TREE METHODS FOR RISK EVALUATION OF THE GLIDER FLIGHT

Tomasz Pancewicz and Tadeusz Szopa
Presented at XXV OSTIV Congress, St. Auban, France

Abstract

The conception, procedure and the algorithm of quantitative risk investigation in the system Man-Glider-Environment is presented in the paper. Basic stages of probability safety assessment i.e. modeling of hazard and modeling of reliability are discussed. Special attention is paid to human factor and the dependence of the glider height on the level of hazard, which are characteristic features of the system. Human factor was analyzed as a cause of human errors and also as the dominant element of the system counteracting hazard after occurrence of an undesirable event. Basic relations for quantitative risk assessment are presented. Probability of casualties during one year of exploitation of a glider is defined as a measure of risk. The analysis consists mainly the estimation of sensitivity of the measure of risk on modifications of various factors characteristic for the system.

1. Introduction

Polish gliding and gliding technique comes from many years experience at one of the leading soaring countries in the world. Poland is also now second, after Germany, as a producer of gliders.

At Warsaw University of Technology, investigations in the field of glider technique have been carried on for more than twenty years. A group of faculty in Power and Aeronautical Engineering worked over five years on their own constructions. The last one, the PW-5, won the open competition declared by the Federation Aeronautique Internationale (FAI). PW-5 gliders are now produced in series in Poland.

Another group involved in Power and Aeronautical Engineering at Warsaw University of Technology also gathered in that same time frame experience and knowledge in the field of reliability and safety of various Man-Technique-Environment systems, including aviation systems, elaborating modeling methods as well as reliability and safety analysis within other investigations.

A team established in 1996 from members of these two groups has started elaboration of a method for reliability and safety analysis of Man-Glider-Environment (M-G-E) systems, which allows rational improvement of construction, technology and exploitation of gliders considering the problem of safety, mainly for the PW-5 glider and its next versions. The model of risk in the M-G-E system is the foundation of such analysis. The work presents the conception and principles of constructing of probabilistic risk model for M-G-E system and describes its utilization for the risk analysis carried out by computer simulation.

2. Modeling of risk in Man-Glider-Environment systems

The reason for losses, that occur in the period of functioning of a particular M-G-E system are so called undesirable events. Let us assume, that in the constructed model only human losses are taken into consideration, it means losses of health and human live - mainly people who take part in the glider flight. Faults caused by a man (a pilot or a ground staff) during action are usually these events, that occur inside the element *M* of the system, any kind of damages in the glider construction as well as defects in the glider starting system inside the element *G* and storms, gusts and all unfavorable natural events inside the element *E*. The occurrence of an undesirable event causes the state of hazard, which can be described by some "potential of danger." The release of that potential may lead to losses.

Before one starts creating the probabilistic model of risk, it is necessary to choose a quantity, that will be treated as a measure of risk. In the case of M-G-E system the probability of casualties during one year of exploitation of a glider was defined as a measure of risk. It can be represented by the following formula:

$$\Lambda = (1/\Delta t) \cdot P\{\mathbf{C}(\Delta t)>0\}, \tag{1}$$

where $\mathbf{C}(\Delta t)$ are the losses, which can appear as a result of undesirable events arising in the period Δt[years] of exploitation of the glider.

In this work, the symbols of random events and variables are printed in bold type.

The risk of losses appearing during the period of functioning of the M-G-E system is generally connected with the possibility of the occurrence of numerous forms (kinds) of undesirable events. In risk modeling, it is reasonable to take into account only these events which can essentially influence the level of the considered risk. Therefore, to determine the level of risk in the considered M-G-E system such events are defined, as for example: a stall of the glider, a blockage of the elevator, or a faulty disconnection of a towing line. Any other undesirable events are neglected. That is one of the most important stages of modeling of risk. Any primary dangerous event (PDE) singled out in such a way may initiate a sequence of next events and lead to an accident and resulting in losses. Let us denote the event of the k-th form by the symbol $\mathbf{A}^{(k)}$, where k=1,2,...,r.

