Flight Safety Margin Theory - A Theory for the Engineering Analysis of Flight Safety

Hung-Sying Jing(✉), Chia-Sheng Sheng, and Yu-Feng Lin

Institute of Civil Aviation, National Cheng Kung University,
Taiwan, People's Republic of China
hsjing@mail.ncku.edu.tw

Abstract. Flight Safety Margin, based on the situation of flight and from an operation point of view, provides a new tool whereby flight safety can be analyzed numerically. The flight operation is viewed moving on a virtual terrain in the abstract situation space. Any normal real flight will thus be delineated by a time-varying continuous curve around the centerline defined by the standard flight condition. The flight safety margin describing how far the present flight situation is from the accident boundary is de-fined as the inverse of the needed performance of the crew to recover the present situation back to the standard condition and scaled from zero to one. A questionnaire is designed to measure the perceived needed performance. With the chosen situation parameters as the inputs, the surveyed results are then converted to the flight safety margin, representing the outputs of the training examples. The expert sys-tem using neural network can thus provide the quantitative flight safety margin given situation parameters from real flight condition. The present methodology has been tested with the FOQA data from final approach in real cases including the Nagoya and Da-Yuang accidents. Meaningful results are obtained although there is still much room for improvement.

Keywords: Flight safety margin theory · Flight safety · Engineering analysis

1 Introduction

There are many models or theories used in the aviation community regarding flight safety, such as the domino theory, the accident chain, and the cheese model among others. Domino theory, proposed by Heinrich [1], described the basic characteristics of industrial accidents. According to Heinrich's theory, any accident can be described as the result of a chain of sequential events – like a line of dominos falling over. Based on Heinrich's domino theory, Boeing [2] established the concept of "accident chain" to de-scribe the process of an accident induced by a chain of real events. From this, by removing any link in the chain, it is possible that the accident can be prevented. The other well-known and similar theory is the so-called cheese model [3]. When the hole of each piece of cheese lines up, the light will pass through all the pieces of cheese representing that the process of an accident is complete. There are certainly other theories which will not be discussed here.

D. Harris (Ed.): EPCE 2015, LNAI 9174, pp. 377–387, 2015.
DOI: 10.1007/978-3-319-20373-7_36

There is one basic feature in all of these models which is the sequential-type thinking. Sequence is the key of all these models obviously. It is thought by the authors that the basic reason for the generation of this type of thinking is from the language. Western languages have an alphabet system, every word has to be read and written in an exact certain sequence without any exception [4]. Moreover, the sequential type of thinking is further reinforced by accident investigation [5, 6]. The general procedure of accident investigation is to collect all the evidence and look backward, according to the causal relation, to identify the chain of events. After the first cause is identified, the final sequence of causes is completed and the investigation process is basically finished. Although the sequential type of thinking is generally accepted by the aviation community, what really happens in any real case of aircraft accident may or may not be simply sequential. When we look back through time, it is natural to conclude that the accident is really a chain of events. But, when we look forward following the advancement of time, it is a different picture. Aviation is no doubt a complex system [7], and for any complex system, there are two characteristics; highly complex and tightly coupled. With these two characteristics, the potential for unexpected nonlinear interactions between subsystems to occur will be likely very high. The main reason is from the so-called common-mode function. Common-mode represents dual or even several functions carried by a single device. Consequently, any event caused by any type of error will generally produce not only one outcome, but several despite the likeliness that only one of the outcomes will be found to be located on the final accident chain. Consequently, when we look forward through time as the natural process of any event or accident, we will see something like a tree instead of a chain, i.e., ramification instead of a sequence. A theory other than sequential type is surely needed to include the complex nature of flight operation.

On the other hand, up to the present time, there is no any theory which can provide quantified analysis of the evolution of flight safety. The main difficulty is that the safety is a perception problem, and it will be different from person to person given the same situation. However, if the safety could not be quantized, the corresponding analysis will be restricted in the qualitative realm. In this case, it will be very hard to expose the whole picture of the evolution of any flight event. Consequently, quantification of flight safety really represents the most important step before any major progress can be accomplished. The flight safety margin theory is a preliminary trial designed to overcome this difficulty.

