Modelling an aircraft flight using the cause-consequences diagram method

This item was submitted to Loughborough University's Institutional Repository by the/an author.

Citation: VYZAITE, G. ... et al, 2006. Modelling an aircraft flight using the cause-consequences diagram method. Proceedings of the 4th Conference on Risk, Edinburgh, March 2006

Additional Information:

- This is a conference paper

Metadata Record: [https://dspace.lboro.ac.uk/2134/3625](https://dspace.lboro.ac.uk/2134/3625)

Publisher: © Gintare Vyzaitė, Sarah Dunnett, John D. Andrews and Goff Tearle

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
Modelling an Aircraft Flight Using the Cause-Consequence Diagram Method

Gintare Vyzaite, Sarah Dunnett, John Andrews, Goff Tearle
Aeronautical and Automotive Engineering, Loughborough University,
Loughborough, UK

Abstract

A system that can be modelled as a mission consisting of a sequence of phases is called a phased mission system. In this case, for successful completion of each phase the system may have to meet different requirements. System failure during any phase will result in mission failure. Fault tree analysis, binary decision diagrams and Markov techniques have been used to model phased missions.

The cause-consequence diagram method is an alternative technique capable of modelling all system outcomes (success and failure) in one logic diagram. The structure of the diagram has been shown to have advantageous features in both its representation of the system failure logic and its subsequent quantification, which can be applied to phased mission analysis.

This paper presents an example of the application of the cause-consequence diagram method to a non-repairable phased mission system. The system considered is an aircraft flight consisting of six phases: take off, climb, cruise, descent, approach and landing. Each phase uses differing functional elements of the system and so the causes of failure in each phase are different. An automated approach is used to construct and quantify the cause-consequence diagram. The causes of mission failure are identified and investigated.

Introduction

A phased mission can be described as a task that a system performs in which the failure logic model of the system changes over the duration of the phased mission. The mission can be divided into consecutive time periods, phases, during which system configuration, system failure characteristics or other parameters may differ from those in any immediately succeeding phase.

The aim of phased mission analysis is to calculate exact, or obtain bounds for, mission unreliability, which is defined as the probability that the mission fails to function in at least one phase. Taking the product of the phase reliabilities to obtain mission reliability results in inaccuracies because the sub-systems are not necessarily independent between the phases. They may be included in more than one logic model of the various phases. Different methods have been proposed to deal with the problem of obtaining the mission unreliability. In the case of non-repairable systems Esary and Ziehn [1] have used fault tree methods with basic event transformations and cut set cancellations to produce one artificial single phase mission. Binary Decision Diagram (BDD) methods have also been used by Zang, Sun and Trivedi [2] and La Band and Andrews [3]. The method proposed by Esary and Ziehn gave an efficient means of calculating the mission unreliability, but was unable to calculate the probabilities of failure of each phase. The extension of this method using BDD's proposed by Zang et al and La Band and Andrews gives a more efficient means of analysis than the fault tree approach but BDD's are difficult to construct directly from a system definition.

Recently it has been shown, Vyzaite et al [4], that the cause-consequence diagram method is an effective alternative to the previous methods for modelling phased missions. The cause-consequence diagram method, originally developed at RISO laboratories in Denmark, presents logical connections between causes of an undesired event and consequences of such an event if one or more mitigating provisions fail. As all consequence sequences are investigated, the method can be useful in identifying system outcomes, which may not have been investigated at the design stage. Ridley and Andrews [5,6] showed that, for some types of system, the final cause-consequence diagram has an identical structure to that of the BDD. They noted, however that the cause-consequence diagram was more concise due to the automatic extraction of common independent sub-modules. As the cause-consequence diagram can be obtained directly from the system description, there was no need to develop and convert from a fault tree to BDD. Since the BDD is a more efficient tool than the fault tree method, then the cause-consequence diagram formulation can also be advantageous.

The cause-consequence diagram has the potential to offer a clear representation of phased mission system analysis and to also provide an effective quantification technique. It also has the capability to model the failure of each phase in addition to the whole mission in one diagram. This was demonstrated to be the case for non-repairable systems by Vyzaite et al where methods for construction and quantification of the diagram were considered.

