CAUSES AND EFFECTS OF CASCADING FAILURES IN AIRCRAFT SYSTEMS

Zdzisław H. KLIM[*], Paweł SZCZEPAŃSKI[**], Marek BAŁAZIŃSKI[***]
[*] Bombardier Aerospace, CA, 400 chemin de la Cote-Vertu Ouest,
Montréal, (Québec) H4S 1Y9, Canada, zdzislaw.klim@aero.bombardier.com
[**] Military University of Technology, Gen. S. Kaliskiego 2 St.,
00-908 Warsaw 49, Poland, pawel.szczepanski@wat.edu.pl
[***] École Polytechnique of Montréal, C.P.6079 - succ. « Centre-ville »,
Montréal, (Québec) H3C 3A7, Canada, marek.balazinski@polymtl.ca

Summary

A cascading failure is a particular type of common-mode failure in which a single event, not necessarily hazardous in itself, can precipitate a series of other failures. The basic characteristic of a cascading failure is the propagation of an initial failure effect throughout the entire system or across and between the different systems. A domino effect is a principal characteristic of cascading failures when an initial event, which has little or no adverse effect on the aircraft, is transmitted downstream and ones of the subsequent failures generates hazardous effects. Cascading failures are considered "low-probability high-consequence events". The prediction and analysis of cascading failures are complex due to their random dynamic involving continuous and switching operations that suddenly change the system's configuration. There are two methods that may be used for the purpose of this analysis: Event Tree Analysis (ETA) and Cause-Mode-Effect Analysis (CMEA).

Keywords*:* safety analysis, cascading failures, risk assessment, reliability, aircraft.

PRZYCZYNY I SKUTKI NIEZDATNOŚCI KASKADOWYCH W SYSTEMACH SAMOLOTU

Streszczenie

Niezdatność kaskadowa jest inicjowana przez pojedyncze (niekoniecznie niebezpieczne) zdarzenie, po którym następują inne – tym razem już niebezpieczne w skutkach – zdarzenia. Cechą charakterystyczną niezdatności kaskadowej jest jej propagacja z miejsca jej powstania na bliższe, a następnie na - dalsze i coraz to dalsze otoczenie. Efekt domina jest jej główną właściwością, gdzie skutek jakiegoś niepozornego zdarzenia przekłada się, dajmy na to, na katastrofę lotniczą, kalectwo lub utratę życia czy też jakiś kataklizm ekologiczny. Niezdatność kaskadową postrzega się z jednej strony jako mało prawdopodobną, z drugiej zaś – jako bardzo dotkliwą w swych konsekwencjach. Przewidywanie tych niezdatności jest niezwykle utrudnione z racji ich znacznej przypadkowości, dynamiki i zmian strukturalnych systemu. Analizę niezdatności kaskadowych przedstawiono z wykorzystaniem dwóch metod: Analizy Drzewa Niezdatności (ETA) oraz Analizy Przyczyn i Skutków (CMEA).

Słowa kluczowe: bezpieczeństwo, niezdatności kaskadowe, szacowanie ryzyka, niezawodność, samolot.

1. INTRODUCTION

Some form of "fail-safe" design concept usually achieves the high levels of safety needed from essential aircraft systems, mainly through redundancy and isolation of systems, components and elements. However, this approach can be ineffective due to the possibility of common mode failure or cascading failures that may lead the aircraft into a hazardous situation with an unacceptable probability level.

Of particular concern when assessing failure conditions are cascading failures. A cascading failure is a propagation of equipment outages, one propagating another [1]. A cascading failure is a particular type of common-mode failure in which a single event, not necessarily hazardous in itself, can precipitate a series of other failures. A cascading failure is not a single point failure or the occurrence of multiple concurrent failures but it is an event in which a component failure in the system/network will induce the failure of other components through normal system dynamics or behavior.

A cascading failure scenario is one in which an initial failure leads to subsequent failures or increases the likelihood of subsequent failures due to direct effects, such as a failed part striking or burning another system element; or due to indirect effects, such as the initial failure increasing the loading on other system elements. Cascading failures are considered "low-probability high-consequence events" [2].

