Inclusion of Reliability and Safety Analysis Methods in Modelica

Christian Schallert
German Aerospace Centre (DLR), Institute of Robotics and Mechatronics
82234 Wessling, Germany
christian.schallert@dlr.de

Abstract

A method is developed to combine techniques of reliability and safety analysis with the Modelica language, which is now widely used for the modelling and simulation of technical systems.

The method allows to perform a reliability or safety analysis on the system model that is created and used for simulation studies. The procedure automatically determines the so called minimal path sets or minimal cut sets of a system, its failure probability and critical components.

The reliability and safety analysis methods are incorporated in a Modelica library that is established for the modelling and simulation of aircraft on-board electrical power systems. The recent trend towards a broader use of electric system technologies on commercial aircraft has motivated the creation of this kind of model library, which supports the conceptual design and optimisation of on-board electrical systems regarding power behaviour, weight, reliability and safety.

Keywords: reliability; safety; fault modelling; redundant system; minimal path sets; minimal cut sets

1 Introduction

Much of the information needed for reliability or safety analysis is contained already in complex system models that are usually built in Modelica. The specific modelling additions needed, as well as the concept of an automated reliability and safety analysis procedure are described in this paper.

The analysis procedures evaluate the physical behaviour of a system model in multiple simulations. Representing not only the normal but also the faulty behaviour of components is needed as an addition to the modelling, as described in section 2.1. Section 2.5 illustrates the scope and method of the reliability and safety analyses and their relevance regarding aircraft on-board systems. A way of minimising the involved computational effort is outlined in 2.5.4.

Then, section 3.1 presents an example model of an electric power system of a recent large commercial aircraft. Subsequently, a safety and reliability analysis are conducted on the model for example scenarios, the results of which are graphically presented and discussed in sections 3.2 and 3.3.

2 Modelling Approach and Outline of Reliability and Safety Analysis Method

2.1 Component Fault Modelling

A variety of object-oriented model libraries has been developed in the Modelica language, as generally known. Typically, each component model contains a description of the normal operational behaviour by differential and/or algebraic equations.

For the purpose of reliability and safety analysis, the component models have to be enhanced to describe also the failure behaviour by physical equations. Basic examples are given hereafter by the model approach taken for some common electric components.

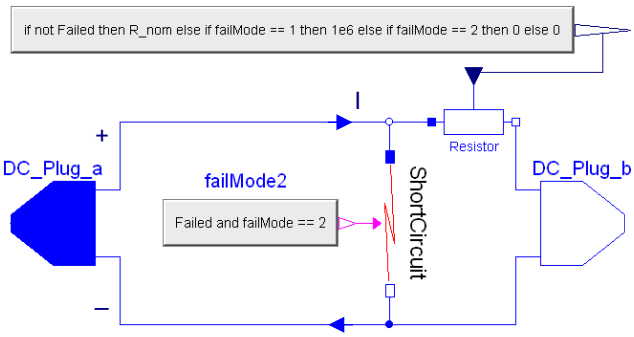


Figure 1: Modelica model of an electrical cable with normal and failure behaviour

A two-core electric cable can be described as an ohmic resistor. For the normal function of the cable, its resistance R is in the order of $R_{nom} \approx 10^{-1}$ Ω. An open circuit (O/C) failure of the cable is characterised by a very large resistance, e.g. 10^{6} Ω, whereas a short circuit failure (S/C) can be desribed by small resistance

of 10^{-5} Ω connecting the two cores of the electric cable. As can be seen in Figure 1, the resistor element used to model the short circuit is always present in the cable model, but it has a large value of 10^{6} Ω in cases other than a short circuit failure.

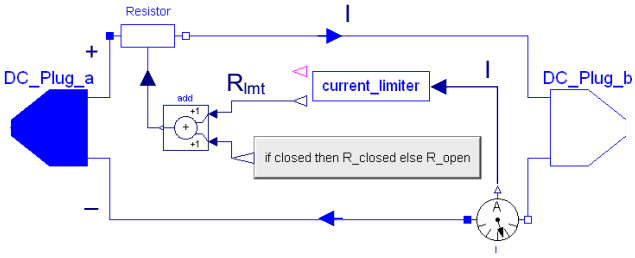


Figure 2: Electric contactor model with normal and failure behaviour and current limitation function

An electrical contactor is also modelled as a variable ohmic resistor, as shown in Figure 2. The opening and closing of the contactor is described by different resistance values, R_{open} = 10^{6} Ω for the open and approximately R_{closed} = $2 \cdot 10^{-3}$ Ω for the closed contactor state. The small resistance of the closed contactor effects a voltage drop, which can be specified by a model parameter. Optionally, this model may be used as a current limiting device, similar to a circuit breaker. Figure 3 shows the current limitation function: By increasing the resistance value R_{lmt} above zero, the limitation function prevents that the actual current, denoted by I, exceeds the nominal current I_{nom} . This kind of model has been selected, since it does not require any resetting after the limitation function has been activated in the simulation, other than a real circuit breaker which must be reset after having tripped. For a contactor or circuit breaker, there are a couple of conceivable failure modes, and the two most relevant of them are described in the model: An open circuit failure, which is modelled in the same manner as for the electrical cable, and a fails to open malfunction. The latter failure mode means a loss of the current limitation function, i.e. failure to protect against overcurrent.

As the examples suggest, a DC modelling approach has been selected for the electrical components. A single or three phase AC component is described by the equivalent DC component with root mean square values for voltage and current. A three phase AC component is respresented by a single phase, assuming that the three phases are symmetrical. Thus, the substitute single phase generates, conducts or uses a third of the entire current and power. Furthermore, the electrical behaviour is described by algebraic physical equations for the normal and several failure modes of each component; differential equations are omitted for simplification. This is judged as adequate regarding the objective of performing network architecture level conceptual design and optimisation, including the analysis of steady-state electric power behaviour, reliability, safety and weight.

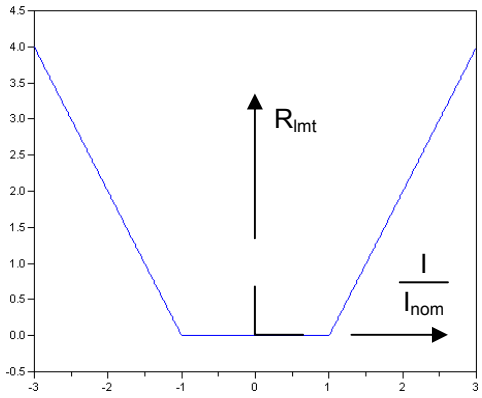


Figure 3: Current limitation function

Each component model has a boolean input signal to control its status, i.e. normal operation, failure mode 1, failure mode 2 etc., as applicable. The status can be shifted during simulation. The failure probability $p_i = 1 - e^{-\lambda_i \cdot t}$ is stored in each component model as a changeable parameter. Constant failure rates λ_i and exponentially distributed lifetimes are a common assumption in reliability and safety analysis.

