation disabled” are empirical values.

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EMA mode management disabled</td>
<td>Switch fault, bus fault</td>
<td>EMA mode stays permanently in active-full or switches unintentionally to active-full</td>
<td>$1 \times 10^{-8}$</td>
</tr>
<tr>
<td>2</td>
<td>Force fight compensation disabled</td>
<td>Switch fault, bus fault</td>
<td>Force fight compensation permanently disabled</td>
<td>$1 \times 10^{-8}$</td>
</tr>
</tbody>
</table>

**Power Core Module PCM**

For the Power Core Module two failure modes have been included in the linear EMA system: “uncommanded switch from active to off mode” and “uncommanded switch from off to active mode”. These failures could for example either be caused by bus faults transferring an incorrect signal or switch faults resulting in an uncommanded mode transition with safety and degrading functions remaining active. Failure rates for these failure modes can again not be specified and are therefore assigned with empirical values.

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Uncommanded switch from active to off mode</td>
<td>Switch or bus fault</td>
<td>Switches to off mode</td>
<td>$1 \times 10^{-5}$</td>
</tr>
<tr>
<td>2</td>
<td>Uncommanded switch from off to active mode</td>
<td>Switch or bus fault</td>
<td>Switches to active mode</td>
<td>$1 \times 10^{-5}$</td>
</tr>
</tbody>
</table>
6.3.2. Failure modes for physical components

Convenient information for physical components can be obtained from the A2015 database [D33.2], which comprehensively lists identified component failure modes with assigned minimum and maximum failure rates. Additional references used are indicated in the descriptions.

**Planetary Gearbox**

There are five failure modes determined for the Planetary Gearbox. A failure rate distribution could not be identified, resulting in the same interval failure rate for each failure mode. Failure mode 1 (wearing) leads to an increase of gear backlash. Failure mode 2 (torque transmission loss) captures all processes such as overload or particles in the lubricant that cause breakage of gear teeth and the therefore associated short loss of power transmission. Failure mode 3 (breakage) describes breakage of shaft or gear that ultimately leads to disconnection of the gears with no further power transfer. The case of jamming is captured in failure mode 4 and results again from overload (bearings or gears) or misalignment, leading to no movement of gears. In failure mode 5 (excessive friction) an increase of friction torque takes place.

**Table 3. Failure modes of planetary gearbox**

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wearing</td>
<td>Fatigue, Overload</td>
<td>Backlash increase</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Temporary transmission loss</td>
<td>Particles in lubricant, low lubricant viscosity, lack of additives in lubricant, external materials, overload</td>
<td>No torque transferred for an amount of time, equivalent to loss of one gear tooth</td>
<td>[6.3·10⁻⁶, 3.28·10⁻⁴]</td>
</tr>
<tr>
<td>3</td>
<td>Breakage</td>
<td>Fatigue, overload (shaft)</td>
<td>Breakage or disconnection of shaft or gear, no further power transferred</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Jamming</td>
<td>Fatigue, overload (bearings or gear), particles in lubricant</td>
<td>No movement of gears</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Excessive Friction</td>
<td>Lack of lubricant, particles in lubricant, misalignment</td>
<td>Increase of friction torque between the gears</td>
<td></td>
</tr>
</tbody>
</table>

**Two-Stage Gearbox**

The failure modes for the two-stage gearbox are similar to the failure modes determined for the planetary gearbox: wearing (failure mode 1), torque transmission loss (failure mode 2), breakage (failure mode 3), jamming (failure mode 4) and excessive friction (failure mode 5). However, different failure causes have been identified for the failure modes. These for example result from the usage of fewer parts (no bearings are used) and therefore ultimately lead to different failure rates.
Table 4. Failure modes of two-stage gearbox

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wearing</td>
<td>Fatigue, Overload</td>
<td>Backlash increase</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Temporary transmission loss</td>
<td>Particles in lubricant, low lubricant viscosity, lack of additives in lubricant, external materials, overload</td>
<td>No torque transferred for an amount of time, equivalent to loss of one gear tooth</td>
<td>[2.74·10^{-6}, 1.24·10^{-5}]</td>
</tr>
<tr>
<td>3</td>
<td>Breakage</td>
<td>Overload, corrosion, fatigue</td>
<td>Breakage or disconnection of shaft or gear, no further power transferred</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Jamming</td>
<td>Overload, misalignment</td>
<td>No movement of gears</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Excessive Friction</td>
<td>Lack of lubricant, particles in lubricant, misalignment</td>
<td>Increase of friction torque between the gears</td>
<td></td>
</tr>
</tbody>
</table>