In multi-channel systems the channels usually share the total system loads, so that in the event of a failure of one channel, its load or part of it, will be shared between the remaining "healthy" channels. This increase in load is likely to produce some increase in the failure rate of the remaining channels. This situation applies to electrical or hydraulic systems, data transfer network or mechanical systems, such as, for example, a flight control system in which two or three actuators share the total load. An increased failure rate of multi-channel systems resulting from additional loading can have a marked effect on the risk of combined failures [3]. The subsequent failure due to an increasing load could be instantaneous or may be delayed by some varying time period. Cascading studies can also be conducted to analyze vulnerability of the system to acts of sabotage [4], [5].

The "classic" cascading failure is characterized by a rapid propagation of failures. However, the cause-effect chain of events, leading ultimately to a hazardous situation, has to be considered, even if the failure propagation is spread over a large period of operation [6]. Moreover, the triggering event may be a permanent or a temporary fault. Therefore, an important attribute of a cascading failure that requires consideration in the analysis is the time factor.

A cascading failure is a progression and generation of equipment outages, one precipitating another. The basic characteristic of a cascading failure is the propagation of an initial failure effect throughout the entire system or across and between the different systems. A domino effect is a principal characteristic of cascading failures when an initial event, which has little or no adverse effect on the aircraft, is transmitted downstream and ones of the subsequent failures generates hazardous effects.

Given the kinds of large, interconnected applications that are increasingly deployed in modern, highly complex aircraft systems; the developers should consider the impact of cascading failures and mitigating strategies to address them. The systems that are exposed to cascading failures may have shared resources and/or shared messages, latencies or complex system human-machine interactions. The cascading failures can accelerate out of control, confounding human operators and denying them a chance for recovery. They may also neutralize redundancies, bypass firewalls or designed load paths, and exploit chance circumstances for which no designer could reasonably plan [7].

It is clear that these chains of contingencies are dependent on each other. In addition, several of them may cascade simultaneously. Consequently, the probability of these cascading failures occurring is much higher than the probability of a random (i.e. independent) tripping of k out of N components of the system.

In considering likely failure sequences, one has to take account of the fact that following a series of failures the flight crew will be under increased stress and may be more likely to make mistakes. Therefore, the crew may contribute to cascading failure propagation by inserting an additional failure.

2. NATURE OF CASCADING FAILURES

2.1. Failure Identification

The prediction of rare events, which are likely to produce cascading failures, is by definition, bound to be very difficult unless previous experience points out the way. However, there are various precautions and techniques, which can considerably reduce the chances of such multiple failures.

The functional segregation of services and the physical separation of the components within the specific aircraft zone may prevent failure propagation or considerably decrease the probability of a cascading failure scenario. The containment of fragments of high-energy devices installed on aircraft in case of a failure and truly redundant (dissimilar) architecture of the system may preclude an initiating of the cascading failure chain. All these precautions and techniques, when correctly applied, result in the development of an in-depth defense strategy at the system and aircraft level against cascading failures. The defense strategy introduces several levels of protection, from a design and operations perspective, in order to preclude the domino effect of cascading failures before it reaches a safety critical point. The approach of minimizing the propagation of failure after the cascade has started is complementary to the usual approach of minimizing the risk of the first few cascading failures [8].

2.2. Characteristic of cascading failures

The nature of cascading failures may vary considerably and it is difficult to provide a common definition or characteristic of such an event that would apply to all possible scenarios. The following list of failure events presents various manifestations generated by cascading failures and highlights the insidiousness of this type of failure.

1. The ejection in flight of the cargo door resulted in the sudden depressurization, which subsequently led to the disruption of the floor structure causing a few passengers and parts of the aircraft to be ejected, rendering one engine inoperative and impairing the flight controls (tails surfaces) so that it would be impossible for the crew to regain control of the aircraft. This sequence of events finally leads to a catastrophe.

   First failure: ejection of cargo door due to incorrect door latching

   Cascading: between different systems

2. One tire blew out/failed during take-off following by a second tire blew-out. Subsequently, the wheels and brakes assemblies started rubbing the runway surface generating excessive heat. Crew decided for rejected take-off and was using the remaining brakes to stop

the aircraft. This action generated additional heat which coupled with the one created by failed tires originates a fire in the body gear wheels. Due to the initial delay in shutting down engines, which hampered the effective fire fighting, and coupled with a certain lack of coordination and proper deployment of the fire fighting equipment, the fire, originally confined to the body gear, grew into a conflagration and ultimately destroyed the aircraft.

