Incorporation of Reliability Analysis Methods with Modelica

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

Abstract

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

The new method allows to perform reliability calculations based on the system model that is created and used for simulation studies. The reliability analysis procedure is started “at the push of a button” and determines the so called minimum path sets and the failure probability of a system automatically.

The incorporated reliability computation methods are realised initially by a new modelling and analysis tool supporting concept design studies of aircraft onboard electric power systems.

Keywords: reliability, fault modelling; model object structure; minimum path set; failure probability

1 Introduction

Much of the information needed for reliability calculations is contained already in compound system models that are usually built in Modelica [1]. The specific modelling additions needed, as well as the fundamentals of an automated reliability analysis procedure are described by this paper.

The procedure evaluates the physical behaviour of a modelled system in multiple simulations. An addition needed to the modelling is the faulty behaviour of components, as described in chapter 2.1.

Prior to evaluating the system model by numerous simulations, its object structure is appraised in order to detect those combinations of components, that represent candidates of so called minimum path sets. Chapter 2.4 gives an overview of the method and definitions, as well as a way of minimising the computing effort that is involved with this kind of automated reliability analysis.

2 Modelling Approach and Integrated Reliability Analysis Concept

2.1 Component Fault Modelling

A variety of object-oriented model libraries have been developed in the Modelica language, as generally known. In each component model, the normal operational behaviour is described by differential and/or algebraic physical equations.

For the purpose of performing reliability analyses, the component models have to be enhanced such that also the failure behaviour is described by physical equations. Basic examples are given hereafter by the modelling assumptions made for some common electrical components:

An electric wire can be described as an ohmic resistor. For the normal function of the wire, its nominal resistance R_{nom} is in the order of 10^{-1} Ω. An open circuit failure of the wire is characterised by a very large resistance, e.g. 10^{6} Ω.

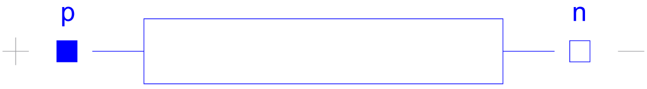


Figure 1: Modelica Object Diagram of an Electric Resistor

In essence, the following code defines the model:

```
model Resistor "Ideal linear resistor"
  Interfaces.Electrical.PositivePin p;
  Interfaces.Electrical.NegativePin n;
  input Boolean FAILED;
  parameter Real lambda = 2e-5 “failure
    rate”;
  parameter SI.Resistance Rnom = 0.1;
  SI.Resistance R = if FAILED then 1e6
  else Rnom;
equation
  v = p.v - n.v;
  0 = p.i + n.i;
  i = p.i;
  R*i = v;
end Resistor;
```

A generator can be represented by its DC substitute properties and the efficiency of converting mechanical into electric power. A basic description of a generator failure is the loss of output voltage, which stems from an internal failure of the generator or from insufficient generator drive speed.

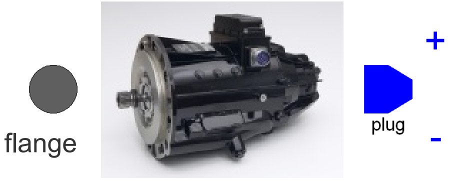


Figure 2: Modelica Object Diagram of a Generator

The following code basically defines this model:

```
model Generator "DC generator with
losses"
  Interfaces.Rotational.Flange_a
    flange;
  Interfaces.Electrical.DC_Plug_a plug;
  input Boolean FAILED;
  parameter Real lambda = 1e-4 “failure
    rate”;
  parameter SI.Power Pnom = 5e4;
  parameter SI.Voltage Vnom = 270;
  NonSI.AngularVelocity_rpm speed;
  SI.Voltage v;
  SI.Power Pelec;
  SI.Power Plosses;
  SI.Power Pmech;
equation
  speed = max(0.1 ,
    to_rpm(der(flange.phi));
  v = if FAILED then 0 else (1-
    exp(-speed/1000))^2*Vnom;
  v = plug.pin_p.v - plug.pin_n.v;
  Pelec = v*plug.pin_n.i;
  Plosses = 3000*speed*Pelec/(14600*
    Pnom);
  Pmech = Pelec + Plosses;
  Pmech = -flange.tau*from_rpm(speed);
end Resistor;
```

Each component model has a boolean input signal *FAILED* to control its status, i.e. operation or failure. The status can be shifted during simulation. Failure rates *lambda* are stored in each component model as modifiable parameters. Using constant failure rates is adequate w.r.t the assumption of an exponentially distributed component lifetime. Other hypotheses on the dependency of failure rates on lifetime can also be taken into account.

Thus, a new Modelica library of electric component models, that are augmented with a basic failure behaviour, is being developed. In doing so, the fundamental concept of creating component models that are usable regardless of the application case or physical context, is being followed. Compatibility with exisiting model libraries is maintained as well.

2.2 Integrated Tool Concept

The new library of electric component models, as well as integrated reliability analysis procedures are part of a new developed concept design tool for aircraft on-board electric power systems. Besides reliability, the tool is prepared to evaluate architecture concepts w.r.t. the electric behaviour and weight, as illustrated by Figure 3.

Large compound models of electric power systems can be assembled using the graphical model editor of Modelica/Dymola [2] in the known fashion.