2 The Flight Safety Margin Theory

Flight safety margin theory is a geometrical type theory. The basic motivation is to establish an approach to reveal how safe a given flight is from a geometrical prospect, i.e., how much “distance” is left for an accident to occur [8]. As it is known to everybody, the core concern in flight safety is the human error, therefore it is appropriate to establish a theory of flight safety from the point of view of operators. Basically, safety can, in principle, be interpreted as room for error. Flight safety margin can thus be designed as the room for error or mistake in flight. However, the same error occurring under different situations will induce different degrees of danger. In other

words, finding out how dangerous the error or mistake is, without referring to the situation, is extremely difficult if not impossible. Consequently, the situation has to be defined first before the discussion can proceed.

In the development of the flight safety margin theory, an abstract situation space is defined first, as shown in Fig. 1. All the situations related to flight safety constitute the space representing the set of all possible situations. In this space, any combination of parameters is represented by a point. Any point represents a specific situation of flight. Since there exist constraints from physical laws about any real flight, realistic flights constitute a hypothetical virtual terrain as the subspace. Hence, every flight can be represented as a time-varying continuous curve traversing on the virtual terrain because as time passes, the parameters change continuously. For every flight mission, there exists a set of perfect, standardized situations required by the related regulations. If all the situation parameters work perfectly, the corresponding curve should represent the safest flight, which is defined as the centerline on the terrain in the situation space. There are also certain combinations of the parameters which constitute the situations of an accident. They are represented as the accident boundaries. Any real normal flight is thus a continuous curve wandering around the centerline because the crew will do their best to maintain the aircraft as safe as possible, i.e., adjusting the situation parameters to avoid deviating away from the centerline. At any given instant, the "distance" between the present situations and the accident boundary can be used as a safety measure. This distance implies how far the present situation is from the occurrence of an accident. Hence, the distance is thus defined as the flight safety margin as shown in Fig. 1.

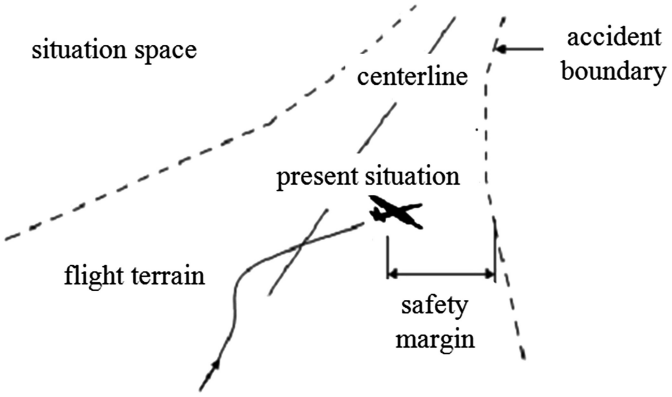

Fig. 1. The abstracted schematic diagram for the concept of flight safety margin

However, it is hard to perceive the "distance" between the flight situation and the accident boundary. Since safety represents, in principle, the room for error, the "distance" to the accident boundary has to be related to the needed effort or performance to neutralize the error and recover the situation back to the centerline. If some error took place, the flight situation will evolve closer to the accident boundary. At this moment, any corrective measure or defensive strategy will try to pull the situation away from the

accident boundary. If the defense can be accomplished easily, it can be said that the situation does not deviate too far from the centerline and the distance to accident boundary is still very large. On the contrary, if the situation is already very close to the accident boundary, the performance needed to recover the situation back will definitely not be minor. Moreover, if the errors have already cumulated to a certain stage which is beyond any possibility for human recovery, the accident is thus unavoidable. The corresponding situation then locates on the accident boundary or even beyond. Concluding the above discussions, the needed performance to recover the present situation back to the most standardized situation could be a feasible tool to delineate the "distance" between the present situation and the accident boundary and can thus be used to define the flight safety margin.

