CEAS Aeronautical Journal (2022) 13:503–520
https://doi.org/10.1007/s13272-022-00572-8

ORIGINAL PAPER

Validation of the safety requirements of the landing gear using fault tree analysis

Leander Iven[1] · **Yaseen Zaidi**[2]

Received: 31 December 2020 / Revised: 24 January 2022 / Accepted: 27 January 2022 / Published online: 12 March 2022

Abstract
We analyze the functionality of the landing system of a regional aircraft in the extension and cruise flight modes and validate safety requirements through the fault tree analysis. The main landing gear system is captured in the electromechanical–fluidic domain and system behavior is abstracted in an elementary hydraulic circuit. The functional representation is then constructed into a fault tree which allows analysis of the failure propagation originating at different branch terminals, for instance, at the main landing gear actuator which extends the gear and holds it retracted during the cruise, door actuator, door uplocks, and hydraulic power supply. Each component is assigned a failure probability. Each failure mode is abstracted as a top-level event having a probability of failure and through Boolean combinations of component failures in the lower branches. Two reliability aspects considered are the availability to fully lower the landing gear and the integrity of inadvertent gear or door extension while cruising. Architectural changes through undercarriage system reconfiguration and component redundancy have been exploited to improve system failure rates. The analysis determines the overall system failure rate against the flight cycles. The process is agile to accommodate design changes with the evolution of architecture during the systems engineering lifecycle.

Keywords Failure mode · Fault tree analysis (FTA) · Landing gear · Reliability · Requirements · Safety · Validation

1 Introduction

Requirements validation for a flight-critical airframe system such as a retractable tricycle landing gear is a complex process. This is partly because of the sheer complexity of the landing gear which is a system of systems comprising of several thousand components and subsystems, such as the struts, columns, brackets, trunnions, cylinders, pistons, retraction subsystem, steering subsystem, braking, wheel assembly, shock absorbers, doors, locking mechanisms, actuators, valves, wiring, and electric or hydraulic power supply. The kinematic nature of the electromechanical design of the gears coupled with a huge role in flight safety imposes a heavy requirement of high reliability through duplication or triplication of critical components and frequent maintenance checks [1]. The leading gear mass and volume affect virtually all major aspects of the aircraft design from gear layout on the airframe, weight and balance, and lift to the aerodynamics performance [2, 3]. In general, the development program requires safety analysis in multiple phases in the product lifecycle [4].

The design space is usually huge and correspondingly the exploration effort to requirements analysis which may follow several trade studies and what-if scenarios. Stakeholder's expectations and realizing the requirements into a functional system at the desired cost and impact propagation on the system performance are challenges to the process of analysis of requirements and conformance. The number of requirements for a commercial aircraft landing gear can easily run into several hundred ranging from design, test, system configuration, functional, system integrity, safety, certification/airworthiness, and program-level requirements [5].

Among the several techniques of quantitative safety analysis and risk evaluation [6–11] for investigating reliability and safety, the fault tree analysis (FTA) is a simple yet practical method that allows certainty that adverse effects will not be caused by some agent under defined conditions

✉ Leander Iven
st171968@stud.uni-stuttgart.de

Yaseen Zaidi
yaseen.zaidi@uwe.ac.uk

[1] University of Stuttgart, Keplerstraße 7, 70174 Stuttgart, Germany

[2] School of Engineering, University of the West of England (UWE Bristol), Coldharbour Lane, Bristol BS16 1QY, UK

anywhere in the product lifecycle—from early requirements analysis down to the concept of operation or critical design and verification & validation (V&V). This paper demonstrates how a complex view of the aft or main landing gear (MLG) may be logically modeled and analyzed for safety criticality in different flight modes and how a culprit source may be isolated through the FTA. The analysis presents possibilities for architectural improvements, either by redundancy or topology changes and estimates the overall failure rates in 5000 flight cycles. A handful of safety requirements are taken to underscore the rigor that goes into analysis, elicitation of requirements, validation, and impact. This is done by underpinning quantitative failure rate data and approximate models of failure prediction that may be used in maintenance planning. As with any systems engineering activity, the process is iterative and can only be concluded in negotiation between a landing gear customer and supplier whether the failure rates of critical and catastrophic failures are acceptable, need improvement by redesigning the baseline system architecture of landing gear, adding redundancy, or using components with the high mean time to failures.

2 Current practices of landing gear safety design

The majority of the literature sources take up one or two aspects of the mechanical design, such as structural integrity [12], the strength of materials [13], gear behavior in a thermal environment [14], vibration and dynamics [15, 16] and shimmy phenomenon [17] including the nonlinear analysis of the structure and deflections in multibody dynamics [18] as well as uncertainty analysis [19]. Such activities are suited for below the preliminary-level of the design.

Besides gear strength and kinematics, a significant interest lies in the safety–critical aspects of the landing gear computer (LGC) extending to federated and popular integrated modular architecture (IMU) [20]. See for instance, [21] and [22]. These approaches mainly focus on flight code, digital logic, and data communications and may be extended to DO-254 hardware and DO-178C software qualification [23]. Therefore, component-level safety may be checked by querying status over the telemetry links and issuing corresponding commands. A further benefit is bringing the redundant devices to live in case of failure of the primary devices so fault detection and isolation recovery (FDIR) [24] or similar diagnostic routines may be run. The verification of the flight code with formal methods [25, 26] is a well-settled practice. An important element in communications is the timed triggered [27, 28] execution of the transactions (SAE AS6003 TTP Communication Protocol) over the data bus interconnecting the IMU.

On the rise are the model-based methodologies [29] that aim to achieve wide lifecycle coverage by digitally threading an array of process, modeling and simulation views into an information-loaded model of the landing gear—a digital twin [30]. The model-based systems engineering (MBSE) approach links requirements throughout the lifecycle phases, such as architecture and functional design, V&V, in-the-loop testing, and DO qualification. Any assorted tools, abstract models or safety analysis may be integrated [31] with multibody dynamics, Physics-based simulations, and even flight controllers to prove requirements traceability, determination of constraints, and valid operating ranges of the mechanics, and isolation of the unintentional behavior.

A widely used inductive method for landing gear safety analysis is failure mode and effects analysis (FMEA) [2, 10, 32].

Our work concerns safety analysis and validating requirements in the conceptual design. In practice, during this phase, the requirements are analysed and the design is refined to move to the preliminary design phase which focuses on the mechanical aspects, such as gear configuration, the position of hydraulic components, loading, sizing, number of wheels in the bogie, and tire diameter. Therefore, safety is paramount and frequent design changes warrant a continuous reassessment of requirements and analysis of safety for the smallest change in new system architecture.

3 Main landing gear safety requirements, functional behavior and baseline system architecture

Figure 1 shows an abstract description of the landing gear extension/retraction system. For simplicity, we consider MLG in one wing. The system has three operating modes: retraction (retracting the landing gear and closing the doors after take-off); cruise (maintaining gear in the retracted position and doors closed); and extension (opening the doors and extending the gear before touchdown). The present work is concerned with the extension and cruise modes only. The aircraft is fly-by-wire hence all command inputs into the system are received from the landing gear computer (LGC). Notice the electrical and data interfaces, and the LGC have been abstracted away as their presence in the system is irrelevant in the current analysis. The gear LGC would run the safety–critical software and regulate the pumps, locking angles, and deployment/extension timing. The actuator and valve power interfaces have not been shown. The collection of telemetry and telecommanding the system are by the LGC which also runs diagnostic routines in case of failures (e.g., FDIR routines) and executes the correct sequence of actuation. We further simplify. The main and redundant hydraulic supplies are not shown and only their lines are.

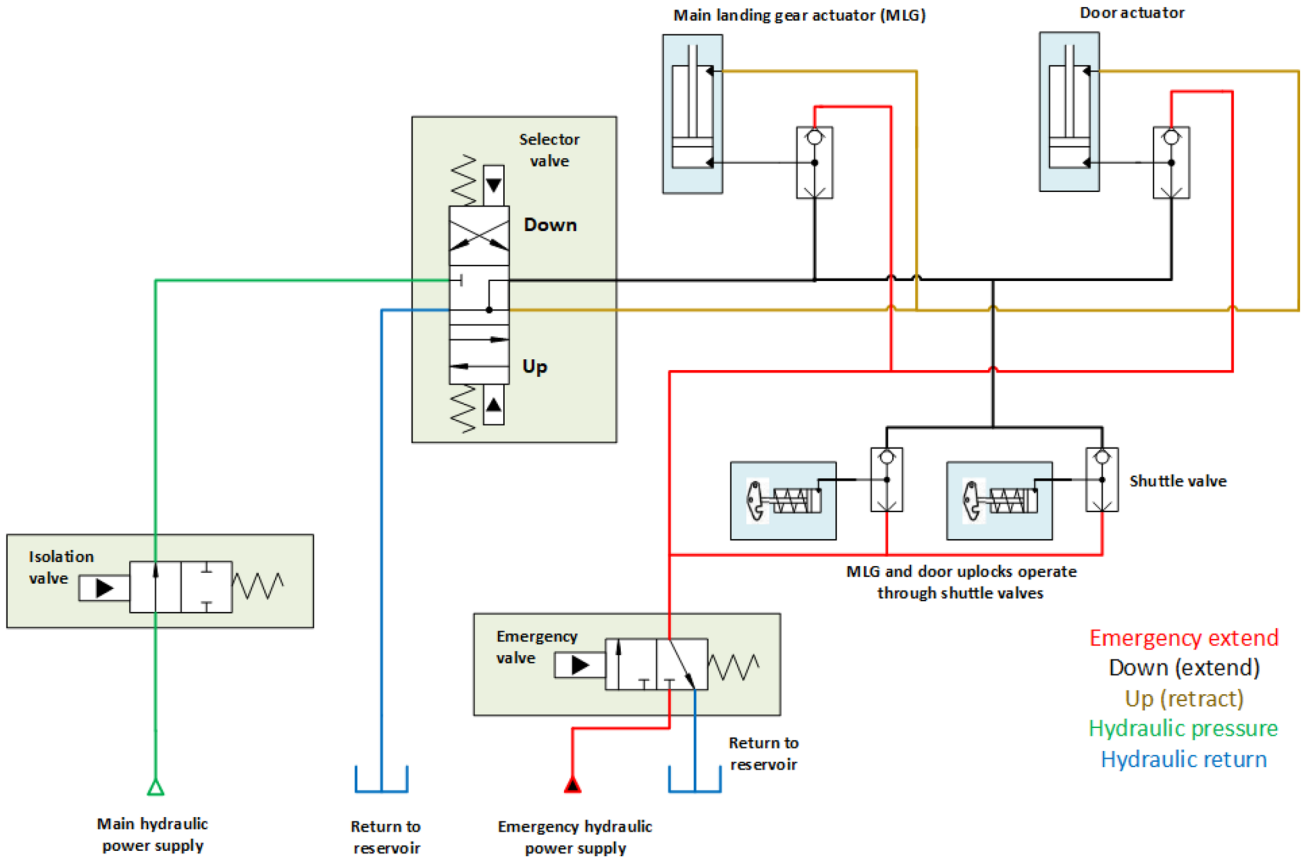

Fig. 1 Baseline main landing gear (MLG) system architecture with redundant hydraulic power sources

The component statuses will be pulled through a data comm interface such as ARINC 429 which is also ignored.