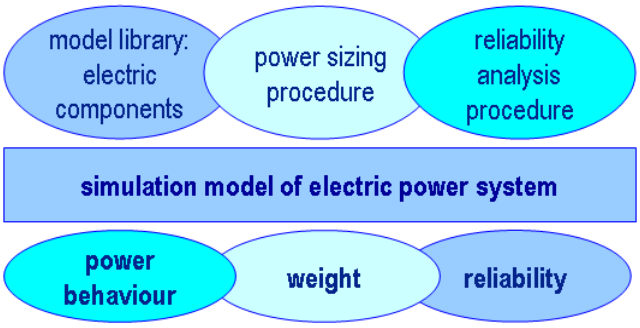

model library: electric components
power sizing procedure
reliability analysis procedure
simulation model of electric power system
power behaviour
weight
reliability

Figure 3: Elements of Modelica based Concept Design Tool for Electric Power Systems

Aircraft electric power systems are of particular interest for reliability analysis, since they supply a multitude of loads, many of which fulfil a function that is essential for safe flight and landing. Also, the electric demands tend to increase, due to the recent trend in the design of transport aircraft to replace hydraulic and pneumatic supplies by electric power [3].

Electric power systems on aircraft are typically split into several independent channels, each comprising an engine driven generator, a distribution network and a number of loads. If failures occur, the electric power system is reconfigured automatically to isolate the fault and to secure power supply to most of the loads, with priority to the essential ones. The redundancies and reconfiguration capability of such systems have to be included in the system model accordingly, by means of open/close logics for the electric network contactors. Thus, the behaviour in various operational scenarios, e.g. normal, abnormal or emergency, can be examined in simulations.

2.3 Modelling Example: Electric Power System

In the following, the integrated modelling and reliability analysis concept is illustrated by the example of an electric power system of a generic twinjet aeroplane. The system model, see Figure 4, has been devised based on a description available in [4].

2.3.1 System Model Features

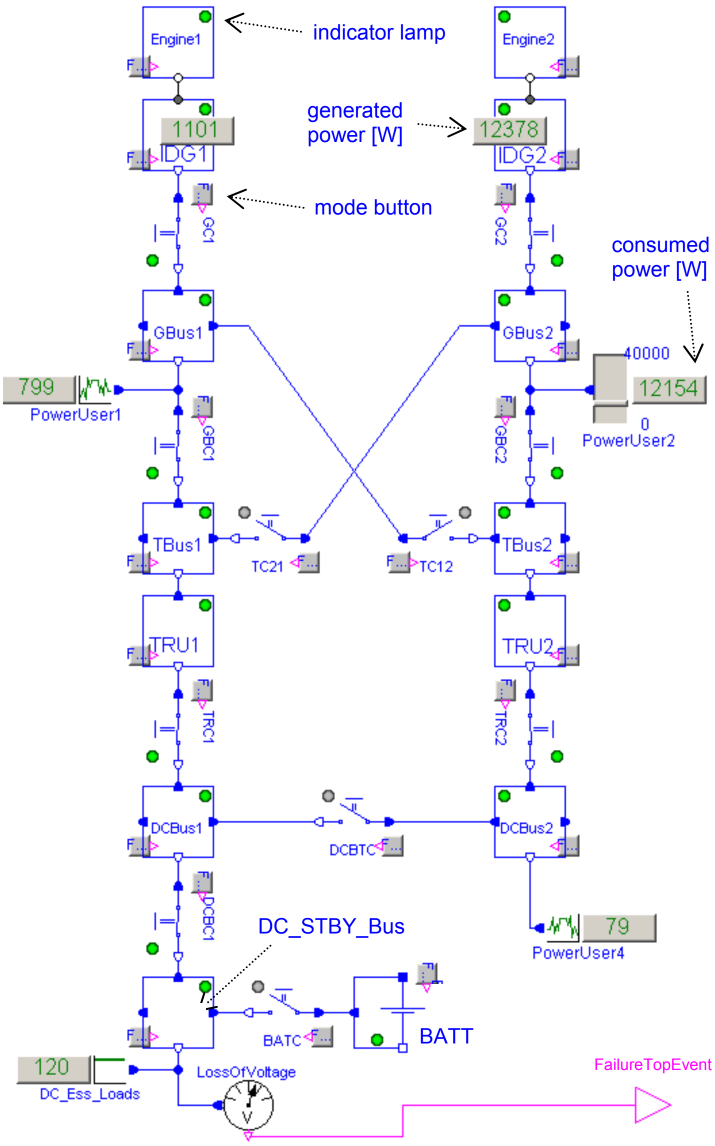


Figure 4: Electric System Model of a Twinjet Short-Range Aeroplane, schematic shows Normal Operation in flight

Figure 4 also shows the object-oriented structure of the system model, which is commensurate with the general philosophy of Modelica. Note that the electric connections include two poles.

The electric system model includes the following, most important components and features:

- Two integrated drive generators *IDG1* and *IDG2*, which are driven by *Engine1* and *Engine2*, respectively. Each generator provides 115V / 400Hz AC power (substituted in the model by 270V DC)
- through a dedicated generator contactor, *GC1* and *GC2*
- on the generator buses, *GBus1* and *GBus2*.
- The main non-essential AC loads, represented by *PowerUser1* and *PowerUser2*, as well as
- the AC transfer buses, *TBus1* and *TBus2* are connected to the respective generator buses. In normal operation with both engines running (as shown in Figure 4), each transfer bus is supplied by its associated generator bus through a generator bus contactor, *GBC1* and *GBC2*.
- The AC cross transfer contactors, *TC12* and *TC21*, are open in this normal operating case.
- 28V DC power is provided by two transformer rectifier units, *TRU1* and *TRU2*, through dedicated switches *TRC1* and *TRC2*, on the DC busbars *DCBus1* and *DCBus2*.
- The two DC busbars can be cross-connected through the *DCBTC* switch. In normal operation (Figure 4), the cross-connection is inactive i.e. the *DCBTC* switch is open.
- Finally, a stand-by busbar *DC_STBY_Bus* provides for the essential loads *DC_Ess_Loads*, which must operate even after a complete loss of generated power, to maintain safe flight and landing. In such a scenario, the essential loads are powered by a battery *BATT* through the *DC_STBY_Bus*.