With the basic concept of the flight safety margin, the key is to establish the causal relation between the parameters of the flight situation and the needed performance. The situation can be any set of parameters, those that comprise the safety of the flight. Given these situation parameters, it is not possible at the present stage to create a precise mathematical relation with flight safety since safety is a perception problem. Only pilots know how much effort is needed, e.g., how safe is the situation. To collect the opinion about safety from the pilots to find out the corresponding causal relation, an expert system [9] is needed. In this study a neural network is used to build the system. A neural network is basically a mathematical method with a learning capability. Knowledge with the proper representation, e.g., training examples, can be learned through adjusting the synaptic weights connecting neurons in the network. Thereafter, the knowledge is not presented through a precise mathematical formulation but stored in the connections of the network. The training examples for the computer to learn should incorporate the un-known causal relation about the relevant phenomenon given in the form of input-output.

With a neural network, the restrictions originating from individually different perceptions about safety can be overcome. In principle, the unknown causal relation between situation and needed performance has to be incorporated in the training example, expressed as the input-output form, for the computer to learn. Naturally, a set of flight situation parameters represents an input. The output is designed to be the safety margin of flight from the needed performance through asking the opinion of the pilots. The neural network can be considered as a tool to learn the knowledge, experience and also perception of human experts. If this can be done, the corresponding expert system can thus supply the unknown causal relation between the situation and safety margin. The entire logical foundation of the flight safety margin theory can then be established.

To establish the corresponding expert system, a questionnaire is needed to collect the expertise of the pilots to supply their knowledge about needed performance. Since the needed performance to recover the flight situation back to the most standardized one is used to represent the distance between the flight situation and the accident boundary, and only the pilots understand how much effort they have to de-vote under the given situation, this questionnaire is designed for the pilots to reasonably classify their perception about the needed performance. After interviewing some senior captains, the needed performance is categorized into two main parts: physiology and psychology. The physiological portion is further partitioned into agility and skill. The psychological portion is partitioned into experience and knowledge. In total, there are

four sub-categories in the questionnaire. The key reason for choosing these four sub-categories is by adding the basic instinctive response in addition to the Rasmussen's skill-rule-knowledge classification of human performance [10]. There are also four items in each sub-category to reveal the magnitude of the needed performance. They are low, medium, high, and be-yond. "Beyond", in this questionnaire, represents that the situation has moved beyond human capability to recover from a given situation, i.e., in this case, the given situation is already out of human control. The corresponding questionnaire can be found in Lin's work [11].

The objective of the designed questionnaire is to collect the perceptions of the experts about the severity of any given flight situation. Once this is done, the perceived severity has to be transformed into the safety margin. The more severe the situation is, the closer one moves to the accident boundary. The flight safety margin thus bears an opposite meaning with the severity. Hence, the flight safety margin can be defined as the opposite of the needed performance for recovery, i.e., the perceived severity. In order to be understood easily, the flight safety margin duplicates the definition of probability to be within zero to one as follows: To obtain a number between zero and one, the needed performance for recovery among each sub-category and magnitude has to be adjusted according to the learning results of the corresponding neural network [11]. The smallest needed performance is set at 1 and the largest is set at infinity, which is represented as "beyond" in the questionnaire. By using the designed questionnaire and the definition of flight safety margin, the training examples can be prepared with the given flight situations as inputs and the safety margin as outputs, a number between zero and one representing the percentage of safety. By collecting enough examples from real flight data, the training process can be accomplished without any difficulty. By completing this, for any given flight situation, the neural network will have the capability to supply a quantified safety measure.

For the neural network to learn reasonably, the training examples have to cover a large enough scope regarding safety and the corresponding flight situations. The real normal flight data as well as the most dangerous data have to be in the pool of training examples. One typical safe flight was chosen where ten instances were selected for the preparation of examples of an airplane descending from three thousand feet to landing. On the other hand, for the neural network to have the capability to supply a safety measure regarding the accident boundary, the data from the Da-Yuang case were used to provide the corresponding information. Ten representative instances in the final approach, from three thousand feet to the occurrence of the accident were picked for use in training. Due to the limitation of the flight data, only seventeen situation parameters from the flight recorder were used. They are speed, altitude, pitch angle, vertical g, angle of attack, engine EPR1, engine EPR2, engine RPM1, engine RPM2, bank angle, descent rate, distance to airport, glide slope (dot), localizer(dot), configuration, gear, and autopilot. In total, seventeen parameters in twenty instances together with the corresponding questionnaire constitute the material for the survey. The local pilots asked to complete the survey all have experience in flying the same type of aircraft as in the Da-Yuang case. Unfortunately, there are not many such experts, only twenty two, for us to interview. In total, there are four hundred and forty training examples for the neural network to learn. As for the construction of the neural network, a multilayer network is

used. To incorporate the knowledge from the four sub-categories in the questionnaire, the network used is 17-9-4-1. The learning scheme used in this study is error correction learning with back propagation.