The system is validated for the safety requirements considered in Table 1. Typically, the requirements will be stipulated by a customer or a regulatory body's airworthiness directive, e.g., the probability of failure for a particular severity level or 5000 flight cycles for a repetitive inspection interval [34, 35].

As the faults originate at the components, knowledge of the functional behavior of the components is imperative to the understanding of the different failure modes.

The failure modes and the component failure rates are listed in Table 2. For completeness, we remark that the failure rates are determined with a mix of empirical and probability methods [33, 36]. Yang [37] develops a failure rate model of an inductive solenoid coil-based valve. The electronic component failure rates may estimated with the procedures given in FIDES handbooks (217Plus, MIL-HDBK-217F, IEC 61164, Siemens SN 29500, Telcordia SR-332) which typically build the failure model with the variables involved in the device operation, such as input and lost power, voltage, ambient temperature, operating frequency, and material properties. The confidence intervals of the models may be improved with accelerated life testing data of the components or in-flight failure data. The Weibull distribution [38] is particularly favored in the reliability

Table 1 Landing gear safety requirements

No.	Requirement statement
Req 1	No single failure shall lead to inadvertent gear or door extension
Req 2	Inadvertent gear or door extension is a catastrophic failure (defined as probability of failure <1E-7 per flight cycle)
Req 3	Failure to fully lower the landing gear is a critical failure (defined as probability of failure <1E-6 per flight cycle)
Req 4	No scheduled maintenance shall be required (overhaul period is 5000 flight cycles)

Table 2 Component-level failure modes and failure rates. The designators e and c in the failure mode events stand for extension and cruise modes, respectively

Failure event	Component	Failure mode	Failure rate per flight cycle
IVe	Isolation valve	Fails to open	1E-8
IVc	Isolation valve	Uncommanded movement to open position	1E-6
SVe	Selector valve	Fails to move to the 'down' position	1E-8
SVc	Selector valve	Uncommanded movement to 'down' position	1E-6
EVe	Emergency valve	Fails to open	1E-8
EVc	Emergency valve	Uncommanded movement to open position	1E-6
HPe1	Hydraulic pump 1	Loss of pressure for the 'main' system	2.5E-5
HPe2	Hydraulic pump 2	Loss of pressure for the 'emergency' system	2.5E-5
ShVe1 (a-d)	Shuttle valve	Jammed in the 'normal' position	1E-8
ShVe2 (a-d)	Shuttle valve	Fail to close in either position	1E-7
MAe1	Main landing gear actuator	Jammed in 'up' position	5E-8
MAe2	Main landing gear actuator	Major leakage	5E-8
DAe1	Door actuator	Jammed in the 'closed' position	5E-8
DAe2	Door actuator	Major leakage preventing function	5E-8
ULe1	Uplock	Fails to unlock	5E-8
ULe2	Uplock	Major leakage preventing function	5E-8
ULc	Uplock	Locking mechanism fails (lock unlocks)	1E-9
DLe1	Door lock	Fails to unlock	5E-8
DLe2	Door lock	Major leakage preventing function	5E-8
DLc	Door lock	Locking mechanism fails (lock unlocks)	1E-9
HPe	Hydraulic pipe	Blockage	1E-9

community due to its wide application to failure behaviors in multi-technology, multi-energy, and diverse materials, such as the electromechanical hydraulic landing gear.

The component correct behavior is briefly described as follows.

- The isolation valve has two states; open and closed. When closed the isolation valve isolates the MLG hydraulics from hydraulic system pressure. When open the isolation valve allows hydraulic system pressure to the MLG hydraulic system. The isolation valve default position is closed, a solenoid opens the valve when commanded by the LGC.
- The selector valve has three states; down, up, and neutral. When the selector valve is in the neutral position it isolates the main landing gear actuator (retraction actuator), door actuators and uplocks from hydraulic pressure. When in the down position the selector valve supplies hydraulic pressure to the uplock unlock piston, the 'open' side of the door actuator, and the 'extend' side of the main landing gear actuator. When in the up position the selector valve supplies hydraulic pressure to the 'close' side of the door actuator and the 'retract' side of the main landing gear actuator. The selector valve default position is neutral, solenoids move the selector valve to the 'up' or 'down' position when commanded by the LGC.
- The main landing gear (MLG) actuator extends and retracts the landing gear. When hydraulic pressure is supplied to the 'extend' side of the MLG actuator piston the landing gear is pushed down into the fully extended position. When hydraulic pressure is supplied to the 'retract' side of the MLG actuator piston the landing gear is pulled up into the landing gear bay, where it engages with the uplock hook which latches closed.
- The door actuator is functionally identical to the MLG actuator. Each door has a door actuator. The door actuator opens and closes the door. When hydraulic pressure is supplied to the 'open' side of the door actuator piston the door is pushed open into the fully open position. When hydraulic pressure is supplied to the 'close' side of the door actuator piston the door is pulled into the fully closed position, where the door engages with the door lock hook which latches closed.
- The uplocks and door uplocks are functionally identical. The uplocks hold the landing gear and doors closed in flight. When hydraulic pressure is supplied to the 'open' side of the piston the hook moves into the unlocked position allowing the landing gear/doors to open. When hydraulic pressure is removed from the uplock a spring pushes the hook back into the closed position. When the hook is in the closed position the landing gear/door can

re-latch with the uplock hook as the actuators pull the landing gear/doors closed.
- The emergency valve has two states; open and closed. When closed the emergency valve isolates the MLG hydraulic system from emergency hydraulic system pressure. When open, the emergency valve allows hydraulic system pressure to the MLG hydraulic system. The emergency valve default position is closed, a solenoid opens the valve when commanded by the LGC.
- The shuttle valves 'shuttle' pressure between the main and emergency systems. The default position of the shuttle valve is to allow main system pressure to the actuators and uplocks. The shuttle valves are pressure biased, so when the emergency system is pressurized they close normal pressure and open emergency pressure to the actuators and uplocks allowing the emergency hydraulic system to extend the landing gear. The system contains four shuttle valves.

4 Fault tree analysis

The FTA is a logical, functional, and causal (event-based) method. FTA is a top-down approach and hence a deductive analysis [39] that identifies a potential failure as a top event and evaluates all possible ways in which this event could occur by considering the interrelationships of basic events or conditions that lead to the top event. A single component may fail in many ways. In addition, the number of failure modes explodes with the refinement of the system at the subsystems and component level and the increase in interconnections. The model refinement as opposed to abstraction is related to breadth and the depth of the tree. There are only 11 components. We can add lower branches by distributing component failures to component internal structures, such as a solenoid or spring-related faults or ball friction in the shuttle valve or cracking. If there is further detail available in the components, the faults can be broken to atomic levels to the discrete parts. This could be an endless exercise and a design space explosion problem. The key is to stay abstract in the model detail and still be able to capture the majority of the failure domain.

All events are statically evaluated. However, dynamic FTA [40, 41] may evaluate event outcome at time t by employing Markov models. Dynamic FTA exploits priority, sequential and spare gates and it is suitable for fault analysis in race conditions or temporal repeatability of failure events. Dynamic FTA may consider causality, time conditions, and dependency requiring advanced statistics. In the real world, most events occur one at a time which suffices static FTA analysis. The static FTA employs conventional AND and OR logic gates. Boolean AND failure event is a product $P(and) = P(\cap) = \prod_i^k P_x$ of all input failure events P_x and Boolean OR is a sum $P(or) = P(\cup) = \sum_i^k P_x$ of input events.

4.1 Assumptions

The following assumptions are necessary for the failure mode analysis:

- The door would not hold the landing gear if the MLG uplock fails.
- The pipe blockage may occur anywhere in the hydraulic network but no more than once at a time.
- The failure events are statistically independent notwithstanding dependencies in component failures for a top-level failure event that may exist. Events A and B are said to be independent when the probability of A given that B has occurred according to Bayes' theorem of conditional probability is $P(A|B) = P(A)$ and $P(B|A) = P(B)$ such that $P(A \cap B) = P(A)P(B)$. One may think of the conditional probability as there is an overall dependency of every component that the gear might extend out. For example, the fluid can flow through the selector valve only if the isolation valve opens. However, an isolation valve failure does not imply a selector valve failure. This also means one failure input does not affect another failure on the same logic gate and hence every failure event could occur separately and would not be triggered by a different component at the same time.
- The cruise and extension flight modes are mutually exclusive or disjoint; therefore, they may not manifest simultaneously [42] and do not have any common outcome. For probabilities of failure $P(Ext)$ for an event Ext in the extension mode and $P(Cr)$ for event Cr in cruise mode, we have

$$\begin{aligned} P(Ext \cap Cr) &= 0 \\ P(Ext \cup Cr) &= P(Ext) + P(Cr) \\ P(Ext|Cr) &= 0 \\ P(Cr|Ext) &= 0 \end{aligned} \tag{1}$$

  Hence, $P(IVe|IVc) = 0$ in Table 2 for 'Fails to open' (extension mode) vs. 'Uncommanded movement to open position' (cruise mode).
- The failure events within a mode are not mutually exclusive such that a non-zero total probability of failure exists with the manifestation of two or more failure events, hence in extension mode:

$$P(Ext_1 \cup Ext_2) = P(Ext_1) + P(Ext_2) - P(Ext_1 \cap Ext_2) \tag{2}$$

  where Ext_1 and Ext_2 are two arbitrary failure events of the extension mode.