Let us assume, that events $\mathbf{A}^{(k)}$ are mutually exclusive. On the base of the theorem about whole probability, it can be shown, that the risk Λ_1 of occurrence of losses within the interval δt=l of a glider flight is:

$$\Lambda_1 = \sum_{k=1}^{k=r} \Lambda_1^{(k)} \tag{2}$$

where, $\Lambda_1^{(k)}$ is the measure of partial risk connected with the event $\mathbf{A}^{(k)}$ It can be proved, that:

$$\Lambda_1^{(k)} = Q^{(k)}(\delta t) \cdot Z^{(k)}, \tag{3}$$

where $Q^{(k)}(\delta t)$ is the probability of occurrence of PDE of k-th form, i.e. the event $A^{(k)}$ within the interval δt, whereas

$$Z^{(k)} = P\{C>0 \mid A^{(k)}\}. \tag{4}$$

The quantity $Z^{(k)}$ can be treated as the **measure of hazard** appearing as a consequence of the event $\mathbf{A}^{(k)}$.

The quantities $\mathbf{Q}^{(k)}(\delta t)$ and $Z^{(k)}$ depend on various factors, such as for example: kind of flight (a cross-country flight, an aerobatics), pilot's features (level of training, experience, psychomotor features), the lay of the land, thermal conditions, a kind of start (using a winch, behind a plane) etc. Moreover, the height of the glider flight in the moment when $\mathbf{A}^{(k)}$ happens as well as a period of response time, in which the pilot-glider system undertakes a counteraction to undesirable events which occur as a consequence of the event $\mathbf{A}^{(k)}$ have a significant influence on the value of $Z^{(k)}$ - compare Suchodolski, et al. [1].

Let us assume, that in the considered period Δt the glider makes N various flights, then in a general case each flight can be ascribed a different level of risk Λ_j, where j=1,2,...,N, determined according to equations (2) and (3). Then the risk defined by use of measure (1), is approximately equal:

$$\Lambda = (1/\Delta t)\sum_{j=1}^{j=N}\Lambda_j \ , \tag{5}$$

where $\mathbf{N=\kappa\cdot\Delta t}$.

The quantity κ[number of flights/one year] can be treated as a measure of intensity of glider flights.

It follows on the above presented considerations, and especially on the form of relations (2), (3) and (5), that **the model of risk** in the considered system should be composed from following major parts:

- **model of hazard**, facilitating determination of hazard measures $\mathbf{Z}^{(k)}$ (k=1,2,...,r),
- **model of reliability**, allowing first of all the determination of probability of events $\mathbf{A}^{(k)}$ as well as the determination of probability of secondary events (pointed out in the model of hazard), which can appear as a consequence of the event $\mathbf{A}^{(k)}$.

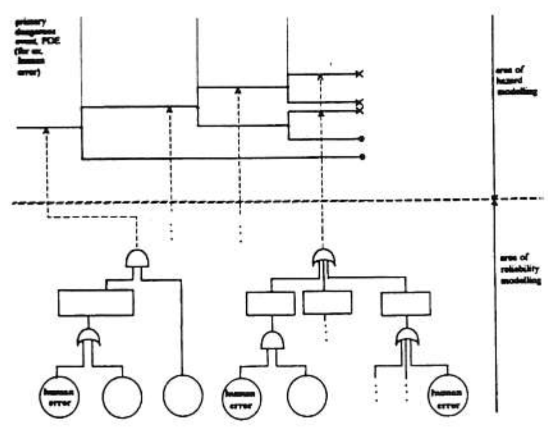

Figure 1. The idea of modelling of risk.

Modeling of hazard in M-G-E system is realized by use of the event tree method (section 3), while modeling of reliability is by using the fault tree method (section 4). The conception of such modeling of risk is presented in the figure 1. The number of such sets of trees as shown in the figure, is equal to the number of singled out PDE (events $\mathbf{A}^{(k)}$).

Remarkable domains of reliability and hazard modeling, and as a result modeling of risk in M-G-E system, are models of:

- human factor, mainly reliability of pilot's actions through the flight,
- influence of environment on the system man-glider,
- proprieties of glider construction and its elements,
- service system,
- course of an accident.

3. Hazard modeling

The state of hazard appears only when at last one of the r distinguished PDEs takes place. The hazard level ("potential of danger") appearing in the case of occurrence of another undesirable event, or in the case when none of the undesirable events occurred, is treated as equal to zero.

Hazard modeling consists mainly in definition of the set of events $\mathbf{A}^{(k)}$ (k=1,2,...,r) and determination of the levels of hazard $\mathbf{Z}^{(k)}$ caused by these events. Definition of an event $\mathbf{A}^{(k)}$ consists of its description, first of all wordy description. Such events are for example:

- A^5 - stall of a glider during winch start,
- A^{21} - blockage of the elevator in free flight.