The weight of a component is given dependent on sizing parameters of the accordant component model, such as the weight of a generator depends on its nominal power and speed.

Thus, a Modelica library of electric component models, that are augmented with a basic failure behaviour and parameterised weights, is developed. In doing so, the concept of creating component models that are usable regardless of the application or physical context, is being followed. Compatibility with existing model libraries is maintained.

2.2 Concept of Model Library with Included Analysis Procedures

The introduced Modelica library of electric component models and accompanying procedures for automated electric loads, reliability and safety analysis forms a tool for the conceptual design of aircraft on-board electric power systems. The tool is named as the Electrical Network Architecture Design Optimisation Tool - ENADOT. Besides reliability and safety, ENADOT is prepared to evaluate electric network architecture concepts w.r.t. to power behaviour and weight, as illustrated by Figure 4.

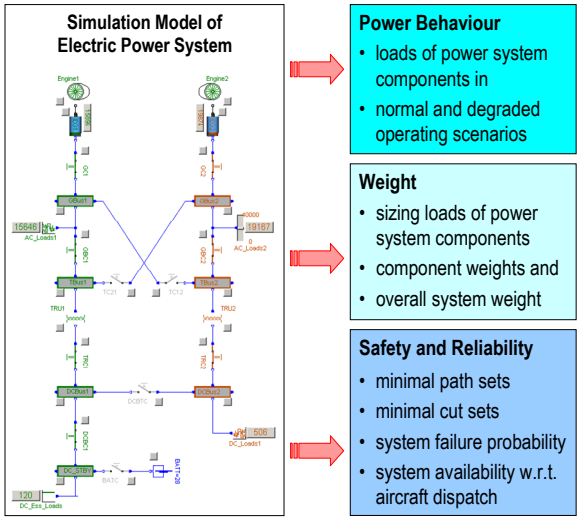


Figure 4: Concept of a Modelica-based tool for electric network architecture design analysis and optimisation - ENADOT

Large and complex models of electrical networks can be composed using the graphical editor of Dymola in the known manner.

Aircraft on-board electrical power systems are of particular interest w.r.t. reliability and safety, since they supply various loads, many of which fulfill a function that is essential for the safety of flight. Due to the recent trend to replace hydraulic and pneumatic supply systems by electric power on-board of commercial aircraft, the electric demands and thus the overall size of the electric system tend to grow. This increase of size and complexity also calls for a comprehensive modelling and simulation tool, due to the limitations of traditional design methods.

2.3 Modelling of Electric System Operating Modes

Electric power systems on-board of aircraft are typically split into several independent channels for redundancy, each comprising an engine driven generator, a distribution network and a number of loads. If failures occur, the network is reconfigured automatically to isolate the fault and to secure power supply to most of the loads, with priority to the essential ones. This reconfiguration capability has to be built into the system model accordingly. It is achieved by including the open / close logics of the various electric network contactors, which link (or cut off) the generators, busbars and loads. Thus, an electric network architecture model can be simulated for a normal and various abnormal operating scenarios.

2.4 Visualisation of System Operation and Interactive Checking

The diagram layer of an electric network architecture model is used also for dynamic and graphic display of the open / closed states of the various contactors, as well as of the resulting flow of electric power by different colours. For this purpose, ENADOT employs the visualisation and real-time simulation capabilities of Dymola and Visual C++.

If a component is energised, i.e. under voltage or conducting current, then its shape is coloured, as shown in Figures 5 and 6. The accordant colour stems from the generator or battery which energises the component. Passive components are shown in grey colour. The user can interactively shift the operating / fault modes of the electric network components, i.e. inject failures by mouse-click, and observe the resulting system behaviour by the visualisation in the diagram layer. That way, the model implementation of an electric network architecture is readily verified with regard to the intended behaviour.

2.5 Automated Analysis Procedures

To evaluate an electric network architecture model, ENADOT provides functions for an electric loads analysis, computation of component weights and overall system weight, a safety analysis which examines the probability of failure of voltage supply to a single or several busbars, a reliability analysis which evaluates the operational availability (→ aircraft dispatch reliability) of an electric network architecture, as well as compilation of a bill of material. The electric loads and safety analyses rely on the capability of an electric network model to simulate various operating modes and to bypass failed components.

These procedures are written as Modelica functions in algorithm syntax. They are part of the ENADOT library and simply rely on Dymola for execution.

2.5.1 Electrical Loads

The electric loads analysis determines the highest electric power generated or carried by a component in the most adverse operating case. To compute the highest electric power (design point) of any component of an electric network model, the function simulates it automatically for normal and degraded operating scenarios. As a result, the design point is provided for each component combined with its temporal occurrence during a flight cycle. Then, the sizing parameters of each component are selected which in turn yields the component weights and the overall weight of an electric network architecture.

2.5.2 Safety

By means of a safety analysis function embedded in ENADOT, the probability of loss of voltage supply to a single or several busbars of the electric network can be computed. Analysing the probability of loss of voltage supply to busbar(s) is particularly relevant if electric loads are connected to them that perform a function which is critical regarding the safety of flight. The scenarios to be investigated have to be supplied by the operator, e.g. "system is functional if at least one DC busbar is energised" or "system has failed if voltage is lost on the AC essential busbar".

Before starting the self-acting safety analysis, the operator can choose between the block-diagram (RBD) or the fault tree analysis (FTA) method.

The former is based on the identification of minimal path sets: A minimal path set is a combination of intact components that causes a system to be functional in the sense of the specified scenario, e.g. "at least one DC busbar energised". Minimal means that a path set contains only as many intact components as are necessary for the system to be functional. Redundant systems are characterised by the existence of several minimal path sets for a specified scenario, e.g. several ways of energising a busbar. By nature, a minimal path sets analysis considers only two states per component: intact or, respectively, failed [2].

The fault tree analysis method corresponds with the determination of minimal cut sets: A minimal cut set is a combination of defective components, which causes the system to fail in the opposite sense of the specified scenario, e.g. "no single DC busbar energised". Here, minimal means that a cut set consists of only as many defective components as causes the system to fail. Minimal cut sets comprise one (1st), two (2nd) or three (3rd order) defective components, and the probability of occurrence of a minimal cut set decreases rapidly with the number of components that belong to it. A redundant electrical system, in turn, is characterised by the fact that no 1st order minimal cut sets exist, apart from own defects of the busbar under consideration, but rather combinations of two or three defective components lead to the loss of voltage on busbar(s) and hence system failure.

Furthermore, the minimal cut sets analysis differs from the minimal path sets analysis by the consideration of all possible states of each component (intact, failure mode 1, failure mode 2, etc.). It is thus more complex and computationally more intensive than the minimal path sets analysis. The result, though, is equivalent to that of the established method of fault tree analysis, which is generally accepted as a verification of system safety. The computationally less intensive minimal path sets analysis provides quicker available results, which are normally used as a first estimate of system safety in the design process.