4.2 Ordering and sequencing

The energy transfer is considered in the following sequence achieving the correct order of hardware actuation:

1. main hydraulic power supply → isolation valve → selector valve (if the main hydraulic power supply fails then emergency hydraulic power supply → emergency valve)
2. shuttle valves
3. door lock → door actuator
4. MLG lock → MLG actuator

5 Fault tree analysis in the extension mode

The hydraulic description in Fig. 1 is logically transformed into a fault tree, as shown in Fig. 2. Using the failure rates listed in Table 2 the overall failure rate for a single flight cycle is computed. The contribution of non-exclusivity of events according to Eq. 2 is − 8.36E-07% for 5000 flight cycles. Ignoring this negligible increase resulted in Eq. 3 which can be deduced from Fig. 2:

$$\begin{aligned} P(Ext) = &(P(EVe) + P(ShVe1) \cdot 4 + P(HPe2)) \\ &\cdot (P(IVe) + P(SVe) + P(HPe1)) \\ &+ (P(DLe1) + P(DLe2) + P(ShVe2a)) \\ &+ (P(ULe1) + P(ULe2) + P(ShVe2b)) \\ &+ (P(DAe1) + P(DAe2) + P(ShVe2c)) \\ &+ (P(MAe1) + P(MAe2) + P(ShVe2d)) \\ &+ P(HPe) \end{aligned} \tag{3}$$

The procedure is extended by scaling failure rate per cycle to 10, 100, 1000, 2500 and 5000 cycles. Eq. 3 gives failure rates shown in Table 3. It can be seen that Req 3 is met for one cycle. The probability is already higher than 1.00E-06 in just 2 cycles. As a consequence, Req 4 is also not met either which expects failures to rise toward the overhaul period and not at the beginning of life.

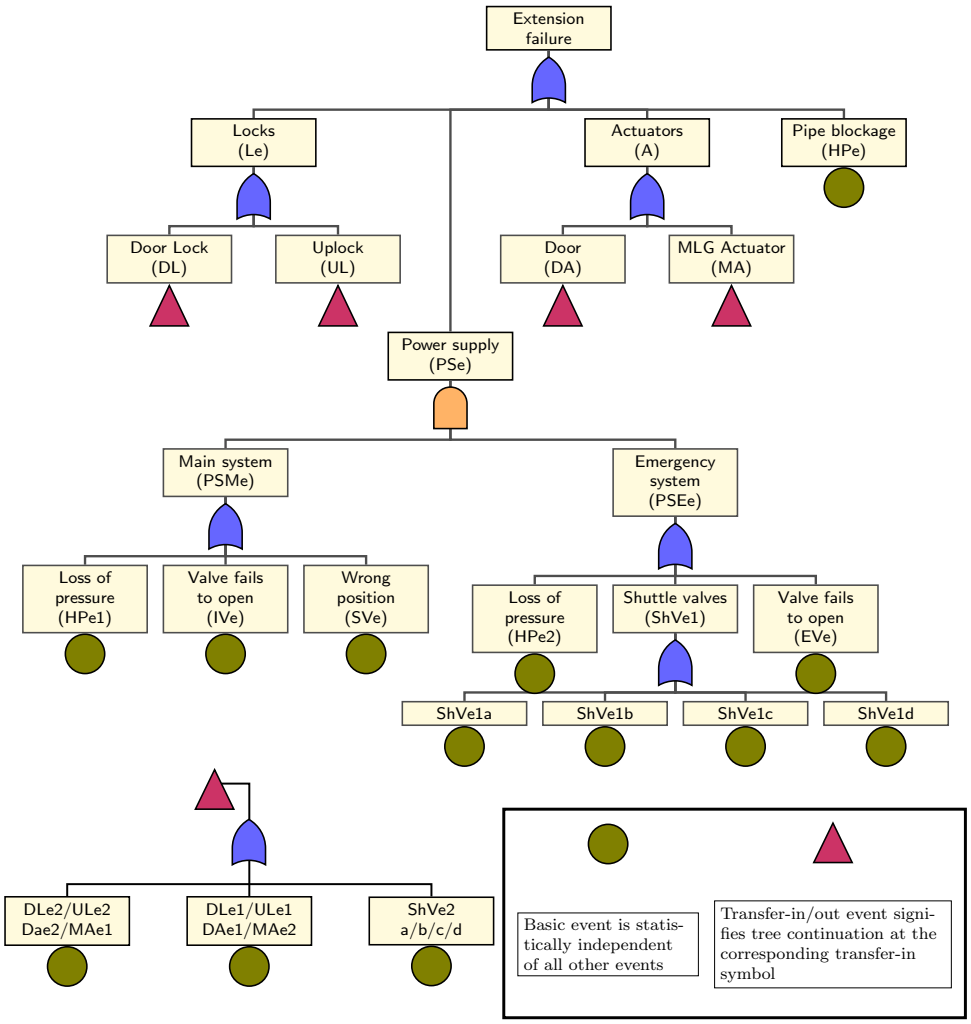

Fig. 2 Physical hydraulic description in Fig. 1 is transformed to logical connections in a fault tree

Table 3 Failure rate linearly rise in the extension mode with flight cycles

Flight cycles	Overall failure rate
1	8.02E-07
10	8.07E-06
100	8.64E-05
1000	1.43E-03
2500	5.92E-03
5000	1.97E-02

5.1 Cut set and minimal cut set

Although there is no explicit requirement for a single-point failure during extension, the single failures are worth investigating, while the gear is being deployed. Besides apprising the customer of the system integrity in the extension mode, this knowledge will be advantageous when architectural changes are contemplated that affect both modes.

A set of basic events that causes a top-level failure is called a cut set. The different combinations of component failures responsible for extension failure are organized in cut sets. The cuts sets may be chalked out in Fig. 2 by inspection. If removal of any event leaves the combination no longer a cut set, the set is called a minimal cut set [42, 43]. To determine the cut sets, the failure events are organized according to component type, e.g., the pipes (HPe), the locks (Le), and the actuators (A). Based on such configuration, the following minimal cut sets ($Cext_i$) for the extension mode are obtained:

$$\begin{aligned} Cext_1 &= \{HPe\} \\ Cext_2 &= \{Le\} \\ Cext_3 &= \{A\} \\ Cext_4 &= \{PSMe, PSEe\} \end{aligned} \tag{4}$$

where

$$\begin{aligned} Le =& \{ULe1 \cup ULe2 \cup DLe1 \cup DLe2 \\ & \cup ShVe2a \cup ShVe2b\} \\ A =& \{MAe1 \cup MAe2 \cup DAe1 \cup DAe2 \\ & \cup ShVe2c \cup ShVe2d\} \\ PSMe =& \{HPe1 \cup IVe \cup SVe\} \\ PSEe =& \{HPe2 \cup EVe \cup ShVe1a \\ & \cup ShVe1b \cup ShVe1c \cup ShVe1d\} \end{aligned}$$

The minimal cut sets reveal system vulnerabilities. A cut set containing a single event is first-order [44]. All first-order cut sets reduce the system availability and reliability. There are 13 such cut sets. Moreover, there are second-order cut sets. The second-order requires that two components fail at a time. There are 18 possibilities that the system could fail in the second-order case, e.g., if the emergency and the main hydraulic power supplies fail ($PSEe \cap PSMe$).

5.2 Comparison to the bathtub lifecycle failure model

We inspect if the failure trends have any similarity to the bathtub reliability model. We derived the trends with polynomials. Typically, one of the targets in a bathtub model is to find a constant failure rate in the useful life. Another target is to get more useful life through the spread of bathtub. If this behavior can be determined, the aircraft maintenance organization can plan. This is required in the Safety Management Systems (SMS) in the airline industry. The constant failure rate is a key parameter, because one can find out when the failures are likely to occur and the span between any two successive failures would tell when the maintenance cycle is due.

The failure rates calculated with the FTA method are illustrated by the solid black line in Fig. 3. This piecewise linear increase in the failure rates continues until the overhaul period. The dotted lines illustrate analytic approximations to other types of failure models. For example, until midway to the overhaul period (2500 cycles), the rates conform well to the power model. This is confirmed by a strong fit with the $R^2 \approx 1$ (coefficient of determination) indicating the dependent variation in the power regression is largely related to the independent variation in the input failure rates computed with the FTA. Beyond the midway, the failure response trend can be approximated with a linear failure model which reflects a higher variation in the response compared to the power model. The FTA predicted trend does not reflect the aging behavior as expected in the composite bathtub model typically developed by splining Weibull [45] or other distributions [46, 47], either in the useful life or in the wear-out period toward the overhaul. The systems analyst may spline the best models to give a full 5000 cycle approximation. Effectively, the task of failure population fitting is similar to identifying the shape, location, and scaling parameters of a cumulative Weibull distribution. $R^2 = 0.69111$ indicates the variation in the response is weakly explained by the input computed with the FTA. Therefore, a constant failure rate (λ) which indicates random failures in the useful life and is typically used in estimating the Mean Time Between Failure ($MTBF = {}^1/_{\lambda}$) is not obvious.