First failure: tire blew-out during take-off
Cascading: between different systems

3. The failure of a joining sections of an air supply duct, causing leakage of hot air which in turn caused multiple failures of essential electrical circuits.

   First failure: fracture of air supply duct
   Cascading: between different systems

4. The loss of cooling provisions for avionic systems will increase the temperature and failure rate of the equipment ultimately leading to a series of cascading failures.

   First failure: loss of cooling
   Cascading: between different systems

   It is also possible to observe a combination of different types of failure scenarios, for instance, an external event like rotor burst may strike many different components simultaneously and initiate cascading failure scenarios on various systems.

It may be concluded, based on the above discussion, that potential cascading failures should be analyzed in conjunction with a Common Cause Analysis, which includes zonal, particular risk, and common mode analyses, and should be considered as an essential and complementary part of the complete safety assessment at the system and aircraft level [9].

3. PREDICTION AND ANALYSIS OF CASCADING FAILURES

3.1. Issue Description

Predicting the evolution and effects of cascading failures has proven difficult. Some of the reasons for this difficulty are as follows. First, cascading failures are a hybrid phenomena due to their random dynamic involving continuous and switching operations (i.e. a discrete event that suddenly changes the system's configuration). Second, the evolution of any cascading failure depends on the initial condition of the system, and there are many possibilities for these conditions. Third, there are uncertainties in the system response when the initiating event occurs and in the availability of the protective devices. Fourth, the impact of latent failures and the intervention of human operators can completely change the course of cascading failures. Therefore, the assessment methodology for cascading failures should include an adequate model of system behavior and sequences of cascading steps. This model should be able to evaluate all alternative cascading scenarios with the same initiating event. There are two methods that may be used for the purpose of this analysis: Event Tree Analysis (ETA) and Cause-Mode-Effect Analysis (CMEA).

3.2. Event Tree Analysis (ETA)

An event tree is a visual representation of all events, which can occur in a system. Event trees can be used to analyze systems in which all components are continuously operating or for systems in which some of the components are in a standby mode or in a latent failed state. The starting point, referred to as the initiating event, disrupts normal system operation. The event tree displays the sequence of events involving success and/or failure of the system components. An event tree may be quantified by using the event probabilities from a Failure Modes and Effects Analysis (FMEA) or Fault Tree Analysis (FTA). The hazard probability for each chain of events is then easily computed.

In the case of safety-oriented systems, the event tree is used to identify various possible outcomes of the system following a given initiating event, which are an unsatisfactory event (component failure) or situation (external event). By analyzing all possible outcomes it is possible to determine those of them, which are leading to an undesirable hazard at the system or aircraft level.

The purpose of an event tree analysis (ETA) is to identify the sequence of events that follows a given failure or error since it could lead to a loss of the system's intended function. An event tree is a graphical illustration of potential outcomes that can result from a specific equipment failure or human error. Event tree analysis considers the response of personnel and safety systems in dealing with the failure. The results of an event tree analysis are "accident sequences" or "failure sequences" – a multi branched, chronological set of failures or errors that define an accident or system failure. ETA is very useful in analyzing the effect of safety systems or emergency procedures on accident prevention and mitigation. It produces useful information when used in parallel with FTA and FMEA.

A key distinction between FTA and ETA is that, in the latter, an initiating event is assumed to have occurred, whereas in FTA the failed state is an event for which the probability of occurrence is determined. The initiating event may be the result of a particular system failure, or it may be caused by some external circumstance such as a lightning or bird strike.

ETA can be used during the development and design phase of the system. It is particularly useful as a tool for demonstrating the efficiency of accident prevention and mitigation techniques. Therefore, the ETA is primarily used for safety analysis and could be very helpful in assessing cascading failures.

3.2.1. Event Tree Analysis Procedure

An ETA consists of the following steps:

1. Identifying an initiating event

The initiating event may be a system failure, equipment failure, human error, external event, or operation process upset that could have any one of several effects. Actual effects, or results realized, depend on how the system or operator responds to the event.

2. Identifying the response

Identifying which system or operator response is anticipated in reaction to the initiating event. This response can include action by subsystems, such as an automatic emergency shutdown triggered by the event, alarms to alert operators, operator actions taken in response to alarms, or even physical barriers to limit the effects of the initiating event. It is important to identify and to list these functions in chronological order of the designed response. For example, possible responses to "fuel level in a tank is too high and is increasing" might be; high-level indication or warning and crew action to close inlet valve. If other systems are affected by the initiating event, they should also be listed.