Roller Screw

Altogether four failure modes have been determined for the Roller Screw: wearing (failure mode 1) which could be caused by fatigue, overload or a lack of lubricant results in the increase of backlash. Failure mode 2 describes breakage of the screw that ultimately leads to a disconnection and therefore no further power transfer. Excessive friction (failure mode 3), capturing an increase in friction torque/force that results from a misalignment or lack of lubricant. Important to include as well is failure mode jamming (failure mode 4), as this component failure has a big impact on the entire EMA. If the screw is blocked with the motor still running and transferring torque, the entirety of the inertial loads from the upstream components (such as motor and inertias) are carried by the screw.

Table 5. Failure modes of screw

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wearing</td>
<td>Fatigue, Overload, lack of lubricant</td>
<td>Increase of backlash</td>
<td>[8.69·10^{-8}, 1.24·10^{-5}]</td>
</tr>
<tr>
<td>2</td>
<td>Breakage</td>
<td>Structural fatigue, Overload</td>
<td>Disconnection</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Excessive Friction</td>
<td>Lack of lubricant, misalignment</td>
<td>Increase of friction torque or force</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Jamming</td>
<td>Fatigue, Overload, lack of lubricant</td>
<td>Jamming</td>
<td></td>
</tr>
</tbody>
</table>

Spherical Bearing – Rod-end

Failure modes determined for the Spherical Bearing/Linkage are close to the failure modes identified for the Roller Screw. An increase of backlash caused by excessive speed and load over a period of time is considered in failure mode 1 (wearing). A structural fatigue, leading to a disconnection of any type and ultimately resulting in no further power transmission is captured in failure mode 2 (breakage).
Furthermore, excessive friction which results from external material or lack of lubricant is described in failure mode 3 (excessive friction). Lastly, failure mode 4 (jamming) includes external jamming failures that can be caused by an external bearing failure or kinematic failure.

### Table 6. Failure modes of bearing – rod-end

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wearing</td>
<td>Load, speed</td>
<td>Backlash</td>
<td>$[6.12\times10^{-8} \quad 5.93\times10^{-6}]$</td>
</tr>
<tr>
<td>2</td>
<td>Breakage</td>
<td>Structural fatigue</td>
<td>Disconnection, no power transferred</td>
<td>$[6.8\times10^{-10} \quad 6.59\times10^{-8}]$</td>
</tr>
<tr>
<td>3</td>
<td>Excessive friction</td>
<td>Lack of lubricant, external material</td>
<td>Increase of friction force</td>
<td>$[8\times10^{-8} \quad 4.6\times10^{-6}]$</td>
</tr>
<tr>
<td>4</td>
<td>Jamming</td>
<td>Fatigue, overload, lack of lubricant, external particles</td>
<td>External jamming failure, no further movement</td>
<td>$[6.12\times10^{-9} \quad 5.93\times10^{-7}]$</td>
</tr>
</tbody>
</table>

**Permanent Magnet Synchronous Motor**

Altogether five failure modes have been determined for the PMSM, two electrical failure modes, one magnetic failure mode and two mechanical failure modes. The electrical failure modes refer to a winding short-circuit failure (failure mode 1) and the second to a loss of electrical power (failure mode 2). The magnetic failure describes magnet demagnetization (failure mode 3) that could result from an excessive current or temperature and leads to torque loss. The last two mechanical failures describe bearing failures, where an increase in friction torque is captured in failure mode 4 and bearing jamming in failure mode 5.