It must be noted that a model-based safety analysis only covers phenomena captured in the scope of modelled physics (section 2.1). Though the analysis is exhaustive to this extent, it is up to the designer to regard other possible threats, e.g. common causes such as humidity or electromagnetic interference.

The key definitions regarding safety analysis based on minimal path and minimal cut sets are as follows.

The common assumption of exponentially distributed lifetimes of the components c_i means component failure rates λ_i that are constant over lifetime. Thus, the probability of a component failure is

$$p_i(t) = \begin{cases} 1 - e^{-\lambda_i \cdot t}, & t \geq 0 \\ 0, & t < 0 \end{cases}$$

The probability of a minimal path set to occur is $P(MP) = \prod_{c_i \in MP} (1 - p_i)$, with the components c_i and the individual failure probabilities p_i. Likewise, the probability of occurrence of a minimal cut set is

$$P(MC) = \prod_{c_i \in MC} p_i$$

The probability of system operation can be computed from m detected minimal path sets as

$$\begin{aligned} P_{system-operation}(p_i) &= P(MP_1 \vee MP_2 \vee \ldots \vee MP_m) \\ &= \sum_{j=1}^{m} (MP_j) - \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} P(MP_i \wedge MP_j) + \ldots \\ &\quad + (-1)^{m+1} P(MP_1 \wedge MP_2 \wedge \ldots \wedge MP_m) \end{aligned}$$

Likewise, the probability of system failure can be calculated from n detected minimal cut sets as

$$\begin{aligned} P_{system-failure}(p_i) &= P(MC_1 \vee MC_2 \vee \ldots \vee MC_n) \\ &= \sum_{j=1}^{n} (MC_j) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P(MC_i \wedge MC_j) + \ldots \\ &\quad + (-1)^{n+1} P(MC_1 \wedge MC_2 \wedge \ldots \wedge MC_n) \end{aligned}$$

Generally, the relation between the probability of operation and failure, for a single component or a complex system is $p_{failure}(t) + p_{operation}(t) = 1$

Since the computation of system operation or failure probability from the above Poincaré formula can lead to a very large number of products, algorithms for sums of disjoint products [4] have been developed to reduce the size of the formula and to facilitate its numerical evaluation.

An analysis example can be viewed in section 3.2.

2.5.3 Reliability

Whereas a safety analysis is focused on failure events that can be critical with respect to the safety of flight, reliability is concerned with the operational availability of a system or entire aircraft. Operational availability or dispatch reliability is a measure for the likelihood of an aircraft fulfilling its mission, that is for a commercial aircraft to make revenue flights on time with passengers and/or cargo. More precisely, the dispatch reliability is defined as the percentage of scheduled flights which depart without having a delay of more than 15 minutes due to technical reasons, or a cancellation [1].

The commercial pressures have instigated the ability to continue to dispatch an aircraft with given system faults. Redundant design of aircraft on-board systems is adopted not only to fulfill the safety requirements, but also for reasons of dispatch reliability. In turn, this requires to examine the ability of a degraded system, when one or more failures have already occurred, to meet the safety requirements.

ENADOT has an embedded function, developed in the Modelica language, for computing system operational availability. It is in essence a minimal path sets analysis, which uses information about allowed component deficiencies, so called MEL-items (Minimum Equipment List), entered by the operator.

Let C_{system} be the set of all system components c_i, C_{MEL} be the given set of n_{MEL} possibly defective components and k the number of intact components required, $k \le n_{MEL}$ and $C_{MEL} \subseteq C_{System}$. Then, $m = \binom{n_{MEL}}{k}$ minimal path sets are generated with the following properties:

Each minimal path set MP_1, MP_2, …, MP_m contains those system components c_i that are not an MEL-item, i.e. not part of the set C_{MEL}.

$$c_i \in C_{System} \setminus C_{MEL} = \left\{ c_i \middle| \left(c_i \in C_{System}\right) \wedge \left(c_i \notin C_{MEL}\right) \right\}$$

As well, k intact components from the set of MEL-items C_{MEL} are included in each minimal path set. E.g. for $k = 2$ and $n_{MEL} = 3$, the $\binom{3}{2} = 3$ following minimal path sets are composed:

$$MP_1 = C_{System} \setminus C_{MEL} \cup \{c_1, c_2\}$$

$$MP_2 = C_{System} \setminus C_{MEL} \cup \{c_1, c_3\}$$

$$MP_3 = C_{System} \setminus C_{MEL} \cup \{c_2, c_3\}$$

An analysis example is provided in section 3.3 for the electric power system introduced by section 3.1.

2.5.4 Minimising the Computational Effort Involved with Safety Analysis

Analysing the effect of combinations of intact and failed components on the occurrence of system function or failure can lead to an exponential growth of combinations to test. Regarding the detection of minimal path sets, 2^n possible states would have to be evaluated for a system of n components, e.g. $2^{20} > 1 \cdot 10^6$ for $n = 20$.

To avoid the unfeasibility of automated analysis caused by an excessive amount of system states to test, strategies are developed to exclude inapplicable combinations of intact / failed components from the procedure.

The minimal path sets analysis procedure of ENADOT draws on two kinds of information contained in a system model. In a first step, the object structure of the system model, i.e. the arrangement of components and connections, is evaluated. Advantage is taken of the fact that the structure of object-oriented models is similar, although not exactly identical with minimal path sets. Regarding the object-oriented model structure as a graph, an adapted depth-first search algorithm is used to find a moderate number of candidates of minimal path sets.

In a second step, the candidates are checked by simulating the system model accordingly, to eventually extract the minimal path sets from the amount of candidates. This two-stage approach – depth-first search and then simulation – considerably reduces the overall computation effort, leading to a procedure that is viable even for systems of a size as shown in section 3.1.

After the minimal path sets of a system have been determined for a given scenario, the probability measures are computed as described in section 2.5.2.

For the minimal cut sets analysis, the theoretically possible number of system states is even higher: Assuming that three states (intact, failure mode 1, failure mode 2) have to be considered for each component of a system, this would lead to 3^n possible system states, e.g. $3^{20} > 3 \cdot 10^9$ for $n = 20$.

Here, the strategy of minimising the amount of system states to check includes at first to determine the minimal path sets, as described above. Then, minimal cut sets are searched for according to heuristic rules that draw on the position of components in the system and their modes of failure. For instance, only combinations of failed components that belong to different minimal path sets or which are located adjacent to a minimal path set, are checked.

