Safety modeling of the man-machine interface in railway signaling systems

George I. Popov, Maria P. Hristova and Hristo A. Hristov

Abstract**—**The question of dependability and safety of the man-machine interface (MMI) in safety related systems is introduced. In the considered aspect, MMI is summarized as a structure of ergosystem, which reconfigures itself after a failure. Behavior of the man-operator (station foreman, driver, dispatcher, etc.) is defined in view of the dependability and safety of the man-machine synergy. Modeling based on the Markov chains tools is proposed.

Keywords**—** Safety-related systems, Signaling, Dependability, Safety, Man-Machine Interface (MMI), Markov modeling.

I. Introduction

THE structure of a man-machine signaling system is shown on Figure 1. The machine (station interlocking, dispatcher interlocking, cab system for locomotive control, etc.) controls railway traffic. Using the direct control facilities (DC), the information is derived from the real-time process and displayed for visualization and indications (V&I). The operator monitors the condition of controlled objects. When a command is sent (by CC – command console), the machine produces control effects and some information is processed and/or transferred. Using the direct control facilities (DC), they are sent to the safety-related technological process (STP) – railway operations. When the command is executed, conformity is established between what must be and what is really in the system of control. The new state is registered by the technical means for visualization and indication (a display board, screen). The picture is kept until a new command is received or a change of the state of any object arises.

Using the direct monitor facilities (DM), the information is derived from the safety-related technological process, processed and displayed for visualization and indication (V&I). After a new command, the ring is closed again. There is interaction between the two components in the Man-machine interface (MMI): the operator and machine.

The control process depends on the man-operator (Fig. 1), on his/her decisions as well as on his/her mistakes. The latter result in inefficiency, e.g. unneeded railway traffic delays. Having made a mistake, the operator could initiate compensative actions to neutralize it but this influences on the system functional effectiveness. Almost all studies, scientific forums on man-machine interface MMI and the respective papers including those about other fields of controlled processes [1, 2, 4], are connected with these consequences.

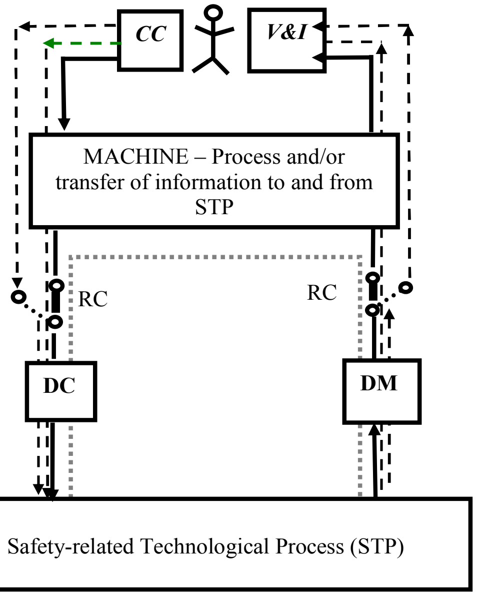
CC
V&I
MACHINE – Process and/or transfer of information to and from STP
RC
RC
DC
DM
Safety-related Technological Process (STP)

Fig.1. Structural scheme of MMI

However, the signaling systems are so designed that any command remains outstanding if it does not comply with the safety requirements. The machine "recognizes" the current situation, "knows" what is permissible or not and does not fulfil commands that belie safety principals. When connected with the conditions of safety, the control does not pass through the man-operator. The responsibility for safety is taken by the machine. From this point of view, the man-machine interface is an ergo-system in regard to the operative feed-back and a non-ergo-system in regard to safety (Figure 1 red dotted line).

Second, the signaling system takes safety condition after a fault or has a preliminarily known safety behavior. Although the approach could hold the safety-related system down, these states are predefined as "lesser evil". Some examples of safety behavior are: false information for track occupancy when in fact the track is free, a lack of control of the switch when the

Manuscript received September 30, 2010.

