3rd International Symposium on Aircraft Airworthiness, ISAA 2013

Failure Propagation Analysis of Aircraft Engine Systems Based on Complex Network

Xiaofeng Liu\textsuperscript{a, b, *}, Siqi AN\textsuperscript{a,b}

\textsuperscript{a}School of Transportation Science and Engineering, Beijing, 100191, China
\textsuperscript{b}Airworthiness Technologies Research Center, NLAA, Beijing, 100191, China

Abstract

To find the failure propagation mechanism from the complex system of aircraft engine, this paper used the topological structure to describe the coupling relations, discussing the role of topological geometry method in the failure propagation. The topological structure statistical properties of the system were analyzed with small world net theory, and a failure propagation model based on the small world clustering was proposed, and the failure propagation paths and relevant key nodes with high pervasion ability were found with the Dijkstra algorithm. The results verify that this method can effectively find the weak point in the system, and provide an important basis for design improvements and failure prevention.

© 2013 Published by Elsevier Ltd. Selection and peer-review under responsibility of ENAC

Keywords: Complex network; Failure propagation; Aircraft engine system

Nomenclature

FADEC Full authority digital engine controller
FMV Fuel metering valve
HMU Hydro mechanical unit
HPC High pressure compressor

* Corresponding author, lecturer, Ph.D. Tel.: +86-10-82316627; fax: +86-10-82316330.
E-mail address: liuxf@buaa.edu.cn.
1. Introduction

Airworthiness is the measure of an aircraft or airborne systems and equipment suitability for safe flight. Certification of airworthiness is initially conferred by a certificate of airworthiness from a national aviation authority, and is maintained by performing the required maintenance actions. The application of airworthiness defines the condition of an aircraft and supplies the basis for judgment of the suitability for flight of that aircraft, in that it has been designed with engineering rigor, constructed, maintained and is expected to be operated to approved standards and limitations, by competent and approved individuals, who are acting as members of an approved organization and whose work is both certified as correct and accepted on behalf of the state. With the development of science and technology of aviation and civil aviation, as well as the deepening of aviation safety, the concept of airworthiness is still continuously developed. Generally speaking, the definition of airworthiness is an abstract of the whole process of the physical collection, and the airworthiness of civil aviation is a quality. This quality requires the aircraft or aircraft part should always be harmonized with its models in the design and safe operation of the state remains.

Safety is something related to all human activities and therefore every civil society is organized (or should be organized) to guarantee public safety in relation to one’s own or others’ activities. This is certainly a moral obligation, but it is also a practical demand because accidents, causing damage to persons and properties, have a social cost. This is also the reason why human activities that could cause damage to persons and properties are controlled by national states through regulations \[1\]. Safety can also be defined to be the control of recognized hazards to achieve an acceptable level of risk.

The ideal objective of system safety is to develop a system free of hazards \[2\]. However, absolute safety is not possible because complete freedom from all hazardous conditions is not always possible, particularly when dealing with complex inherently hazardous systems, such as aero engines, commercial aircraft, and nuclear power plants.

Safety analysis is a necessary part of the process of showing that a system is safe to deploy. It is often necessary to construct a safety case containing the results of safety analysis and to present this to a certification authority in order to get authorization to deploy the system \[3\].

The ultimate objective of a safety analysis is to ensure that the risk to the aircraft from all engine failure conditions is acceptably low. The basis of a safety analysis is the concept that an acceptable total
engine design risk is achievable by managing the individual engine risks to acceptable levels. This concept emphasizes reducing the likelihood or probability of an event proportionally with the severity of its effects. The safety analysis should support the engine design goals so that major or hazardous engine effects resulting from engine failure modes do not exceed the required probability of occurrence.

Numerous models and methodologies have been developed to describe, predict and prevent failures or faults. These models and methodologies include classical probability principles based models [4], Markovian theory based models [5], Poisson theory based models [6], Bayesian theory based models [7], Monte Carlo simulation based models [8], Fault Tree Analysis (FTA) [9], Failure Modes and Effect Analysis (FMEA) [10, 11], and hybrid models [12].