To determine the level of hazard $\mathbf{Z}^{(k)}$ one maps the sequences of events which may occur as a result of each selected event $\mathbf{A}^{(k)}$ as well as predicting the hazard levels $\mathbf{Z}^{(k\upsilon)}$ for every such sequence (υ is the number of sequence). The set of predicted sequences of events is usually represented by means of event trees. The example of a model of hazards for one of the events $\mathbf{A}^{(k)}$ is represented, in an illustrative form, in Figure 2. In this case, the considered event is the earlier mentioned event $\mathbf{A}^{(21)}$.

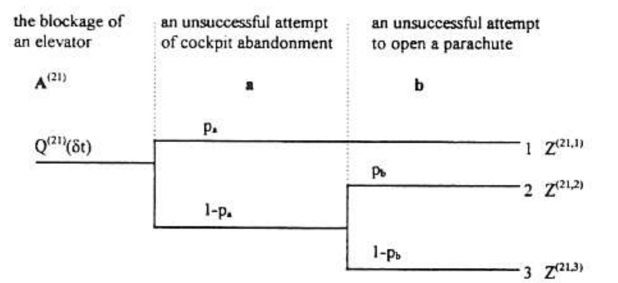

Figure 2. An example event tree for one of the undesirable events which can occur during a glider flight.

Most of the events $\mathbf{A}^{(k)}$ may occur at any height $\mathbf{h}^{(k)}$, naturally in some specified range. The height, in the case of M-G-E systems, is one of the most important factors which decides about the level of hazard $\mathbf{Z}^{(k)}$. It determines the time which is in the pilot's disposition to counteract the hazard. Pilot reliability in such dangerous situations is the second very important factor determining the success of an action, which counteracts the hazard. The success of that action depends on the disposal time, which is connected with the height $\mathbf{h}^{(k)}$ and on the other hand on the duration of pilot actions counteracting the hazard. In the example shown in Figure 2, the reliability of pilot action in dangerous situation determines probabilities p_a, p_b.

A model of hazard brought about by the occurrence of the event $\mathbf{A}^{(k)}$ may also be represented in more concise form defining the measure of the resultant hazard $\mathbf{Z}^{(k)}$, which can be ascribed to this event. One can make it out that in general case:

$$Z^{(k)} = \sum_{v=1}^{v=\rho_k} q^{(kv)} \cdot Z^{(kv)} \tag{7}$$

where ρ_k is the number of sequences in k-th event tree, and $q^{(kv)}$ is the probability of occurrence of the v-th sequence of events in this tree. The probabilities $q^{(kv)}$ are determined by multiplying the probabilities of events occurring in the sequence. For example, the resultant hazard connected with the event $\mathbf{A}^{(2)}$ (Figure 2) is equal to:

$$Z^{(21)} = p_a \cdot Z^{(21,1)} + (1-p_a)p_b \cdot Z^{(21,2)} + (1-p_a)(1-p_b)Z^{(21,3)} \tag{8}$$

To every event $\mathbf{A}^{(k)}$ the range of height $\mathbf{h}^{(k)}$, at which this event may appear, should be ascribed. Also the probability distribution of the random variable $\mathbf{h}^{(k)}$ should be determined. It was initially assumed that distribution functions are uniform with different density of probability for every flight phase (i.e. start, free flight, landing).

4. Reliability modeling

As it follows on the considerations presented in sections 2 and 3, especially according to relations (3) and (7), in order to carry out a quantitative risk analysis it is necessary to define:

- the probabilities $\mathbf{Q}^{(k)}$ of events $\mathbf{A}^{(k)}$,
- the probabilities of events distinguished during hazard modeling in each of the k-th event trees. It can be accomplished in different ways, for example:
- by using statistical data,
- according to opinion of experts,
- through calculations, employing appropriate reliability models.

Statistical data are obtained from different sources - including various literature (Swain, et al.[2], Lloyd, et al.[3]) and reports from the commission for investigation of glider accidents.

The second source of data and other information, needed for modeling of risk in an analyzed system is a group of experts which consists of glider pilots, instructors, and test pilots.

The most suitable in the analysis of risk is, however, mentioned above – the third way of probability determination. It makes it possible to not only assess the requested probabilities of events, but also to point out the reasons for too high unreliability and the possibility of diminishing it. This method needs a set of reliability models to be constructed - separately for each of the events $\mathbf{A}^{(k)}$. As mentioned in section 2, causes of events $\mathbf{A}^{(k)}$ may lie in every element of the M-G-E system. Nevertheless, mentioned models will be conventionally called reliability models.