G.I.Popov is with the Department of Computer Systems, Faculty of Computer Systems and Control, Technical University - Sofia, 8 Kliment Ohridski blvd, 1000 Sofia, Bulgaria, e-mail: popovg@tu-sofia.bg

M.P.Hristova is with the Department of Mathematics and Informatics, University of Transport - Sofia, 158 Geo Milev str.,1000 Sofia, Bulgaria, e-mail: hristovam@vtu.bg

H.A.Hristov is a Rector of European University in Bulgaria., 23 St.St. Kiril and Metodij str., 2300 Pernik, e-mail: rector@epu.bg

train has passed a level-crossing, but the turnpike remains down, when a fuse for permissive signal has burnt and it has closed, etc.

Such failures are called fail-safe. Fail-safe failures limit the functionality and hold the performance of statutory functions. The switch cannot be turned, the signal cannot be cleared, the turnpike cannot be raised, the train stops or slows down under the permitted speed, and so on. By the system fail-safe behavior, the failure causes the necessity to remove it and this necessity appears immediately.

However, even that the probability is small, the machine may not go to a safe state. The following examples can be given: the track is occupied but die to the failure information about free track is transmitted to the machine, a switch is turned in a wrong way but due to the false information it can be used to set a route, the switch turning is hazardous because of the failure effect it turns, the turnpike raises before the train has passed the level crossing, etc. The failure occurred in such case is hazardous. The failure as a result of which the machine properties to stop the operator's hazardous actions are lost can be also hazardous.

When a safe failure occurs in the machine (or its failure part), the operator takes the control directly. In order not to break the STP, he/she enters the commands himself/herself by the reserve control facilities (RC) (Fig.1). For example, instead to set a normal objectively controlled route, the operator switches on a substitution signal for a train, which the machine is not responsible for; turns directly a switch, as he is assured subjectively that the means for its control provide false occupancy; raises the turnpike by a direct command when the train has passed away and the turnpike remains down, etc. Undertaking the control, the operator is responsible also for the traffic safety. But in this situation who can stop the operator to gives hazardous commands? It is the case when accidents happen most often. Because of that the commands during the mode of reserve control are controlled. If they are done by buttons, they are sealed and proved with counters. When they are given by the computer mouse or keyboard, they are entered in a special mode and are saved in an achieving device.

The signaling system turns again into an ergo-system because the operator becomes a decisive unit in the contour having taken the control in the mode of reserve control (MC). But this ergo-character refers also to safety as the latter depends on the operator. At that it refers to moments when unordinary problems have to be solved in unordinary situations, which do not repeat as a routine in operative control. That puts the operator under extreme conditions where the probability of errors increases.

II. Problem Formulation

Reliability is connected with all possible failures – hazardous and safe [5]. The MMI reliability indicators are the probability of flawless work R(t) or the mathematical expectation of the Mean Time To Failure MTTF. To these reliability indicators until the first failure, belong also the probability of failure $Q(t)$, the distribution density $f(t)$ of worked operations t until a failure and failure rate λ(t).

Safety is connected only with the hazardous failures. Safety indicator can be the probability of object operation without hazardous failures R_{nHF} or Mean Time to Hazard Failures MTTHF. In the repairable systems the indicator is the availability of operation without hazardous failures A_{nHF} or Mean Time between Hazards Failures $MTBHF$ [5].

If the machine was high dependable and/or available, the transitions to a reserve control (RC) would happen very rarely and direct operator's intervention in the STP would not be necessary. The MMI safety would be determined only by the machine safety. But it is not so in the real systems. The lower is the availability; the greater is the probability of operator's intervention by reserve control facilities.

The operator's actions could be presented as a set of operations (manipulations) consisting of two subsets: correct and incorrect decisions (Fig. 2). At that the errors can have hold effect but could be hazardous as well.