The following apparent features are included in the system model:

- Each contactor has an animated rocker switch to depict its open / closed status.
- Each component model is fitted with an indicator lamp. During simulation of the model, the operational (green), passive (grey) or failed (red) status of each component is shown by the associated indicator lamp.

A component is defined as operational when turning (e.g. engine), energised with voltage (e.g. busbar) or conducting current (e.g. switch), whatever is applicable. The passive status is specified as the component being intact but not energised. If a component has failed, it cannot be energised with voltage or conduct current, whatever is applicable.

Each component model is provided also with a mode button for an interactive control of its operative / failed status. Pressing the mode button of a component, by mouse-click, during simulation will toggle the status (operational or passive ↔ failed) of the component.

By means of the mode buttons and indicator lamps that are provided with the component models, the behaviour of a system model can be examined interactively during simulation. This is useful when developing the network switching logics, since the resulting behaviour at system level can be checked quickly and readily.

Furthermore, the following features are included in the system model:

- Generic power users, which can be connected to any busbar as needed. The power users are described by basic resistive properties, which can be set by parameter entries or interactively: The *PowerUser2* shown in Figure 4 has an adjustable slider bar, which is set by mouse-dragging during simulation.
- Each power user model, as well as the generator (IDG) models have a numerical indication of the generated / consumed power in W(att).
- A *FailureTopEvent* definition at system level [5], so that the system reliability w.r.t. this event can be computed. In the present example shown by Figure 4, the system failure top event is defined as a loss of voltage on the *DC_STBY_Bus*.

As can be seen in Figure 4, the definition of the system *FailureTopEvent* has been implemented by connecting a specific voltage sensor named *LossOfVoltage* to the *DC_STBY_Bus*. The sensor will flag a voltage drop-out below a defined threshold by its logical output signal. This specific voltage sensor model class is provided by the model library.

Other system failure event definitions are conceivable, e.g. a loss of voltage on other busbars or combined events, such as the loss of voltage on *DCBus1* and *DCBus2*. Any meaningful failure event definition can be implemented in an accordant manner, by use of the provided sensor class and logical gates.

2.3.2 Degraded System Operation

In Figure 5, a degraded operational mode of the electric system, caused by failures of *Engine2* and *TRU1*, is shown. The component failures have been injected in the model by pressing the corresponding mode buttons during simulation.

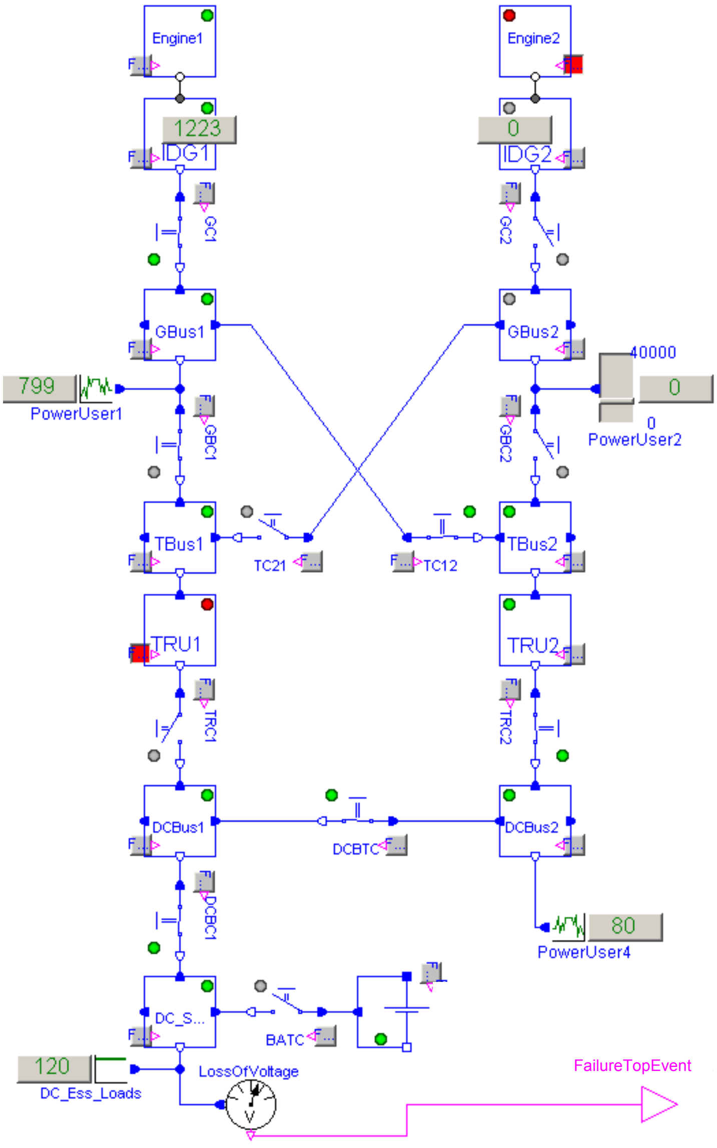


Figure 5: Twinjet Aeroplane Electric System Model, Engine2 and TRU1 have failed

The failure effects are, as can be seen in Figure 5:

- *IDG2* does not operate. Consequently, the *GBus2* is de-energised, as well as the connected *PowerUser2*.
- *TBus2* is now energised by the opposite side through the *TC12* switch, which has been closed automatically.
- All DC busbars *DCBus1*, *DCBus2* and *DC_STBY_Bus* are now supplied by *IDG1* through *TRU2*.
- Although degraded, the system is still operational in the complementary sense of the defined *FailureTopEvent*.