This paper demonstrates how the method can be applied to an aircraft flight.
Cause-Consequence Diagram Method

The construction of the cause-consequence diagram is based on the occurrence of a critical event, where a critical event may be defined as the failure of components or subsystems that are likely to produce hazardous consequences. Once a critical event has been selected, the cause-consequence diagram method describes all relevant causes of it, and develops its potential consequences using two conventional reliability analysis methods – fault tree analysis and event tree analysis, Nielsen [7]. Fault tree analysis is used to investigate the causes of an undesired event, while event tree analysis shows the consequences that such a critical event may lead to, if one or more protection systems do not function as desired.

Figure 1 illustrates a typical cause-consequence diagram. The main symbol used in the construction of the cause-consequence diagram is a decision box containing a system condition. It is an identical representation of the ‘YES-NO’ branches seen on an event tree structure. Considering the outlet branches YES and NO of the decision box the diagram is developed. The causes of each decision box event are developed using fault tree analysis (FT1, FT2). The cause-consequence diagram terminates in consequence boxes when the causes developed completely determine the system outcome (MS, MR).

![Cause-Consequence Diagram](image)

**Figure 1. Simple cause-consequence diagram**

Cause-Consequence Analysis of Phased Missions

**Cause-Consequence Constructions for Phased Missions**

The construction of cause-consequence diagram for phased missions was discussed in Vyzaite et al [4]. Failure of each phase is represented by fault tree. To be able to consider component failures in different phases basic event transformation has to be applied to each fault tree. That means that each component is substituted by OR gate inputs to which are component failures in each phase up to and including the phase that is considered. Component $A$ failure in phase $i$ is represented as $\overline{A}_i$ and functioning of component $A$ in phase $i$ is represented as $A_i$. This notation is extended to consider several phases in a concise way, $A_y$ will note failure of a component at some time from start of phase $i$ to end of phase $j$. $\overline{A}_y$ notes that the component $A$ is working from start of phase $i$ to end of phase $j$. So, if we have component A in the fault tree of phase 3, it would be substituted by an OR gate which would have $A_1$, $A_2$ and $A_3$ as inputs. The construction of the diagram would start with deciding the order in which component failures are to be considered. Two methods to construct the cause-consequence diagram were proposed [4].

First method would consider each component failure following the given order and add to diagram as a decision box one by one. After adding the component failure event the mission (phase) failure and success conditions are checked and if system fails when this component fails a consequence box stating mission (phase) failure is attached to YES branch of the decision box. Then next component failure would be added to NO branch and so on. If the mission (phase) doesn’t fail after failure of this component, then next decision box would be attached to both YES and NO branches of this decision box. Components are considered one after another until the conditions are met for mission success or failure.

The alternative method is based on the fact that the whole cause-consequence diagram contains events which are both repeated and inconsistent. The construction of the diagram starts with listing phase failures in decision boxes. The causes of each phase failure are developed using fault tree and attached to the decision box. As this cause-consequence diagram contains both repeated and inconsistent failure events, these must be extracted one by one following the normal cause-consequence analysis procedure described be Andrews and Ridley [5,6]. This results in a final cause-consequence diagram for phased mission that has no repeated or inconsistent events.
Qualitative analysis

The qualitative analysis of the cause-consequence diagram will produce the list of causes for each outcome condition. Conditions causing any outcome event are established by investigating each decision box on the path to the outcome and listing the component failure or success in the phase as indicated by the exit path from the decision box. These combinations of basic events are called prime implicants. The notation described earlier enables us to define algebra over the phases to manipulate the logic equations. In the equations the symbol "\( \cdot \)" is used for AND and "\( + \)" is used for OR. Algebraic laws defined by La Band and Andrews [3] are as follows:

\[
\begin{align*}
A_i \cdot A_j &= A_i \\
A_i \cdot A_j &= 0 \\
A_i \cdot A_j &= A_i \\
\bar{A_i} \cdot A_j &= 0 \\
\bar{A_i} \cdot A_j &= A_i \\
A_i, A_{j}, \ldots, A_j &= A_y \\
A_i + A_{i+1} + \ldots + A_j &= A_y
\end{align*}
\]