The basic part of such a model is the model of the reliability network of a fragment of the considered M-G-E system. In risk analysis, such a network is usually represented in the form of a fault tree (Figure 1). The principles of reliability modeling, especially by using fault trees, are well elaborated and represented in literature.

All undesirable events which may occur in M-G-E system and influence the risk of its functioning can be divided into two groups (compare Figures 1 and 2):

- the set of events, which may occur during the period of normal functioning of the system, i.e. primary dangerous events $\mathbf{A}^{(k)}$,
- the set of secondary events, which occur after any of events $\mathbf{A}^{(k)}$ take place.

Constructing reliability models used for determination probabilities of events $\mathbf{A}^{(k)}$ it was assumed that the process of appearing of these events in following years, i.e. in time units $\delta t=1$ (compare section 2), is a Poisson process. It sufficiently satisfies the condition of singularity and lack of successions. Stationarity of the process was generally assumed, too. Then, the probability of occurrence of the event $\mathbf{A}^{(k)}$ within one glider flight can be written in the form:

$$Q^{(k)}(\delta t) = 1 - \exp(-\lambda^{(k)} \cdot \delta t)\,, \tag{9}$$

where $\lambda^{(k)}$ is the intensity of events. The above mentioned reliability models, for example in the fault trees form, can be used for direct determination of the probabilities $\mathbf{Q}^{(k)}$, or the intensity $\lambda^{(k)}$.

Statistical data shows that the highest values of $\mathbf{Q}^{(k)}$ are connected with these events $\mathbf{A}^{(k)}$ which are ascribed to so-called human factor, i.e. to the element M in the M-G-E system. The dominant influence on the level of risk in that domain has the pilot-flight supervisor system, but first of all the pilot.

Still greater is the influence of human factor on the sequence of secondary events, i.e. after occurrence of the event $\mathbf{A}^{(k)}$. In the example shown in Figure 2, such secondary events are events a and b. Reliability of human action in that time is determined by the probability of successful execution of actions necessary for counteracting the hazard. Following the analysis presented in section 3, these probabilities can be defined by equations:

$$R(\tau^{(k)}_{disp}) = P\{\, \Delta\tau^{(k)} < \tau^{(k)}_{disp} \,\} \tag{10}$$

or

$$R(h^{(k)}) = P\{\, \Delta h^{(k)} < h^{(k)} \,\}\,, \tag{11}$$

where $\Delta\tau^{(k)}$ is the total period of time for counteraction to hazard caused by an occurrence of the event $\mathbf{A}^{(k)}$, $\tau^{(k)}_{disp}$ is the time in pilot's disposal which is connected with the height $h^{(k)}$, $\Delta\mathbf{h}^{(k)}$ is the loss of height within the time $\Delta\tau^{(k)}$.

For example, probabilities ρ_a and ρ_b of undesirable events pointed out in the event tree following the event $A^{(2)}$ (compare Figure 2), can be determined according to relation (11). They are equal to:

$$\rho_a = 1 - R_a(h^{(21)})$$

$$\rho_b = 1 - R_b(h^{(21)})\,. \tag{12}$$

In that case:

$$p_a = 1 - P\{\ \mathbf{\Delta h_a}^{(21)} \geq h^{(21)}\ \}\ , \quad (13)$$

$$p_b = 1 - P\{\ \mathbf{\Delta h_a}^{(21)} + \mathbf{\Delta h_b}^{(21)} \geq h^{(21)}\ \mid\ \mathbf{\Delta h_a}^{(21)} < h^{(21)}\ \}\ , \quad (14)$$

where Δh_a and Δh_b are the quantities describing the loss of height within the period of pilot's actions shown in Figure 2.

In some cases for determination of human reliability in M-G-E system, for example by use of relations (10) or (11), the construction of suitable fault trees is needed. Mostly for modeling and determination of human reliability during counteractions to hazard (connected with events $\mathbf{A}^{(k)}$) THERP and HCR methods are used, which were presented by Swain, at al. [2] and Kosmowski, at al. [4].

5. Risk analysis in the M-G-E system

The set of event and fault trees constructed on the stage of risk modeling can be treated as a nominal model. It is sufficient in the case of the qualitative analysis. On the base of the analysis of the event sequences enclosed in the event trees, indication of the most dangerous paths is possible. It makes possible an efficient action leading to the probability of the minimization of an occurrence of such dangerous sequence, which leads to a minimization of the level of risk.

In the case of quantitative analysis, a mathematical form of adequate models is needed. The model of risk constructed according to the conception presented in previous sections is complicated enough that risk investigations are carried out by computer simulation.