2.4 Reliability Analysis Procedure

The reliability analysis procedure is capable of automatically determining the so called minimum path sets for a given system model. A minimum path set is a combination of operative components that causes a system to operate in the complementary sense of the defined failure top event. Further on, the procedure computes reliability measures, i.e. system failure probability w.r.t. the defined top event, as well as component importances. For further illustration, results are shown in chapter 2.5 for the modelling example introduced in chapter 2.3.

The reliability analysis procedure draws on two kinds of information contained in a system model, as will be depicted: Chapter 2.4.1 explains a method to evaluate the system model behaviour in terms of operation or failure by multiple simulations. Then, chapter 2.4.2 introduces a method to interpret the object structure of the system model. Finally, chapter 2.4.3 describes how the two methods are combined to an automated reliability analysis procedure.

2.4.1 System Model Evaluation by Simulations

A simulation based method evaluates the system model for combinations of operative and failed components in a specific order. Minimum path sets are detected by the occurrence of system operation, i.e. the logical signal *FailureTopEvent* flagged as false.

Each system model contains the n components C_1, C_2, … , C_n. At first, the system model is simulated for single (k = 1) intact components. Each row 1, 2, … , n in Table 1 represents one set of operative (OK) and failed (-) components to test in the simulation.

Table 1: Intact/Failed Components to Simulate, k = 1

	C_1	C_2	…	C_n
1	OK	-		-
2	-	OK		-
…			…	
n	-	-		OK

If the system is operational for a row of Table 1, then the intact component of that row is stored as a minimum path set.

The method continues with simulating for two (k = 2) intact components, as depicted in Table 2. Again, each row stands for one set of operative and failed components to test. If minimum path sets of lower order (k < 2) were found, then those rows of Table 2 that contain all intact elements of a previously detected minimum path set are not tested in the simulation. This way, it is ensured that each detected path set is minimum, meaning that it does not contain any subset of other path sets.

Table 2: Intact/Failed Components to Simulate, k = 2

	C_1	C_2	…	C_n
1 2	OK	OK		-
…			…	
1 n	OK	-		OK
…			…	
2 n	-	OK		OK
...			…	

If the system is operational for a row of Table 2, then the intact components of that row are stored as a minimum path set.

In an analogous manner, the method continues with the determination of minimum path sets by simulating the system model for intact components up to an order of k = n, see Table 3.

Table 3: Intact/Failed Components to Simulate, k = n

	C_1	C_2	…	C_n
1 2 … n	OK	OK	…	OK

Apparently, this simulation based method has a character of systematic trial and error. Yet, the computing effort increases significantly with the number of components contained in a system model. For a system model comprising n components, a total of up to N sets (rows) have to be checked by simulations:

$$N \leq \sum_{k=1}^{n} \binom{n}{k}$$

Table 4: Estimation of Computing Effort

n	1	2	3	4	…	10	…	20
N	1	3	7	15		1023		1048575

Consequently, this method of minimum path set determination is only practical for systems including relatively few components. On its own, this method is not suitable for analysing the example model shown in Figure 4, which represents an electric system including 25 components.

So far, the system model is checked only in simulations. A further possibility is to evaluate the object structure of the system model, as described in 2.4.2.

2.4.2 Object Structure of the System Model

Another method exploits the object structure of the system model, i.e. the arrangement of components and connections. Advantage is taken of the fact that the structure of object-oriented models is similar, although not exactly identical, to minimum path sets.

Thus, a specific algorithm is devised to analyse the succession of connected components. As a result, the algorithm yields the different paths of consecutive and non-repeating components that exist in a system model. The paths that are determined in this manner are considered as minimum path set candidates.

The fundamentals of this kind of algorithm are described hereafter. It is realised as a recursive model parser in Modelica. In the listing, the notations component1, component2 and path indicate variables.

1. Begin at the FailureTopEvent gate of the system model and add it as component1 to the path.
2. Find all components connected to component1.
3. If no components are connected to component1 then terminate the actual recursion branch.
4. If one component is connected to component1 then take it as component2 and continue with the actual recursion branch,
5. else if more than one components are connected to component1 then start a new recursion branch for each component taken as component2, respectively.
6. If component2 is not contained in path yet then add component2 to path and resume at step 2 taking component2 as the next component1,
7. else terminate the actual recursion branch.

The result of this system model object structure analysis are paths that are considered as minimum path set candidates. These are illustrated graphically in Figure 6 for the electric system introduced in chapter 2.3. A representative selection of the 29 paths determined for this example is shown.

2.4.3 Combination of Object Structure Analysis with Simulation Based Method

As mentioned, the found paths are considered as minimum path set candidates. Therefore, these candidates are checked by simulating the system model accordingly, to eventually extract the minimum path sets from the list of candidates.

In this method, the system model is simulated for each candidate, such that the components belonging to a candidate are switched to the intact mode one after another, while all other components of the system are failed. System operation or failure is detected in the simulation by evaluating the logical signal *FailureTopEvent*. If the system operates, then the causing set of intact components is stored as a minimum path set.