### Table 7. Failure modes of PMSM

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Winding short circuit</td>
<td>Winding insulation degradation, shocks, rupture, corrosion</td>
<td>Overcurrent</td>
<td>$[1.25\times10^{-8} \quad 1\times10^{-7}]$</td>
</tr>
<tr>
<td>2</td>
<td>Loss of electric power</td>
<td>Electrical power outage</td>
<td>Torque loss</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Magnet demagnetization</td>
<td>Excessive current or temperature</td>
<td>Torque loss</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Bearing excessive friction</td>
<td>Overload or excessive temperature</td>
<td>Friction torque increase</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Bearing jamming</td>
<td>Overload or excessive temperature</td>
<td>No movement of shaft</td>
<td></td>
</tr>
</tbody>
</table>

**EMA Sensors**

For each of the utilized sensors (force, LVDT, and RVDT) two failure modes have been introduced. Failure mode 1 for the force sensor describes erroneous sensor information that is caused by overload or humidity and results in a sensor offset. Failure mode 2 represents the complete loss of the sensor signal caused by either extreme shocks or extreme vibrations.
## Table 8. Failure modes of force sensors

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Erroneous sensor</td>
<td>Overload, humidity</td>
<td>Sensor offset</td>
<td>$[1.86 \cdot 10^{-6}, 8.0 \cdot 10^{-5}]$</td>
</tr>
<tr>
<td>2</td>
<td>Loss of signal</td>
<td>Extreme shock or vibrations</td>
<td>Returns no signal</td>
<td></td>
</tr>
</tbody>
</table>

The failure information identified for the LVDT/RVDT position sensors are listed in Table 9 as they are also based on the same principles. Here, again two failure modes are distinguished with failure mode 1 representing erroneous position information caused by a leakage in the magnetic field and failure mode 2 capturing a zero position signal. This could either be caused by excessive temperature or shocks.

## Table 9. Failure modes of position sensors

<table>
<thead>
<tr>
<th>Num.</th>
<th>Failure Mode</th>
<th>Failure cause</th>
<th>Failure effects</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Erroneous sensor</td>
<td>Leakage magnetic field, winding fault</td>
<td>Sensor offset</td>
<td>$[5.0 \cdot 10^{-8}, 9.0 \cdot 10^{-5}]$</td>
</tr>
<tr>
<td>2</td>
<td>Loss of signal</td>
<td>Excessive temperatures, shocks</td>
<td>Returns no signal</td>
<td></td>
</tr>
</tbody>
</table>
7. Tool case application

In the following the preparation of the algorithm for the automated simulation of faults and failures and subsequent identification of minimal cut-sets will be presented. It will be shown how the top events were defined for the system at hand, and what reliability objectives were considered. Afterwards the results of the simulations and the analysis of results for three important Top Events will be presented.

7.1. System extension and Top Event Definition

The reliability analysis performed in this investigation is based on the Top Events shown in Table 10. Two system-level (aileron) Top Events and one actuator-level Top Event have been considered for the analysis. For the Top Event “loss of load limitation” the failure rate objective corresponding to an actuator disconnection [1] has been selected since critical overloads can lead to breakage of actuator parts.

The method and algorithm that have been developed are to be validated by comparing the analysis results to the failure rate objectives for each Top Event. In order to define thresholds for the occurrence of these Top Events the system is first extended with Simulink-simouts that output variable data to the MATLAB workspace. They are placed at all different sensor outputs to make sure that every failure effect is detected. Due to the fact that sensor failures have also been implemented, additional ideal sensors are added to the model to guarantee correct system observation. In this context, Simulink-simouts are placed at the force sensors output, at the LVDT/RVDT sensors to collect position and velocity data.

Table 10. Analyzed Top Events and their required failure rate

<table>
<thead>
<tr>
<th>Top-Event</th>
<th>Classification</th>
<th>Failure rate [1/FH]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of control of one aileron</td>
<td>HAZ</td>
<td>1·10⁻⁷</td>
</tr>
<tr>
<td>Safety effect: surface is jammed</td>
<td>(system-level)</td>
<td></td>
</tr>
<tr>
<td>Loss of control of one aileron</td>
<td>HAZ</td>
<td>1·10⁻⁷</td>
</tr>
<tr>
<td>Safety effect: surface runaway</td>
<td>(system-level)</td>
<td></td>
</tr>
<tr>
<td>Loss of load limitation</td>
<td>HAZ</td>
<td>1·10⁻⁸</td>
</tr>
<tr>
<td>Safety effect: actuator overload leading to parts disconnection</td>
<td>(actuator-level)</td>
<td></td>
</tr>
</tbody>
</table>

Although some signals measured in the model are normally not provided by the available system sensors, such signals are used in order to capture all deviations from the nominal system behavior that can lead to a Top Event. The objective of model-based reliability analysis is to search for system states that can be deemed a Top Event and not to analyze the performance of the system or controller for which it would only valid to use the real sensor signals.