Whenever there is a situation in the list of causes for an outcome where a component is working in an earlier phase, but fails in a later phase, the event that the component was working in earlier phase can be cancelled out, as failure in later phase implies that it was working before, as described by the new algebraic laws described above. So, for example, if the list of conditions is as follows:

\[
\overline{A_i} \cdot B_3 \cdot \overline{C_1} \cdot \overline{A_i} \cdot B_2 \cdot A_i \cdot B_3.
\]

It can be simplified to

\[
\overline{C_1} \cdot A_i \cdot B_3.
\]

Quantitative analysis

The reduced or simplified lists of component conditions leading to each outcome are in an appropriate form for the quantification. This is because each of the outcome event sequences are mutually disjoint. Under these conditions the probability of achieving any particular phase failure is the sum of the probabilities leading to that outcome.

Quantification of the diagram starts with the calculation of the probabilities for each event \( A \) failing in phase \( i \) having worked throughout the previous phases, \( P(A_i) \), which is described as:

\[
P(A_i) = \int f_x(u) \, du
\]

where \( f_x(u) = \lambda e^{-\lambda u} \).

This method does however need to account for the fact that on the path through the diagram which has the working state of the component with the inconsistent failure modes its probability is 1 minus the probability of the inconsistent failure modes. Therefore, if there is a component working in two (or more) consecutive phases, for example, 'component \( A \) works through phase 1' and 'component \( A \) works through phase 2', probability of this is calculated as:

\[
P(\overline{A_i} \cdot \overline{A_j}) = 1 - P(A_i) - P(A_j)
\]

Coherent Approximation

Application of coherent approximation can help to reduce the size of the problem. A coherent approximation is obtained by assuming that all working states of components are TRUE (i.e. the probability of the component working through the phase is very close to 1). For example, \( \overline{C_1} \cdot A_i \cdot B_3 \) above would reduce to \( A_i \cdot B_3 \). This will produce cut sets. Minimal cut sets can be obtained by minimizing these cut sets. Then the approximate result is obtained by using inclusion-exclusion formula on of these minimal cut sets:

\[
P(\text{mission failure}) = \sum_{i=1}^{N} P(c_i) - \sum_{i=1}^{N} \sum_{j=1}^{N} P(c_i \cdot c_j) + \ldots + (-1)^{N-1} P(c_1 \cdot c_2 \cdot \ldots \cdot c_N),
\]

where \( c_i \) is a minimal cut set, \( N \) is the number of minimal cut sets. This approximation technique gives good results for very reliable systems. As the second and later terms of the sum are generally much smaller than the first, it is a reasonable approximation to take into account just the first summation.
For reliable systems this is a very close result to the exact one.

**Aircraft flight system**

To illustrate the use of the CCD method for complex systems an aircraft flight has been considered. The flight considered will consist of 6 phases: take off, climb, cruise, descent, approach and landing. A diagram of the flight is shown in Figure 2.

![Aircraft Flight Diagram](image)

**Figure 2. Aircraft Flight Diagram**

Each phase of the flight may utilise different systems within the aircraft. For example, the landing gear is required only in the take off and landing phases. The aircraft systems that were used in this model are:

- Propulsion system, which consists of:
  - Twin turbofan engine.
  - The control of engine thrust is achieved by altering the fuel flow to the combustion chamber of the engine.

- The flight control system is considered as two subsystems:
  - Primary flight control. The aim of primary flight control is to control manoeuvre of the aircraft about each of its axes.
  - Secondary flight control. The secondary flight control is used intermittently to change the value of lift and drag generated by the aircraft surfaces, but not to affect the trajectory.

- The fuel system which provides an effective means of replenishment, storage and fuel feed to the engines under all anticipated operating conditions. It is considered as two subsystems:
  - A fuel feed system which provides a flow of fuel to the engines.
  - A fuel transfer which provides a means of fuel transfer between tanks and via external sources in flight and during ground situations.

- Pneumatic supply. This system not only facilitates starting, but also supplies low pressure air for other aircraft services such as anti-icing and water tank pressurisation.