Although a number of them have been proposed in the literature and used successfully sometimes, these methods have very limited applications, especially in the complex coupled systems. All these methods, more or less, require information about system layout, failure probability, failure effects of components and systems, which are often too expensive to obtain. And these models or methods have been mainly developed on the assumption that failures are independent. However, with the progress in structure and integration, modern aircraft engines have become more and more complex, and have shown that the assumption of independent failures has been unrealistic and has led to unacceptable analysis errors. Therefore, the concept of dependent failures was introduced and has been described in [13].

The subject of dependent failures has attracted the interest of researchers for decades. The most discussed dependent failures are: cascading failure, negative dependency failure and common cause failure [13]. Cascading failure is defined as multiple sequential failures. These failures are initiated by the failure of one component, which leads to sequential failures of other components. A component failure changes the system topology, which consequently increases the failure probabilities of remaining components and a second moment method for estimation the reliability of a system with cascading dependency failures [14]. In many real-world networks, the failure of a single or a very few nodes can trigger a cascading failures, which can disable the whole network almost entirely [15–18].

This paper introduces a new method for safety analysis based on the conclusions of complex networks. From the topological perspective, the relationship between the structural properties of such networks and cascading failures in these coupled complex systems is investigated. The network of the aircraft engine system is constructed and studied, and by using the methods mentioned in [16,17], the purposes of protecting existing system, locating the most critical nodes are studied. This paper is organized as follows: In Section 2, the network of aircraft engine system is constructed, and some definitions of terms and measured quantities to study the topological properties are provided. A model for cascading failures based on the dynamic redistribution of the load on the network, and the mechanism of cascading is analyzed is studied in Section 3. In Section 4, the safety analysis of the aircraft engine system is illustrated. Finally, conclusions are provided in Section 5.

2. Network of aircraft engine system

2.1. Construct the network of aircraft engine system

In the typical aircraft engine system, there are many kinds of components, such as HPC and HPT are on one shaft (driven by the High Speed Rotor), while the Fan, Booster and LPT are on the other shaft (driven by the Low Speed Rotor), Combustor, FADEC, sensors and other valves. All these components and devices are connected into a whole system, and the relationship between components and devices may be the control information, the energy transmitted by mass flow, etc. The scheme is shown in [19] figure 1.
The aircraft engine system was described as a network, the components and devices can be represented by the nodes, and the relationship between any two equipment can be represented by the edges as shown in Fig. 1 and Tab. 1. Obviously, the network of the system is a relatively complex. Once failures, faults or disturbs happened, which maybe caused by a sensor, a valve or other components of the system, it can be propagated and amplified, some of these faults can cause cascading failures.

Fig. 1. Network structure of the aircraft engine

Table 1. An example of a table

<table>
<thead>
<tr>
<th>Node</th>
<th>Name</th>
<th>Node</th>
<th>Name</th>
<th>Node</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fan</td>
<td>9</td>
<td>FADEC</td>
<td>17</td>
<td>LVDT of ( w_f )</td>
</tr>
<tr>
<td>2</td>
<td>Booster</td>
<td>10</td>
<td>HMU</td>
<td>18</td>
<td>Sensor of LPT outlet temperature</td>
</tr>
<tr>
<td>3</td>
<td>HPC</td>
<td>11</td>
<td>FMV</td>
<td>19</td>
<td>Sensor of HPC outlet pressure</td>
</tr>
<tr>
<td>4</td>
<td>Combustor</td>
<td>12</td>
<td>VSV</td>
<td>20</td>
<td>Position sensor of HPC stator vane</td>
</tr>
<tr>
<td>5</td>
<td>HPT</td>
<td>13</td>
<td>VBV</td>
<td>21</td>
<td>Sensor of Fan outlet temperature</td>
</tr>
<tr>
<td>6</td>
<td>LPT</td>
<td>14</td>
<td>HPTACC Valve</td>
<td>22</td>
<td>Position sensor of booster bleed valve</td>
</tr>
<tr>
<td>7</td>
<td>Nozzle</td>
<td>15</td>
<td>RVDT of ( n_H )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>TL</td>
<td>16</td>
<td>RVDT of ( n_L )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2. Definitions of Quantities

The topological statistic parameters are given in this section. Firstly, degree of node \( k \) is the number of edges connected to a node. \( K \) is the average degree of nodes.

