RELATION BETWEEN STRUCTURES OF AN INTERLOCKING SYSTEM AND TEST DIAGNOSTICS REQUIREMENTS[1]

Karol RÁSTOČNÝ and Jiří ZAHRADNÍK

Department of Information & Safety Systems
Faculty of Electrical Engineering
University of Žilina, Vel'ký diel, 010 26 Žilina, Slovakia
Fax: +421 89 5252241, e-mail: {rastoc|zahra}@fel.utc.sk
Phone: +421 89 5133-250

Received: June 30, 1999

Abstract

In the development phase of an interlocking system realised as a two-channel system with SW comparison and feedback, there is necessity to define maximum fault detection-plus-negation times on the base of known reliability parameters and to support them by an appropriate way of test diagnostics. Using example of the analysis of a two-channel system with two switching points and feedback and a two-channel system with three switching points and feedback, in the paper there is discussed an influence of a choice of the interlocking system structure on maximum fault detection-plus-negation times. For better understanding, in the paper there are given values of maximum detection-plus-negation times for faults of considered system elements that are calculated using the values of fictitious element failure rates.

Keywords: interlocking system, hazardous state, fault detection, test diagnostics.

1. Introduction

Railway traffic control is attended by a risk of hazard situations caused by failure of an interlocking system that can lead not only to material but also human damages and losses. For that reason the interlocking system must be designed in such a way that even under faulty conditions it performs required functions exactly according to the pre-defined algorithm, in accordance with safety requirements. Measures taken to ensure this system behaviour can be applied on the system level or on the level of functional units and system elements. On the system level a choice of an appropriate system structure is the main matter. Measures applied on the level of functional units and elements aim mainly at detection of a fault and negation of its effects. The maximum detection-plus-negation times for individual faults can only be calculated on the base of the analysis of fault effects on system safety with known reliability parameters of system elements and known safety requirements to the system or its part.

[1] The paper is elaborated with support of the grant VEGA No 1/5230/98 'Theoretical Apparatus for Safety Analysis of the System with Defined Level of Safety'

The analysis of fault effects on system safety can be performed for example with the use of the *Fault Tree Analysis* (FTA). The readers not too familiar with the FTA can be referred e.g. to the paper (LEE, W. S. et al, 1985). The FTA is a deductive method of the analysis aimed at the exact identification of causes and their combinations that can bring about the defined top event. The top event may represent inception or existence of hazardous conditions or inability of the system to perform required functions. If the fault tree contains n primary events and u_i is the state indicator of the i^{th} primary event ($i = 1, 2, \ldots, n$), then the relationship between primary events of the fault tree and the top event can be described by the logical function:

$$\psi(\boldsymbol{u}) = \coprod_{j=1}^{m} R_j(\boldsymbol{u}) \, , \tag{1}$$

where $R_j(\boldsymbol{u})$ is a logical function of the j^{th} minimal cut, m is a number of the minimal cuts and $\boldsymbol{u} = (u_1, u_2, \ldots u_n)$ is a vector of the primary events. Then the binary order of the primary event states and the top event state is as follows:

$$\begin{aligned} u_i &= 1, && \text{if the primary event has occurred},\\ u_i &= 0, && \text{if the primary event has not occurred},\\ \Psi(\boldsymbol{u}) &= 1, && \text{if the top event has occurred},\\ \Psi(\boldsymbol{u}) &= 0, && \text{if the top event has not occurred}. \end{aligned} \tag{2}$$

On the base of the known logical function (1) a methodology given in the standard (ENV 50 129, 1998) can be used to calculate detection-plus-negation time for a fault of the system element. The method is based on the following premises, concerning the fault effects on system safety:

- No single fault can cause a hazardous state occurrence.
- If simultaneous faults of two mutually independent elements can be hazardous then the detection-plus-negation time should not exceed the value

  $$t_0 = \frac{1}{1000 \cdot s}, \tag{3}$$

  where s is the sum of the failure rates of elements or their parts whose simultaneous malfunctioning could be hazardous.
- If simultaneous faults of three mutually independent elements can be hazardous and there is no possible hazardous combination of faults of two elements, then the detection-plus-negation time of a fault of the element should not exceed the value

  $$t_0 = \frac{2}{s} \, . \tag{4}$$
- If simultaneous faults of four mutually independent elements can be hazardous and there is no possible hazardous combination of faults of three elements and the sum of the failure rates of considered elements $s \leq 2 \cdot 10^{-4} \, h^{-1}$, then the system need not include any mechanism for detection of these faults.