When Top Events are defined, it is made sure that each Top Event is entirely and specifically described by the data provided by the Simulink-simouts and that the Top Events are actually reachable. It has been waived to include Top Events that are only triggered when the actuator is in operation for a long period of time — this is the case of Top Event “Overheating”. Since multiple simulations are run, simulating the system each time for more than 10 seconds would lead to very long total simulation time.

7.1.1. Top Event implementation

The position command and load situation have been already introduced in sections 6.1 (Load profiles) and 6.2. (Position command profiles). These are very important for the simulation and analysis since the occurrence of a Top Event depends partly on the system inputs. In order to determine thresholds that thoroughly describe each Top Event, the system is observed at nominal behavior and under the influence of different failure states. For nominal behavior the system reaches the commanded deflection
of 7° (screw retraction of -5.6 mm) slightly after 0.5 s as seen in Figure 13. The triggering time for component failures is therefore set to 0.3 s when the actuators are still in motion and with nearly the maximum possible load as this has been identified to be the situation where failures have the greatest impact.

**Top Event “control surface jamming”**

For Top Event “control surface jamming” several system states have been analyzed that mostly include component jamming failures. With a bearing jam in the motor (blue signal) a screw rod position of -4.6 mm is reached as seen in Figure 13. This system behavior brings the actuators to a complete stop well before the commanded screw position of -5.6 mm is reached. A bearing jam in the motor yields the maximum screw rod position that can be reached with a jamming condition in the system since the non-jammed actuator keeps stiffening up the upstream components of the jammed actuator until it stops. In this context upper (−4.8 mm) and lower (−4 mm) screw position thresholds (red lines) are defined to capture all jammed system states. In order to completely describe the Top Event “jamming” an additional velocity threshold is defined that indicates that the actuators actually come to a complete stop. The screw velocity is therefore not to exceed $|10^{-4}|$ m/s after the jamming occurs.

![Figure 13. Threshold definition for jamming Top Event](image)

**Top Event “control surface runaway”**

Top Event “control surface runaway” is implemented in two different ways. It shall be distinguished between “powered” and “unpowered” runaway. In the first case the commanded position of the actuators is exceeded or the end-stops are reached due to an erroneous command (often sensor failures). In the case of “unpowered runaway” the control surface is not powered by the actuators due to a complete loss of power or an erroneous transition of both actuators to off mode; the surface deflects to an aerodynamic force equilibrium state.

![Figure 14. Threshold definition for runaway Top Event](image)

In Figure 14 an unpowered actuator runaway system state (blue signal) is displayed and compared to the nominal behavior (black signal). Due to the fact that the actuators are coupled by the control surface, the exceedance of a runaway threshold in one actuator reflects also the runaway of the control surface.
In this sense, an upper threshold (upper red line) of 0 mm is defined to capture all unpowered actuator runaways after the failures are triggered at 0.3 s, and a lower threshold of −6.5 mm is set (lower red line) to capture all system states that exceed the commanded position.

**Top Event “Loss of load limitation/critical overload”**

As long as no internal EMA failures or external overloads occur that could lead to critical loads in the system components, the effects of the Top Event “loss of load limitation” are not noticeable. To define this Top Event physically, the secondary effects of losing the load limitation function rather than the loss of the function itself are considered. It is therefore assumed that the load limitation function has already been lost and the actuator load cannot be limited to \( F_{\text{LIM}} = 32 \text{kN} \) [REQ]. The threshold for identifying a critical load is then set to \( 1.2 \cdot F_{\text{LIM}} \) and it is not distinguished between transient or permanent overloads as any load of this magnitude is structurally critical.

### 7.1.2. Considerations on automated faults/failures analysis

In this subsection a few aspects concerning the automated faults/failures analysis are explained. First to name is that the torque sensor downstream the motor is removed from the analyzed model as its only function is to observe the system; its information is not fed back to the monitoring or control modules. Second to name is the faults/failures analysis run time, which is significantly influenced by the simulation time for one system state. In order to guarantee an adequate analysis run time, the simulation time for each system state is set to 2 seconds. This has shown to be enough time for the system to reach its final values (steady state).