From Fig. 1, we can see that the capacity or intensity of the relationship between nodes may be heterogeneous and the direction of the links is crucial in dynamical processes occurring in this network, such as information spreading, etc. Therefore, the aircraft engine system network is represented as a
weighted directed graph $G$, with $N$ nodes and $E$ edges. Each edge connects exactly one pair of nodes, and a node-pair can be connected by maximally one edge, i.e., multiconnection is not allowed. In addition, we introduce the weight matrix $W = [w_{ij}]$, where $w_{ij} \neq 0$ for $i \neq j$ and $w_{ii} = 0$ for $i \in N$. The adjacency matrix $A = [a_{ij}]$ of a directed weighted graph is a matrix with all zeros on the main diagonal, and off-diagonal elements

$$a_{ij} = \begin{cases} w_{ij} & \text{with probability } p_{ij} \\ 0 & \text{with probability } 1 - p_{ij} \end{cases}$$

for $i \neq j$. Where, an edge from vertex $i$ to vertex $j \neq i$ in the set $N$ is determined and independently of other edges with probability $p_{ij} \in [0, 1]$, we collect the probabilities $p_{ij}$ in the probability matrix $P = [p_{ij}]$.

There are several ways of measuring the functionality of networks. One key quantity is the average path length $L$

$$L = \frac{1}{N(N-1)} \sum_{i \in \mathcal{P}} \sum_{j \in \mathcal{P}} d_{ij}$$

where $d_{ij}$ is the length of the shortest path between $i$ and $j$, i.e., the number of edges in the shortest path connecting the two, and the factor $\frac{1}{N(N-1)}$ is one over the number of pairs of nodes.

Another is clustering coefficient $\gamma$ intends to measure the average degree of the local transitivity in a network. Let $|\Gamma_n|_E$ denote the number of edges in the neighborhood $\Gamma_n$ of $n \in N$ then

$$\gamma_n = \frac{|\Gamma_n|_E}{\binom{k_n}{2}}$$

is called the local clustering coefficient of the node $n$. Here the degree $k_n$ of $n$ is defined as the number of nodes in $|\Gamma_n|$, i.e., $k_n = |\Gamma_n|$. And $\binom{k_n}{2} = \frac{k_n(k_n-1)}{2}$. The clustering coefficient is then defined as the average of $\gamma_n$

$$\gamma = \frac{1}{|N|} \sum_{n \in N} \frac{2|\Gamma_n|_E}{k_n(k_n-1)}$$

In the studies of networks, the centrality is an important concept that tries to capture the prominence of a node in the embedding structure. It should be noted that the node with a low degree can have a high centrality and thus attacking the network by removing nodes with high centralities may differ from that by degrees. Among many centrality measures we focus on the node betweenness centrality $B_n(v)$ defined for a node $n \in N$ as follows

$$B_n(v) = \sum_{s,t \in N, s \neq t} \frac{\sigma_{st}(n)}{\sigma_{st}}$$
where $\sigma_{st}$ is the total number of shortest paths from node $s$ to node $t$ and $\sigma_{st}(n)$ is the number of those paths that pass through $n$. Note that the betweenness centrality of a node scales with the number of pairs of nodes as implied by the summation indices. Therefore the calculation may be rescaled by dividing through by the number of pairs of nodes not including $v$. Similarly, one can define the edge betweenness centrality $B_E(e)$ for an edge $e \in E$ as

$$B_E(e) = \sum_{s \in V \setminus e} \frac{\sigma_{st}(e)}{\sigma_{st}}$$

(6)

where $\sigma_{st}(e)$ is the number of shortest paths from node $s$ to node $t$ that includes the edge $e$. Throughout the present paper, we call $B_N(v)$ and $B_E(e)$ as the node betweenness and the edge betweenness for brevity. Fig. 2 to Fig. 4 show the aircraft engine system network’s quantities.