In the first stage, the level of hazard was determined for every event $\mathbf{A}^{(k)}$. Calculation of $\mathbf{Z}^{(k)}$ is realized on the base of a previously constructed event tree. Figure 3 presents an algorithm of computation. In the first step of the algorithm, a consecutive secondary event signed out in the event tree is taken into consideration (compare Figure 2). About the occurrence of the secondary event (for example a), or a complementary event, decide conditions of height and time according to equations (10) and (11) which are checked in the next step of the algorithm.

It should be mentioned that in the majority of cases branching in the event tree describes the result of pilot action. Inspection of height and time conditions lets us determine whether the pilot's action was successful or not.

The condition of height decides about the success of the pilot action in these cases, when the height of a glider flight $h^{(k)}$ in the moment of occurrence of event $A^{(k)}$ is compared with the loss of height $\Delta h^{(k)}$ needed for counteracting the hazard. The loss of height is connected by equations of glider motion with the response time of a pilot-glider system for the undesirable event.

The condition of time is significant in these cases, when the lack of pilot action in due time effects in occurrence of next secondary event. For example, no pilot action on stall leads to spin. As it follows in the above consideration, the correctness of hazard determination depends on the conditions checked in the step check height and time conditions, where in a non-explicit way the model of glider steering is included. Inside that block, the response time of a pilot glider system on an event $A^{(k)}$ or secondary event is randomly selected according to the assumed probability distribution.

At the end of every sequence of events there is a call to determine losses. In that way it is considered that, for

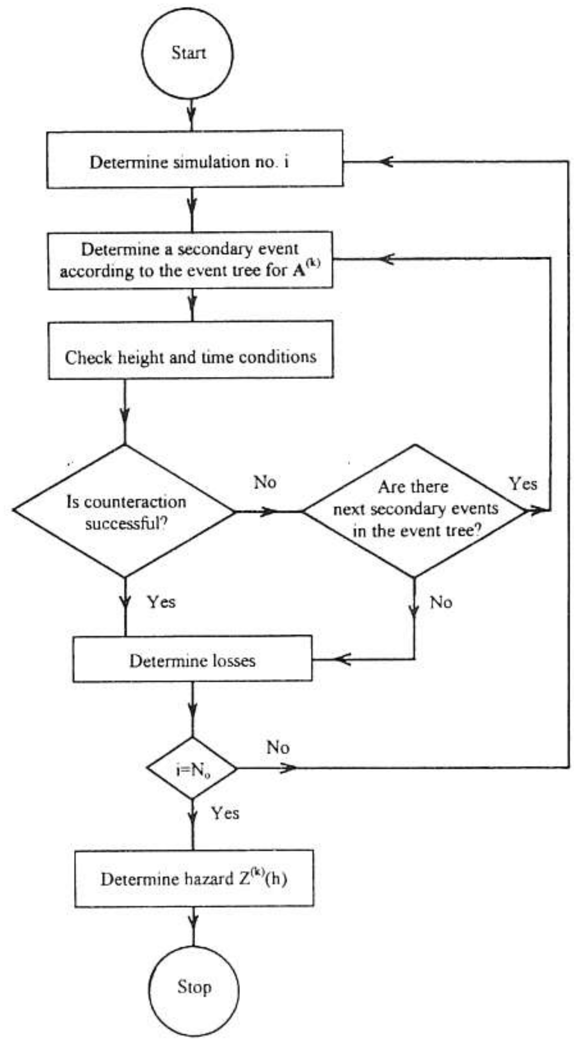

Figure 3. The alogorithm of hazard determination.

example, the probability of survival in the case of live-saving parachute jump is close to 1 – but not equal to 1. Similarly, in the case of a clash with the ground, the probability of pilot's death is not equal to 1.

According to previous assumptions, the hazard is a function of height $h^{(k)}$. Therefore to determine $\mathbf{Z}^{(k)}$ (h) a hazard simulation for each event $\mathbf{A}^{(k)}$ are carried on for the full range of flight height.