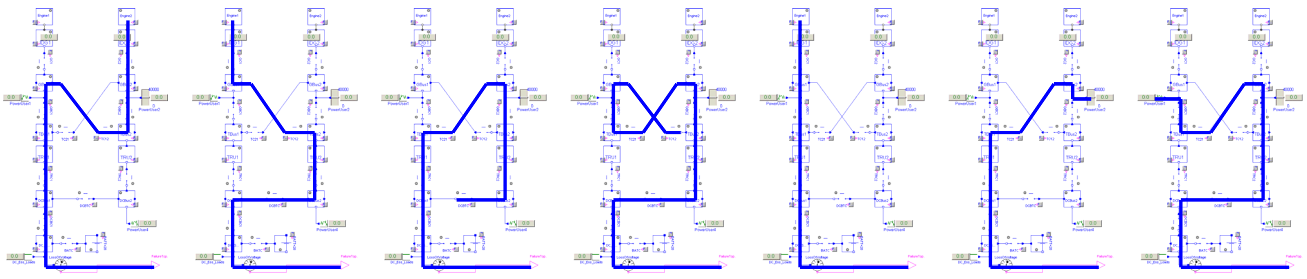
The number of path candidates to be checked in the simulation is limited, hence conducting an object structure analysis first and then simulation minimises the overall computing effort. Thus, the combination of both leads to a reliability analysis procedure that is viable even for large systems with many components.

After the minimum path sets of a system have been determined, reliability measures can be computed.

The probability of occurrence belonging to each minimum path set, i.e. the system operates, MP_i is $P(MP_i)=\prod_{C_i\in MP_i}(1-p_i)$, with the components C_i and the individual failure probabilities p_i.

Assuming an exponentially distributed lifetime [6] for the components C_i leads to failure rates λ_i that are constant over lifetime. The probability of a component failure is

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



…

Figure 6: Model Object Structure Analysis: Graphical Representation of Several Minimum Path Set Candidates

Since the occurrence of at least one minimum path set causes the system to operate, the probability of system operation can be calculated according to Poincaré's formula [6] as

$$P_{system-operation}(p_i) = P(MP_1 \vee MP_2 \vee \ldots \vee MP_n)$$

$$= \sum_{j=1}^{n}(MP_j) - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} P(MP_i \wedge MP_j) + \ldots$$

$$+ (-1)^{n+1} P(MP_1 \wedge MP_2 \wedge \ldots \wedge MP_n)$$

with n being the number of minimum path sets.

Generally, i.e. for a single component or a complex system, the following equation holds

$$p_{failure}(t) + p_{operation}(t) = 1$$

which eventually allows to calculate the probability of system failure.

Another useful reliability measure are component importances, which help to identify potential weak points or unnecessary redundancies in a system. Several definitions of importances exist. Here, the definition of marginal importances, that indicate the structural and probabilistic influence of a component i in a system, is given by

$$I_{marg}(i) = \frac{\partial P_{system-operation}(p_i)}{\partial p_i} \quad \text{with } 0 \le I_{marg}(i) \le 1$$

To summarise, Figure 7 gives an overview of the entire concept of incorporating a reliability analysis procedure with the Modelica language.

2.5 Reliability Analysis Results for Modelling Example

To illustrate the reliability analysis procedure, results are shown below for the modelling example of 2.3.

Table 5 lists the components that appear in the system model with the related failure rates λ_i.

The exposure time is set to t = 1h for simplicity, so that the failure probabilities are: $p_i(t) \approx |\lambda_i|$

Table 5: Electric System Model Components List

i	C_i	λ_i [1/h]
1	Engine1	10^{-5}
2	Engine2	10^{-5}
3	IDG1	10^{-4}
4	IDG2	10^{-4}
5	GC1	10^{-6}
6	GC2	10^{-6}
7	GBus1	10^{-7}
8	GBus2	10^{-7}
9	TBus1	10^{-7}
10	TBus2	10^{-7}
11	GBC1	10^{-6}
12	GBC2	10^{-6}
13	TC12	10^{-6}
14	TC21	10^{-6}
15	TRU1	$2 \cdot 10^{-4}$
16	TRU2	$2 \cdot 10^{-4}$
17	DCBus1	10^{-7}
18	DCBus2	10^{-7}
19	TRC1	10^{-6}
20	TRC2	10^{-6}
21	DCBTC	10^{-6}
22	DC_STBY_Bus	10^{-7}
23	BATT	0.001
24	BATC	10^{-6}
25	DCBC1	10^{-6}