3 Modelling and Analysis Case Study

This section illustrates the capabilities of ENADOT with respect to safety and reliability analysis by the example model of an aircraft on-board electric power system. Figure 5 shows the model, the basic structure and characteristics of which are oriented to the electric power system of the Airbus A380. The model complies with the typical configuration and functionality of electrical systems of this aircraft category, and it is thus adequate for a demonstration of the scope of ENADOT. The model has been developed based on a description, conceptual sketch and listing of the key electrical loads, which have been found in section 5.12.1 of reference [5]. It may differ in some minor respect from the actually built and flying electric system of the A380, yet, this does not affect the description of the scope of ENADOT.

3.1 Electric Power System Modelling Example

The schematic shown in Figure 5 is a direct snapshot of the electric power system model. It includes the following, salient components and features:

- four engine driven 3-phase 115 VAC / 150 kVA Variable Frequency (VF) generators, identified as G1, G2, G3 and G4
- two 3-phase 115 VAC / 120 kVA Constant Frequency (CF) generators, driven by the Auxiliary Power Unit (APU), denoted as AG1 and AG2
- a 70 kVA Ram Air Turbine (RAT) driven emergency generator, named RatG
- three 300 A Battery Charger Regulator Units (BCRU) – these are regulated Transformer Rectifier Units (TRU) – named EssBCRU, BCRU1 and BCRU2
- a 300 A TRU identified as APU_TRU
- four 28 VDC batteries, denoted as ESS_BAT, BAT1, BAT2 and APU_BAT
- a static inverter, named INV, for emergency supply of the AC_EMER busbar

3.1.1 System Functionality

Figure 5 shows the normal in-flight operation of the electric power system. As can be seen, each engine driven generator G1 (blue), G2 (green), G3 (magenta) and G4 (bronze) energises its associated busbar AC_1, AC_2, AC_3 and AC_4. The two APU driven generators AG1 (purple) and AG2 (yellow) are available, but not engaged. If a generator fails, the neighboured generator will take over by closing the ACTC1 or ACTC5 contactor. If both generators on one side fail, then cross-transfer through the ACTC2, 3 and 4 contactors will sustain all AC busbars energised, with yet decreased overall available power. Split generator operation is maintained in all cases since the engine driven AC generators are variable frequency, each dependent on the speed of the related engine.

The AC buses supply the non-essential cabin loads Galley1, 2, 3 and 4 and In-Flight Entertainment (IFE) 1 and 2. These form an intermittent load of up to ~320 kVA (~80 kVA per galley including cooling) and ~60 kVA (IFE). Those AC loads that are vital for the safe operation of the aircraft are connected to the AC_ESS and AC_EMER busbars. These are airspeed probes and windshield heating, as well as motor driven hydraulic pumps and a set of Electro-Hydrostatic flight control Actuators (EHAs) needed to maintain a minimum acceptable level of airplane controllability. The AC essential loads sum up to ~60 kVA. The AC_ESS and AC_EMER busbars are supplied either by the AC_1 busbar (normal case) or, if AC_1 fails, from the AC_4 busbar. Should all engine generated power fail, then the RAT driven generator RatG can accept the AC_EssLoads and AC_EmerLoads. The latter can also be powered by battery through the static inverter INV, e.g. during RAT transit.

Other than the AC part of the electric power system, the 28 VDC part offers a no-break power capability even during changes of system status, which is crucial to the functioning of vital control systems, such as engine and flight control computers, avionics systems, flight deck instruments and radio communication. These loads are represented in the model by DC_EssLoads, DC1_Loads and DC2_Loads and account for ~4 kW altogether. The cabin lights make up ~15 kW of power, supplied by the non-essential part of the DC system.

3.1.2 Degraded System Operation

Figure 6 shows the electric power system in a conceivable mode of degraded operation. The failed components Engine1, G2, APU and BCRU2 are marked in red colour. Since the power supply from G1 and G2 is lost, the AC_1, AC_2, AC_3, DC_1 and DC_2 busbars are energised by G3 (magenta). Failure of the BCRU2 has been recovered by closing the DCTC2 contactor. The other remaining generator G4 (bronze) energises the AC_4, as well as the essential busbars AC_ESS, AC_EMER and DC_ESS. As the scheme also shows, half of the cabin loads – galleys, IFE and lights – have been suspended, whereas the essential loads remain fully satisfied.