3. Constructing the event tree

First, the initiating event must be clearly defined and put on the left-hand side of the page (see below). Then, a chronological list of the functional responses must be defined and located across the top of the page. Next, it is necessary to define whether or not the success-failure of the function could affect the course of the events. If the answer is "yes", the event tree is branched to distinguish between success and failure of the function; success branches upward, failure downward. If the system function has no effect, the tree does not branch, but proceeds to the next system function (to the right).

4. Describing the event sequence

The event sequences are a variety of outcomes that could occur following the initiating event. Some of the sequences may represent success (e.g. a return to normal state or an orderly shutdown). Sequences that result in failure should be studied with the objective of improving the responses to the event in order to minimize the probability of failure or severity of the effects.

3.2.2. Event Tree Analysis Examples

Example 1

The residential gas-fireplace is held primarily in standby. Anticipating a potential gas leak, a cascading failure scenario, using the event tree method, is assessed as follows (fig. 1).

Example 2

The residential gas-fireplace is held primarily in standby. The installation is equipped with an automatic gas leakage detection and shutdown device. Anticipating a potential gas leak, a cascading failure scenario, using the event tree method, is assessed as follows (fig. 2).

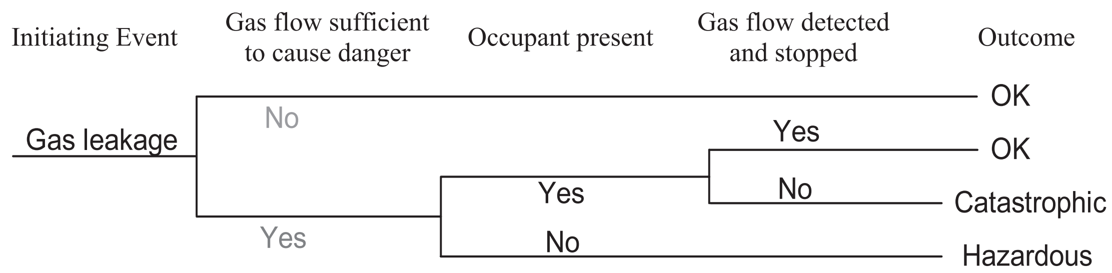

Fig. 1. Event tree analysis – example 1

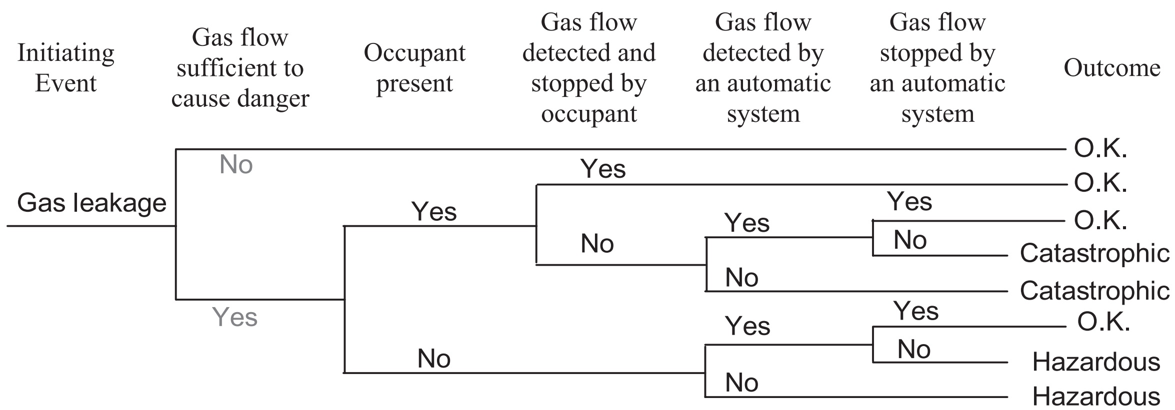

Fig. 2. Event tree analysis – example 2

3.2.3. Event Tree Flexibility

In an event tree there is considerable latitude in the definition of the event headings; functions, systems, and components can be shown on the same tree. Moreover, it is easy to combine multiple systems on the same tree if the initiating event can impact more than one system. These various event possibilities are listed as headings that represent the functions or systems required to mitigate an event's consequences.

