Method of Increasing Reliability of Semi-ergatic Systems in Extreme Situations

GEORGE POPOV  
Computer Science Dept  
Technical University - Sofia  
8, Kl. Ohridsky, Blvd  
Bulgaria  
popovg@tu-sofia.bg

MARIA HRISTOVA  
Informatics Dept  
High Transport School-Sofia  
Geo Milev, Str 158  
Bulgaria  
mariah@vtu.bg

HRISTO HRISTOV  
Rector  
EPU - Pernik  
23, Kiril i Metodiy” Str.  
Bulgaria  
ac@epu.bg

Abstract: - This paper presents a model of Man Machine Interface with automatic control unit (autopilot) and two operators (pilots). In main cases, the output decision is received by quorum 2v3. In case of conflict, each participant has its own priority for solving a problem. Otherwise of all homogeneous systems, every operator here is different as person and there are three diversity channels- two men and control algorithm. This scheme with can be applied at high risk control systems in nuclear plants, military areas, aviation and etc.

Key-Words: - MMI, M²MI, human interface, diversity, reliability, control systems, pilot

1 Introduction

1.1 MMI

The Man-Machine system is most often a control system in real time (Real Time System) including interaction between a human operator and his product, the machine [1]. This interaction is known as man-machine interface MMI (Man-Machine Interface) MMI. The Man-Machine interface is used to manage processes of high responsibility in military activities, industry, nuclear power plants, control of trains and cars, manned and unmanned flights, aerospace operations, etc. When an individual is the crucial link in the outline of control, many references mark the control sets of this type as ergatic systems.

The modeling of an MMI is a subject of many papers [2, 3, 4, 5]. It is typical that the models depend on the scope and requirements faced by the MMI. According to [6, 7] the existence of 100% human or 100% automatic control of a space flight is impossible. It can be also said for the control of trains, even though the system called “auto engine driver” has been in operation for decades.

The main problem in high-responsibility MMI systems is reliability depending on human reliability, and it is known that any system which depends on human reliability is unreliable [8].

To increase human reliability air companies use two pilots for control of single-pilot aircrafts. The authors of [9] have even offered to deny insurance of flight or the insurance is so high that flights with one pilot are not profitable to exist.

An essential feature of MMI systems explicates with the presence of extreme conditions. When it does not refer to routine actions but to extraordinary emergency conditions, a problem arises: what happens if the person makes an error, especially when one rarely (unusually) carries out such reactions? It is clear that it can cost a lot: a human life, health, loss of large values, etc. Then the so-called human factors appear, when under the influence of an unusual risk environment the man changes his/her features and can admit a fatal error (human error) and cause an accident with a threat to human life and material damage. In [10] there is a detailed classification of over 120 human factors leading to incorrect decision-making of the operator (human failures) and damages of significant consequences. The references show specifications of human factors leading to an error in the marine [11], aviation [12, 13] and nuclear power stations [14, 15]. Over 72% of air accidents [12] are a result of human errors.

To investigate the influence of extreme conditions, the a MMI model is made or simulators are used [16,17,18] where the human operator is placed in unusual situations.
As a result of the review of the studies carried out it has been observed that the different human factors [19, 20, 21, 22] cause human errors of different operators in a different way. That has confirmed the popular thesis that each human operator has diversity behavioural nature.

1.2 Diversity

As it is known, diversity is a method of problem solving (mathematical, logical, technical, etc.) in two (A and B) different ways (kinds, methods, algorithms, implementations) with the same input data.

This method is applied as an effective tool for:

a. detection of errors in construction, technology, design, algorithmic and software ensuring for decision (diversity as fail-safe means).

b. increasing the reliability of the system ensuring the decision [23] - diversity as fault-tolerance means.

Diversity as fail-safe means [24,25] is based on the assumption that with an error in one of the two ways, the manner or method of solution (A or B), the alternative one gives the correct result. The results are different and with comparing the error "is captured" at the system output and the operation of the controlled object is ceased until the error is removed. When there are errors in both sites, they are also detected because they do not have one and the same impact on the output results, which are wrong but different. This approach is applicable to cases of off-line diagnostics of faults or of on-line real-time control but of processes whose suspension leads to safety (non-dangerous) or alarm conditions. There are such conditions in railway transport, security equipment, some processes in industry, military activities, etc.

If the task is solved twice in one and the same way (e.g. in A way), it refers to systems of homogeneous (2A) channels (ways, kinds, methods, modules, etc.). The difference with diversity (A and B) consists in the fact that if with a homogeneous solution there is an error with both solutions, one and the same wrong result is obtained and therefore the errors remain undetected.