Hazard $Z^{(k)}$ (h) is used in risk calculations according to equation (3). An algorithm of simulation computation is presented in Figure 4. In calculations in the first approximation it was assumed, that during any one glider flight only one PDE $\mathbf{A}^{(k)}$ may occur. That simplification is justifiable, because of small probability of occurrence of events $\mathbf{A}^{(k)}$. Such approach to the problem neglects the fact that after counteraction to an event $\mathbf{A}^{(k)}$ the probability of pilot error is much higher than before the occurrence of that

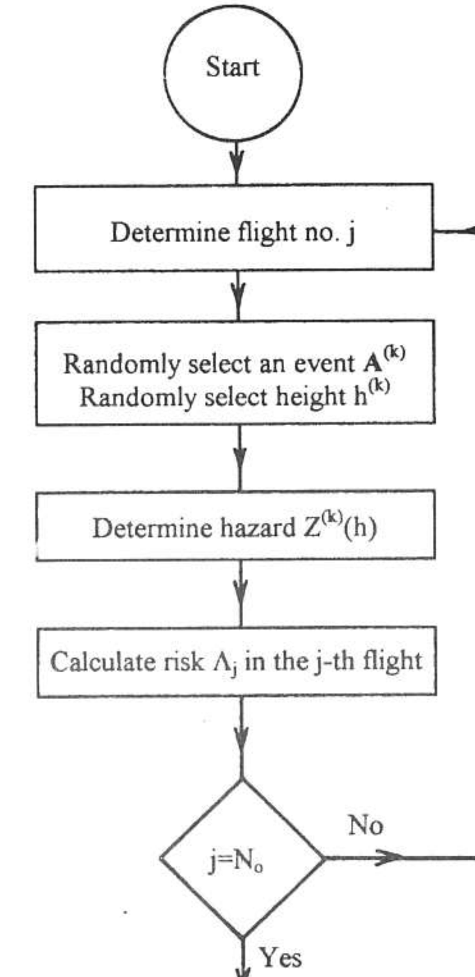

Figure 4. The alogorithm of hazard determination.

event. On the other hand quantitative determination of these changes is very difficult.

Pointed out events $\mathbf{A}^{(k)}$ together with an event during flight there is no PDE create a complete event space. Therefore the random selection of an event $\mathbf{A}^{(k)}$ is carried out in to steps. First it is checked whether in j-th flight any PDE occurred. Then, in the case of positive answer in the second sampling it is checked in which event $\mathbf{A}^{(k)}$ occurred. Inside that block of the algorithm the height of glider flight $h^{(k)}$ when the event occurred is randomly selected. That sampling is realized according to probability distribution of an event $\mathbf{A}^{(k)}$ appearance in relation to height.

In following steps of the algorithm, the risk in j-th flight is determined according to (2). In the presence of assumption about single PDE in j-th flight, the calculations are simplified to identification of risk Λ_j with hazard $Z^{(k)}$ (h). In the last step of an algorithm, risk Λ is determined according to (5). It should be noticed that N_o is the number of simulations which can be treated as the number of gliders in the population, whereas the number N denotes the number of glider flights in one year.

6. Conclusions

The conception, procedure and the algorithm of the quantitative risk assessment is based on the event and fault trees methods. A characteristic feature of the M-G-E system is the lack of an automatic system which counteracts the hazard. If PDE occurs then the sequence of events depends in the first place on pilot and ground staff action.

Therefore, human factor was especially emphasized in the model. The problem of human reliability was built into the model by dependence of the realized event sequence on the efficiency of pilot action. The action was treated as successful when it was started and finished in due time.

Because of dependence of the hazard on the flight height in the moment of occurrence of PDE, that height was treated as an independent parameter of the model.

Risk analysis for selected glider flight phase carried out according to the presented method was published by Suchodolski, et al. [1]. The significance of these results consists not on the numerical value of risk, but on the sensitivity of that value on modifications of parameters of the model. Results of investigations may be the reason for modification of the structure, the way of functioning and cooperation of the M-G-E system to minimize the level of risk.

Acknowledgments

The authors wish to acknowledge the Scientific Research Committee (KBN) for granting of that work in the project no. 9 T12C 012 08.

7. References

1. Suchodolski S., Wisniewski J., Zak P.: *Risk evaluation in selected flight phase of the glider*. Proc. of XXV OSTIV CONGRESS, Saint Auban France 3- 11 July 1 997.

2. Swain A.P., Guttmann H.E.: *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. (final report)NUREGICR-1278F,SAND-800200,RXAN printed August 1983.

3. Lloyd E., Tye W.: *Systematic safety. Safety assessment at aircraft systems*. Civil Aviation Authority, London 1982.

4. Kosmowski K.T., Degen G., Mertens J., Reer B.: *Development of advanced methods and related software for human reliability evaluation within probabilistic safety analysis*. Institut für Sicherheitsforschung und Reaktortechnik Jülich, 1994.