The end result of each sequence is assumed to be either a successful, or safe, termination of the postulated sequence of events or a system failure state. In developing event trees for specific systems, care must be taken to correctly specify the expected system failure state. Care must also be exercised to ensure that the event headings are consistent with actual system response modes and are precisely related to system success criteria that can be translated to top events for system modeling.

The events are placed across the tree either according to the sequence of their occurrence (proceeding from left to right) or some other logical order reflecting operational interdependence. Consequently, the initiating event is always shown first and the total system outcome response is always shown last. The paths of vertical and horizontal lines below the event headings represent the various sequences. At a horizontal-vertical line junction, the system is successful if the path is upward; the system fails if the path is downward. A column at the far right of the tree identifies the various outcome events resulting from the path sequences.

This information is then used to determine the severity of the event sequence outcome and the level of attention that each component receives. In those areas where the system's state reveals the potential for unacceptable consequences, the qualitative tree analysis may be completed by quantification of the probability of success or failure at each junction. Then, the probability of the various system states can be estimated.

3.3. Cause – Mode – Effect – Analysis (CMEA)

Cascading failures can be also analyzed by the Cause-Mode-Effect method built for this purpose and considered as a complementary safety assessment procedure to the basic techniques used for aircraft safety assessment, such as, Failure Modes and Effects Analysis, Fault Tree Analysis, Zonal Safety Analysis, Particular Risk Analysis and Common Mode Analysis.

The Cause-Mode-Effect-Analysis (CMEA) is based on the "What if" method, the one most commonly used, as a concept, in developing a Failure Modes and Effects Analysis (FMEA) or a Hazard and Operability Study (HAZOP) procedures of the failure analysis.

The CMEA is considered basically a qualitative method; however quantification of the hazard under study may be added by using the related data and numerical methods for the probability calculation.

The Cause-Mode-Effect-Analysis represents a complete review of the potential chain of events (cascading failures), by assessing at each step of the analysis, the relationship between root cause, failure mode or degradation mechanism and resulting effect from the safety perspective. This analysis starts with a clear definition / description of the initiating event which may be a system component failure, external event or human error. The CMEA displays the sequence of the subsequent events based on the deductive / inductive analysis of the cause-mode-effect relationship. The analysis process is continued up to the ending failure mode called the final outcome and the effect of the outcome hazard at the aircraft level is the subject of the safety assessment.

3.3.1. Cause – Mode – Effect Concept

The relativism of the cause-mode-effect notion has to be clearly understood. These three elements could very easily lead to confusion. The basic definitions are as follows:

Cause – initiating event (failure, external event, human error),

Mode – type / nature of failure manifestation,

Effect – failure consequence on the user or operation from a safety perspective.

However, depending on the system breakdown for the purpose of the failure analysis, an effect may become the mode or be considered as the cause. This "floating" character of the failure attribute is widely explored by the Cause-Mode-Effect procedure. The initiating event may be described in terms of failure cause or failure mode and the first conclusion has to establish the effect of this event. Afterwards, this effect is considered as the next cause leading to the following effect. This procedure is continued up to the final outcome effect description and the assessment of its severity.

3.3.2. Propagation Prevention In-Depth Analysis

At each step of the analysis an additional question is asked about the available protection or mitigation, which would be able to stop the cascading failure propagation. This assessment is related to the inherent design characteristic of the system being able to preclude the propagation of a cascading failures chain.

The qualitative analysis should identify the level of hazard based on the outcome severity and the likelihood of occurrence despite the additional protection or mitigating measures. Should there be doubts regarding the effectiveness of the additional protection or mitigating measures intended to preclude a cascading failure, the analysis may be enhanced through the addition of a quantitative analysis (i.e. assigning probabilities to each event).

3.3.3. Cause – Mode – Effect Analysis Examples

The following examples are an application of the CMEA procedure on actual cascading failure scenarios. The CMEA is performed on a cargo door failure and tire burst both considered as initiating events in respective cascading failure scenarios.

Example 1– Cargo Door

The ejection in flight of the cargo door resulted in the sudden depressurization, which subsequently led to the disruption of the floor structure causing a few passengers and parts of the aircraft to be ejected, rendering one engine inoperative and impairing the flight controls (tails surfaces) so that it would be impossible for the crew to regain control of the aircraft. This sequence of events finally leads to a catastrophe (tab. 1).