Diversity as fault-tolerance means has a principally different purpose. It is not looked for error detection but to preserve serviceability. It is relied on the fact that the alternative way gives a correct result and the system can continue operating despite the refusal of the other channel. That is a good method for improving reliability with control of processes where ceasing is dangerous: systems for life support, air transport, aerospace, etc. If the systems are with homogeneous channels, then the alternative channel will lead to failure due to the same error.

This article is dedicated to looking for a solution in the above mentioned aspect.

2 Problem Formulation

To increase the reliability it is proposed to use diversity contained in the MMI-Real Time System with two operators. The operators are of a priori diversity: no two people on Earth are exactly the same by their biological, functional and psychological features.

This system is designated as a Man Man Machine Interaction M2MI, where the second M is an automatic control device. Taking into account the already known research results, new opportunities of diversity are suggested. The idea is that normal (routine) control is performed by an automatic device (the second M) but with responsible operations and under extreme conditions essential for safety, both operators are included to work in parallel with the automatic device.

In [6] differentiation and classification of MMI into 7 groups (spectrum, modes) depending on the degree of human involvement in the system control are given. According to the idea being under consideration in this paper, operators are included in responsible decisions only sporadically. During the rest of time the system operates automatically by prescribed algorithm ALG and appears to be ergatic only under extreme conditions. That is why in the context of this classification it is called semi-ergatic: non-ergatic under routine conditions and ergatic in unusual situations.

The task set here is to model the reliability of the MMI interface and suggest methods for its increasing considering the favourable features of diversity.

3 Problem Solutions

3.1 Behavioral

Let be a Man-Machine Interface MMI with a system of automatic control ALG and two operators (Fig. 1). Normally it is only the automatic control ALG that operates and operators A and/or B have the role of a controller, i.e. monitoring.

In current practice (Fig. 1), with emergency the system reliability is ensured by the proper operation of operator A: in aviation by the first pilot, in rail transport by the engine driver, dispatcher, etc., who
are responsible for control. With the failure of A, operator B is included: co-pilot, assistant engine driver, etc.

Automatic control ALG has no sensitivity to critical and extreme situations (catastrophic natural phenomenon, enemy fire, etc.), which cannot be provided and set in the algorithm. Therefore ALG cannot respond or responds inadequately. The idea is that when the proper behaviour is not programmed and does not exist in ALG, to include operators A and B to control simultaneously with the software for automatic control ALG (see Fig. 2). The man gets faster and more information possesses more intelligence, competence and creativity and can quickly find the correct irregular solution.

![Fig.1. System reservation with automatic control ALG and two operators A and B](image)

Automatic control ALG has no sensitivity to critical and extreme situations (catastrophic natural phenomenon, enemy fire, etc.), which cannot be provided and set in the algorithm. Therefore ALG cannot respond or responds inadequately. The idea is that when the proper behaviour is not programmed and does not exist in ALG, to include operators A and B to control simultaneously with the software for automatic control ALG (see Fig. 2). The man gets faster and more information possesses more intelligence, competence and creativity and can quickly find the correct irregular solution.

![Fig.2. A model of M²MI system](image)

To enable all three channels to operate simultaneously on-line, one of the known quorum systems, which take out the result by output criteria of domination, majoring or consensus can be applied. The decisions of the three channels in the form of signals, i.e. controlling impacts made by them are compared and enter the entrance of Comparative Unit CU, which produces the control signal to the CS (controlled system). Here it is suggested that the decision is made by majoring by criterion "2 of 3". Due to the priori diversity of the three channels, controlling M²MI Man-Machine set will provide more efficient and proper management than the one under the scheme in Fig. 1. In its essence it is a triple diversity system, since both operators are players with different qualities and ALG is a machine.

What new properties and qualities has the system acquired in its current form? If the automatic pilot fails due to inability to identify the state or make decision, the two operators can continue controlling. The possible conditions of the proposed system in Fig. 2 are as follows:

1. ALG operates, operators A and B are in the state of monitoring;
2. Critical situation. The leading operator switches the system to mode "2 of 3". The following cases can be created:
   a. All three elements ALG, A and B make the same decision, the system responds adequately;
   b. One, A or B, deviates from the correct decision, but other operator and ALG have one and the same correct decisions and according to them by the criteria a decision is made, it is assumed that the system responds adequately;
   c. Due to impossibility to provide each situation or due to lack of sensitivity ALG fails or does not respond adequately. However:
      • the two operators A and B make one and the same decisions, it is assumed that the system provides adequate response by criterion "2 of 3";
      • the two operators A and B make different decisions. It is not possible to make a decision by the criterion; the system does not respond adequately.