3 Case Studies

Due to the difficulty in obtaining data from real flights, only four different cases were used in this study to validate the proposed theory. They are normal flights, landing in heavy fog, the Nagoya accident, and the Da-Yuang accident.

3.1 Normal Flights

Normal flights represent flights without any FOQA event. None of the situation parameters were over the limit set by the management. There are in total 39 sets of normal flight data in this study. The corresponding safety margins varying with time were plotted in Fig. 2. In this figure, the changing safety mar-gins for the final approach were shown. As it can be seen, starting from 3000 ft above the ground, the situation is quite safe as perceived by the local pilots. The safety margin is around 0.98. As the airplane gradually descends, the margin of safety is compressed accordingly. The process is very smooth. When the airplane is closer to the ground, the corresponding safety margin is lowered more drastically, similar to a parabola. The closer the airplane is to the ground, the quicker the safety margin is compressed. That represents, in the minds of the local pilots, that the variation of the room for error is not linear with respect to the altitude. At touchdown, the average safety margin of 39 flights is 0.531. Clearly, it can not be zero since zero illustrates the flight situation being already on the accident boundary. Also, the variation of safety margin becomes greater when the airplane is closer to the ground. It delineates that safety is becoming more and more uncertain and sensitive. A minor change in situation parameters will result in a fairly

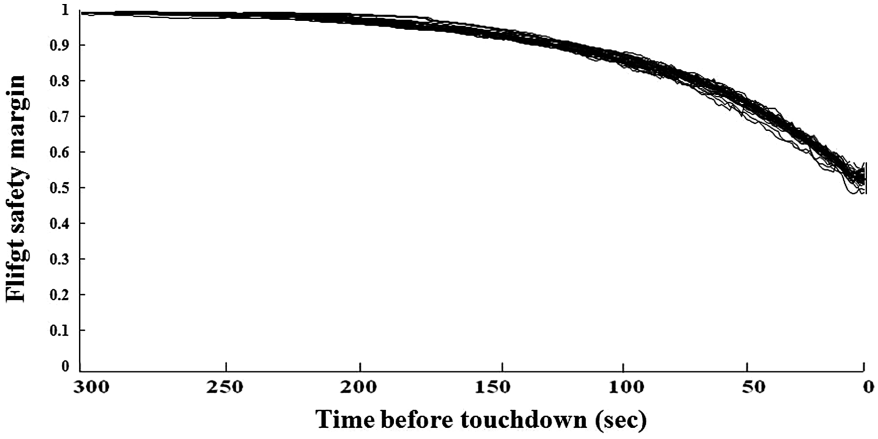

Fig. 2. Variations of flight safety margins of 39 normal flights

considerable alteration of the safety margin. It also represents that any minute error or even carelessness in the maneuver of pilots when the airplane is close to the ground will more likely produce an unexpected outcome.

3.2 Landing in Heavy Fog

One FOQA data set from a safe landing in heavy fog was chosen here to test the validity of the proposed theory of flight safety margin in a more obscure case. According to the regulations, the visibility permit-ted landing in this case. Again, data starting from 3000 ft above the ground to touch down were the in-puts of the present expert system. After calculations, the changing of the corresponding safety margin was given in Fig. 3 with the average of 39 normal flights as a reference. As it can be seen, the difference of the safety margin compared to the normal flights is quite obvious, although the general tendency is still almost the same. At touchdown, the calculated flight safety margin is 0.483, 9 % lower than the average of normal flights. At three thousand feet, the influence of the heavy fog on the safety margin was not significant. Around 1000 feet, the safety margin started to deviate from that of normal flight, and the deviation was gradually enlarged representing the influence becoming more and more severe. A nine percent difference at touchdown is relatively large, indicating that the influence of heavy fog on safety is something which cannot be overlooked.