The constant failure rate is not obvious as the analysis does not use failure population behavior that the Weibull or a similar curve would provide. For such analysis, a large data set in different lives, e.g., infant, random failure life, and the wear-out is required. Since such data is not easily available, we use component failure rates without any regard to the failure distribution (exponential, Gaussian, Poisson,

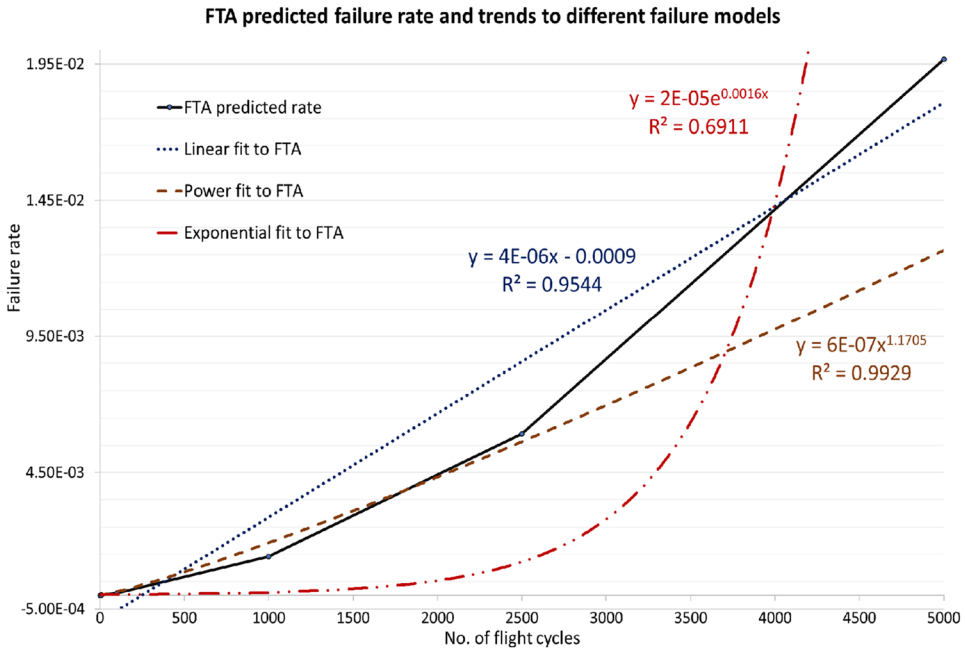

Fig. 3 Extension mode failure rate over time and fitness to mathematical approximations of failure rates

Weibull, etc.) that the rates follow. We then curve fit failure behaviors at the component-level and system-level. From the specific cases of algebraic plots, we attempt to draw a general constant failure rate which typically is obtained through statistical analysis in the reliability theory. In Fig. 3, the constant failure rate will exist in 500–2800 cycles and it will be less than 4.5E-3.

5.3 Subsystem and component failures

Before architectural improvements are considered, it is important to investigate the sources of failures. The impact of each event would be helpful to justify the improvement. To pinpoint the relevant error causes multiple FTAs were created and their culminated data is shown in Table 4. In every analysis, one component is assumed to be perfectly functional. The zero entries illustrate the components set at zero failure rate, e.g., the failure rate of the event HPe = 0 per flight cycle (no loss of pressure). The single failure rate is subtracted from the new and better overall system failure. Subsequently, the resulting delta for every fault tree is compared. The highest delta is produced by the component that caused the biggest impact. The deltas were summed up to calculate a percentile impact that each event had on the overall system reliability. This process is repeated for 1, 10, 100, 1000, 2500 and 5000 flight cycles. Thus, the contribution of each component to the overall failure is visible over time.

Figure 4 illustrates varying behavior in failure rates considering the subsystems. The hydraulic failure exponentially grows with the increase in flight cycles, while actuators and locks failures follow an inverse trend, i.e., exponential decay. The early cycles are dominated by the failure of actuators and locks. The blockage failure rate is time-independent.

Further insight into the subsystem failures is obtained in Fig. 5 which illustrates the contribution by a single component over time. However, some failures might occur several times, such as a leak, a shuttle valve jamming, and unjamming or two uplocks failing. Therefore, for one cycle the total impact is 49.9% for the 4x shuttle valves and 24.9% for leakages in 1x door actuator, 1x MLG actuators and 2x uplocks. Over 5000 cycles, the pumps are a major contributor to the failure rate and induce positive exponential rates. Therefore, consideration for redundant pumps warrants care.

To get insight into Req 4, approximate failure models are developed to tell (1) the culprit components (2) the maintenance due time in the current architecture. This enables an SMS organization determine maintenance requirements and plan maintenance operations much sooner in the product lifecycle, i.e., right at the preliminary design level. In addition, as stated earlier, the customer would weigh the merits of design improvement (new architecture) vs. extra maintenance cost (present architecture).

6 Fault tree analysis in the cruise mode

Failure analysis is simpler in the cruise mode, since the problem concerns holding the mechanisms in the upright position avoiding any multibody dynamical movement. The integrity failure of inadvertent extension of gear or door $P(Cr)$ is determined with the fault tree in Fig. 6.

The cut set analysis allows investigation of the single point failures in the system that need to be eliminated to

Table 4 Full fault tree computations for the top-level event failure to fully extend the landing gear in 5000 cycles are used to isolate the failure contribution of components and analyze their impact on the system

Events	Failure rates												
Top	5.6E-04	5.6E-04	5.6E-04	4.0E-04	5.6E-04	5.6E-04	5.6E-04	5.6E-04	5.6E-04	4.0E-04	5.6E-04	5.3E-04	5.3E-04
HPe	5.0E-07	0.0E+00	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07
Pse	1.6E-04	1.6E-04	1.6E-04	3.1E-07	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.3E-07	1.6E-04	1.6E-04	1.6E-04
PSEe	1.3E-02	1.3E-02	1.3E-02	2.5E-05	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02
EVe	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06
HPe2	1.3E-02	1.3E-02	1.3E-02	0.0E+00	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02
ShVe1a	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06
ShVe1b	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06
ShVe1c	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06
ShVe1d	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06
PSMe	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.0E-05	1.3E-02	1.3E-02	1.3E-02
IVe	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06	5.0E-06	5.0E-06
HPe1	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	0.0E+00	1.3E-02	1.3E-02	1.3E-02
SVe	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	0.0E+00	5.0E-06	5.0E-06
Le	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	1.8E-04	1.8E-04
UL	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	7.5E-05	7.5E-05
ULe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00	2.5E-05
ULe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00
ShVe2a	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05
DL	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04
DLe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
DLe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
ShVe2b	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05
A	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04
MA	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04
MAe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
MAe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
ShVe2c	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05
DA	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04
DAe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
DAe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05
ShVe2d	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05

Table 4 (continued)

Events	Failure rates												
Top	5.1E-04	5.3E-04	5.3E-04	5.1E-04	5.3E-04	5.3E-04	5.1E-04	5.3E-04	5.3E-04	5.1E-04	**Delta**	Impact (%)	
HPe	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	5.0E-07	0.07	
Pse	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	1.6E-04	**PSe**	43.90	
PSEe	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	PSEe	21.95	
EVe	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
HPe2	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.6E-04	21.91	
ShVe1a	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
ShVe1b	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
ShVe1c	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
ShVe1d	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
PSMe	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	PSMe	21.95	
IVe	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
HPe1	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.3E-02	1.6E-04	21.93	
SVe	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	5.0E-06	6.3E-08	0.01	
Le	1.5E-04	1.8E-04	1.8E-04	1.5E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	2.0E-04	**Le**	28.02	
UL	5.0E-05	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	UL	14.01	
ULe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
ULe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
ShVe2a	0.0E+00	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	7.00	
DL	1.0E-04	7.5E-05	7.5E-05	5.0E-05	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	DL	14.01	
DLe2	2.5E-05	0.0E+00	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
DLe1	2.5E-05	2.5E-05	0.0E+00	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
ShVe2b	5.0E-05	5.0E-05	5.0E-05	0.0E+00	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	7.00	
A	2.0E-04	2.0E-04	2.0E-04	2.0E-04	1.8E-04	1.8E-04	1.5E-04	1.8E-04	1.8E-04	1.5E-04	**A**	28.02	
MA	1.0E-04	1.0E-04	1.0E-04	1.0E-04	7.5E-05	7.5E-05	5.0E-05	1.0E-04	1.0E-04	1.0E-04	MA	14.01	
MAe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
MAe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	3.50	
ShVe2c	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	0.0E+00	5.0E-05	5.0E-05	5.0E-05	5.0E-05	7.00	
DA	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	1.0E-04	7.5E-05	7.5E-05	5.0E-05	DA	14.01	
DAe2	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00	2.5E-05	2.5E-05	2.5E-05	3.50	
DAe1	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	2.5E-05	0.0E+00	2.5E-05	2.5E-05	3.50	
ShVe2d	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	5.0E-05	0.0E+00	5.0E-05	7.00	
											Sum	7.1E-04	100.0

In the first column, all components have non-zero failure rates. In other columns, one component (0 entries) is kept ideal at 0 failure rate. The difference in failure rate from the original top-level failure rate is given by the Delta. No component has a net failure rate of 0

