RISK ANALYSIS OF TRANSPORT SYSTEMS

Zbigniew Smalko

Air Force Institute of Technology
Księcia Bolesława 6, 01-494 Warsaw 46, Poland
tel. +48 22 685 20 05, fax: 4822 836 44 71
e-mail: zbigniew.smalko@itwl.pl; smalko@it.pw.edu.pl

Abstract

It is assumed that the decision analysis is to be used to create rational premises of safe operation of controlled systems under uncertainty conditions. Diagnosis & Decision System is described on the system which consists of the environment diagnostic facilities human being controlled system. The function of this system is to recognise dangerous operating situations and to generate a warning that some danger might occur as well as to create rational premises for prevention of incorrect decisions that are made during the operation of the controlled system. The processing of messages is carried out in compliance with the conventional Calculus of logic including the double negation law. The Diagnosis & Decision model presented in this paper is universal to a great extent. The block diagram of the diagnosis & decision system, tree of events in a DD system, message creation tables are presented in the paper. The block diagram of the diagnosis & decision system includes Environment, Controlled System, Human Being (Operator, Diagnostician), Diagnostic Facilities, Controlled System or Environment Output State, Hazard Symptom, Warning Signal, Operation Decision. Tree of Events includes occurrence of a controlled system inoperativity or operativity state, presence or absence of: a symptom, a signal; controlled system operation permitting or inhibiting decision, message identity or negation processing law. Message Creation Tables includes presence or absence of: a false symptom, a true symptom, a false alarm, a true ALARM; correct or incorrect: permission, controlled system operation inhibition.

Keywords*: ...*

1. Introduction

The risk analysis discussed in this paper is concerned with the operation of transportation systems where both controlled systems and natural environment occur.

It is assumed that the decision analysis is to be used to create rational premises of safe operation of controlled systems under uncertainty conditions[1]. To be more particular, the lowering of the risk[2] of the decisions-making[3] with respect to the operation of the plants in severe internal and external circumstances[4] is the goal.

2. Diagnosis & Decision System

Possibility of breakdown and/or *catastrophe*[5] is the basic hazard in reaching the objectives (tasks). To this end, a Diagnosis & Decision System DD similar to that shown in Fig. 1 is described on the EFHS system which consists of the environment (F) - diagnostic facilities (H) - human being (C) – control-led system (S).

---

[1]*Condition**s*** are to be understood as limiting circumstances that define the manner in which the controlled system operates in the environment.

[2]*Risk* is to be understood as a possibility to make an incorrect decision resulting in responsibility for damages and loses to which the operator and others might be endangered.

[3]*Decision-making* depends on selection of one of possible approaches to the objective (project).

[4]*Circumstances* are to be understood as the situation created by coincidence of various events.

[5]*Breakdown* is to be understood as a damage to the controlled system resulting in system's disability or reduced operativity. *Catastrophe* is understood as a collision of the controlled system and the environment resulting in huge damage including critical ones.

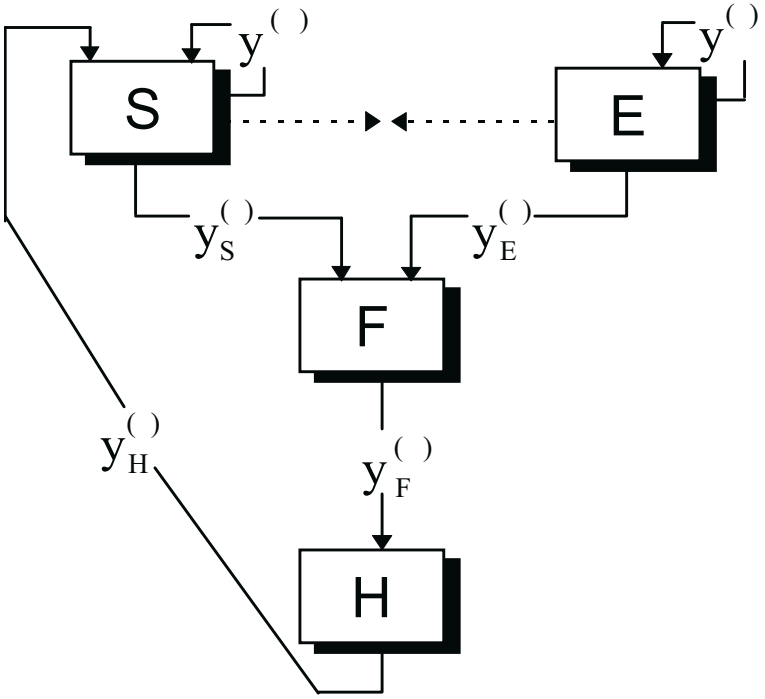

Fig. 1. Block Diagram of the Diagnosis & Decision System

Legend: E - Environment, S - Controlled System, H - Human Being (Operator, Diagnostician), F - Diagnostic Facilities, y_E - Controlled System Or Environment Output State, y_S - Hazard Symptom, y_F - Warning Signal, y_H -Operation Decision.