Lastly, the order of failure combinations that are to be analyzed are set to order one and two, which means that system states with only one failure mode active at the time are first analyzed. Subsequently, system states with a maximum of two different failures active are analyzed. For 20 components in which overall 66 failure modes have been implemented, 66 failure combinations of order one and 2051 failure combinations of order two were simulated. Depending on the performance of the computer processing, the simulation and analysis take an estimated time of about 12 hours for all different system states; about 21 seconds for the simulation of each system state.

### 7.1.3. Reliability Analysis and Validation

The following results are gained out of the automated faults/failures analysis on the reference system and the application of the minimal cut-set identification algorithm. Results are displayed in the form of Fault Trees and Reliability Block Diagrams. For each Top Event it is analyzed why specific failures lead to the triggering of the Top Events. In addition, it is analyzed if the reliability objectives introduced earlier in this chapter can be fulfilled by the reference model.

In the reliability block diagram representation obtained from the program Cosyra [6] it is unfortunately not possible to display interval failure rates which had been assigned to component failure modes in the preliminary preparation process. Therefore all reliability block diagram component blocks shown in this chapter contain the corresponding component minimum failure rate.

**Top Event “control surface jamming”**

Figure 15 shows the output RBD of Top Event “control surface jamming”. It can be seen that 10 order-one failures lead to a jammed system state; Table 11 lists the failures as well. These failures include jamming in all physical components of actuator 1 and 2. The effects these failures cause on the system have already been explained in the system observation preliminary to setting Top Event thresholds, where it was observed that at the time jamming failures in single components occur, both the associated actuator and the control surface come to a complete stop before the commanded position is reached. A jamming failure is detected through the “overcurrent” safety function implemented in the EMA Mode Management. The mode management cannot prevent jamming of the actuation system, but it reduces its effects.
Table 11. Order-one failures for Top Event "actuator jamming"

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure mode</th>
<th>Failure order</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMSM 1/2</td>
<td>Jamming</td>
<td>one</td>
</tr>
<tr>
<td>Planetary gearbox 1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two stage gearbox 1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roller screw 1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spherical bearing 1/2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A sudden stop in the power transmission chain of one of the actuators produces a permanent high current that exceeds the maximum allowed current for a defined period of time. Once an exceedance of the limit current is detected in one EMA, its mode is switched from “active-full” to “off-locked”. In this mode, the force-fight compensation function remains active and prevents the load of the EMAs to further increase, resulting in both EMAs to be brought to a common position (the position of the jammed actuator). With the help of INTLAB a minimum and maximum failure rate for Top Event “Jamming” is determined as follows,

\[
\lambda_{\text{min}} = 5.8 \cdot 10^{-6} / FH \\
\lambda_{\text{max}} = 7.034 \cdot 10^{-4} / FH
\]

The failure rate objective of \(1 \cdot 10^{-7} / FH\) is not met for either minimum or maximum failure probabilities. A reason for not meeting the required objective can be that the component failure rates utilized for the system-level calculation are only failure rates of order-one failures. Additionally, since the jamming failure rate of the two stage gearbox alone does not even meet the objective, it is clear that the sum of the jamming failures rates of other components will not either. With the use of aerospace components failure rates the reliability objective might be met.

Figure 15. RBD for Top Event "Jamming"

Top Event “control surface runaway”

Order-one failure combinations: Table 12 lists all order one failures with their associated components. Evaluating these faults reveals that both LVDT position sensor failures, erroneous position information (offset) and zero signal, trigger the safety function of the EMA Mode Management against an uncommanded motion. This one compares the input command to the output position, and switches the corresponding EMA to off-free mode (FFC switches off) if the commanded position is exceeded.

In the case of a positive offset or zero signal faults in one of the EMAs position sensors, the position controller commands further retraction/extension although the commanded position has been already reached. This leads to exceeding the commanded position and the actuator with the problem is then switched to off-free mode. Since FFC does not switch off, a further position offset is fed back to the still active actuator and this instantaneously leads to an exceedance of its commanded position too. In consequence the whole system is switched to off-free mode, resulting in a single failure that leads to the Top Event. This could be avoided by further development of the actuator mode management.
Table 12. Order-one failures for Top Event "control surface runaway"

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure mode</th>
<th>Failure order</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMSM 1/2</td>
<td>Demagnetization, loss of power</td>
<td>one</td>
</tr>
<tr>
<td>LVDT position sensor 1/2</td>
<td>Offset, zero signal</td>
<td></td>
</tr>
<tr>
<td>PCM 1/2</td>
<td>Uncommanded switch from active to off mode</td>
<td></td>
</tr>
</tbody>
</table>

The two motor failures, loss of power and demagnetization, yield an effect that cannot be detected by the EMA Mode Management; it detects power transmission losses by comparing the angular velocities of the motors. In case of breakage of transmission components this permits the detection of such failures. However, with a motor demagnetization or power loss, the difference in the angular velocities of the EMA motors is not big enough to trigger the necessary protection function, leading instead to a large positioning error (also caused by further functioning of FFC) that causes the passivation of both EMAs and thus an unpowered runaway of the control surface.