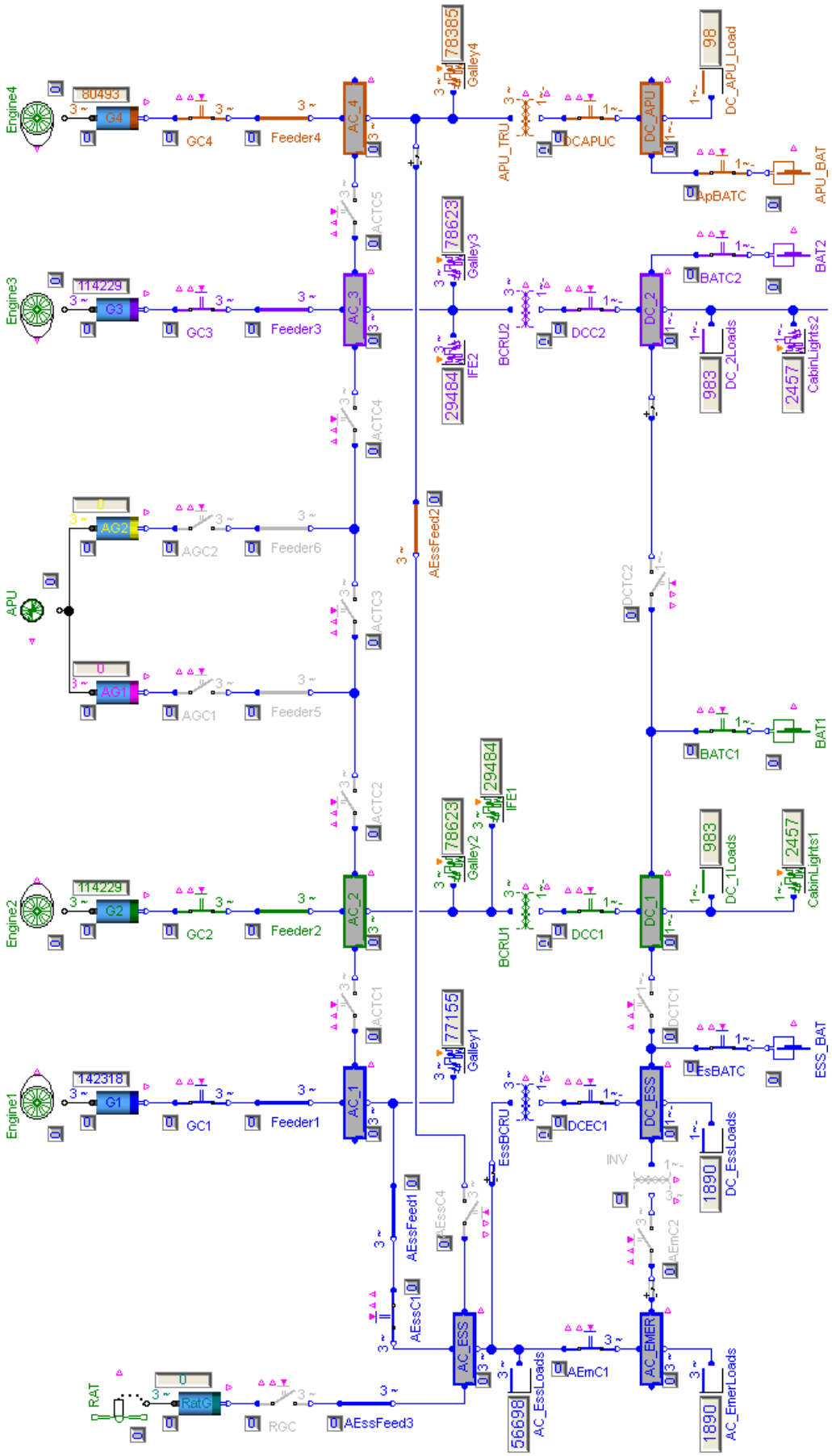


Figure 5: Electric network model of a recent four-engine long range aircraft, scheme shows normal operation in flight

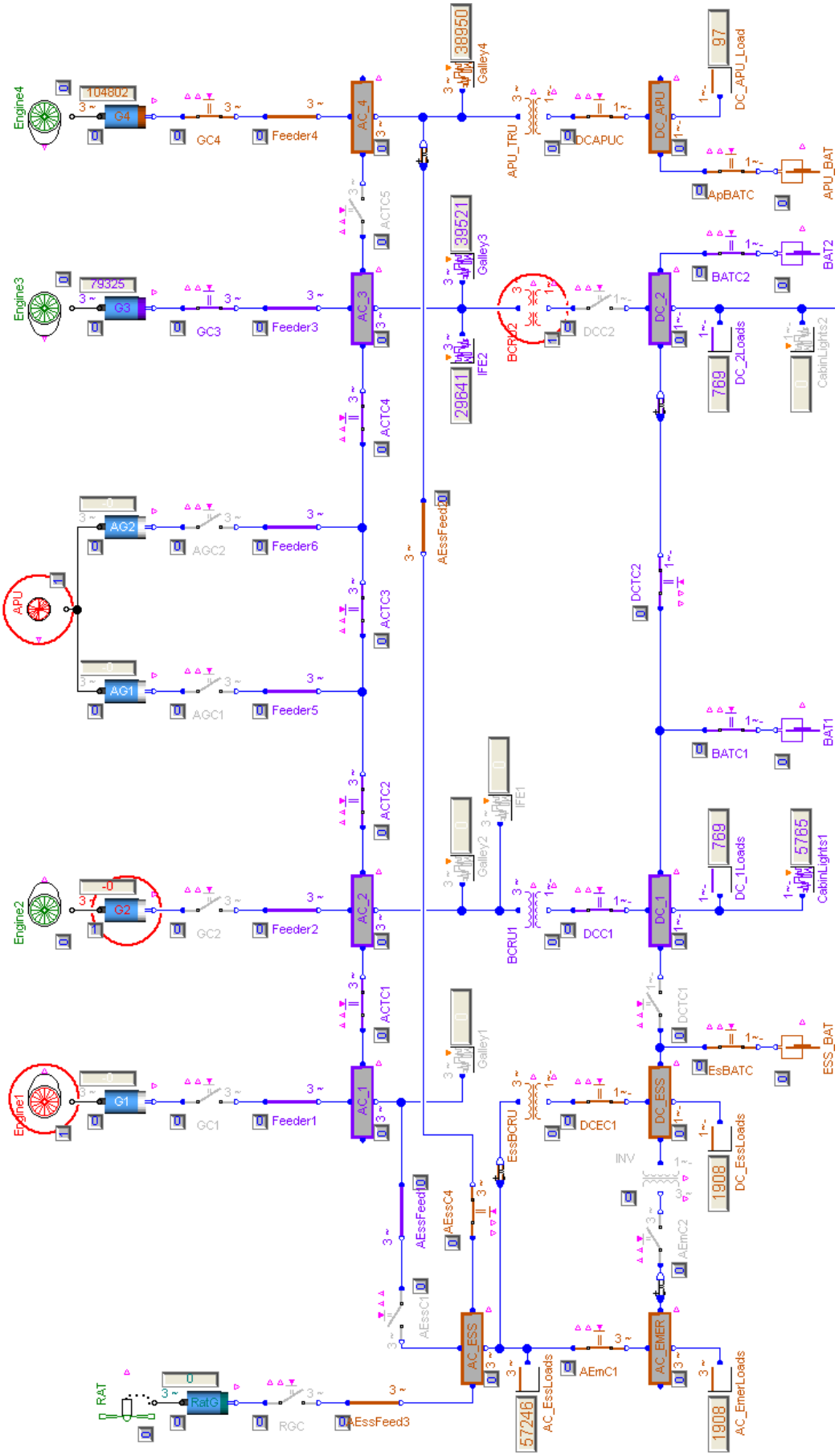
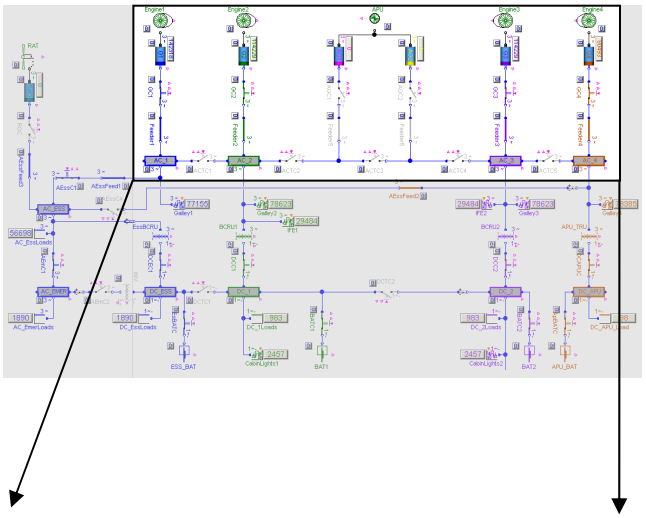


Figure 6: Electric network model of a recent four-engine long range aircraft, scheme shows degraded operation in flight after Engine1, Generator2, APU and BCRU2 failure

3.2 Safety Analysis Example Result

This section shows the result of a safety analysis conducted for the supply to the AC_1 busbar of the introduced electric system. This non-essential busbar has been selected to serve as an example, since the result is relatively compact.