The function of this system is to recognise dangerous operating situations and to generate a warning that some danger[6] might occur as well as to create rational premises for prevention of incorrect decisions that are made during the operation of the controlled system.

The states of controlled system and its environment are described by a set of features for which defined requirements[7] are formulated.

The qualitative requirements for the DD system under discussion are formulated as follows. The controlled system should present defined diagnostic ability providing means of recognition of its inoperativity symptoms. The diagnostic facilities should enable the accurate conversion of the symptoms into warning signals to be provided. The operator (diagnostician) should take the proper decisions efficiently on the grounds of the received signals or of the absence of signals.

A dynamic model of such a system is presented in the form of a tree of events in Fig. 2. The Diagnosis & Decision processes depend upon conversion and processing of the messages in the DD system.

The processing of messages is carried out in compliance with the conventional Calculus of logic including the double negation law. By using this law, the contradictory messages are reduced in pairs. For results of such a procedure refer to the message creation tables in Fig. 3.

Defined periodical random circumstances are superimposed onto these procedurally-accurate proceedings. The inoperativity of the controlled system can or cannot be recognised owing to its random destruction process. The diagnostic facilities might be unreliable[8] owing to the random variations in the controlled system performance. The human beings (operator, diagnostician) might

[6]*Danger* is to be understood as circumstances that create a peril for somebody or something. *Hazard* is to be understood as a possibility of being cast in damages and loses.
Dangerous is to be understood as able to create damage.

[7]*Requirements* are to be understood as demands concerned with the maintenance of an allowable state by the controlled system and/or operation of the controlled system in a prescribed manner in allowable circumstances.

[8]*Unreliability* is to be understood as a feature consisting in ability to fail and, in consequence, to loss of its operating capabilities.

fail too owing to various randomly-variable load factors[9]. Thus disturbances that are incorrect-decision-making-friendly might occur in a Diagnosis & Decision process.
This is illustrated in the message creation tables in Fig. 3. Tab. 1 presents the recognition of controlled system state, Tab. 2 presents the warning integrity, and Tab. 3 presents the decision-making correctness.