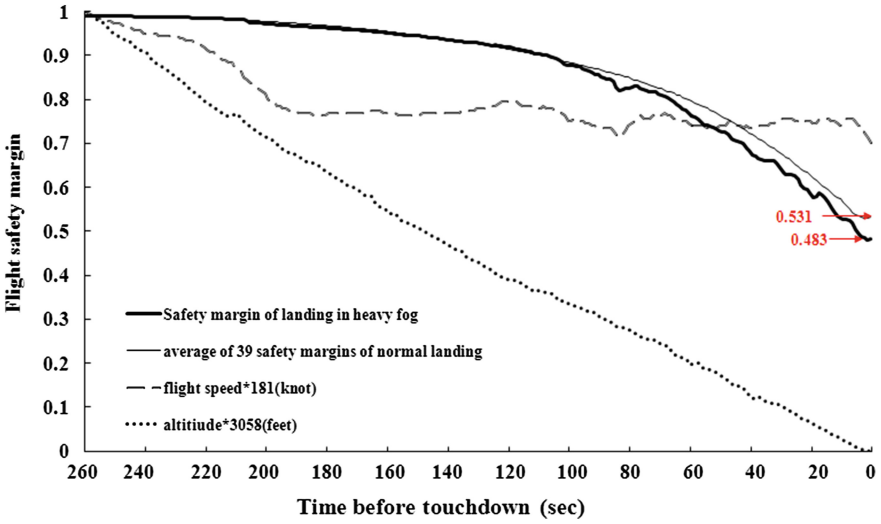

Fig. 3. The flight safety margin of a flight landing in heavy fog

3.3 The Nagoya Accident

To validate the present theory having the capability to reveal the variation of safety in a real accident, the Nagoya case was chosen to be the demonstrating example. The data from the accident report issued by the Japanese authorities were collected [12]. Starting

from 2400 ft to ground zero, 258 s in total, the changes of all the corresponding situation parameters were put into the expert system. The calculated safety margin was given in Fig. 4. One thing which should be noted is that the final safety margin for accident is calculated down to 0.05, which is statistically zero. After that, the accident was thought to be unavoidable and could not theoretically be recovered by any human. After that, the calculation was stopped.