Figures 7 to 12 show the six determined minimal path sets. They are depicted graphically and directly in the model diagram, after completion of the analysis procedure. Components belonging to a minimal path set appear in the colour of the connected generator, failed components in grey. In normal operation, AC_1 is supplied by generator G1 (Figure 7), which can be transferred to another engine or APU driven generator in abnormal operating cases. Hence,



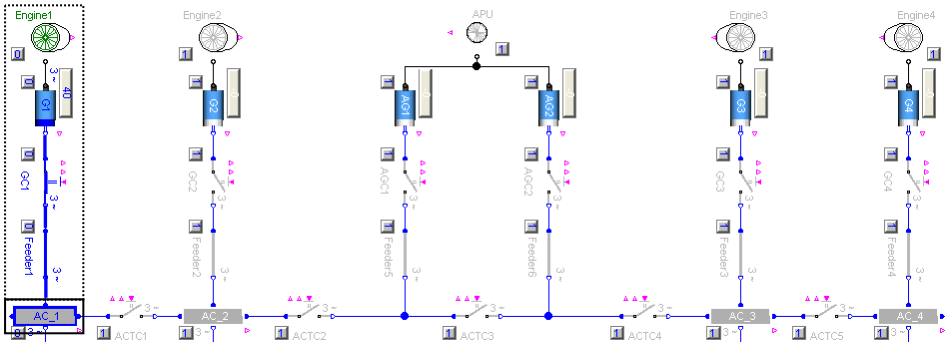


Figure 7: Minimal path set 1 - AC_1 busbar energised by G1

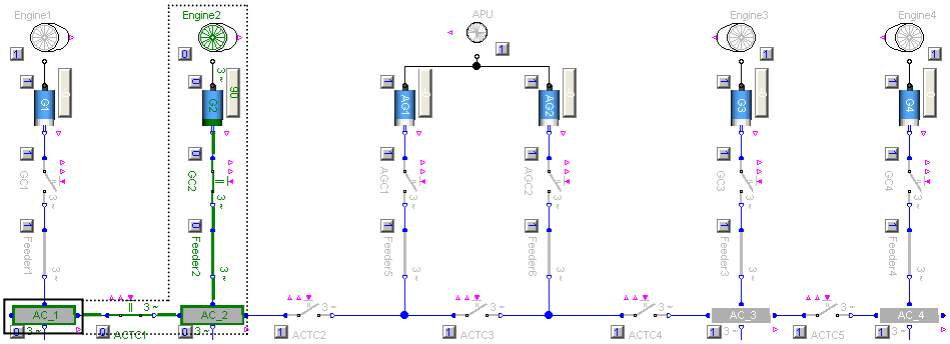


Figure 8: Minimal path set 2 - AC_1 supplied by G2 across AC_2

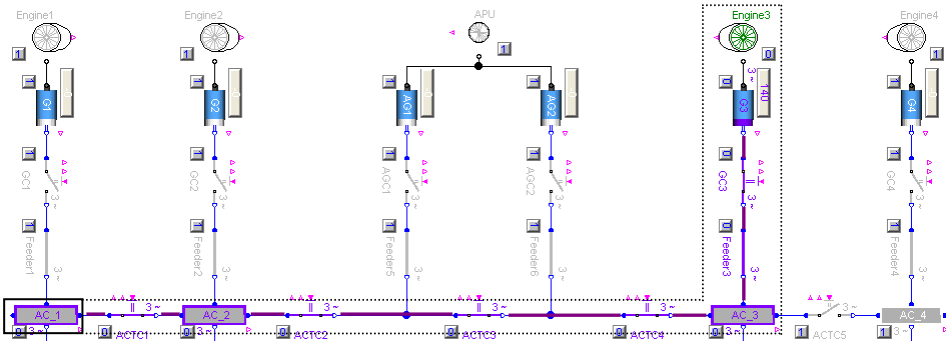


Figure 9: Minimal path set 3 - AC_1 fed by G3 through AC_3 and AC_2

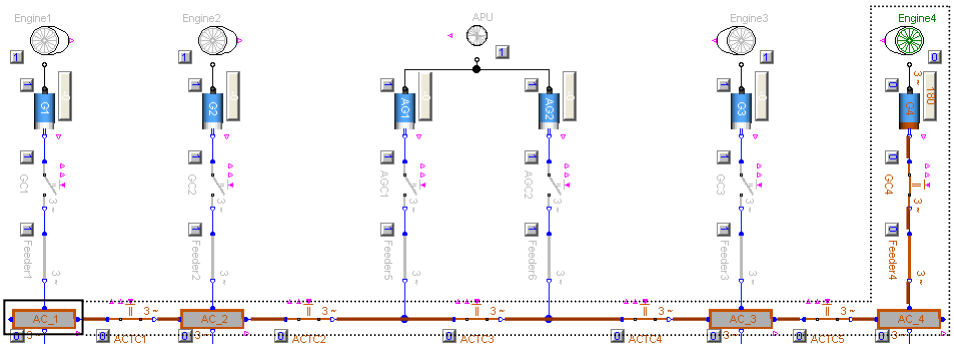


Figure 10: Minimal path set 4 - AC_1 energised by G4 across AC_4, AC_3 und AC_2

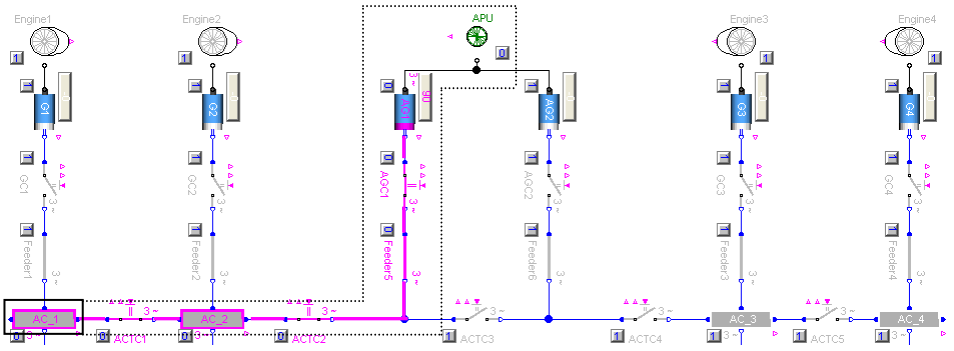


Figure 11: Minimal path set 5 - AC_1 fed by AG1 through AC_2

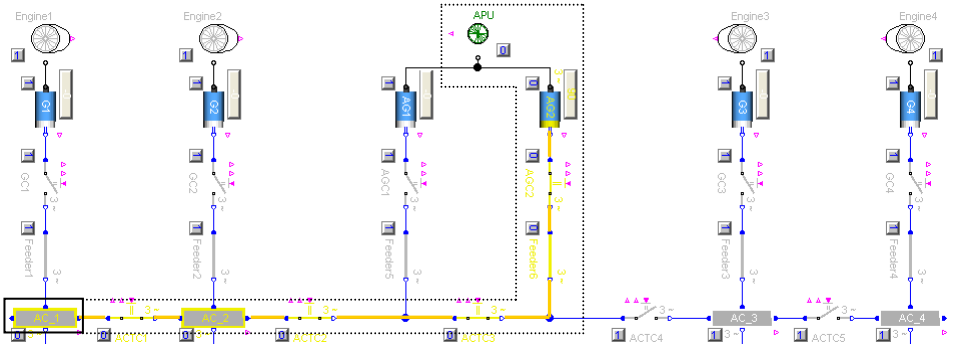


Figure 12: Minimal path set 6 - AC_1 supplied by AG2 across AC_2

AC_1 has multiple redundancy as to voltage sources.