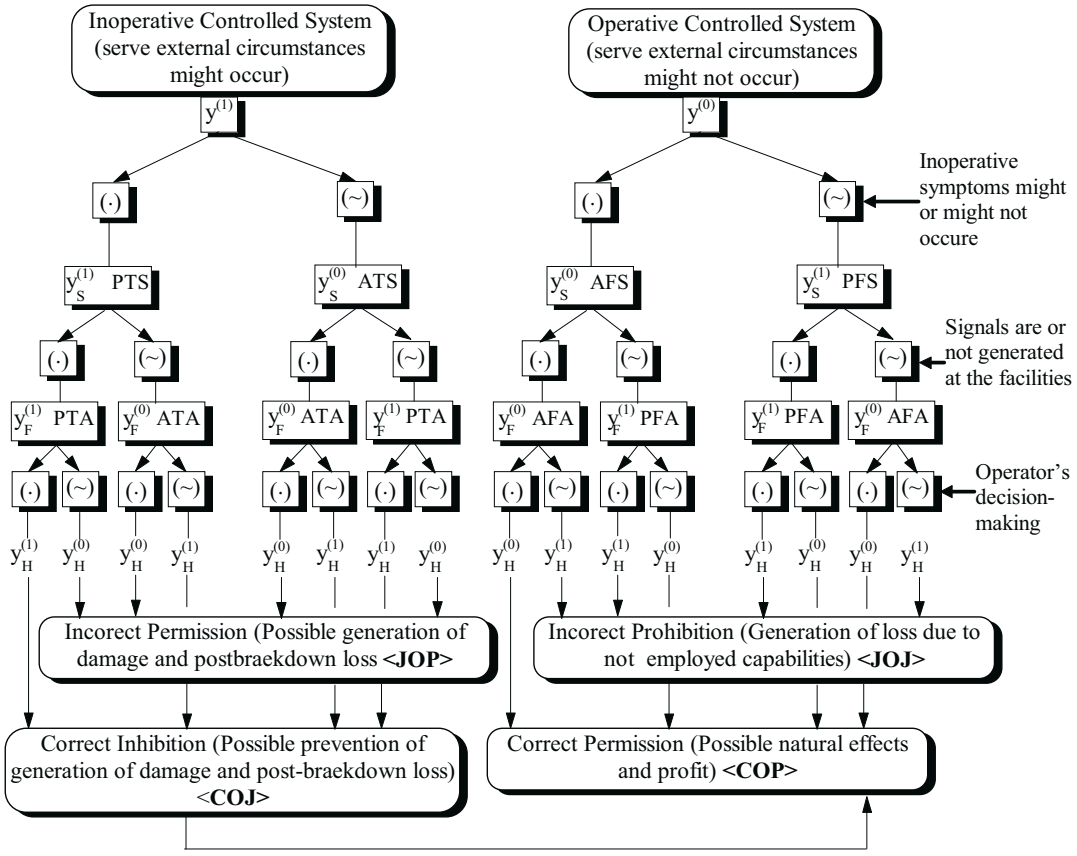

Fig. 2. Tree of Events in a DD System

Legend: $y^{(1)}$, $y^{(0)}$- Occurrence of a controlled system inoperativity or operativity state, respectively, $y_S^{(1)}$, $y_S^{(0)}$ *- Presence or absence of a symptom, respectively,* $y_F^{(1)}$, $y_F^{(0)}$ *- Presence or absence of a signal, respectively,),* $y_H^{(1)}$, $y_H^{(0)}$ *- Controlled system operation permitting or inhibiting decision, respectively, (•), (~) - Message identity or negation processing law, respectively, For the explanations of acronyms refer to Fig. 3.*

3. Statistical decision analysis

By assuming that the proper statistic values[10] are known, a number of quantitative measures can be defined according to the DD system tasks. These are to be used for performing the statistic decision analysis.

A formal discussion of making human errors of the 1-st and 2-nd types can be presented in the following way.[11]

[9]*Factor* is to be understood as one of the causes resulting in a defined effect or as a system component which forms or conditions something.

[10]*Expert data* intended to establish the defined scale of the *subjective similarities* (say, those improbable, not very probable, little probable, probable, highly probable, very highly probable, fully probable) and assigned with their numerical values of 0 to 1 can be employed too.

[11]*Human error of 1-st type* is to be understood as an error depending on rejection of a true statistic hypothesis. *Human error of 2-nd type* is to be understood as an error depending on acceptance of a false statistic hypothesis.

Table 1

	$y_S^{(0)}$	$y_S^{(1)}$
$y^{(0)}$	**AFS**	**PFS**
$y^{(1)}$	**ATS**	**PTS**

Table 2

	$y_F^{(0)}$	$y_F^{(1)}$
$y_S^{(0)},y^{(0)}$ $y_S^{(1)},y^{(0)}$	**AFA**	**PFA**
$y_S^{(0)},y^{(1)}$ $y_S^{(1)},y^{(1)}$	**ATA**	**PTA**

Table3

	$y_H^{(0)}$	$y_H^{(1)}$
$y_F^{(1)}, y_S^{(1)},y^{(1)}$ $y_F^{(0)}, y_S^{(1)},y^{(1)}$ $y_F^{(0)}, y_S^{(0)},y^{(1)}$ $y_F^{(1)}, y_S^{(0)},y^{(1)}$	**JOP**	**COJ**
$y_F^{(0)}, y_S^{(0)},y^{(0)}$ $y_F^{(1)}, y_S^{(0)},y^{(0)}$ $y_F^{(1)}, y_S^{(1)},y^{(0)}$ $y_F^{(0)}, y_S^{(1)},y^{(0)}$	**JOJ**	**COP**

Fig. 3. Message Creation Tables

Legend: DFS, AFS - Presence or absence of a false symptom, respectively, DTS, ATS - Presence or absence of a true symptom, respectively, DFA, AFA - Presence or absence of a false alarm, respectively, DTA, ATA - Presence or absence of a true ALARM, respectively, JOP, COD - Correct or incorrect permission, respectively, JOJ, COJ- Correct or incorrect controlled system operation inhibition.