Lastly, the Power Core Module failure “uncommanded switch from active to off mode” causes one EMA to switch to off mode with the Force Fight Compensation function still. The load difference between the EMAs increases suddenly and so does the position error generated by the force fight compensator. This generates a large positioning error for the control surface, which leads to switching the entire system to off mode. The control surface then deflects to its force equilibrium position.

Order-two failure combinations: Evaluating all second order failure combinations which have led to Top Event “control surface runaway” reveals a couple of similar patterns that are rather presented instead of analyzing each failure combination on its own.

1. Breakage in both EMAs: If breakage of physical components occurs in both EMAs, which effectively means that both actuators are not capable of carrying load, it is quite clear that nothing except inertias and damping in the actuators is opposing the air load and the control surface moves to its force equilibrium position instead of moving to the commanded position.

2. Breakage + jamming in the same EMA: If both mechanical breakage and jamming failures occur in the same EMA, an unpowered actuator runaway takes place. This is caused by the switching of the jammed EMA to off-locked mode due to the exceedance of a current threshold. In combination with mechanical breakage in the same EMA, the actuator becomes movable again; meanwhile Force Fight Compensation stays active and it generates a large position error that is fed back to the actuator controllers. Consequently due to the large difference between commanded position and actual surface position the entire system is switched to off mode and the control surface moves to its position of force equilibrium.

3. Breakage + motor excessive friction in the same EMA: Similar to the previous pattern, the combination of breakage and motor excessive friction in the same EMA triggers the “overcurrent” safety function of the EMA Mode Management and switches the associated EMA to off-locked mode. With a subsequent breakage and force-fight combination remaining active, the resulting behavior is as explained in 2.

4. Breakage + temporary transmission loss in different EMAs: In this failure combination an unpowered actuator runaway is generated. The breakage and subsequent passivation of one EMA effectively increases the load of the adjacent one due to the latter being the only one transmitting further power. A sudden and short torque loss in the healthy EMA due to gear failure produces a load and current peak which accidentally trigger the “overcurrent” safety function. The EMA that was still active is then switched to off-locked mode and the entire surface moves to its force equilibrium position.

5. Force sensor loss of signal + excessive friction in the same EMA: With this failure combination the EMA Mode Management protection function against component disconnections or torque loss is accidentally triggered. Due to one force sensor feeding back a zero signal, the position error generated by the force fight compensator is permanently erroneous. Excessive friction generates a force fight between the actuators that is not correctly compensated and thus the actuators are driven to an erroneous position yielding thus a powered runaway.
6. **Breakage + EMA Mode Management disabled in the same EMA:** The Mode Management of the broken EMA is disabled and the actuator cannot be switched to off-free mode when breakage occurs. As a result, the force fight compensator stays active and due to the existing force differences in the actuators and the position error it provides, a large surface positioning error is produced. The healthy EMA is passivated and the entire system is driven to the position of force equilibrium by the air loads.

An overall Top Event failure rate has been calculated from the resulting minimal cut sets and a reliability block diagram has been derived as seen in Figure 16. The resulting minimum and maximum failure rate values for the Top Event “control surface runaway” are,

\[ \lambda_{\text{min}} = 2.02 \cdot 10^{-5} / FH \]
\[ \lambda_{\text{max}} = 4.224 \cdot 10^{-4} / FH \]

The required failure rate objective for Top Event “control surface runaway” is set to \(1.0 \cdot 10^{-7}/FH\), which is not reached by the calculated failure rates. Since order-one failure combinations have a much bigger impact on the overall Top Event failure probability, their number has to be reduced in order to meet the required Top Event failure rate. To reduce the Top Event failure rate determined in this analysis, the PCM failure that occurs as an order-one failure has to be specifically emphasized. Its assigned failure rate is based on an empirical value originating from general power electronics applications and it lowers the overall failure probability by a great amount. If a failure rate for aerospace power electronics was used, a more convenient statement could be made concerning the fulfillment of the reliability requirement.