The minimal path sets analysis accounts for the connections of components, their potential faults and network reconfiguration logics. The result, e.g. the six minimal path sets found for the AC_1 busbar, is thus also a check of the correct functioning of the system and its implementation as a model.

As explained, two states are considered for each component, intact or failed, in the minimal path sets analysis. Many components yet have two or more failure modes. Amongst others, the following are realised in the modelling: “open circuit” and “short circuit” for a cable or a busbar, “open circuit” and “fails to open” for a contactor, “loss of output voltage” for a generator. The minimal cut sets analysis accounts for every failure mode of all components and the resulting effects on the electric network.

A total of 5 first order and 21 second order minimal cut sets were identified by the analysis procedure and are listed in Table 1. Figures 13 to 19 show typical cases for the scenario “loss of voltage on AC_1”.

Besides own possible faults of the AC_1 busbar – open circuit (Figure 15) or short circuit – other single component faults exist that lead to a loss of voltage on AC_1: e.g. a short circuit of cable Feeder1 (Figure 14), which is directly connected to the busbar, or in the same manner a short circuit of cable AEssFeed1 (Figure13). Typical examples of 2nd order minimal cut sets are a failure of a component that feeds AC_1 in normal system operation, in combination with another component failure that prevents cross-transfer through AC_2 and ACTC1. Examples can be viewed in Figures 16 and 18.

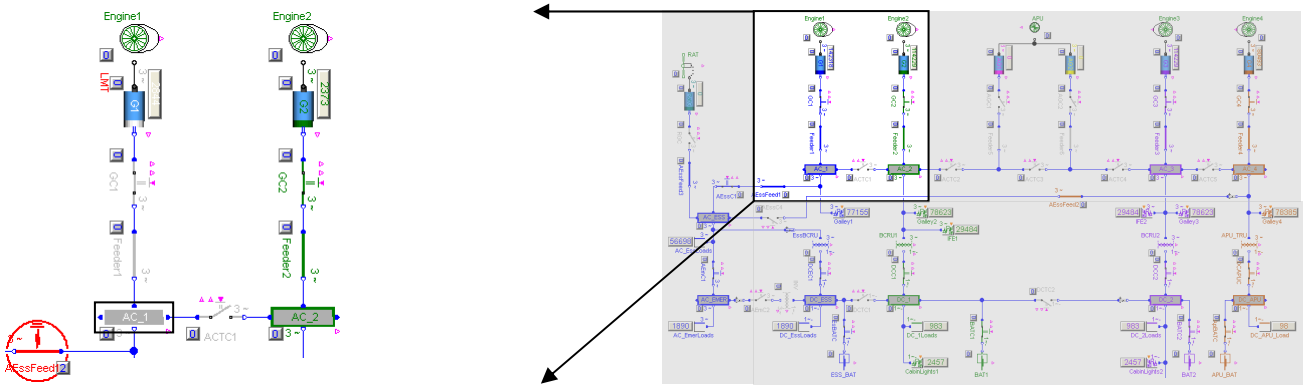


Figure 13: Minimal cut set 1-2: short circuit of cable leads to loss of voltage on AC_1 busbar

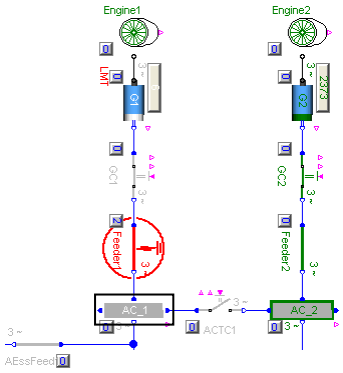


Figure 14: Minimal cut set 1-3: cable short circuit causes failure of AC_1

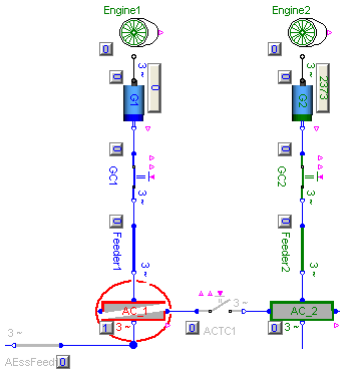


Figure 15: Minimal cut set 1-5: open circuit leads to loss of AC_1

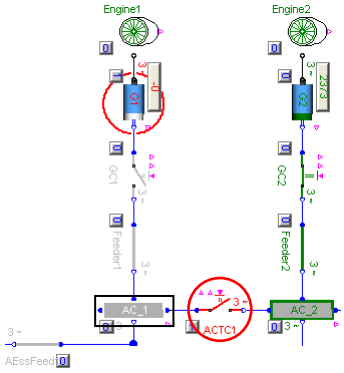


Figure 16: Minimal cut set 2-7: G1 fault and open contactor cause AC_1 failure

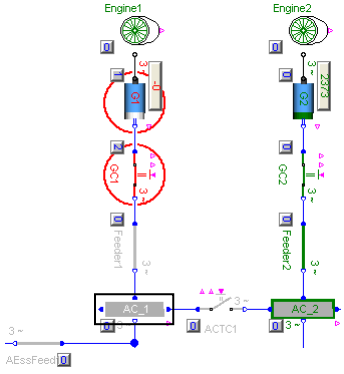


Figure 17: Minimal cut set 2-14: G1 fault and stuck closed contactor lead to loss of AC_1

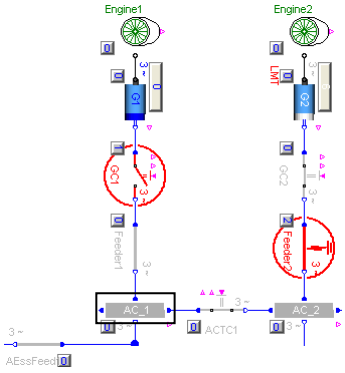


Figure 18: Minimal cut set 2-5: open contactor and shorted cable lead to AC_1 failure

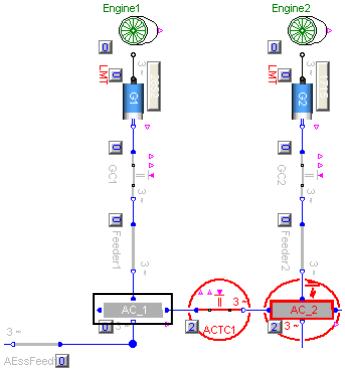


Figure 19: Minimal cut set 2-21: short circuit of AC_2 and stuck contactor cause loss of AC_1

Furthermore, a stuck closed contactor in combination with a generator fault (Figure 17) or in combination with a short circuit (Figure 19) can cause a loss of voltage on the AC_1 busbar, the probability of which has been computed for a duration of t = 1 Fh (flight hour) as $4.0 \cdot 10^{-4}$.