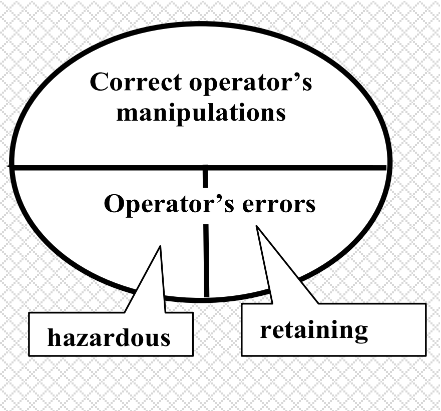

Fig. 2 Set of operator's errors

The hold effect (safe) errors lead to inefficiency but not to hazard for the traffic. Some examples of such errors are to set a route on an improper track, turn a switch by a mistake, close a signal not in due time, etc. The machine checks the safety traffic conditions and if they are not kept, the manipulations remain without consequences. Otherwise, if they are kept, the route is set. As a result the signal can show a permissive sign that is not provided for that train. After such decisions, the vehicle has to be displaced by shunting and corrective actions have to be undertaken to neutralize the error. Both time and power will be lost and every delay has also economic dimensions.

The operator's hazardous errors (the bottom left sector) have different consequences when the machine operates and when it is in a failure state. In the first case the errors are not realized because the machine does not implement them. When the machine is in a failure state, the prohibition to implement hazardous errors could not exist. Then the hazardous error is realized and can cause an accident.

The operator's errors in his/her interaction with the machines are a subject of a number of publications [1, 3, 5, 8, 9]. There are studies also on the operators of Signaling systems [6, 7]. But the studies that have established how the operators influence on the system efficiency are prevailing. With a few exceptions [8, 9], safety has not been examined as an independent problem and the models of quantity assessment of safety values by selected indices are even less presented.

The purpose of this study is to put the issue of MMI safety in Signaling systems and make an attempt for quantity assessment.

III. Problem Solution

A. Selection of a method and mathematical tools

The solution is looked for by adequate mathematical models. The solution of a method is predetermined by the problems to be solved and the prerequisites to be considered. The methods suggested are Stochastic [5], Petri Nets [10], etc.

The paper presented is based on the understanding that the interaction between the operator is far from determined nature although it follows certain algorithms. There is a sequence of events: signals opening and closing, switches turning, vehicles stopping and pulling off, rolling stock movement, operator\s decisions, manipulations, monitoring and control. It is not preliminarily known what will happen at which moment and the probabilities to happen at different moments of time t are different. It is referred to a flow of pseudo-random events. Although being regulated (e.g. in the rail traffic schedule), in practice they happen at a random time.

To these regulated events failures are added and the latter are random, unregulated and lead the MMI to one of the three states: Availability, Hazard and Safety. The flow of failures and recoveries as well as the transition between the states evidently possess ordinary nature and lack of sequence and can be compared to Poisson. If this thesis is assumed, the MMI safety indices can be: interface availability to operate without failures A_{MMI} and mean time $MTBHF_{MMI}$ between MMI hazardous failures.

The problem of the MMI quantity assessment is reduced to finding out an adequate analytical model. As a result formulas of A_{MMI} and $MTBHF_{MMI}$ have to be worked out. They will be used to define the safety factors and explicitly show how the indices depend on the factors. It is necessary to find out tools to control their values and hence the MMI safety.

For these problems and with these preconditions, of all the methods examined it is the method of Markov processes and circuits that suits the best. The adequacy of such a model depends on to what degree the assumption that the examined processes meets: for states and time is true. .

The first Markov condition hardly needs proving for the practice of Signaling. If the transition intensities between the MMI states (Availability, Hazard и Safety) are constant, they can be modeled as homogeneous Markov chains. In case that they are variable, the second condition does not exist and they have to be examined as semi-Markov. It does not change the model proposed below but only the solution, it leads to. In the simple case a system of differential equation of Kolmogorov with constant coefficients is solved. When the coefficients are functions of time, the model is semi-Markov and solutions are looked for using input Markov chains.