Force-fight compensation has shown to have a deciding influence on the failure behavior of the system. If it stays switched on when torque loss failures in the system occur, the effects of it are detrimental to the system in case a second failure happens. It shall be carefully investigated how these effects can be mitigated within the EMA Mode Management.
Figure 16. RBD for Top Event "control surface runaway"
Top Event “Loss of load limitation/critical overload”
For Top Event “loss of load limitation/critical overload” two single failures and 30 order-two failures could be identified to cause an exceedance of the actuator load threshold $1.2 \cdot LIM$. The related Reliability Block Diagram is shown in Figure 17. As previously mentioned, it is assumed that both actuators in the system are working without the load limitation function, and thus critical overloads can be reached by some failure combinations. Even if components like the force sensors or the CMM-COMs are responsible for the loss of the load limitation function, these are considered as initially functional in the following analysis. In this sense, the validity of this analysis is limited to the assumption that the load limitation function has been lost due to an internal conflict in the CMM-COMs and not due to failures in the force sensors.

Order-one failure combinations: The only order-one failures that have been identified are jams of the EMAs spherical bearings or linkages i.e. external jams. Without the load limitation function, external jams can only be detected by the motor overcurrent safety function, however due to that the motor is far upstream to the external jam, the time until a mode switching is commanded is too long and a critical overload occurs. On the other hand, when internal jams occur and the load limitation function is disabled, the generated loads are alleviated by the force fight compensation function.

Order-two failure combinations: In the following segment second-order failures are interpreted. For structuring reasons not every system cut-set identified is analyzed on its own. When similarities are noticeable, cut-sets are summarized and presented together as a specific pattern. However, the second order cut-sets can be seen in the RBD of Figure 17.

1. Breakage + jamming in the same EMA: At this failure combination overload is reached for the EMA that remains active after failures in the adjacent one occur and it is switched to off mode. Important for this to happen is the order in which breakage and jamming occur in the faulty EMA. In this case this is characterized by breakage occurring before jamming in the transmission chain. The EMA Mode Management correctly detects the breakage failure and it triggers a safety function that switches the faulty EMA to off-free mode (off without Force Fight Compensation). In difference to a single breakage failure, the additional jamming failure in the faulty EMA brings the control surface and therefore the adjacent EMA to a stop. Since no Force Fight Compensation is active, the healthy EMA is opposing the air load and additionally working against the jammed faulty EMA. In consequence its load increases until it exceeds the limit load.

2. Force-fight compensation disabled + jamming in EMA 1/2: This system state is characterized through a jamming failure in one EMA and disabled Force Fight Compensation in the system. When the faulty EMA jams it is switched to a off-locked mode (due to a motor overcurrent), where force fight compensation stays active in order to alleviate the loads caused by the jamming condition. However with force fight compensation and load limitation being disabled, the non-jammed actuator keeps trying to reach the commanded position until an overcurrent is detected in the motor and it switches to off mode; by this time a critical overload has occurred already.

3. LVDT offset/zero signal + Force sensor loss of signal in the same EMA: The LVDT failures lead the associated EMA to exceed the commanded position due to the error in the position feedback. As a result the faulty EMA retracts ahead of the adjacent EMA yielding an increasing load. This circumstance is worsened by the force sensor feeding back a zero signal and thus an erroneous feedback to the force fight compensator. As a result the faulty EMA takes more load until eventually the limit load is exceeded due to a large force-fight.

Under the assumptions previously explained, the determined minimum and maximum failure rates of Top Event “loss of load limitation/critical overload” turn out to be,

$$\lambda_{\text{min}} = 1.01 \cdot 10^{-7} / FH$$

$$\lambda_{\text{max}} = 6.573 \cdot 10^{-4} / FH$$

The reliability objective $\lambda = 1.0 \cdot 10^{-8} /FH$ is not met. However it shall be mentioned that the single failure identified only occurs in combination with a loss of the load limitation function and is thus in reality a second order failure. Under this assumption a minimum failure rate of about $1.0 \cdot 10^{-12} /FH$ would be achieved. The analysis of this Top Event has demonstrated that even with the loss of the load limitation
function, the system can cope safely with overloads and thus a component breakage due to overloads is highly improbable.