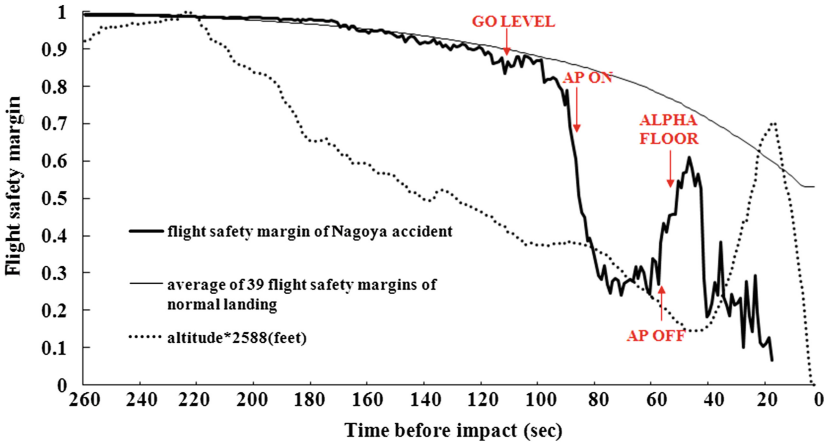

Fig. 4. The variation of flight safety margin in the nagoya accident

In Fig. 4, the average of safety margins of normal flights was also given for comparison. From the very beginning, the calculated safety margin was relatively the same as that of a normal flight. At the time when the go-level was triggered accidentally by the F/O, the safety margin started to decrease dramatically. At this moment, the automatic flight system started to execute the go around order while the pilots still wanted to land. Because the efficiency of the trimmable horizontal stabilizer controlled by computer is larger than the elevator controlled by the pilots, the plane began to level off. Up to this point, the pilots still could not convert the go-around mode to land mode. The conflict continued and became more serious with the enlarged difference between the elevator and trimmable horizontal stabilizer. At 880 ft, the trimmable horizontal stabilizer reached -12.3 degrees while the elevator +8.5 degrees. The margin of safety left under this situation was only 0.25. Normally, the safety margin should be 0.82 at this altitude. At 700 feet, the autopilot switched off. The conflict between human and machine was partially relieved resulting in an increase of the safety margin. However, the speed of the airplane was still decreasing. Further, the angle of attack was increased to 11.5 degrees. Unfortunately, the α-floor protection was activated at this time. The thrust was increased to the maximum resulting in a pitching up moment to additionally raise the nose of the plane. The margin of safety was then further lowered and reached an unrecoverable situation. Finally the zero margin was attained.

3.4 The Da-Yuang Accident

Apparently very similar to the Nagoya case, the Da-Yuang accident [13] originated from an entirely different beginning. The time history of the safety margin in this case is shown in Fig. 5 with reference to the average of normal flights. From the very beginning, the altitude of the plane was higher than required. After the pilots recognized that the altitude was too high, the action they took was to deplete the altitude by increasing the drag, lowering the flap and the gear. This maneuver did not correct the error of an approach too high. Consequently, the safety margin continued to be squeezed without any sign of recovery. As the speed was decreased, the altitude was further lowered. When the airplane passed the outer marker, the altitude was still 1000 ft higher than the normal altitude. This was not a stabilized approach. This mistake was never corrected throughout the entire flight.

Several seconds later, it was found from the recorder that the angle of attack was lowered from 7 degrees to 5 degrees. The speed of the airplane was then gradually increased because of the drag reduction. The resulting safety margin recovered back a little bit and was close to 0.6 as shown in Fig. 5. However, there was no sign of change in engine RPM. The increase in speed was not from the power of the plane. At the present situation, since the safety margin was as low as that at touchdown in a normal case, the airplane should commence the go-around immediately. However, the captain still wanted to land by telling the F/O to further bring down the flap to increase the drag. As expected, the speed of the plane was decreased further. The flight safety margin was already below 0.5 and advancing toward an even lower value. After the flap was lowered, the deviation in the safety margin from normal was further enlarged without any recovery. Even worse, to compensate for the decrease of the speed, the angle of attack was increased. The safety margin was further compressed. Eventually, the α-floor protection was activated to save the plane from this dangerous situation. Due to the increase of pitch, the safety margin was squeezed further instead of being recovered by the activation of the α-floor protection. Noticing the rise of the nose, the

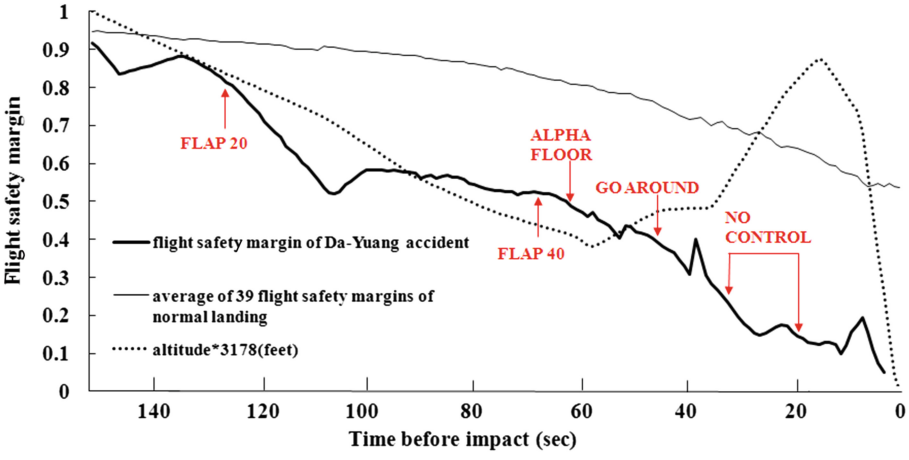

Fig. 5. The variation of flight safety margin in the Da-Yuang accident

crew pushed the control to lower it, resulting in the disengagement of the autopilot. The safety margin was slightly raised by this action. Since the speed of the plane was still decreasing, the resulting safety margin dropped again. At this instant, the safety margin was already below 0.4. After the crew decided to go around and released control to the automatic flight system to fly the plane without knowing that it had been disconnected by their own action, there was no control, human or computer, of the plane for 11 s. At this time, the safety margin left was only 0.15. With an increasing angle of attack, the airplane stalled. No one could recover the plane since the safety margin was already almost zero. The calculation of the safety margin was stopped at the statistically zero, 0.05.