B. MMI safety modeling

The operator is one of the two elements of MMI and the other one is the machine. Let us define the following:

λ_H is the intensity of operator's (man's) errors;

p_H - probability of human errors to be safe (i.e. to be compensated and not resulting in hazard but only in inefficiency);

μ_{HdH} - intensity of getting out of a hazardous error state;

μ_{HS} - intensity of getting out of a state of restraint errors.

If it is assumed that after an error the operator takes up compensative actions to neutralize it, the graph of the man-operator is of the kind shown in Fig.3.

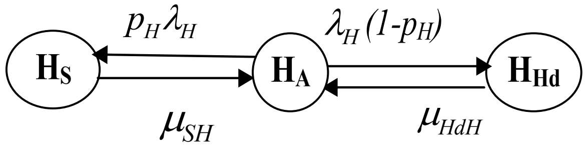

Fig.3 Graph of the states of the signaling system man-operator

The machine has analogical three-position graph (Fig.4), where:

1. MA – Machine Available state;
2. MHd- Machine Hazardous state;
3. MS – Machine Safe state;

$\lambda(t)$ – intensity of the machine failures;

$\mu_{Hd}(t)$ – intensity of recovery from the hazardous state;

$\mu_S = \mu$ – intensity of recovery from the safe state;

p – probability of the machine failure being safe.

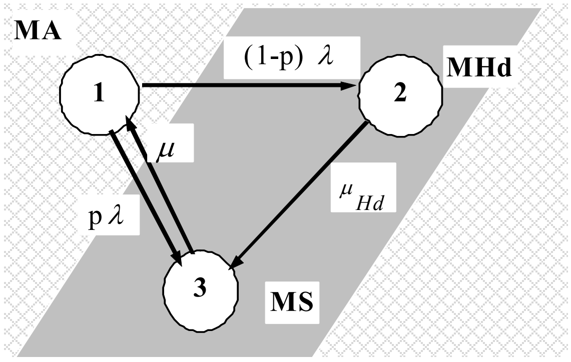

Fig. 4. Graph of the states of Signaling-system (machine)

The two parts of the man-machine interface enter into interrelation. Each state of the both sides can enter into combination with every state from the other part. So the total states number in the MMI model is 32 = 9.

What kind of transitions can happen in this graph is visible from the partial states and connecting arcs (Fig.5). The corresponding intensity is also marked with each of these partial states.

The following suggestions are accepted to define the proposed model:

1. The process is homogeneous Markov, i.e. the transition parameters are stable in time. This limitation is not compulsory for this graph to be in force.

2. The machine state changes horizontally and the operator's state changes vertically on the drawing.

3. The stream is a Poisson stream and that means also an ordinary one. Thus, simultaneous events in the Machine and the Man or events due to common reason causing transitions diagonally in the graph do not exist. There are only orthogonal transitions.

4. When the machine operates hazardously MHd, then the MMI is also in a hazardous state. The machine influences directly on the process irrespectively of the interface. The three partial states 3, 6 and 9 are hazardous, too.

5. When the machine is in a safe state MS, only state 2 is hazardous when the man-operator makes hazardous errors.

6. Also, state 1 could be hazardous, if it can occur at all. It takes place when with machine operating MA there are non-provided and uncovered (due to resources and other reasons) spaces where the operator is given a possibility of interference in safety. Furthermore it is considered that the intensity of man's faults depends on the state of the machine. When the machine is fit to work, (MA) is perfectly created:

a) intensity of errors λ_H', is too low because with a trouble-free machine the operator performs routine manipulations, which he/she has got used to and often works like an auto-motor. It is calculated as a reciprocal value of the mean time between two operator's errors made one after the other.