- Hydraulic system. Many of the aircraft services are powered by hydraulic power including flight control systems, flaps, retractable undercarriages and wheel brakes.

- Environmental control system. The environmental control systems overall aims are to minimise the risk to the safe operation of the aircraft in all anticipated weather and operational conditions and to ensure the safety and comfort of the people on board. It is considered to be made up of the two subsystems:
  - Anti-icing system.
  - Cabin conditioning. This subsystem has to provide safe oxygen levels, ensure comfortable cabin temperature and control humidity.

- Landing gear. Landing gear is defined as those components necessary to enable take-off and landing to be carried out safely. It excludes thrust reversal and control surfaces. Two failure modes have been considered:
  - Retraction – up
  - Lowering – down

- Flight navigation system. This is made up of 4 subsystems:
- INS. An inertial navigation system which measures the position and altitude of a vehicle by measuring the accelerations and rotations applied to the system's inertial frame.
- GPS. Global Positioning System (GPS) is an accurate means of providing continuous worldwide navigation information using a system of satellites.
- VOR/ADF/DME. VOR (VHF Omni-Range) is an internationally recognised short-range navigation aid. The principle of operation is based on a ground-based transmitter providing radial signal output, this is received by equipment on the aircraft to provide bearing information to an identified beacon. Automatic Direction Finding (ADF) function identifies bearing to a beacon to which the aircraft receiver is tuned. Distance Measuring Equipment (DME) is often integrated with VOR to provide range and bearing information.
- ILS/MLS. Instrument Landing System (ILS)/Microwave Landing System (MLS) is a landing aid providing both lateral and vertical guidance

- Electrical system. The primary function of an aircraft electrical system is to generate, regulate and distribute electrical power throughout the aircraft. The aircraft electrical power system is used to supply power for services including lighting, avionics, fuel system booster pumps and valves, control of hydraulic system components, in-flight entertainment, flight control systems and aircraft environmental control. Essential power is power that the aircraft needs to be able to continue safe operation.

The aircraft flight chosen was taken to be one that included flying over the ocean for a flight time of 460 minutes. Also, for modelling purposes it was decided to consider a twin-engine aircraft. It was assumed that all components are non-repairable whilst in flight.

In Table 1 the failure modes considered and notation adopted are shown.

<table>
<thead>
<tr>
<th>System</th>
<th>Subsystem</th>
<th>Failure mode description</th>
<th>Notation</th>
<th>Failures/10^6 flying hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propulsion</td>
<td>Engine</td>
<td>Failure of engine 1</td>
<td>E1</td>
<td>0.999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of engine 2</td>
<td>E2</td>
<td>0.999</td>
</tr>
<tr>
<td></td>
<td>Thrust</td>
<td>Failure of thrust to engine 1</td>
<td>T1</td>
<td>0.295</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of thrust to engine 2</td>
<td>T2</td>
<td>0.295</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of thrust reverser</td>
<td>TR</td>
<td>0.467</td>
</tr>
<tr>
<td>Flight control system</td>
<td>Primary flight control</td>
<td>Failure of primary flight control</td>
<td>PFCF</td>
<td>0.147</td>
</tr>
<tr>
<td></td>
<td>Secondary flight control</td>
<td>Failure of secondary flight control</td>
<td>SFCF</td>
<td>0.139</td>
</tr>
<tr>
<td>Fuel system</td>
<td>Fuel feed</td>
<td>Failure of fuel feed</td>
<td>FFF</td>
<td>0.393</td>
</tr>
<tr>
<td></td>
<td>Fuel transfer</td>
<td>Failure of fuel transfer</td>
<td>FTF</td>
<td>0.393</td>
</tr>
<tr>
<td>Pneumatic supply</td>
<td>Pneumatic supply</td>
<td>Failure of pneumatic supply</td>
<td>P</td>
<td>0.288</td>
</tr>
<tr>
<td>Hydraulic system</td>
<td>Hydraulic system</td>
<td>Failure of hydraulic system</td>
<td>HS</td>
<td>0.446</td>
</tr>
<tr>
<td>Environmental control system</td>
<td>Anti-icing system</td>
<td>Failure of ice sensing</td>
<td>AIS</td>
<td>0.086</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of ice removal</td>
<td>AIR</td>
<td>0.131</td>
</tr>
<tr>
<td></td>
<td>Cabin control system</td>
<td>Failure of pressure control</td>
<td>CCPC</td>
<td>0.139</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of temperature control</td>
<td>CTC</td>
<td>0.148</td>
</tr>
<tr>
<td>Landing gear</td>
<td>Landing gear</td>
<td>Failure of landing gear retraction up</td>
<td>LGU</td>
<td>0.205</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of landing gear retraction down</td>
<td>LGD</td>
<td>0.205</td>
</tr>
<tr>
<td>Flight navigation system</td>
<td>Flight navigation system</td>
<td>Failure of INS</td>
<td>INS</td>
<td>0.0257</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of GPS</td>
<td>GPS</td>
<td>0.237</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of VOR/ADF/DME</td>
<td>VOR</td>
<td>0.309</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure of ILS/MLS</td>
<td>ILS</td>
<td>0.0026</td>
</tr>
<tr>
<td>Electrical system</td>
<td>Electrical system</td>
<td>Failure of power</td>
<td>ESP</td>
<td>0.0676</td>
</tr>
</tbody>
</table>