Example 2 – Tire Burst

One tire blew-out / failed during take-off followed by a second tire burst. Subsequently, the wheel and brake assemblies started rubbing the runway surface generating excessive heat. The crew decided to perform a rejected take-off and was using the remaining brakes to stop the aircraft. This action generated the additional heat which coupled with the one created by failed tires originated a fire in the body gear wheels. Due to the initial delay in shutting down engines, which hampered the effective fire fighting, and coupled with a certain lack of coordination and proper deployment of the fire fighting equipment, the fire, originally confined to the body gear, grew into a conflagration and ultimately destroyed the aircraft (tab. 2).

3.4. Documentation of the CMEA

The results from the Cause-Mode-Effect Analysis are presented in a tabulated format. For each initiating event there is a separate table. The first column provides the initiating event description. The subsequent columns present the evolution of the cascading scenario propagation and include all related information. It is easy, performing the analysis, to consider a next level failure within the same system or interconnected systems as well as human errors or an external event. The final column describes the outcome from cascading failures and includes an assessment of the final effect's severity. The separate row on the bottom table is used to summarize the designed protection or mitigation against failure propagation. The probability computation, if necessary, is provided in an adequate format (formula, Fault Tree, etc.).

The conclusion of the cascading failure analysis should discuss the final effect and severity, the available protection or mitigating measures and the probability of final outcome, if applicable.

Table 1. Cause – Mode – Effect Analysis: - Example 1– Cargo Door

Initiating Event	First Immediate Effect	Mode/Effect Cause/Action	Mode/Effect Cause/Action	Mode/Effect Cause/Action	Mode/Effect Cause/Action	Outcome and Severity
Cargo door ejection in flight	Sudden depressurization	Disruption of the floor structure	Passengers ejected			
			Parts of the aircraft ejected	Damage to the flight control surface on the tail	Loss of aircraft control	Loss of aircraft
				Engine inoperative due to parts ingestion		Catastrophic

POTENTIAL PROTECTION / MITIGATION					
Design features	NONE	Design modification	NONE	NONE	NONE
Crew procedures					

Table 2. Cause – Mode – Effect Analysis: - Example 2–Tire Burst

<table>
<tr><th rowspan="2">Initiating Event</th><th rowspan="2">First Immediate Effect</th><th>Mode/Effect</th><th>Mode/Effect</th><th>Mode/Effect</th><th>Mode/Effect</th><th rowspan="2">Outcome and Severity</th></tr>
<tr><th>Cause/Action</th><th>Cause/Action</th><th>Cause/Action</th><th>Cause/Action</th></tr>
<tr><td>Tire blew out during take-off</td><td>Second tire blew out due to increased load</td><td>Wheels and brakes started rubbing the runway</td><td>Excessive heat generated</td><td rowspan="2">Originated fire</td><td rowspan="2"></td><td></td></tr>
<tr><td></td><td></td><td>Pilot using brakes on the remaining wheels</td><td>Overloading brakes generate excessive heat</td><td>Loss of aircraft</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">Delay in shutting down the engines</td><td>Hampered the effective fire fighting</td><td rowspan="2">Catastrophic</td></tr>
<tr><td>Lack of coordination and proper deployment of fire fighting equipment</td></tr>
</table>

POTENTIAL PROTECTION / MITIGATION					
NONE	NONE	NONE	NONE	Review emergency procedure for engine shut down	Review training and deployment procedures for fire fighting department

4. CONCLUSION

All analyses related to cascading failures start with an initiating event. This event may be selected from the FMEA/FTA for each catastrophic failure scenario. Some supplementary initiating events may be generated through a Common Cause Analysis, primarily through a Zonal Safety Analysis or a Particular Risk Analysis.

Analyses related to cascading failures may be qualitative or quantitative. To show compliance to the regulatory requirements it is considered that the typically, a qualitative analysis is sufficient to demonstrate compliance, if this analysis shows that the adequate protection or mitigating measures are implemented in order to preclude the failure propagation and to protect the aircraft against a catastrophe.

In some cases, appropriate protection or mitigation may not preclude the hazard. In such cases, a probability computation of the cascading failure scenario should be performed. This probability, which has to be related to the final effect outcome, must be shown against this outcome's criticality. In order to demonstrate compliance, the level of hazard should be less critical than the level prescribed by the regulatory requirements.