b) the transition $(1-P_H)\lambda_H'$ from partial state 4 to partial state 1 must not exist since the operator, even he/she wants to, cannot cause a hazardous situation. The space where he works (the bottom left corner in Fig. 2) is a zero set. It corresponds to the possibility for the operator to influence on safety in the machine availability state MA. There is no probability exists to implement erroneous manipulations as hazardous, i.e. e. $p_H = 1$.

c) when the machine has stopped safely MS, the operator takes the control directly switching to a reserve control (MC) to perform the actions provided by regulations for coordinating, unsealing buttons, control, etc. It happens to him/her rarely, he/she is in an extreme situation and the error rate increases considerably. The intensity of transition from partial state 5 to 2 is different – $(1-p_H')\lambda_H''$.

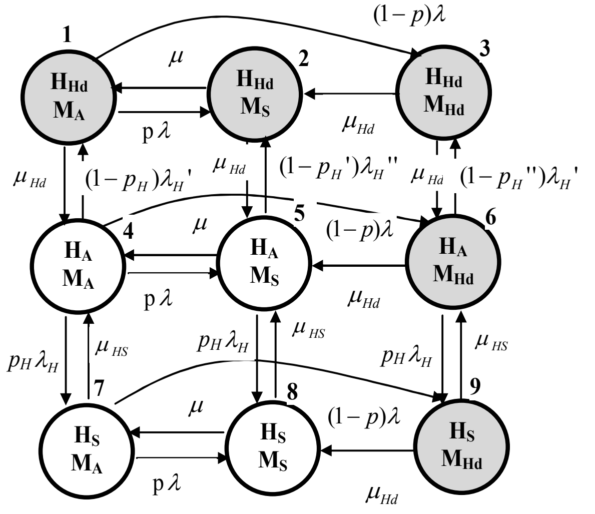

Fig.5. Graph of the man-machine interface states

When the machine has stopped in hazardous state MHd, the operator is not in a critical situation. He does not know about the hazardous failure. But its failures influencing on the safety-related technological process are not the only hazardous ones. The operator's errors are also hazardous because now some of the faults eliminate the restriction for the operator to make manipulations contradicting to safety conditions. The relation between the types of errors is changed and the transition from 6 to 3 is $(1-p_H'')\lambda_H'$. It is evident that signaling system has only two states: Availability and Hazard. If the operator's errors are hazardous, the man-machine interface may operate hazardously but there are no safety stands. Under the safety condition of machinery the operator introduces commands and the synergy works although by another technology: through the reserve control (RC).

This setting is specific for signaling and distinguishes the MMI safety problem under examination from the reliability of man-machine systems as a whole.

To obtain the analytical model of the MMI safety, it is necessary to present the graph from Fig.5 in generalized form [5]. All presented states could be presented through only two states of the generalized graph: interface Availability state A_{MMI} and interface Hazard state Hd_{MMI}. The probability of A_{MMI} state is the sum of probabilities for each of partial state involved in its set. Each partial state is a product $W_{pc} = W_{iH}W_{jM}$ of the probabilities of two components – the operator (man) and the machine should be in a state relevant to partial (ij), where:

$i \in \{H_A, H_{Hd}, H_s\}$

$j \in \{M_A, M_{Hd}, M_S\}$

The availability of the man-machine interface after time $t \to \infty$ to safety operation is the sum of probabilities of its stay in states 4, 5, 7 and 8:

$$K_{A.MMI} = P_A K_{AM} + P_A K_{SM} + P_S K_{AM} + P_S K_{SM} = (P_A + P_S)(K_{AM} + K_{SM}) \quad (1)$$

After time $t \to \infty$ the man-machine interface will operate hazardously in compliance with the sum of probabilities of its state in states 1, 2, 3, 6 and 9.