Phase 1

Phase 1, the take off phase, will be completed successfully, if all systems required in this phase operate successfully. These systems are: propulsion system (both engines have to function properly), flight control, fuel feed, pneumatic supply, hydraulic system, anti-icing system and landing gear. The fault tree for failure in phase 1 is shown in Figure 3 which has minimal cut sets shown in Table 2.
Phase 2

For phase 2, the climb phase, propulsion, hydraulic and pneumatic systems are required to work as in phase 1. Also required are: fuel transfer, primary flight control, environmental control, the flight navigation systems GPS and VOR/ADF/DME. The fault tree for failure in phase 3 is shown in Figure 4 which has minimal cut sets shown in Table 2.

Phase 3

During the cruise phase, propulsion system failure will be caused by the failure of both engines which will lead to aircraft failure. The thrust wouldn't cause critical failure in this phase.

Fuel feed, flight control, hydraulic system and pneumatic supply are required to work the same way as in phase 2.
Anti-icing system failure may not be critical during cruise, but cabin conditioning failure would as it is necessary to keep cabin pressure and temperature within a comfortable range. Failure of the navigation systems GPS or INS would lead to failure in this phase as would electrical system failure (power failure). The fault tree for failure in phase 3 is shown in Figure 5 which has minimal cut sets shown in Table 2.

![Figure 5. Fault tree for Phase 3](image)

**Phase 4**

Causes of system failure in phase 4, the descent phase, are shown in the fault tree in Figure 6. Failure will occur if the pneumatic, hydraulic, fuel, flight control and environmental control systems fail in the same way as in phase 2. The propulsion system failure will be caused by the failure of both engines which will lead to aircraft failure. The thrust wouldn’t cause critical failure in this phase. The failure of the GPS navigation system will also lead to phase failure. The minimal cut sets for this phase are shown in Table 2.

![Figure 6. Fault tree for Phase 4](image)

**Phase 5**

During approach, phase 5, the propulsion system, pneumatic supply and hydraulic system are required to work as in the previous phase. For environmental control – only anti-icing system failure may be critical. Flight control system will again depend on both primary and secondary flight controls—failure of any of them would be critical. During descent flight navigation needs GPS, VOR/ADF/DME and ILS/MLS and hence failure of any of them will lead to phase failure. The fault tree for failure in phase 5 is shown in Figure 7 which has minimal cut sets shown in Table 2.
Phase 6

Failure will occur in the landing phase if the hydraulic system and flight control system fail. Also failure of the flight navigation system ILS/MLS and the landing gear is critical. In addition, the electrical system and propulsion system (both engines and thrust reverser) are required to work. See the fault tree in Figure 8 with minimal cut sets given in Table 2.