How to proceed in the latter case? To continue the control of the process, the "principle of domination" known in the quorum functions can be applied. For example, as the first operator has more weight (importance) being given more responsibilities and his/her decision is enacted. This does not mean sufficient adequacy but relevant responsibility.
3.2 Adequacy

If it is assumed that the area of adequacy (correct decisions) is outlined with a trefoil clover (Fig. 3) where the decisions of at least two from three elements of the majority system intersect, then the system "2 of 3" is the better solution. It is because when Man-Machine Interface is with one operator, the area of adequacy is lower (the upper left and bottom leaves). When it works with auto-operator ALG = C covers the upper two leaves. If a second operator who covers the upper right sheet is added, adequacy increases and might get close to complete (100%) adequacy.

![Fig.3. Area of correct decisions of “2 of 3” system](image)

To what extent the three elements cover the entire area of adequacy depends on their competence and diversity. If all three elements solve the problem in one and the same way and it is embedded in software ALG, the effect of majoring will be zero. It is obvious that all extreme situations cannot be foreseen beforehand in order to be programmed. Due to ALG leaves uncovered area (lower leaf). The man gets faster and more information, possesses more intelligence, competence and flexibility but is susceptible to emotions, stress and consequent inadequacy. Moreover, although being of high-level competence, if they are more different (from different schools, in temperament, sensitivity, etc.), the diversity is deeper and the probability to cover the adequately area is higher. The problem of measuring adequacy and the factors it depends on (including psycho-physical, educational and qualification ones) is the subject of a separate study.

3.3 Reliability modelling

Failure is a functional disability may be due to:

- Fault - Short circuit, holes, breaks, industrial defects, overheating, wear-and-tear, fatigue, fracture, etc.;
- Error - an error, inappropriate behaviour, which may be due to insufficient training, incompetence, lack of volitional qualities of the man or quick reactions, incorrect or incomplete algorithm in automatic control.

3.3.1 Reliability in the context of case "a"

The indicator of reliability in systems in Fig. 1 is their availability to operate properly. Let us denote the availability of automatic device ALG with $A_{alg}$ and of the two operators by $A_a$ and $A_b$ respectively. Considering that the scheme is with reservation, through substitution we can write the formula for reliability of the whole system [26]:

$$A = A_{alg} + (1 - A_{alg}) A_a + (1 - A_{alg})(1 - A_a) A_b$$

This is a well-known model, which assumes that $A_{alg}$, $A_a$ and $A_b$ go out of action in sequence one after another.

The failures in the three elements of the system in Fig. 2 occur randomly and independently from each other. It can be looked for quantitative assessment similar to that of formula (1). If all three elements have different reliability (standby) states, it can be written that:

$$A = A_{alg} A_a A_b + (1 - A_{alg}) A_a A_b + (1 - A_{alg}) (1 - A_a) A_b + A_{alg} (1 - A_a) A_b$$

Formulas (1) and (2) do not consider diversity. They will be correct both with homogeneous and readily diversity channels $A_1$, $A_2$ and $A_3$, when their failures are due to loss of serviceability due to Fault. Diversity does not concern case "a".

3.3.2 Reliability in the context of case "b"

Reliability is equivalent to adequacy and depends on correct decisions. If all three channels operate in one and the same way and make one and the same errors, the three-channel nature is pointless. It is alike as if a single channel operates. If $A_{alg}=A_a=A_b$, the availability of the system $A_s$ is the same. However, with diversity channels it increases and some more reliability that comes from diversity might be added to it. How much it will be depends on the value of the indicator "ready" and the depth of diversity. When decisions are made completely independently with three absolutely different channels operating by fundamentally different algorithms in a way not to admit one and the same
errors, the reliability models in case «а» and case «b» and ideally are reduced to (2).

4. Conclusion

1. A way to improve reliability by a three-channel diversity semi-ergatic Real Time System with participation of two operators simultaneously working in extreme situations has been suggested.
2. Spatial models of control that show adequacy improvement of a Real Time System by the proposed way have been presented.
3. The diversity three-channel semi-ergatic Real Time System with participation of two operators working simultaneously has been modelled in relation to reliability in extreme situations.

References:

[8] Gilb's Laws of Unreliability
[20] Burchell, Bill, Human Factors: Still Trying to Catch On Despite ample evidence supporting the value of human factors training and awareness, the aviation industry has been slow to embrace the concept. Overhaul & Maintenance, VI, 10, 21.


**Acknowledgement:** The work presented in this paper was supported within the project DTK02/59 - 17.12.2009