$$K_{dMMI} = K_{Hd} + P_{HdH}(K_{AM} + K_{SM}) \qquad (2)$$

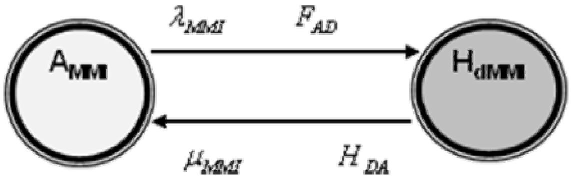

Fig.6. Generalized model of the graph (from Fig.5)

The mean time $MTBHF_{MMI}$ between the MMI hazard failures can be found as a reciprocal value of frequency F_{HdMMI} of the entrance in a hazardous state (Fig.6). The frequency F_{HdMMI} is a sum of all partial frequencies of the entrance.

From the graph and the equations mentioned in Fig.5 it is possible to find out:

$$\begin{aligned} F_{HdMMI} &= K_A\{K_{AM}[(1-p_H)\lambda_H' + (1-p)\lambda] + \\ &+ K_{SM}(1-p_H')\lambda_H''\} + K_S K_{AM}(1-p)\lambda \end{aligned} \qquad (3)$$

For the mathematical expectation of the time between the man-machine interface hazard failures it is obtained:

$$MTBHF_{MMI} = \\ = \frac{1}{K_A\{K_{AM}[(1-p_H)\lambda_H' + (1-p)\lambda] + K_{SM}(1-p_H')\lambda_H''\} + K_S K_{AM}(1-p)\lambda} \qquad (4)$$

It is assumed that the data about the machine have been obtained by solving the problem according to the previous models. The particular values of intensity of human errors are the study subject in the particular case of MMI. Some data, which can be used as a base for calculations, can be found in special references.

IV. Conclusion

In this paper the question of reliability and safety of the man-machine interface (MMI) in signaling systems has been raised:

1) The MMI has been summarized as a structure of ergosystem, which reconfigures itself after a failure.
2) The man-operator's behavior has been defined from the viewpoint of reliability and safety of the man-machine synergy.
3) Modeling based on the Markov chains tools has been proposed.
4) A graph model, which allows deducing analytical equations to establish quantitative dependency on indicators influencing on reliability and safety

References

[1] Hollnagel, E. *Human reliability analysis: Context and control. London*, Academic Press, 1993.

[2] Kirwan B., *A Guide To Practical Human Reliability Assessment* (Hardcover), Taylor & Francis, 1990.

[3] Savie S., Vukovic L., Andelkovic B. *Human operator as a risk factor in technological system*, Proceedings of III International Conference "Risk in Technological Systems and the Environment", Faculty of Occupational Safety, Niš, 1997.

[4] Apostolov, Evg., S. Minkov, *Dependability of the man-machine system*, Medicine and Sports, Sofia, 1980

[5] Христов Хр., *Основи на осигурителната техника*. Техника, София, 1990 (Hristov, Hr. Fundamentals of Signaling Techniques, Tehnika, Sofia, 1990).

[6] John Aitken, *Wide Communication System for Rail Operators*, IRSE Technical Convention Australia, Adelaide, 2003.

[7] Baranyi E., Gábor Racz, Géza Szabo and Balázs Saghi, *Traffic and Interlocking simulation I Railway operation: theory and practical solutions*. Periodica polytehnika ser. Transp. Eng. Vol. 33, No. 1–2, pp. 177–185, 2005.

[8] Embrey David. *Qualitative and quantitative evaluation of human error in risk assessment. Human Factors for Engineers*, Chapter 8, Institution of Engineering and Technology, London, (pp.151-201

[9] Sandom, Carl. *Safety assessment and human factors*, Chapter 14, Human Factors for Engineers, Institution of Engineering and Technology, London, (pp.333-347), 2004

[10] P. Barger, W. Schön & M. Bouali. A study of railway ERTMS safety with Colored Petri Nets, The European Safety and Reliability Conference (ESREL'09), Prague : Czech Republic (2009)