Table 2. Minimal cut sets for each phase

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
<th>Phase 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFCF</td>
<td>T2</td>
<td>AIR</td>
<td>HS</td>
<td>HS</td>
<td>INS</td>
</tr>
<tr>
<td>AIR</td>
<td>T1</td>
<td>AIS</td>
<td>P</td>
<td>FTF</td>
<td>CCTC</td>
</tr>
<tr>
<td>AIS</td>
<td>P</td>
<td>E2</td>
<td>PFCF</td>
<td>P</td>
<td>CCPC</td>
</tr>
<tr>
<td>E2</td>
<td>PFCF</td>
<td>E1</td>
<td>GPS</td>
<td>PFCF</td>
<td>FTF</td>
</tr>
<tr>
<td>E1</td>
<td>LGU</td>
<td>FTF</td>
<td>VOR</td>
<td>E1·E2</td>
<td>P</td>
</tr>
<tr>
<td>HS</td>
<td>T1</td>
<td>CCPC</td>
<td>ESP</td>
<td>PFCF</td>
<td>PFCF</td>
</tr>
<tr>
<td>FFF</td>
<td>T2</td>
<td>CCTC</td>
<td>GPS</td>
<td>E1·E2</td>
<td>E1·E2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Construction of the Cause-Consequence Diagram

In order to construct the cause-consequence diagram it is necessary to assume a certain order in which the component failure events will be considered. Failures of each phase have to be ordered separately and then all failures joined in one list omitting any repeated event if the probability of failure in each phase is important. If probabilities of phase failure are not important and it is just an overall mission failure that is of interest, then all failures of the mission can be ordered together. In some examples the later method produced much smaller cause-consequence diagrams. For this example failures of each phase have been ordered separately and we assume the following order:

$$F_F < P < H_S < T_L < T_L < E_1 < E_2 < P_{FCF} < S_{FCF} < A_{IS} < A_{IR} < L_{GU} < L_{GU} < F_F < F_F < P_{FCF} < \ldots$$

where the notation adopted for the component failures is that given in Table 1 and the subscripts refer to the phase in which the failure occurs.

The program allows the order to be entered manually, or to be automatically generated it from the fault trees. The order of events shown above is automatically generated by the program, where the components are considered in the order that they appear in fault tree data files.

Following the order of component failures given, each component failure event is added to the diagram as a decision box one by one. That means first consider event $F_F$ (Fuel feed) in phase 1: if the event $F_F$ fails in phase 1, then the system state is determined and the system fails in phase 1 and the mission is failed. If the event $F_F$ does not occur throughout phase 1, then consider the next event in the ordering $P$ in phase 1: if the event $P$ occurs in phase 1, then the mission is failed in phase 1. If the event $P$ doesn't occur throughout phase 1 and other event required for phase 1 failure do not occur, then mission progresses to phase 2. Events are again considered one after another until the conditions are met for phase 2 failure or progression to phase 2. The diagram is finished when system progresses to phase 6 and conditions for failure or success of this phase are investigated.

The resulting diagram output by the program is represented in a list form. Each decision/consequence box is assigned a number and the program lists the numbers of the decision/consequence boxes it is pointing to on the YES and NO branches. For each box, the program also gives the number of the previous box in the branch.

Analysis of the Cause-Consequence Diagram

In order to quantify the resulting cause-consequence diagram and obtain the probability of mission failure it is necessary to input data for the subsystems. Estimated failure data is included in Table 1. The durations for the phases were taken to be those shown in Figure 2.

**Qualitative analysis**

Conditions causing any outcome event (implicants) are established by investigating each decision box on the path to the outcome and listing the component failure or success in the phase as indicated by the exit path from the decision box. In the example considered there are 383 outcomes. The component conditions for each of these outcomes were determined and some of them are listed below. The notation used for the events is that given in Table 1.