REFERENCES

[1] Hines P., Huaiwei L., Dong J., Talukdar S., "*Autonomous Agents and Cooperation for the Control of Cascading Failures in Electric Grids*", Proceedings of the IEEE Conference on Networking, Sensing, and Control, Tucson, USA, March, 2005.

[2] Hardiman R. C., Kumbale M., Makarov Y. V., "Multi-Scenario Cascading Failure Analysis Using TRELSS", CIGRE/IEEE PES International Symposium on Quality and Security of Electric Power Delivery Systems, Montreal, Quebec, Canada, October, 2003

[3] Klim Z. H., Balazinski M., "Risk Assessment for Continuing Airworthiness", 6e Congrès international de genie industriel, Besançon, France, juin, 2005.

[4] Makarov Y. V., Hardiman R. C., "*Risk, Reliability, Cascading and Restructuring*", Proceedings of the IEEE PES Annual Meeting, Toronto, Ontario, Canada, July, 2003.

[5] Motter A. E., Lai Y-Ch., "*Cascade-Based Attacks on Complex Networks*", Physical Review, E66, 0651021R, 2002.

[6] Talukdar S., Dong J., Hines P., Krogh B., "*Distributed Model Predictive Control for the Mitigation of Cascading Failures*", Proceedings of the 44th IEEE Conference on Decision and Control, Seville, Spain, December, 2005.

[7] Klim Z. H., "*Preliminary Hazard Analysis for the Design Alternatives Based on Fuzzy Methodology*", Nord American Fuzzy Information Processing Society, NAFIPS, 2004 – Fuzzy Sets, 23rd International Conference of NAFIPS, Banff, Alberta, Canada, June, 2004.

[8] Dobson I., Carreras B. A., Newman D. E., "*A branching process approximation to cascading load-dependent system failure*", 37th Hawaii International Conference on System Sciences, Hawaii, January, 2004.

[9] ARP 4761 – *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, Society of Automotive Engineers, 1996.

Dr **Zdzisław KLIM** is a Senior Engineer Specialist at Bombardier Aerospace Reliability, Maintainability and Safety Department. His responsibilities include reliability and safety analysis for in service aircraft systems, technical support for new programs and developing the new methods for reliability and safety assessment. He currently teaches reliability to graduate students in the Department of Mechanical Engineering of the Ecole Polytechnique of Montreal. His research interests are in the fields of systems reliability and maintainability analysis, and safety and risk assessment. Mr. Klim holds bachelor and master degrees in mechanical engineering and a Ph.D. in reliability from Technical University of Wroclaw, Poland. He previously was an associate professor of mechanical engineering at Technical University of Wroclaw, Poland, and University of Sciences and Technologies of Oran, Algeria. He has more than 30 years of experience in the field of reliability, maintainability and safety analysis. He is the author of more than 50 technical papers and technical reports. He is a member of the Society of Automotive Engineers (SAE), Association of Professional Engineers of Quebec (O.I.Q.) and president of the Montreal Chapter of Society of the Reliability Engineers (SRE).

Dr **Paweł SZCZEPAŃSKI** is a specialist in the area of diagnostic of technical systems. He obtained his bachelor and master degrees in engineering from the Military University of Technology, J. Dąbrowski in Warsaw. He holds a doctoral degree (Ph.D.) from the same University based on his thesis presented in 1990 on the "Diagnostic of complex technical systems with multiple failures". Dr Szczepański is currently an assistant professor at the Institute of Mechatronic Systems of the Military University of Technology. He is the author of more than 50 research papers as well as two manuals. He is a member of the PTDT and PNTTE.

Dr **Marek BAŁAZIŃSKI** is a specialist in the area of manufacturing, fuzzy logic and genetic algorithms. He has obtained his bachelor, master and doctoral degrees from the Technical University of Cracow in Poland. Over the last several years, he has focused on metal cutting of hard and difficult to machine materials and on application of fuzzy logic and genetic algorithms in manufacturing.

Dr Bałaziński is currently professor and head of the Manufacturing Section in the Department of Mechanical Engineering at École Polytechnique of Montréal. Over the last ten years, he has published over 100 research papers and he is an active member of CIRP (The International Academy for Production Engineering).