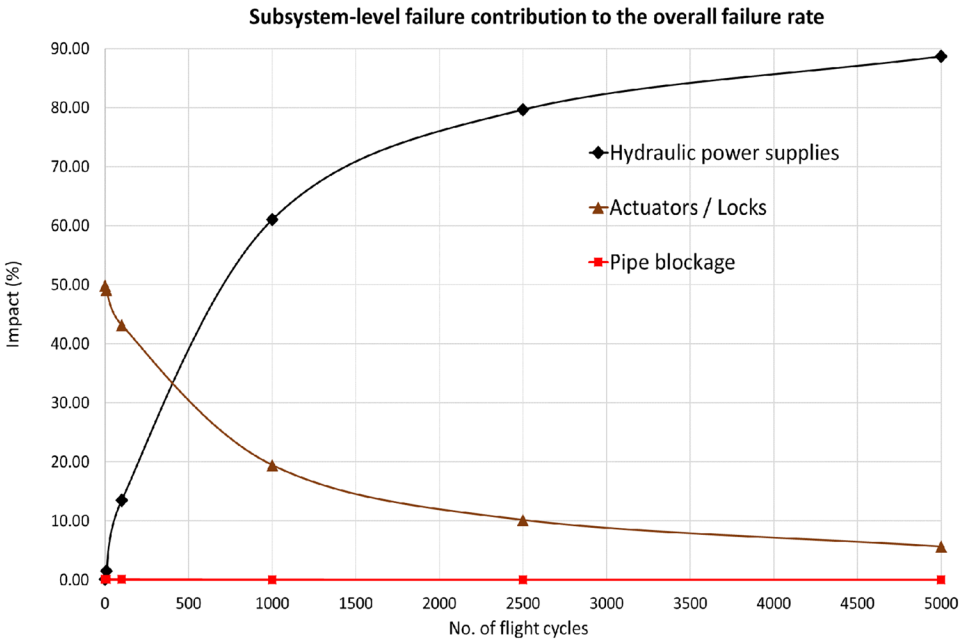

Fig. 4 Impact of the subsystems to the overall failure rate over time in the extension mode

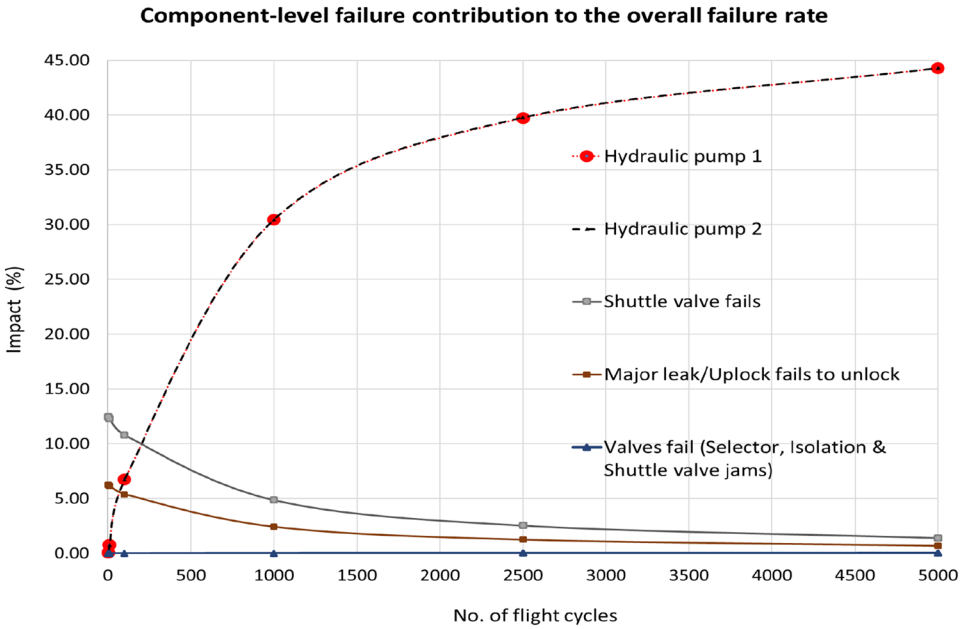

Fig. 5 Impact of a single component type to the overall failure rate over time in the extension mode

meet Req 1. The components participating in the cruise mode were organized in locks and hydraulic system giving the following minimal cut sets (Ccr_i) in the cruise mode:

$$\begin{aligned} Ccr_1 &= \{DLc\} \\ Ccr_2 &= \{ULc\} \\ Ccr_3 &= \{IVc, SVc\} \\ Ccr_4 &= \{EVc\} \end{aligned} \tag{5}$$

Reviewing the cruise mode fault tree from the top again, we can state

$$\begin{aligned} P(Cr) &= P(Lc) + P(PSc) \\ P(Cr) &= P(DLc) + P(ULc) + \\ P(IVc) &\cdot P(SVc) + P(EVc) \end{aligned} \tag{6}$$

As DLc and ULc have the same failure rates (1E-9) as well as IVc, SVc and EVc (1E-6), we let

$$\begin{aligned} a &= P(DLc) = P(ULc) \\ b &= P(IVc) = P(SVc) = P(EVc) \end{aligned} \tag{7}$$

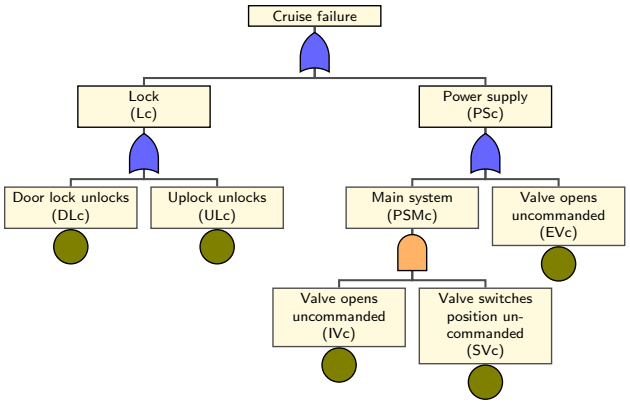

Fig. 6 Cruise mode fault tree

Table 5 Failure rate linearly rise in the cruise mode with flight cycles then flatten out

Flight cycles	Overall failure rate
1	1.00E-06
10	1.00E-05
100	1.00E-04
1000	1.00E-03
2500	2.51E-03
5000	5.035E-03

Therefore

$$P(Cr) = (a + a) + ((b \cdot b) + b) \tag{8}$$

The Boolean absorption rule [48] $(x + (x \cdot y) = x)$ eliminates a cut set that has common events contained in another cut set. The idempotent rule $(x \cdot x = x)$ eliminates duplicate failures within a cut set, e.g., same type of valves failing together [49]. With such algebraic reductions, we get

$$P(Cr) = a + b \tag{9}$$

Thus, the cruise mode cut sets are

$$\begin{aligned} Ccr_1 &= \{a\} \\ Ccr_2 &= \{b\} \end{aligned} \tag{10}$$

If the emergency valve opens uncommanded or one of the locking mechanisms fails, a single point failure would occur, so Req 1 is not met. Although the contributing events are non-exclusive, the method from Eq. 2 is neglected again as the difference is not considerable (− 2.00E-07%). Eq. 6 determines the probabilities of failure listed in Table 5.

6.1 Comparison to the bathtub lifecycle failure model

Req 2 and 4 were not met as can be seen in Table 5 and Fig. 7. The figure illustrates failure rate behavior to different trend models with $R^2 > 95\%$ in all cases. While the linear approximation is a perfect fit, it might not be practical. If the rise in the failure rate because of wear and tear is not steep, the linear model may be suitable for less than 2500 flight cycles. Beyond 2500, non-linear models match better.

In Fig. 7, the constant failure rate is pronounced. It would lie somewhere between 1000 to 2500 cycles and the average rate would be less than 1.4E-3. With more cycles, the wear-out will get worse. Recall failure rates are per flight cycle so scaling will be going on. One of the goals is to find a constant failure rate and let the stakeholder know when wear-out

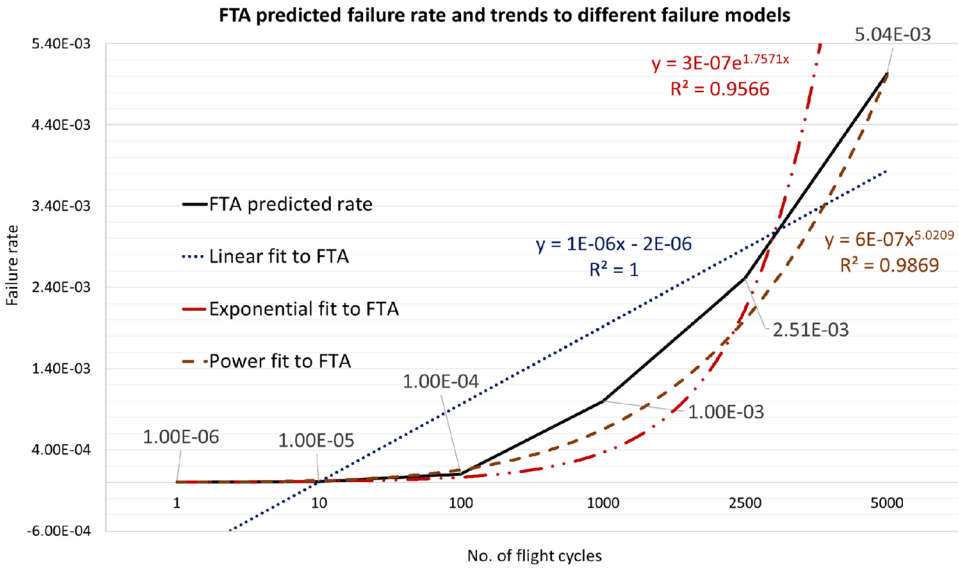

Fig. 7 Cruise mode overall failure rate over time

would begin. This is already happening much earlier than 5000 cycles.

6.2 Subsystem and component failures

The procedure for extension mode failure isolation from Section 5.3 is used. Figure 8 shows the contribution of subsystems to the overall failure rate. For one cycle, the locks contribute very little to the top failure event. This changes rapidly up to 10 cycles beyond which the failure rate is very steady. The impact due to locks in 100 cycles is 39.92% and for 5000 cycles it is 40%. Although the flight cycles increase by 4900%, the impact only rises by 0.05%.

It is not necessary to split the subsystems in Fig. 8 into components as the failure rates were similar, e.g., both locks had the same failure rate and thus, the same impact. The same applies to the valves for the hydraulic pressure supplies and their valves. Every component had the same impact ($\approx$ 20%) between the mid to overhaul cycle. However, the main hydraulic system is less probable to fail as both valves would have to malfunction simultaneously (IVc and SVc).