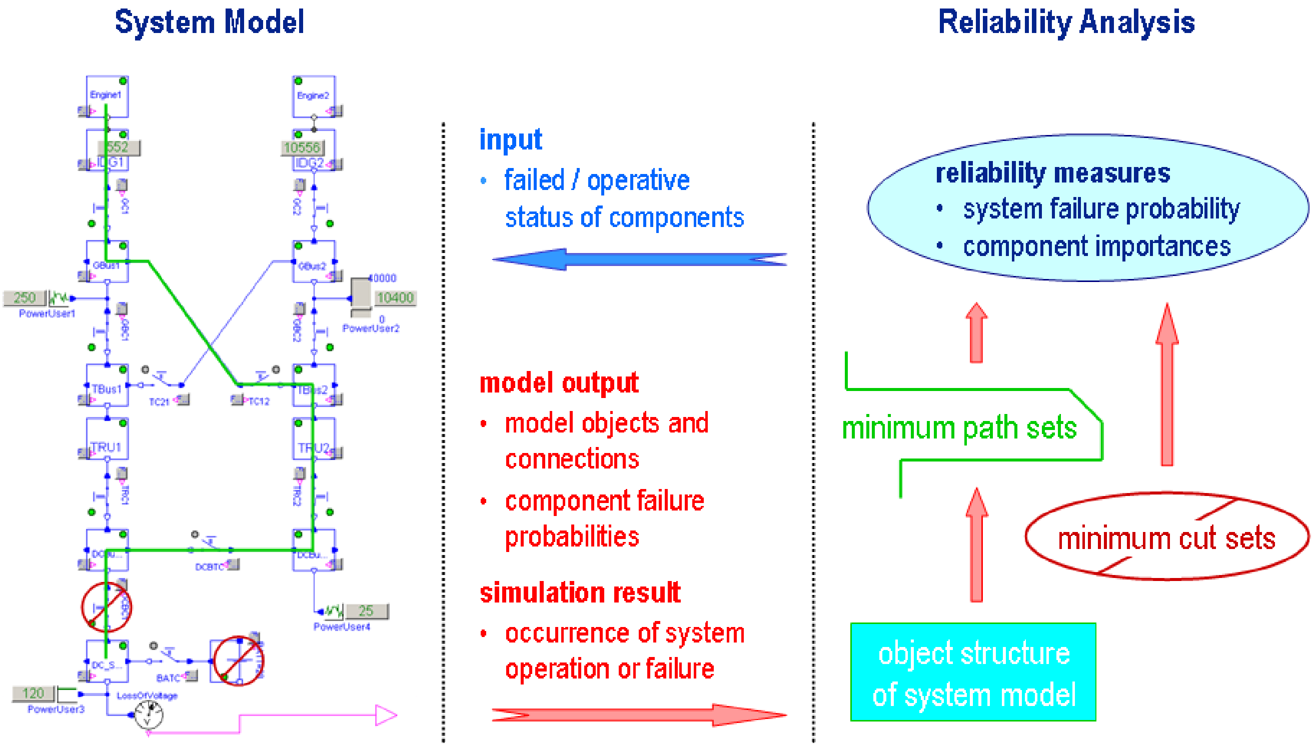


Figure 7: Concept of Reliability Analysis Incorporation with Modelica

2.5.1 Scenario 1: DC STBY Bus Energised

In Figure 8, the five minimum path sets determined for the electric system and the scenario "*DC_STBY_Bus* energised", which is the complement of "loss of voltage on *DC_STBY_Bus*", are graphically shown. The system operates, i.e. the *DC_STBY_Bus* is energised, if all components of either minimum path set are operational. For the opposite case, the probability of system failure is computed as

$$P_{system-failure} = 1.012 \cdot 10^{-7}$$

Figure 9 shows a plot of the component importances. Altogether, the analysis result can be interpreted such that for the given scenario, the system failure probability is dominated by a failure of the *DC_STBY_Bus* itself, followed by failures of the *DCBus1* and the contactor *DCBC1*. The influences of the three redundant voltage sources *IDG1*, *IDG2* and *BATT*, that can energise this busbar are much smaller.

2.5.2 Scenario 2: DCBus1 and DCBus2 Energised

In a different scenario, the loss of voltage on *DCBus1* OR *DCBus2* (or both) is examined for the same electric system. Figure 10 shows the implementation of this scenario in the system model. In the complementary sense, system operation means that both busbars, *DCBus1* and *DCBus2*, are energised.

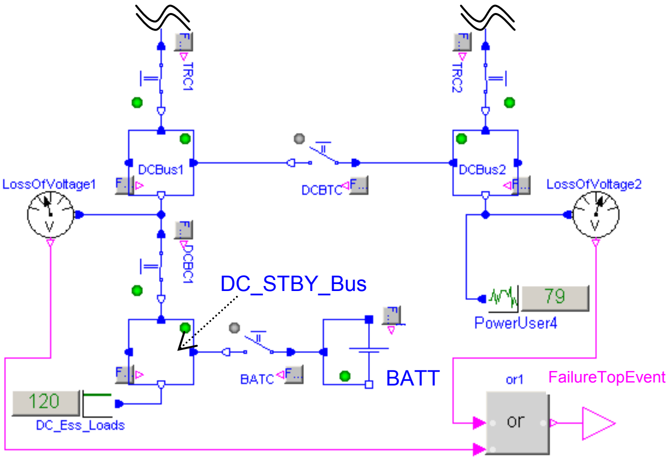


Figure 10: Implementation of Scenario 2 in System Model

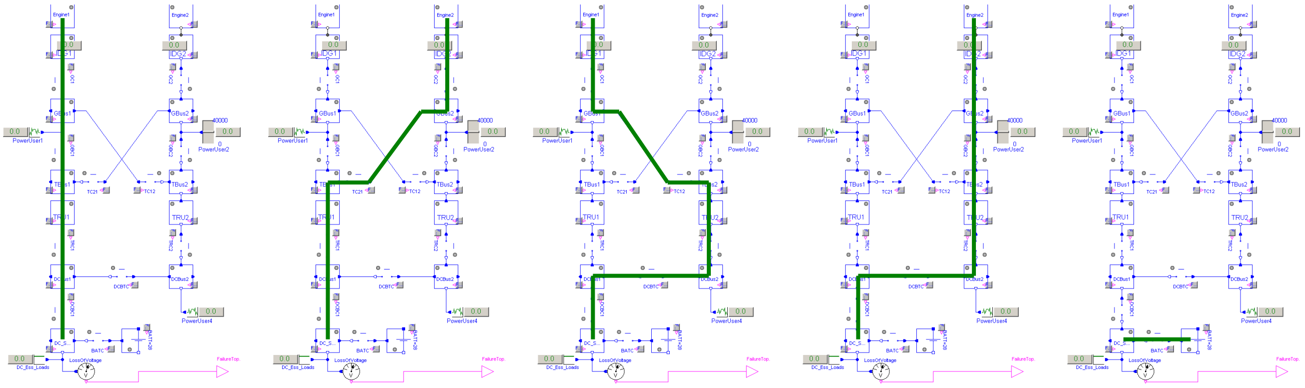


Figure 8: Graphical Representation of the five Minimum Path Sets for Scenario 1 "DC STBY Bus energised"