4 Summary and Recommendations

In this study, we have proposed a trial geometrical type theory for flight safety. The Flight Safety Margin Theory provides a very rough holistic measure instead of sequential for the safety of flights using a neural network to overcome the corresponding perception difficulty. From the results of the case study, some basic characteristics can be addressed. First, the proposed Flight Safety Margin Theory is scientific. Although the perceptions of the local pilots were included, the whole process was established scientifically and independent of individual opinion. Second, the present theory is quantitative. It can provide a measure for flight safety in different situations numerically. Third, this theory is reasonable and acceptable. According to the results, the present theory can provide a description, agreed upon by local pilots regarding the safety of given real flight data of normal operations to accident. Most important, the Flight Safety Margin Theory is obviously not a sequential type theory.

With Flight Safety Margin Theory, the simulation capability can be basically established. It can also provide a tool to numerically evaluate the risk of human error. Combining these, the influence of human errors or other factors on the safety of flight can be estimated and compared. It could definitely be helpful to the management of flight safety since the defense can be placed reasonably at the needed spot. In addition, with the proposed theory, some kind of early warning capability could also be established. During flight, if the situation had already evolved into an unsafe situation, yet still not severe enough to trigger the warning system, the flight safety margin could provide an indicator showing that the situation should be noted. Concluding the present study, the main contribution of the present Flight Safety Margin Theory is the quantification of the perceived safety of flight; however, additional studies could be conducted for improvement of the system.

References

1. Heinrich, H.W.: Industrial Accident Prevention. McGraw Hill Books, NY (1950)
2. Boeing Commercial Airplane Group: Flight Safety and Accident Investigation. Workshop of Institute of Aero-nautics and Astronautics, National Cheng Kung University, Tainan, Taiwan R. O. China (1994)

3. Reason, J.: Human Errors. Cambridge University Press, New York (1990)
4. Jing, H.-S.: Grouping pattern of chinese and its influence on the understanding of the flight operation manual. Civil Aviat. J. Q. **3**(4), 43–58 (2001)
5. Wood, R.H., Sweginnis, R.W.: Aircraft Accident Investigation. Endeavor Book, WY (1995)
6. Strauch, B.: Investigating Human Error: Incidents, Accidents, and Complex Systems. Ashgate Publishing Limited, England (2002)
7. Perrow, C.: Normal Accidents: Living with High Risk Technologies. Princeton University Press, NJ (1984)
8. Jing, H.-S.: Indigenous concept about flight safety. Conference for the Examination and Promotion of Flight safety, National Cheng Kung University, Taipei (in Chinese) (1998)
9. Giarratano, J., Riley, G.: Expert Systems: Principles and Programming. PWS Publishing Company, Boston (1994)
10. Rasmussen, J., Jensen, A.: Mental procedures in Real-life tasks: a case study of electronic troubleshooting. Ergonomics **17**, 293–307 (1974)
11. Lin, Y.-F.: Safety Margin-Evaluation of the Risk Induced by human Error in Flight. M.S. Thesis, National Cheng Kung University (In Chinese) (2006)
12. Aircraft Accident Investigation Commission, Ministry of Transport, Japan: Aircraft Accident Investigation Report - China Airlines, Airbus Industries, A300B4-622R, Nagoya Airport 1994.4.26 (1996)
13. Civil Aeronautics Administration, Ministry of Transport, R. O. China: Aircraft Accident Investigation Report - China Airlines, Airbus A300B4-622R, B-1814, Da-Yuang, Tao-Yuang, 1998.2 (2000)