7 Architectural improvements

The failing requirements may be met by modifying the architecture, relaxing the requirements, or sourcing high-rel components. We explore new reconfiguration of the landing gear architecture using existing components, because their failure rates are known. This may be done by introducing redundancy.

A natural dilemma arises whether to use parallel or series redundancy often weighing unfavorable and competing options, for example, achieving better reliability while adding mass, power, volume, flight software complexity, and cost. A shuttle valve stuck close will leave the hydraulic network unresponsive, whereas an open flow shuttle valve will also leave the system behavior undesired, since the fluid flow will always complete some path through the emergency or main hydraulic network, whether required or not. The problem, therefore, is determining the optimum number of series shuttle valves.

Canonical series and parallel structures [50] can be considered in the fault tree analogy and the contribution of redundant components may be assessed. Consider quad-valve topology in Fig. 9. An ideal shuttle valve 's' selects the high source between the main and emergency supplies. To actuate the landing gear door either the generic valves 'a' and 'b' may be opened using the main hydraulic power line or valves 'c' and 'd' may be opened using the emergency hydraulic supply. The valves 'a' and 'b' are in series to each other and 'c' and 'd' are also in series but 'a', 'b' together are in parallel to 'c' and 'd'. Let the probability that each series valve closes be p. Since one line may be used at a time and assuming that each valve functions independently of the others, the probability that pressure will through from the supply port P to the reservoir return port R is $P((A \cap B) \cup (C \cap D)) = P(A \cap B) + P(C \cap D) - P(A \cap B \cap C \cap D) = p^2 + p^2 - p^4 = 2p^2 - p^4$.

In the above elementary example, the goal is to trade-off the probability of success with the number of valves, and without applying constraints. To meet the safety requirements and failure rates this method is adequate but it does not consider the impact on the rest of the system domains, such as mass, volume, area, power and monetary cost. Barlow [51] suggests constraint-driven redundancy optimization. Mathematical constraints of mass and cost in the objective function help allocate optimal redundancy whether the

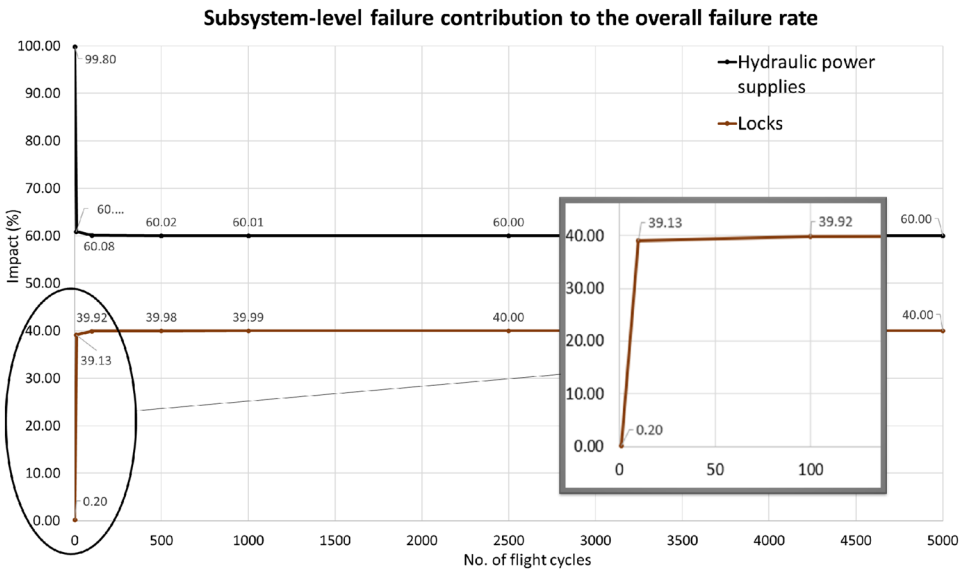

Fig. 8 Impact of the subsystems to the overall failure rate during cruise

Table 6 Overview of possible architecture improvements for the landing gear extension mode

Cycles	1	5000	1	5000
Architectural change	Overall failure rate		Failure rate improvement (%)	
1x redundant pump in main and emergency systems	8.01E-07	4.25E-03	0.08	78.38
1x shuttle valve (instead of 4x)	4.02E-07	1.77E-02	49.90	9.94

spare units are in series or parallel configuration. Constraint-driven optimization should be taken up at the program level when mission objectives are well-defined.

Our analysis shows a high failure rate of the pumps in early life. Improving failure rates of single components requires sourcing even better quality components. However, we restructure the system, use standby hardware, and analyze the new overall failure behavior due to all components without constraints.

7.1 Extension mode

Table 6 lists suggested architectural changes following a reconfiguration of the system in extension mode and Req 3 is met. These changes achieve good overall failure rate improvement incurring a minimal increase in the hardware. This is because the failure response of components is different in both short-term (infant/beginning of life) and long-term (wear-out/close to overhauling) operations and considering both modes. Moreover, a healthy battle exists between availability, integrity, and maintainability [52]. Therefore, it is feasible to address improvements for an overall optimal objective rather than improving a particular life segment. The designer should consider this trade-off for an overall objective function, e.g., removal of three shuttle valves increases the reliability but reduces the system availability and incurs a single-point failure.

Table 8 Summary of cross mode improvements

Flight mode	Overall failure rate	
	1 Cycle	5000 Cycles
Extension baseline	8.02E-07	1.97E-02
Extension improvement	4.01E-07	3.98E-03
% extension improvement from baseline	50%	80%
Extension improvement with cruise improvement (overall improvement 1)	5.01E-07	4.98E-03
% overall improvement 1 from extension baseline	38%	75%
Cruise baseline	1.00E-06	5.04E-03
Cruise improvement	4.00E-18	2.50E-07
% cruise improvement from baseline	100%	100%
Cruise improvement with extension improvement (overall improvement 2)	5.00E-18	3.75E-07
% overall improvement 2 from cruise baseline	100%	100%

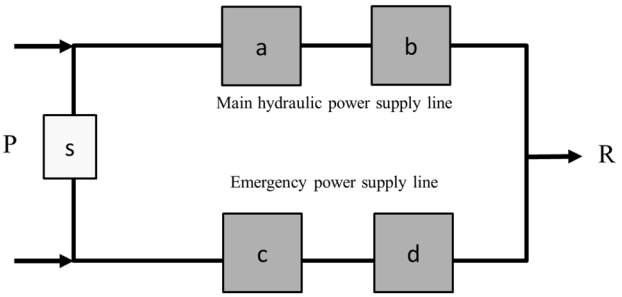

Fig. 9 Availability trade-off for series or parallel redundant components

7.2 Cruise mode

Table 7 shows improvement for long-term and short-term operational lives in the cruise mode. The third improvement eliminates single point failures and thus Req 1 is met. No first-order cut sets can be found in the system anymore. Req 2 fully meets as the overall failure rate is 4.00E-18 per flight cycle.

Table 7 Overview of possible architecture improvements for the landing gear cruise mode

Cycles	1	5000	1	5000
Architectural change	Overall failure rate		Failure rate improvement (%)	
1 × redundant emergency valve	2.00E-09	6.00E-05	99.80	97.61
1x door uplock, 1 × MLG uplock, 1 × redundant emergency valve	2.00E-12	2.50E-05	100.00	99.00
1 × redundant main valve, 1 × door uplock, 1 × MLG uplock, 2 × redundant emergency valve	4.00E-18	2.50E-07	100.00	99.99

7.3 Cross mode failure propagation

Any architectural improvement in one mode impacts the failure rate in the other mode. Therefore, a new FTA in the other mode becomes imperative. Table 8 captures the failure rate impact due to the changes in each mode. In extension mode, the overall improvement 1 from the extension improvement is 25% for 1 and 5000 cycles, while in the cruise mode, the overall improvement 2 from cruise improvement is 25% for 1 cycle and 50% for 5000 cycles. The overall probability of failure substantially decreased in each mode separately, however, improved compared to the baseline system. If the suggested improvements are applied simultaneously, the probability of failure decreases substantially but to a lesser degree. This trend is evident in Fig. 10 which shows the new bathtub is flatter during the useful life of the extension mode and the rise toward the overhaul period is gradual. The cruise mode failure trend is even flatter. Approximate polynomial models give excellent fits for failure models in both modes. Req 1, Req 2, and Req 3 still met as can be seen in Table 8. There is a tradespace analysis here as to the mission requires better reliability in what mode. The new architecture incorporating the improvements is presented in Fig. 11. In addition to a lower overall failure rate, the blockage probability is reduced as fewer pipes are required.

7.4 Impact on requirements

So far, we have proved Req 1, Req 2, and Req 3; refer to Sects. 7.1, 7.2, Table 7, and Fig. 11. The analysis shows that for 5000 cycles an overall failure rate below 1E-7 (Req 2 catastrophic failure in cruise mode) and 1E-6 (Req 3 critical failure in extension mode) are unachievable even though redundancy and system reconfiguration significantly reduced the rate. Thus Req 4 is open for negotiation as it is not fully met for both modes, although, maintenance is required after 2 cycles in the extension mode, while the cruise mode is maintenance-free for as many as 3223 flight cycles. For short-term operations, improvements were needed to prevent the shuttle valves from jamming and leakage. For long-term operations redundant pressure supplies were necessary.

Component failures rates given in Table 2 can be allocated to the component internal structure thereby lowering the abstraction to capture different types of jamming failures [53]. For instance, the event ULe1 uplock fails to unlock may be broken down to spring and hook failures. Doing this will increase the tree depth to an even finer level giving more insight into failure propagation upward in the tree.