F1 – Mission failure in Phase 1

- $F_F$
- $P < F_F$
- $H_S < P < F_F$
- $T_L < H_S < P < F_F$
- $E_1 < E_2 < T_L < T_L < H_S < P < F_F$
- $P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$
- $S_{FCF} < P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$
- $A_{IS} < S_{FCF} < P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$
- $A_{IR} < S_{FCF} < P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$

Implicants for the later phases contain more events due to the consideration of the earlier phases. For example, one implicant for phase 2 is:

- $L_{GU} < L_{GU} < A_{IR} < A_{IS} < S_{FCF} < P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$

For the example shown, component $L_{GU}$ works throughout phase 1 and then fails in phase 2. After simplification the outcome would be:

- $L_{GU} < A_{IR} < A_{IS} < S_{FCF} < P_{FCF} < E_2 < E_1 < T_L < T_L < H_S < P < F_F$
Just considering the failed states for the systems which lead to mission failure give minimal cut sets. The minimal cut sets leading to phase failures in phases 1-3 are shown in Table 3. The notation used for the events is that given in Table 1. These minimal cut sets are obtained after basic event transformation was applied to fault trees of each phase. The minimal cut sets in Table 2 list minimal cut sets before the basic event transformation is applied to fault trees.

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR₁, FFF₁, SFCF₁</td>
<td>AIR₂, CCTC₂, GPS₁, VOR₁, CCPC₂, ESP₁, INS₁</td>
<td>AI₂, E₁, GPS₁, VOR₂, CCTC₂, FFT₁, INS₂</td>
</tr>
<tr>
<td>AIS₁, HS₁, T₁</td>
<td>AIS₁, E₁, HS₁, E₂, GPS₂, P₁</td>
<td>AIS₂, GPS₂, VOR₂, CCTC₂, FFT₁, INS₂</td>
</tr>
<tr>
<td>E₁, P₁, T₂</td>
<td>CCPC₁, E₂, HS₁, E₁, E₂, GPS₃, P₁</td>
<td>E₁, E₂, GPS₃, P₁</td>
</tr>
<tr>
<td>E₂, PFCF₁, LGU₁</td>
<td>CCPC₂, FFT₁, P₂</td>
<td>ESP₁, HS₁, PFCF₁</td>
</tr>
<tr>
<td>CCTC₂</td>
<td>CCTC₂, FFT₁, PFCF₂</td>
<td>ESP₂, INS₁</td>
</tr>
</tbody>
</table>

Quantitative analysis

The results for mission failure and success have been obtained using the developed program for phased mission analysis and are shown in Table 4.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Probability (exact)</th>
<th>Probability (coherent approximation)</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed in phase 1</td>
<td>0.00028726</td>
<td>0.00028727</td>
<td>-0.00000001</td>
</tr>
<tr>
<td>Failed in phase 2</td>
<td>0.00049395</td>
<td>0.00049412</td>
<td>-0.00000017</td>
</tr>
<tr>
<td>Failed in phase 3</td>
<td>0.00087139</td>
<td>0.00087238</td>
<td>-0.00000099</td>
</tr>
<tr>
<td>Failed in phase 4</td>
<td>0.00015541</td>
<td>0.00015566</td>
<td>-0.00000025</td>
</tr>
<tr>
<td>Failed in phase 5</td>
<td>0.00022142</td>
<td>0.00022183</td>
<td>-0.00000041</td>
</tr>
<tr>
<td>Failed in phase 6</td>
<td>0.00040186</td>
<td>0.00040272</td>
<td>-0.00000086</td>
</tr>
<tr>
<td>Completed</td>
<td>0.99755885</td>
<td>0.99755927</td>
<td>0.00000098</td>
</tr>
</tbody>
</table>

As the system investigated is very reliable, the coherent approximation results are very close to the exact results with the difference starting in the 6th decimal place.

For the generated data the probability of the aircraft completing flight successfully was found to be 0.997562. This is an example that was only used to demonstrate the application of the method developed.

Conclusions

- A phased mission example illustrating aircraft flight was developed. Mission was divided in six phases: take off, climb, cruise, descent, approach and landing. Each phase is represented by a fault tree.

- The cause-consequence is constructed by a program developed earlier for cause-consequence diagram construction. It also calculates the probabilities of phase failure and of mission failure and success.

- Exact quantification technique (result produced by program) and coherent approximation technique produced very close results. This was not surprising for this example as coherent approximation usually produce results close to the exact calculation for very reliable systems.

References