The failure of AC_1 is dominated by faults of the connected cables. If necessary, this situation can be improved by introducing contactors with current limitation between the cables and the busbar, which prevent the propagation of the effects of short circuits.

For most of the single component faults, this would avoid the effect of losing voltage on the AC_1 busbar. Since there is multiple redundancy in terms of voltage sources, a decrease of the probability of loss of voltage on AC_1 is then limited only by possible own defects of the busbar.

1st order minimal cut sets:

1-1	Feeder1	O/C	0.0002
1-2	AEssFeed1	S/C	0.0001
1-3	Feeder1	S/C	0.0001
1-4	AC_1	S/C	$2 \cdot 10^{-7}$
1-5	AC_1	O/C	$1 \cdot 10^{-7}$

2nd order minimal cut sets:

2-1	G1	loss	Feeder2	O/C	$8 \cdot 10^{-9}$
2-2	G1	loss	Feeder2	S/C	$4 \cdot 10^{-9}$
2-3	GC1	O/C	Feeder2	O/C	$2 \cdot 10^{-9}$
2-4	Engine1	loss	Feeder2	O/C	$2 \cdot 10^{-9}$
2-5	GC1	O/C	Feeder2	S/C	$1 \cdot 10^{-9}$
2-6	Engine1	loss	Feeder2	S/C	$1 \cdot 10^{-9}$
2-7	G1	loss	ACTC1	O/C	$4 \cdot 10^{-10}$
2-8	GC1	O/C	ACTC1	O/C	$1 \cdot 10^{-10}$
2-9	Engine1	loss	ACTC1	O/C	$1 \cdot 10^{-10}$
2-10	AEssC1	s.c.	AEssFeed3	S/C	$1 \cdot 10^{-11}$
2-11	ACTC1	s.c.	Feeder2	S/C	$1 \cdot 10^{-11}$
2-12	G1	loss	AC_2	S/C	$8 \cdot 10^{-12}$
2-13	G1	loss	AC_2	O/C	$4 \cdot 10^{-12}$
2-14	G1	loss	GC1	s.c.	$4 \cdot 10^{-12}$
2-15	GC1	O/C	AC_2	S/C	$2 \cdot 10^{-12}$
2-16	Engine1	loss	AC_2	S/C	$2 \cdot 10^{-12}$
2-17	GC1	O/C	AC_2	O/C	$1 \cdot 10^{-12}$
2-18	Engine1	loss	AC_2	O/C	$1 \cdot 10^{-12}$
2-19	Engine1	loss	GC1	s.c.	$1 \cdot 10^{-12}$
2-20	AC_ESS	S/C	AEssC1	s.c.	$2 \cdot 10^{-14}$
2-21	AC_2	S/C	ACTC1	s.c.	$2 \cdot 10^{-14}$

Table 1: List of minimal cut sets sorted by probability, for loss of voltage on AC_1 busbar, t = 1 Fh

3.3 Reliability Analysis Example Result

This section shows the result of a dispatch reliability analysis conducted for the introduced electric power system, see Figure 5. The following set of $n_{MEL} = 6$ allowed component deficiencies (MEL-items) is assumed: C_{MEL} = {G1, G2, G3, G4, (APU & AG1), (APU & AG2)} i.e. six generators two of which in combination with the auxiliary power unit. For $k = 6$ required intact components, i.e. no allowed deficiences, the analysis determines one minimal path set $MP_1 = C_{System}$ which includes all system components. With given component failure rates λ_i (not listed due to extensiveness) and a duration of $t = 200$ Fh for 10 consecutive days of flying without maintenance, a dispatch reliability of 0.869 is computed.

For $k = 5$, i.e. one allowed deficiency, 6 minimal path sets are generated

$MP_1 = C_{System} \setminus C_{MEL} \cup$ {G1, G2, G3, G4, (APU&AG1)}

$MP_2 = C_{System} \setminus C_{MEL} \cup$ {G1, G2, G3, G4, (APU&AG2)}

…

$MP_6 = C_{System} \setminus C_{MEL} \cup$ {G2,G3,G4,(APU&AG1),(APU&AG2)}

The dispatch reliability is 0.911 for $t = 200$ Fh.

For $k = 4$, i.e. two allowed deficiencies, 15 minimal path sets are compiled

$MP_1 = C_{System} \setminus C_{MEL} \cup$ {G1, G2, G3, G4}

$MP_2 = C_{System} \setminus C_{MEL} \cup$ {G1, G2, G3, (APU&AG1)}

…

$MP_{15} = C_{System} \setminus C_{MEL} \cup$ {G3, G4, (APU&AG1), (APU&AG2)}

leading to a dispatch reliability of 0.929 for 200 Fh.

As obvious, allowing system deficiences for dispatch improves the reliability. This is however limited by the failure probabilities of components that are always required to be intact for dispatch. Also, the degraded system must have sufficient safety margin.

4 Conclusion

This paper outlined the capabilities of the Modelica based modelling and analysis tool ENADOT regarding concept design and optimisation of aircraft onboard electric power systems, which have recently gained in relevance, installed power and criticality.

In addition to means for the dimensioning of electric network components regarding power and weight, the system safety and operational reliability can be evaluated in terms of an automated minimal path sets and minimal cut sets analysis.

Future work will be oriented to a transfer of the analysis methods to other physical domains.

Acknowledgements

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) for the Clean Sky [3] Joint Technology Initiative under grant agreement no. CSJU-GAM-SGO-2008-001. The author wishes to thank the electric engineering department of Airbus-France for the kind support and company.

References

[1] Bineid M, Fielding J P: *Development of an aircraft systems dispatch reliability design methodology.* The Aeronautical Journal, pp. 345-352, June 2006.

[2] Birolini A: *Reliability Engineering – Theory and Practice.* Fifth Edition, Springer Verlag Berlin, 2007.

[3] CleanSky project, http://www.cleansky.eu

[4] Heidtmann K D: *Smaller Sums of Disjoint Products by Subproduct Inversion.* IEEE Transactions on Reliability, Vol. 38, No. 3, pp. 305-311, August 1989.

[5] Moir I, Seabridge A: *Aircraft Systems - Mechanical, electrical and avionics subsystems integration.* John Wiley & Sons Ltd, 2008.