![Figure 17. RBD for Top Event "loss of load limitation/critical overload"](image)

### 7.1.4. Evaluation of the CSIA algorithm

Using the Cut Set Identification Algorithm for reliability analysis has revealed several advantages and disadvantages that are discussed in the following segment.

A great advantage of CSIA that also distinguished this method from others is the fact that it can be applied to hybrid systems that model logical and physical system behaviour in Matlab/Simulink/Simscape. Although extending the system with failure behaviours for logical and physical components uses different approaches, the basis is the same and enables the user to quickly
work into method of implementing failures. It is also simple to include additional functions in the failure extension process and therefore adapt the algorithm to the user’s demands. An example represents the failure triggering time.

Furthermore it is possible to extend the algorithm with external MATLAB based tools such as the interval computing tool INTLAB, and enables the user to add specific features to the analysis. Concerning analysis run time good results can be achieved by using the reduction approach, which proved to be useful for high-order failure combinations. The CSIA also allows displaying the analysis results in two common representations – Fault Trees and Reliability Block Diagrams. The generated output structures are intuitive and clear and allow an interpretation of the obtained results without needing to perform further structuring work. One premise is that the engineer has to understand the model and failure effects well enough to be able to conduct the analysis with the CSIA. This is especially required once it comes to implementing Top Events that rely on a comprehensive and convenient description. At this point it is significantly decided whether or not the generated results are representative of the system. One disadvantage of the developed cut set identification algorithm that has been identified is that only one Top Event can be analysed at a time. Therefore the required simulations to cover all failure combinations need to be repeated for each Top Event, increasing the simulation time significantly.
8. Conclusions and Outlook

Based on Task 3.3.4 and Task 3.3.5 “Safety and reliability assessment tool including uncertain parameters” and “Tool case application” respectively, the implementation of the model-based reliability tool developed has been described, and a case study has been chosen as means of validating the tool. Design robustness and weaknesses of the reference system have been exposed as a result of the reliability analysis. These shall serve as means of improving the existing safety functions implemented in the Mode Management of the EMAs under design in A2015.

The implementation of the developed Cut-Set Identification Algorithm CSIA utilized for model-based reliability analysis was summarized with regard to its main functions. Since FMEA failure rates exhibit uncertainties and the data sources provided maximum and minimum failure rates, the algorithm has been provided with the capability to make the required reliability computations using interval arithmetic. This was realized through the tool INTTerval LABoratory INTLAB

Subsequently a reference actuation system was introduced and failure modes and effects for its components were determined out of an existing FMEA performed in Task 3.3.2 of SP3. It was necessary to extend the list of existing failure modes with additional functional failure modes in order to be able to comprehensively represent the reference system’s failure behaviour. The model of the reference system was then extended with the selected failure modes.

The algorithm developed was tested with a case in which three relevant Top Events were investigated. These represent reliability concerns at system-level such as aileron loss of control due to jamming or actuator runaway and at actuator level such as overload. Thresholds were defined to describe each Top Event and the analysis was conducted for order one and order two failure combinations. The results obtained from the analysis were displayed in the form of Reliability Block Diagrams. Each Top Event was analysed, interpreted and assessed upon reliability requirements.

Although none of the required failure rates for the investigated Top Events was reached, the calculated failure rates were not too far from meeting the requirements. The reasons for not meeting the requirements were clearly identified. They can be partly regarded to the fact that reliability values for industrial components were used; additionally the EMA Mode Management proved to be incapable of mitigating certain failures in order to not reach the Top Events. A further development of the EMA Mode Management module is necessary; based on the identified failures that lead to Top Events it is presumed that all single failures can be prevented with an improved design of the Mode Management laws.

Outlook

As already addressed, there is still work to be done regarding failure detection and mitigation for the reference system. It seems realizable to optimize existing protection functions to a point where all single failures can be mitigated. In the coming period it is planned to validate the model of the reference system with real hardware (exactly the same system). Once this is done and the Mode Management is enhanced, it will be worth it to perform again a model-based reliability analysis using the tool developed and verify the occurrence of the selected Top Events. Due to the flexibility of the tool developed, it can be used for further case studies in the A2015 program.
9. References