8 Outlook

The FTA may be extended to other flight modes, e.g., taxiing and retraction mode. The low-level failures rate may be categorized to the agreed definition of major and minor severity levels. The impact and mitigation of major and minor levels

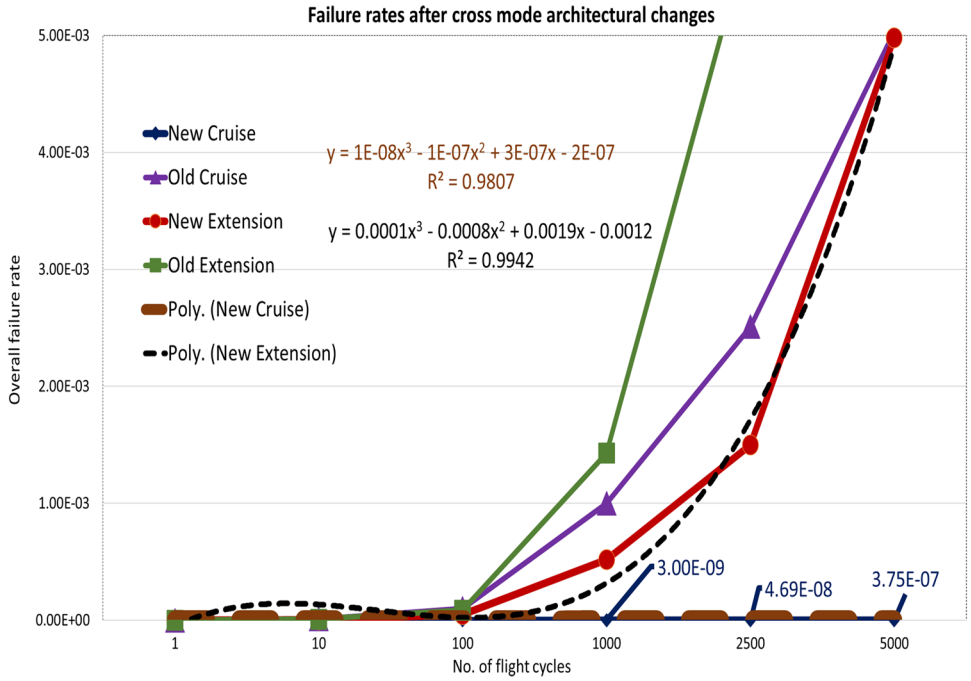

Fig. 10 Illustration of improved failure rates after cross mode architectural changes

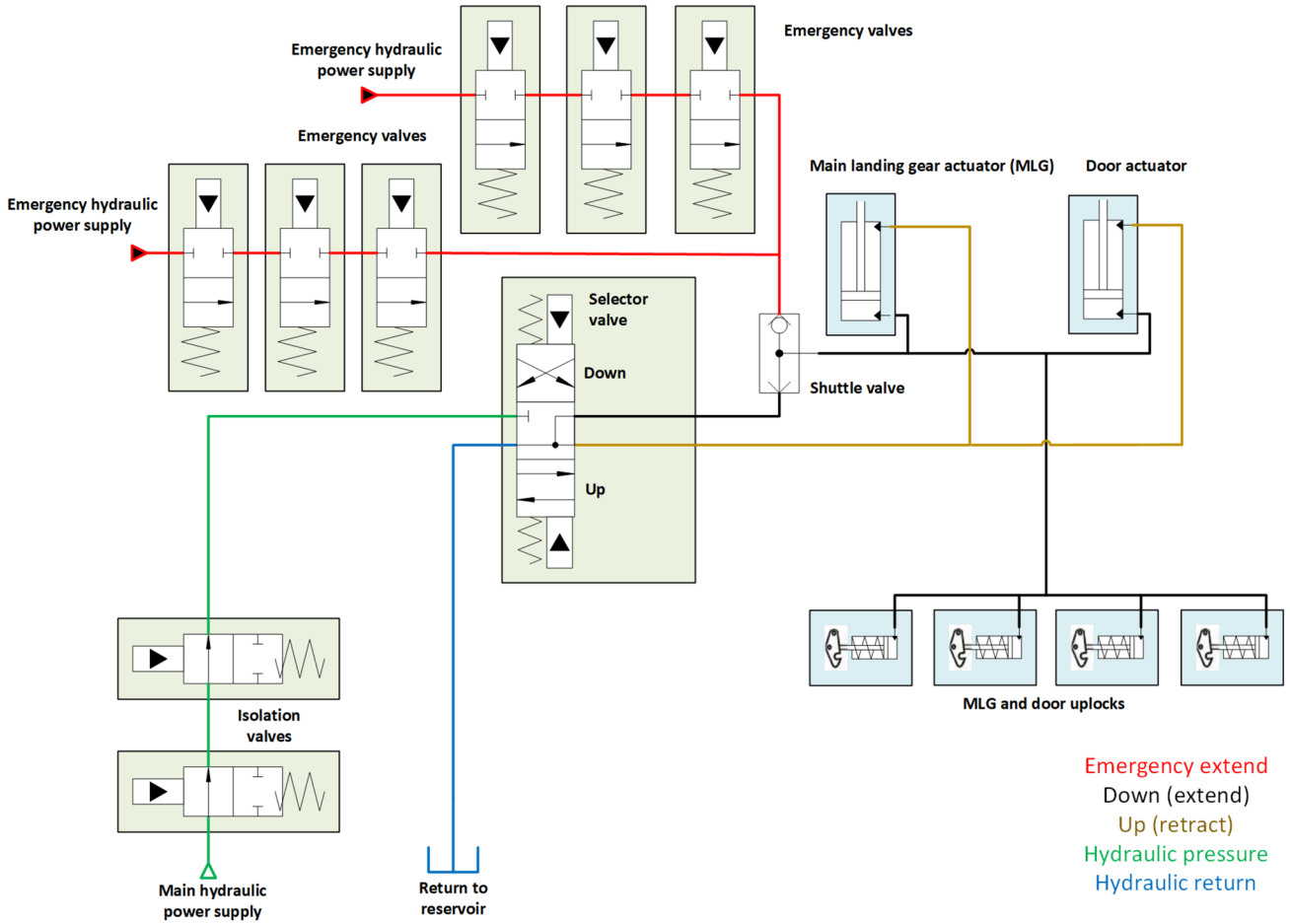

Fig. 11 Improved architecture achieves a compromise in extension and cruise modes safety

should be looked into as these types of failures do not render the system completely dysfunctional but their long-term manifestation or their frequency of occurrence may appear into a permanent failure or a failure with a higher severity level. In the extension mode, the system did not account for the direction of motion whether folding inward to the fuselage or fore. Such refinements of the model will complicate the abstractions and consequently the FTA. Dormant failures usually shroud in the backup components. These could be analyzed in the emergency hydraulic supply or the suggested redundancies. Timing analysis is required to estimate the operation time each actuator takes to fully deploy. This kind of analysis would have derived requirements from a top-level system requirement of gear full deployment, e.g., 15 s. Furthermore, a necessary analysis is the correct sequencing of component operation when commanded by the LGC to avoid a race condition of actuators and controllers, such as the gear beginning to extend, while the door uplock angle has not widened enough. Similarly, retraction should not start unless, for instance, the downlock disengages the angle reduces by 5 degrees to allow margins for separation clearances. The kinematic constraints on time to free mechanical movement and multibody separation dynamics make up the component-level requirements and induce additional failure modes. Correct sequencing is necessary for safety–critical software routines of the LGC or a manual procedure at the cockpit. The safe angular velocity of deployment imposes requirements on hydraulic pressure, force, torque, and locking angles. In the present state, there are no downlocks and thus the gear will bounce back on a touchdown. Therefore, a new architecture is needed for touchdown mode. during taxiing the gear has the backward motion of the wheels, the steering system is involved as well as braking. Touchdown considers the tilt of the gears either aft or fore. These functions are not taken up in the current architecture and their failure modes and faults would exponentially explode with the number of components.

The customer will be apprised about the possibilities and given the mitigation options. Any capability not meeting and needing to be still met will be shared with incurring cost, extension in schedule, and risk to the development program as well as the performance that can be ultimately met.

The customer and supplier will agree to a further course of action.

9 Conclusion

We have shown a process of validating safety requirements for the main landing gear hydraulic system architecture that was given with failure rates of components. FTA method was used to determine the top-level failure rates asked in the requirements. The first pass of our analysis shows that all requirements cannot be validated in the given architecture for both cruise and extension modes. By incorporating redundancy, the safety requirements can be partially met to a better degree. However, 5000 flight cycles is still a very long period to the overhaul and certain components require upkeep sooner. This result is a starting point between a supplier and customer to re-negotiate the requirements and the architecture on using even highly reliable components, additional trade studies for redundancy, and eventually merits of weight and balance, cost, and schedule. Other options are simply relaxing the severity level or cutting down the number of flight cycles for maintenance. The analysis showed when the components are due maintenance. This was done by approximating the failure behavior of the landing gear in both extension and cruise modes and isolating the individual impact of components on the system failure. The analysis shows the increase in wear and tear for cruise and extension modes of the flight sooner than 5000 flight cycles. The result can be used for planning maintenance. The analysis also showed that serial redundancy in the emergency valve and a single shuttle valve reduces the system failure; however, this introduced a single-point failure. All these directions to further analysis are up for dialogue between the supplier and customer and require further trade studies. Other architectural improvements are also possible. The new architecture should satisfy all types of requirements, not just safety.

The design space is huge for exploring architectural improvements and the possibilities are numerous. The impact of the change in each architecture would need a fresh look at the whole system. We leave the discussion open to the stakeholder with some potential options for improvement and meeting safety. The stakeholder would decide the impact on weight and balance and the static envelope in the fuselage. Therefore, the new architecture, while meeting safety would need to be justified for mass/power/volume and cost.

Our work has shown, for a few safety requirements there is a huge tradespace in the landing gear lifecycle activities. The FTA can be an exhaustive exercise. The number of fault trees to be developed for safety analysis and their depth in the product hierarchy depend on the system selected and should be agreed upon in a contractual binding between the supplier and the customer at the program level. We did not mean to be rigorous but we showed that FTA gives useful insight into system behavior which could drive important systems engineering lifecycle activities, such as the requirements engineering, architecture trade studies, estimation of margins in the reliability budget, operational safety analysis, and planning for preventive maintenance.