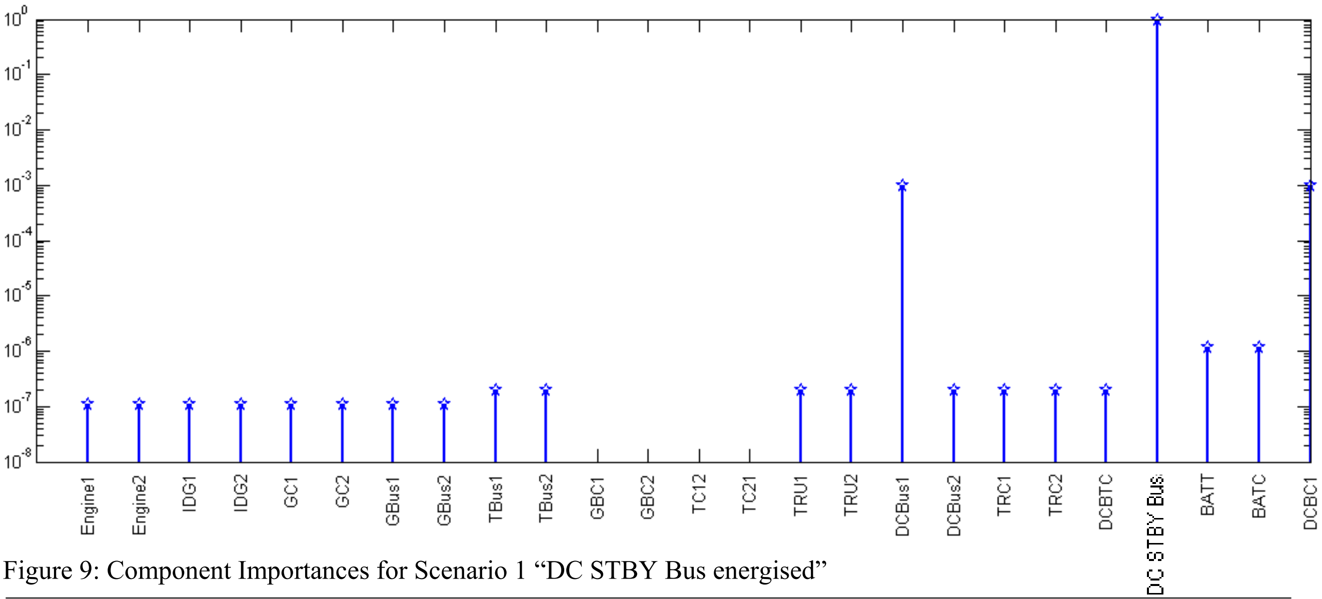


Figure 9: Component Importances for Scenario 1 "DC STBY Bus energised"

In Figure 12, the eight minimum path sets are depicted that were identified for this scenario. The probability of system failure has been calculated as

$$P_{system-failure} = 2.532\cdot10^{-7}$$

An interpretation of this result is that again the system failure probability is influenced mostly by busbar failures themselves, as it is indicated also by the importances shown in Figure 11. Other contributions arise from the busbar cross contactor *DCBTC* and from most of the upstream electric network components. The *DC_STBY_Bus* and the *BATT* have no influence since *DCBus1* and *DCBus2* can be energised only by the generators *IDG1* or *IDG2* through the network.

In summary, the example results demonstrate the capability of the novel reliability analysis procedure incorporated in Modelica to evaluate complex system architectures. The procedure is started “at the push of a button” and automatically computes the results without any further action required from the user.

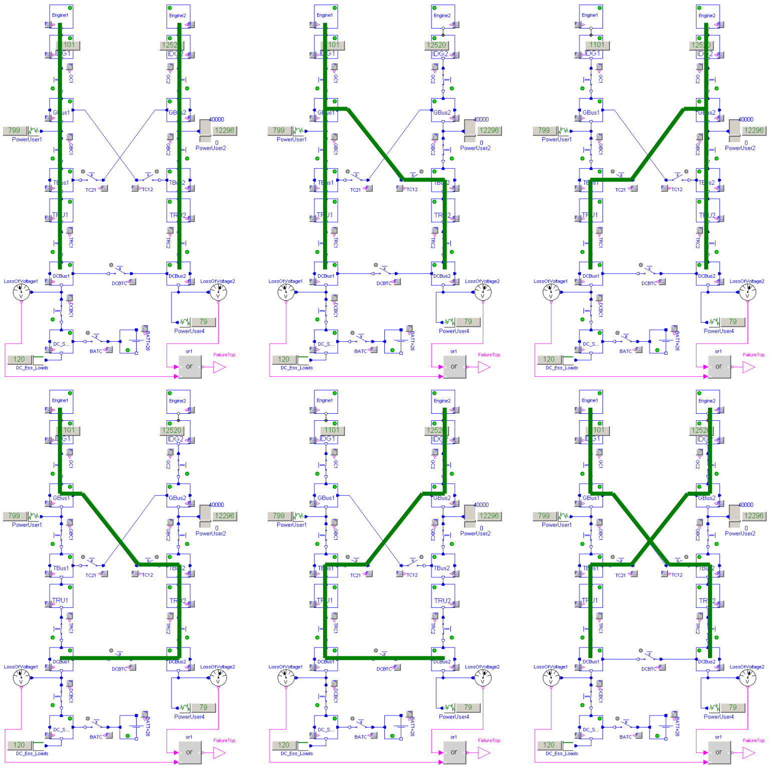


Figure 12: Graphical Representation of the eight Minimum Path Sets for Scenario 2 “DCBus1 and DCBus2 energised”