Fig. 2. Node degrees of this network

Fig. 3. Node betweennesses of this network
3. Analysis of failure propagation

3.1. Cascading Failure Modes

A cascading failure is a failure in a system of interconnected parts in which the failure of a part can trigger the failure of successive parts. Such a failure may happen in many types of systems, including power transmission, computer networking, finance and bridges. Cascading failures usually begin when one part of the system fails. When this happens, nearby nodes must then take up the slack for the failed component. This overloads these nodes, causing them to fail as well, prompting additional nodes to fail in a vicious cycle. These random edges significantly facilitate propagation of contagions such as disease and information. For simple propagation-such as the spread of information or disease-in which a single active node is sufficient to trigger the activation of its neighbors, random edges connecting otherwise distant nodes achieve dramatic gains in propagation rates by creating shortcuts across the graph.

In aircraft engine systems, many significant accidents are caused by a small fault. In fact, the breakdown of a single component or device not only has direct consequences on the performance of a system, but also can cause an overload and consequently the partial or total breakdown of other components, thus generating a cascading effect.

3.2. Model for Cascading Failures in Complex Networks

A generic graph $G$ with $N$ nodes and $E$ edges is considered. $G$ is assumed to be unweighted, i.e., edges are all equal, sparse $|E| \ll N(N-1)/2$, and connected; i.e., there exists at least one path connecting any two nodes with a finite number of steps. $G$ is therefore represented by simply giving the adjacency matrix, i.e., the $N \times N$ matrix whose entry $a_{ij} = 1$ if there is an edge joining node $i$ to node $j$ and is $a_{ij} = 0$ otherwise. We define a matrix $l$ is physical distances of a network. The number $l$ can be the space distance between the two nodes or the strength of their possible interaction: we suppose $l$ to be known even if in the graph there is no edge between $i$ and $j$. Of course, in the particular case of an unweighted graph $l_{ij} = 1 \forall i \neq j$. The shortest path length $d_{ij}$ between two generic points $i$ and $j$ is the smallest sum of the physical distances throughout all the possible paths in the graph from $i$ to $j$. The matrix $d_{ij}$ is therefore calculated by using the information contained both in matrix $a_{ij}$ and in

![Fig. 4. Edge betweennesses of this network](image)
We have \( d_{ij} \geq l_{ij}, \forall i,j \), the equality being valid when there is an edge between \( i \) and \( j \). Let us now suppose that the system is parallel, i.e., every node sends information concurrently along the network, through its edges. The efficiency \( e_{ij} \) in the communication between nodes \( i \) and \( j \) can then be defined to be inversely proportional to the shortest distance: \( e_{ij} = 1/d_{ij}, \forall i,j \). When there is no path in the graph between \( i \) and \( j \), \( d_{ij} = \infty \) and, consistently, \( e_{ij} = 0 \). The average efficiency of \( G \) [20] can be defined as

\[
E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} e_{ij} = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}
\]  

and is used as a measure of the performance of \( G \).

As mentioned above, for a given network, suppose that at each time step one unit of the relevant quantity, which can be information, energy, etc., is exchanged between every pair of nodes and transmitted along the shortest path connecting them. The load at a node is then the total number of shortest paths passing through the node that is the node betweenness (\( B_W \)) [17]. The capacity of a node is the maximum load that the node can handle. In man-made networks, the capacity is severely limited by cost. Thus, it is natural to assume that the capacity \( C_j \) of node \( j \) is proportional to its initial load \( L_j \)

\[
C_j = \alpha L_j, \quad j = 1,2,\cdots,N
\]