A risk α of false inhibition of operation of an operative controlled system in circumstances that are not dangerous (human error of 1-st type) can be described in the following way:
owing to inefficiency of human being

$$\alpha_{JOJ} = P\left(y_H^{(1)} | y_F^{(0)}, y_S^{(0)}, y^{(0)}\right), \quad (1)$$

owing to incorrectness of facilities

$$\alpha_{JOJ} = P\left(y_H^{(1)} | y_F^{(1)}, y_S^{(0)}, y^{(0)}\right), \quad (2)$$

owing to lack of diagnostic ability

$$\alpha_{JOJ} = P\left(y_H^{(1)} | y_F^{(1)}, y_S^{(1)}, y^{(0)}\right). \quad (3)$$

A risk β of false permission of operation of an inoperative operative controlled system in circumstances that can be dangerous (human error of 2-nd type) can be described in the following way:
owing to inefficiency of human being

$$\beta_{JOP} = P\left(y_H^{(0)} | y_F^{(1)}, y_S^{(1)}, y^{(1)}\right), \quad (4)$$

owing to incorrectness of facilities

$$\beta_{JOP} = P\left(y_H^{(0)} | y_F^{(0)}, y_S^{(1)}, y^{(1)}\right), \quad (5)$$

owing to lack of diagnostic ability

$$\beta_{JOP} = P\left(y_H^{(0)} | y_F^{(0)}, y_S^{(0)}, y^{(1)}\right), \quad (6)$$

where:
$y_H^{(1)}, y_H^{(0)}$ - decisions that inhibit and permit operation of the controlled system, respectively.

By making an error of 2nd type, the effects can be inestimable and result in huge damages and losses[12]

By making an error of 1st type, the effects are not confined in material damages but they can result in a defined loss of money due to the work that could be done owing to the available capabilities but has been not done.

4. Conclusions

The Diagnosis & Decision model presented in this paper is universal to a great extent. It provides grounds for applying the decision analysis to a number of plants operated under uncertainty conditions.

Denotations

y_F - State of facilities,
y_H - State of operator,
y_S - State of controlled system,
y_E - State of extend circumstances,
α - Human error of 1-st type,
β - Human error of 2-nd type.

References

[1] Blanchard, B. S., Fabrycky, W. J., *Systems Engineering and Analysis*, Prentice Hall, New York 1990.
[2] Eide, A. R., Jenison, R. D., Mashow, L. H., Northup, L. L., *Engineering Fundamentals and Problem Solving,* Mc Graw Hill Co., New York 1979.
[3] Hall, A. D., *Podstawy Techniki Systemów*, PWN Warsyawa, A Methodology for Systems Engineering, Van Nostrand Co., New York 1962.
[4] Hall, A. D., *Metasystems Methodology - A New Systhesis and Unification*, Pergamon Press, New York 1989.
[5] Hicks, P. E., Introduction to Industrial Engineering and Menagement Science, Mc Graw Hill, New York 1977.
[6] Mothes, J., *Sytuacje niepewne a podejmowanie decyzji w przemyśle*, WNT, Warszawa 1972.
[7] Raiffa, H., *Decisions Analysis*, Addison-Wesely. California, London, Ontario 1968.
[8] Smalko, Z. *Definiteness of the statistical inference in diagnostic processes. Statistical monitoring and control of the required technical condition*. Archives of Transport, Vol. 6, Issue 1-4, Warsaw 1994.
[9] Smalko, Z., *Pięć podstawowych pojęć w technice*, Komitet Naukoznawstwa PAN.1987.
[10] Smalko, Z., *The basic maintenance strategies of machines and equipment*, Archives of Transport. Quarterly Polish Academy Sciences, Committee of Transport, 1 Vol. 3, Warsaw 1991.
[11] Taha, H. A. *Operations research,* Macmillan Publishing Co, New York 1982.
[12] Waelchli, F., *Eleven Theses of General System Theory (GST),* System Research, Vol. 9, No. 4, pp. 3-8 1992.

[12] *Damage* is to be understood as a loss in value (harm, destruction) experienced by somebody or something. *Loss* is to be understood as that which is lost with respect to both natural and financial aspects.

"The author's reward was sponsored by Society of Collective Management of Copyrights of Creators of Scientific and Technical Works KOPIPOL with registered office in Kielce with duties obtained on the ground of the art. 20 and art. 20^1 of law on copyrights and related rights."