Acknowledgements The authors are grateful to Dr. Steve Wright, Senior Researcher at UWE Bristol and formerly of Airbus, Filton, UK. Thanks also go to the anonymous reviewers who thoroughly reviewed the article to bring it to the present form. Funding for this work was provided by the Enterprise and Partnership office of UWE Bristol.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Kroes, M.J., Watkins, W.A., Delp, F., Sterkenburg, R.: Aircraft maintenance and repair, 7th edn. McGraw-Hill Publishing, New York (2013)
2. Currey, N.S.: Aircraft landing gear design: principles and practices. American Institute of Aeronautics and Astronautics, Inc, Reston, Virginia (1988)
3. Schmidt, R.K.: The design of aircraft landing gear. SAE International, Warrendale (2021)
4. NASA Systems Engineering Handbook, Revision 1., (Ed) Garrett Shea, National Aeronautics and Space Administration (NASA) NASA/SP-2007-6105, Washington, DC, USA (2007)
5. A guide to landing Gear system integration, AIR5451A Aerospace Standard, A-5 Aerospace Landing Gear Systems Committee, SAE International (2017)
6. System safety handbook. Federal aviation authority (2000)
7. System safety handbook. National Aeronautics and Space Administration (NASA) (2011)(2014)
8. NASA fault tree handbook with aerospace applications, version 1.1. National Aeronautics and Space Administration (NASA), Washington, DC, USA (2002)
9. Rausand, M., Hoyland, A.: System reliability theory: models, statistical methods, and applications, 2nd edn. Wiley-Interscience, Hoboken, New Jersey (2004)
10. Ericson, C.A., II.: Hazard analysis techniques for system safety. John Wiley & Sons, Inc, New Jersey (2005)
11. Hlinka, J.: Safety/reliability analyses of GA aircraft in design and certification stage in Czech Republic. Aviation **11**(4), 14–23 (2007)

12. Ossa, E.A.: Failure analysis of a civil aircraft landing gear. Eng. Fail. Anal. **13**(7), 1177–1183 (2006). (**ISSN 1350-6307**)
13. Bagnoli, F., Dolce, F., Colavita, M., Bernabei, M.: Fatigue fracture of a main landing gear swinging lever in a civil aircraft. Eng. Fail. Anal. **15**(6), 755–765 (2008). (**ISSN 1350-6307**)
14. Chang, Q.-C., Xue, C.-J.: Reliability analysis and experimental verification of landing-gear steering mechanism considering environmental Temperature. J. Aircraft **55**(3), 1154–1164 (2018)
15. Arena, M., Chiariello, A., Castaldo, M., Di Palma, L.: Vibration response aspects of a main landing gear composite door designed for high-speed rotorcraft. Aerospace **8**(2), 52 (2021)
16. Pritchard, J.: Overview of landing gear dynamics. J. Aircraft **38**(1), 130–137 (2001)
17. Sharma, S., Coetzee, E.B., Lowenberg, M.H., Neild, S.A., Krauskopf, B.: Numerical continuation and bifurcation analysis in aircraft design: an industrial perspective. Philos. Trans. Royal Soc., A **373**, 20140406 (2015)
18. Knowles, J.A.C., Krauskopf, B., Lowenberg, M.H., Neild, S.A., Thota, P.: Numerical continuation analysis of a dual-sidestay main landing gear mechanism. J. Aircraft **51**(1), 129–143 (2014)
19. Liu, X., Geng, S., Yu, X., Tong, J., Wang, Y.: Improved uncertain method for safety analysis of aircraft landing gear. Proc. Inst. Mech. Eng. (IMechE) Part G: J. Aerosp. Eng. **235**, 2547 (2021)
20. Alena, R. L., Ossenfort, J. P., Laws, K. I., Goforth, A., Figueroa, F.: Communications for integrated modular avionics. In: Proceedings of the 2007 IEEE Aerospace Conference, pp. 1–18 (2007)
21. Arcaini, P., Gargantini, A., Riccobene, R. E.: Development process of a safety-critical system: from ASM models to Java code. Int. J. Softw. Tools Technol. Transf. **19**, 247–269 (2017)
22. Teodorov, C., Dhaussy, P., Le Roux, L.: Environment-driven reachability for timed systems: safety verification of an aircraft landing gear system. Int. J. Softw. Tools Technol. Transf. **19**, 229–245 (2017)
23. Daniels, D.: Safety aspects of a landing gear system. In: Redmill F., Anderson T. (ed.) Developments in risk-based approaches to safety. In: Proceedings of the Fourteenth Safety-critical Systems Symposium, Bristol, UK, 7–9 February (2006)
24. Bittner, B., et al.: An integrated process for FDIR design in aerospace. In: Ortmeier, F., Rauzy, A. (eds.) Model-based safety and assessment. IMBSA. 2014 lecture notes in computer science, vol. 8822. Springer, Cham (2014)
25. Zhang, Y., Huang, Y., Xu, T., Liu, C., Tao, L.: Impact analysis and classification of aircraft functional failures by using improved FHA based on gray correlation. Grey syst.: Theory Appl. **11**(2), 213–221 (2021)
26. Boniol, F., Wiels, V., Aït-Ameur, Y., Schewe, K.-D.: The landing gear case study: challenges and experiments. Int. J. Softw. Tools Technol. Transf. **19**, 133–140 (2017)
27. Lu, L., Lei, J.: Design and reliability prediction of a distributed landing gear control system. Aircraft Eng. Aerosp. Technol. **82**(1), 15–22 (2010)
28. Banach, R.: The landing gear system in multi-machine hybrid event-B. Int. J. Softw. Tools Technol. Transf. **19**, 205–228 (2017)
29. Lindsey, N.J., Alimardani, M., Gallo, L.D.: Reliability analysis of complex NASA systems with model-based engineering. Available online: https://ntrs.nasa.gov/api/citations/20200000582/downloads/20200000582.pdf
30. Brown, E., Brown, J., Zaidi, Y.: MBSE approach to early lifecycle analysis of aircraft landing gear, presentation to model based systems engineering (MBSE). Interest Group of the International Council on Systems Engineering (INCOSE), UK (2021)
31. Haider, S.: Applying model based safety assessment for aircraft landing gear system certification, Annual Reliability and Maintainability Symposium (RAMS), pp. 1–7 (2020)
32. Failure modes, effects (and criticality) analysis (FMEA/FMECA): European Cooperation for Space Standardization (ECSS). ECSS-Q-ST-30-02C (2009)
33. DeLozier, R.C., Wilkinson, V.K.: A method of forecasting repair and replacement needs for naval aircraft: phase II, ORNL/TM 10179. Oak Ridge National Laboratory, Oak Ridge (1986)
34. Airworthiness directives, McDonnell Douglas Model 717-200 Airplanes, Docket No. FAA-2004-19987; Directorate Identifier 2004-NM-203-AD; Amendment 39-14105; AD 2005-11-03, Federal Aviation Administration (2005). Available online: https://ad.easa.europa.eu/blob/20051103.pdf/AD_US-2005-11-03_1
35. Airworthiness Directive, Landing Gear Control Handle Assembly, Bombardier Inc. Model CL-600-2B19 "Canadair Regional Jet" aircraft, serial numbers 7375 through 7632. Transport Canada (2003). Available online: https://ad.easa.europa.eu/blob/CF-2003-03_English.pdf/AD_CF-2003-03_1
36. Ramesh, A., David Twigg, D., Sharma, T.: Advanced methodologies for average probability calculation for aerospace systems. In: 26th International Congress on the Aeronautical Sciences (ICAS), International Council of the Aeronautical Sciences (2008)
37. Yang, J.W., Wang, J.H., Huang, Q., et al.: Reliability assessment for the solenoid valve of a high-speed train braking system under small sample size. Chin. J. Mech. Eng. **31**(47), 1–11 (2018)
38. Weibull, W.: A statistical distribution function of wide applicability. ASME J. Appl. Mech. **18**, 293–297 (1951)
39. Mobley, R.K.: Root cause failure analysis. Newnes, Boston, Massachusetts (1999)
40. Fault tree analysis (FTA). IEC 61025. International Electrotechnical Commission (IEC) (2006)
41. Merle, G., Roussel, J.-M., Lesage, J.-J., Bobbio, A.: Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events. IEEE Trans. Reliab. **59**(1), 250–261 (2010)
42. Rausand, M.: Reliability of safety-critical systems. John Wiley & Sons Inc, Hoboken, New Jersey (2014)
43. Kececioglu, D.: Reliability engineering handbook, vol. 2. Prentice Hall Inc, New Jersey (1991)
44. Denning, R.: Applied R&M manual for defence systems. GR-77. UK Ministry of Defence, London (2012)
45. Kao, J.H.K.: A graphical estimation of mixed weibull parameters in life-testing of electron tubes. Technometrics. **1**(4), 389–407 (1959)
46. Rinne, H.: The Weibull distribution a handbook. Chapman & Hall/CRC, Boca Raton, Florida (2009)
47. Abernethy, R.B.: The new Weibull handbook, 5th edn. R. B. Abernethy, North Palm Beach, Florida (2010)
48. Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F.: Fault tree handbook, NUREG-0492. Nuclear Regulatory Commission, U.S (1981)
49. Walker, M., Papadopoulos, Y.: Qualitative temporal analysis towards a full implementation of the fault tree handbook. Control Eng. Pract. **17**, 1115–1125 (2009)
50. Birolini, A.: Reliability engineering, 5th edn. Springer, Heidelberg (2007)
51. Barlow, R.E., Porschan, F.: Mathematical theory of reliability. Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania (1996)
52. Reliability, Maintainability, and Availability (RMA) Handbook. RMA-HDBK-006B. Federal Aviation Authority (2014)
53. Hussain, Y.M., Burrow, S.G., Henson, L., Keogh, P.: A review of techniques to mitigate jamming in electromechanical actuators for safety critical applications. Int. J. Progn. Health Manag. **9**(3), 1–11 (2018)