where the constant \( \alpha \geq 1 \) is the tolerance parameter, and \( N \) is the initial number of nodes. Where \( \alpha \gg 1 \) is the tolerance parameter, and \( N \) is the initial number of nodes. \( \alpha \) can be thought of as a measure of the stress that the network is under at time \( t = 0 \). \( \alpha = 1 \) means that network is operating at maximum capacity. \( \alpha \gg 1 \) depicting a network carrying a light load. But, the removal of nodes in general changes the distribution of shortest paths. The load at a particular node can then change. If it increases and becomes larger than the capacity, the corresponding nodes fail. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur. This step-by-step process is what we call a cascading failure, or a cascade. It can stop after a few steps but it can also propagate and shutdown a considerable fraction of the whole network. If a node has a relatively small load, its removal will not cause major changes in the balance of loads, and subsequent overload failures are unlikely to occur. However, when the load at the node is relatively large, its removal is likely to affect significantly loads at other nodes and possibly starts a sequence of overload failures. According to [17]: global cascades occur if (1) the network exhibits a highly heterogeneous distribution of loads; (2) the removed node is among those with higher load. Otherwise, cascades are not expected. The distribution of loads is in turn highly correlated with the distribution of edges: networks with heterogeneous distribution of edges are expected to be heterogeneous with respect to load so that on average, nodes with larger number of edges will have higher load.

When a node in the system network fails, it will gradually spread to other nodes. In the propagation process, the fault or failure will diffuse through those edges which have the larger propagation probability.

The core idea of this model introduced in this paper is when one node is attacked by random/premeditated attack or environmental disturbances:

1) Node fails, and its load spreads to its neighbors,
2) All downstream nodes share the spread load, the proportion of shared load is decided by the propagation intensity of edges which connected with the failed node and its downstream nodes,
3) Any downstream node fails and spreads to its connected nodes till its capacity is less than its total load, on the contrary, the node is safe.

Explanation to the core idea of this paper:

1) Node fails: failure of node has two types, one is by attack or vanish abnormally of the network, the other is node’s load higher than its capacity, and the capacity of one failed node is0
In order to describe the propagation intensity of edge, in this paper we define the intensity as

$$I_y = w_s(w_p \cdot P^k_y + w_d \cdot d^k_j / \sum d^k_j)$$

(9)

Where $w_s$ is cross-clustering coefficient (related with structure of the network, $w_s \in [0, 1]$). $w_p$ is weighted coefficient of propagation probability. $w_d$ is weighted coefficient of node degree. And $w_p + w_d = 1$. $P^k_y$ represents the one propagation wave probability from node $i$ to node $j$. $d^k_j$ is node degree of $j$, and $k$ is propagation step.

According to the introduced cascading failure model and the explanation, the algorithm procedure is shown in Fig. 5.
4. Simulations and analysis

4.1. Safety-Critical Components

First, Fig. 6 shows the efficiency of the network after cascading failure triggered by the removal of one node of all 23 nodes respectively. While the efficiency is significantly reduced in the case of some node (e.g. the node 9, 10), which means the damage caused by a certain node is large, even can destructive the whole aircraft engine system network. This result is in agreement with intuition, because not all of a small failure can lead to a cascading failure in the network, while some failure which maybe often neglected will cause a cascading and bring a huge damage.

According to the definition of load of a node, we can find that the betweenness of a node is the initial load of each node shown in Fig. 3. Obviously, the network exhibits a highly heterogeneous distribution of loads, that is, some nodes have a high load while the others have a relatively low load. The Fig. 3 also indicates that the damage caused by triggers of higher load (e.g. the node 9 and 10, which FADEC and HMU respectively in the system) is much larger than that by triggers of low load, as can be seen from a comparison between Fig. 3 and Fig. 6. In order to understand this result, consider the topological properties of the network. The network has a heterogeneous distribution of node degree distribution (see Fig. 2; the distribution of loads is highly correlated with the distribution of edges, so that on aver-age, nodes with larger number of edges will have higher load. If the node has large load, its removal is likely to affect significantly the load at other nodes and possibly starts a sequence of overload failures. However, when the load at the node is small, its removal will not cause major changes in the balance of loads and possibly cause a small failure. That is to say that the FADEC and HMU are the safety-critical components in this topological network.