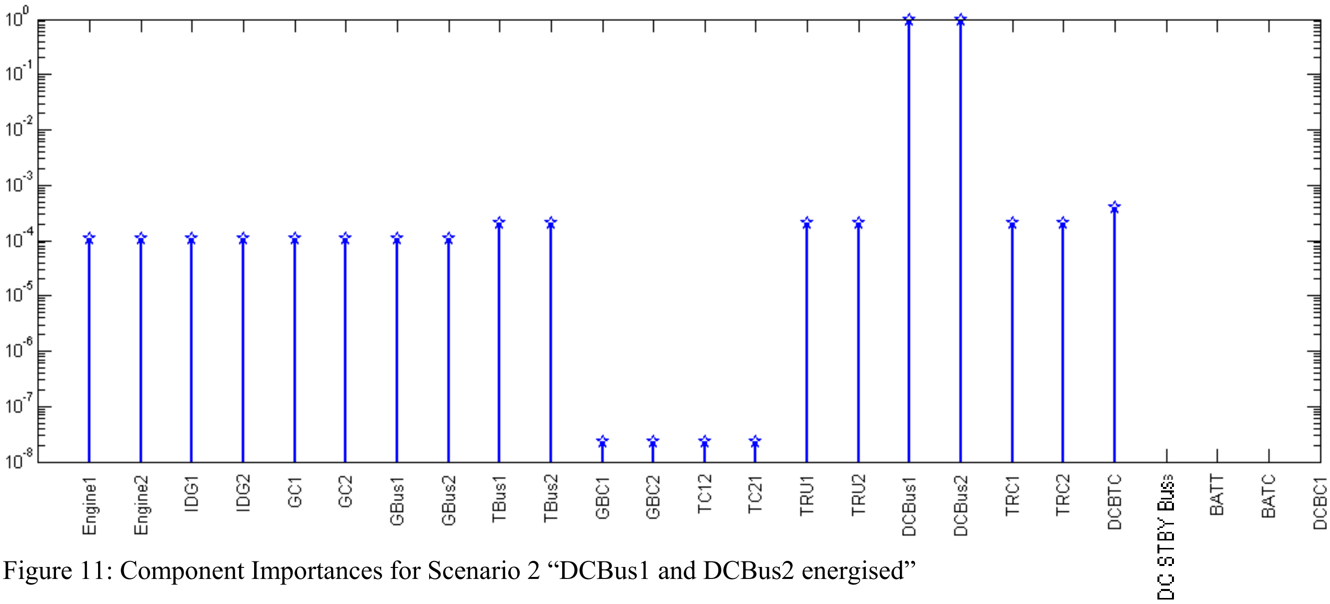


Figure 11: Component Importances for Scenario 2 “DCBus1 and DCBus2 energised”

3 Conclusions and Outlook

A new method to enhance Modelica with the capability of conducting reliability analyses is outlined.

The incorporation of automated reliability analysis methods with Modelica broadens the scope of the language, thus being able to support design studies of redundant and safety critical systems, where sufficient system reliablity has to be demonstrated.

The methods are realised initially by a new, Modelica based modelling and analysis tool for aircraft onboard electric power systems. System models can be built and simulated in the known fashion using components from existing and a specific new model library. Then, a reliability analysis can be performed for the same system model "at the push of a button".

The analysis procedure automatically detects the so called minimum path sets of a system. Further on, reliability measures are computed, like system failure probability, e.g. for the partial or total loss of voltage, as well as component importances. These give insight to potential weakness or unnecessary redundancy that may exist in the design of a system.

Future work will oriented to

- an extension of the reliability analysis procedure, such that it can examine models containing differential equations. The procedure is devised initially for system architecture studies, which are usually carried out on models that solely consist of algebraic equations.
- the creation of an automated power sizing analysis: Minimum path sets represent the different operational scenarios of an electric system, so these scenarios can be evaluated in simulations to determine the maximum power that each component carries [7]. This is affecting the sizing and hence the weight of components. Another possibility is to conduct a power availability analysis, i.e. to compute probabilities for the amount of electric power available on a busbar.
- a widening of the fault modelling, such that each electric component model can be simulated for several kinds of malfunction, e.g. open circuit, short circuit, short circuit to ground etc. This will permit to run so called minimum cut sets analyses, leading to an even more comprehensive assessment of system safety and reliability.
- developing features for an improved graphical representation of the analysis results.
- a transfer of the methods to other physical domains, as well as non-aerospace applications.

Acknowledgements

This research is being conducted in the frame of the MOET project (More-Open Electrical Technologies), a FP6 European Integrated Project [8].

The author wishes to thank the electrical engineering department of Airbus-France for their support being the first beta tester of the tool prototype.

References

[1] Modelica Language. http://www.modelica.org

[2] Dynasim Dymola. http://www.dynasim.se

[3] Moir, I. and Seabridge A. (2001). *Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration.* AIAA Education Series, ISBN 1-56347-506-5.

[4] Wild, T. W. (1996). *Transport Category Aircraft Systems*. Jeppesen Sanderson, Inc. ISBN 0-88487-232-7.

[5] Lloyd E. and Tye W. (1982). *Systematic Safety – Safety Assessment of Aircraft Systems.* Civil Aviation Authority (CAA), London, ISBN 0 86039 141 8.

[6] Meyna A. and Pauli B. (2003). *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik.* Carl Hanser Verlag München Wien, ISBN 3-446-21594-8.

[7] Schallert, C. (2007). *A Novel Tool for the Conceptual Design of Aircraft On-Board Power Systems.* SAE AeroTech Congress and Exhibition, Los Angeles, CA.

[8] MOET Project. http://www.moetproject.eu