4.2. Failure Propagation Procedure Analysis

According to the model of propagation path, we can get the probable failure node when one node fails which shown in Table 2. Fig. 7 show the intentional attacking with nodes by nodes (the purple node is the attacked node, and the orange nodes are the propagated nodes), and the result of attacking nodes 15 to 22 is same like the (o) shows. And according to the Dijkstra algorithm, the most possible propagation path
(5 → 6 → 2 → 3 → 19 → 9 → 10 or 5 → 6 → 2 → 3 → 20 → 9 → 10) is shown in (p). That is to say, when FADEC fails, it will cause a fault of HPC, for example, compressor surge that is not allowed. This finding has important practical application in safety analysis in aircraft engine control system; we can identify some crucial components and take a perfect protection to ensure the whole system performance. In addition, it can provide guidance in designing more attack-robust system.

Table 2. Probable failure node

<table>
<thead>
<tr>
<th>Initial Node</th>
<th>Probable Failure Node</th>
<th>Initial Node</th>
<th>Probable Failure Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2, 21, 22</td>
<td>12</td>
<td>3, 19, 20</td>
</tr>
<tr>
<td>2</td>
<td>3, 19, 20, 22</td>
<td>13</td>
<td>2, 3, 22</td>
</tr>
<tr>
<td>3</td>
<td>4, 9, 19, 20</td>
<td>14</td>
<td>3, 5, 6, 15</td>
</tr>
<tr>
<td>4</td>
<td>3, 5, 6, 15</td>
<td>15</td>
<td>9, 10</td>
</tr>
<tr>
<td>5</td>
<td>3, 4, 6, 19, 20</td>
<td>16</td>
<td>9, 10</td>
</tr>
<tr>
<td>6</td>
<td>1, 2, 7, 16, 18</td>
<td>17</td>
<td>9, 10</td>
</tr>
<tr>
<td>7</td>
<td>Null</td>
<td>18</td>
<td>9, 10</td>
</tr>
<tr>
<td>8</td>
<td>9, 10</td>
<td>19</td>
<td>9, 10</td>
</tr>
<tr>
<td>9</td>
<td>10, 14</td>
<td>20</td>
<td>9, 10</td>
</tr>
<tr>
<td>10</td>
<td>11, 12, 13, 14, 5</td>
<td>21</td>
<td>9, 10</td>
</tr>
<tr>
<td>11</td>
<td>9, 17</td>
<td>22</td>
<td>9, 10</td>
</tr>
</tbody>
</table>
Fig. 7. Typical failure mode

Selecting node 1 is a failure node, and the downstream node is node 2, so the load of node 1 is transferred into node 2. While the capacity of node 2 is less than its load, and the node 2 is failed. Consequently, downstream nodes of node 2 are node 3 and node 22, the load of node 2 is propagated proportionally into node 3 and node 22, and the two capacities of node 22 and 3 are less than their loads
respectively, so the cascading failure is still going on. The downstream node of node 22 is node 9, and the
capacity of node 9 is higher than its load, so the node 9 is in safety state. However, the downstream of
node 3 is node 20 and node 19, but their capacities are less than their loads respectively, so the cascading
failure is still occurred. Then the downstream node of node 20 and node 19 is the same node 9. Because
of the larger capacity of node 9, so the cascading failure is stop, and the cascading failure propagation is
shown in Fig. 8.

Fig. 8. Typical failure mode
Conclusions

In this paper, we introduce a new method for safety analysis and assessment based on recent advances in complex networks. First, we construct the networks and study the topological properties. The model is based on a dynamical redistribution of the flow triggered by the initial breakdown of a component of the system. The results show that the breakdown of a single node is sufficient to affect the efficiency of a network up to the collapse of the entire system if the node is among the ones with the largest load. This is particularly important for networks with a highly heterogeneous distribution of node loads. The results verify that this method can effectively find the weak point in the system. Therefore, we can identify the components of a system network that are crucial to the functioning of the system, which can be used for protection and design a safe of complex system.

Acknowledgements

This work was supported by National Natural Science Foundation of China (61104146) and Innovation Plan of Aero Engine Complex System Safety by the Ministry of Education Chang Jiang Scholars of China (IRT0905).

References