Usability of this methodology for the analysis of fault effects on the interlocking system is discussed e.g. in the works (SZABÓ, G. and TARNAI, G., 1999) and (RÁSTOČNÝ, K., 1998).

The paper refers to the coherence of the system structure and requirements for test diagnostics, all on the platform of the comparison of two different structures of the two-channel system with software comparison and feedback. It is a typical problem that must be solved, e.g. in relation with control of external (peripheral) elements of interlocking and signalling equipment (signal bulb, point operating device, etc.).

2. Two-Channel System with Software Comparison and Feedback

The interlocking system with composite fail-safety is involved whose required function is realised double. Correct and safe operation is conditional on correspondence of results, mutual independence of processes, in-time detection and negation of a fault.

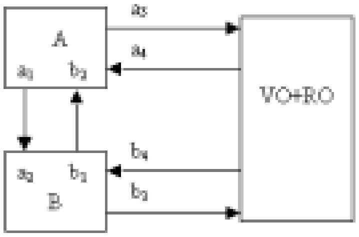


Fig. 1. Two-channel system with software comparison and feedback

The heart of the matter of the two-channel system with software comparison (*Fig. 1*) can be characterised in the following way:

- Both in the unit A and B there is performed software comparison of output signal values from the units A and B of the interlocking system ($a_1 = b_2$, $a_2 = b_1$).
- In the case of successful comparison operation each unit separately issues the command a_3, b_3 to the controlled object RO.
- The state of the controlled object and correct operation of the system are also checked on the base of evaluating signals a_4, b_4.

The output part of the system VO (an interface between A, B and the controlled object RO) can be realised using standard electronic elements, special elements with inherent fail-safety or with their combinations. Required characteristics of elements used in the chosen structure of the two-channel system with software comparison and feedback can result from the safety analysis.

2.1. System with Two Switching Points and Feedback

The units A and B connect the controlled object RO to the power source. Connecting and disconnecting the controlled object RO to/from the power source (terminals $Z1$, $Z2$) are realised through the switches S_A and S_B, directly controlled by commands from the units A, B (*Fig. 2*). The only information given to the units A and B from current sensors P_A and P_B is information whether the electric current flows through the controlled object or not. The individual states of the switches S_A and S_B are monitored by an appropriate test procedure.

If the faulty connection of the controlled object RO to the power source (top event $\boldsymbol{O}$) at time when it should be disconnected is considered hazardous then the fault tree describing behaviour of the structure shown in *Fig. 2* with faulty conditions of individual elements (*Fig. 3*) can be built. In the process of making a tree there is considered a fact that due to faulty information from the sensor $P_A(P_B)$ the unit $A(B)$ can generate faulty command to the switch $S_A(S_B)$. This fault may be hazardous if occurring simultaneously with a fault in the latter channel.

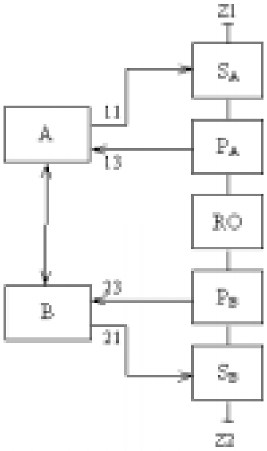


Fig. 2. Two-channel system with two switching points and feedback

Following states of the top and primary events according to (2) the logical function for faulty conditions of the two-channel system with two switching points can be expressed as:

$$\begin{aligned} \boldsymbol{O} = \boldsymbol{A}\cdot\boldsymbol{B} + \boldsymbol{A}\cdot\boldsymbol{S}_B + \boldsymbol{B}\cdot\boldsymbol{S}_A \\ +\boldsymbol{S}_A\cdot\boldsymbol{S}_B + \boldsymbol{A}\cdot\boldsymbol{P}_B + \boldsymbol{B}\cdot\boldsymbol{P}_A + \boldsymbol{S}_A\cdot\boldsymbol{P}_B + \boldsymbol{P}_A\cdot\boldsymbol{S}_B + \boldsymbol{P}_A\cdot\boldsymbol{P}_B, \end{aligned} \qquad (5)$$

where $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{S}_A$, $\boldsymbol{S}_B$, $\boldsymbol{P}_A$, $\boldsymbol{P}_B$ are the primary events of elements (unit A, unit B, switch S_A, switch S_B, sensor P_A, sensor P_B) of the structure under consideration.

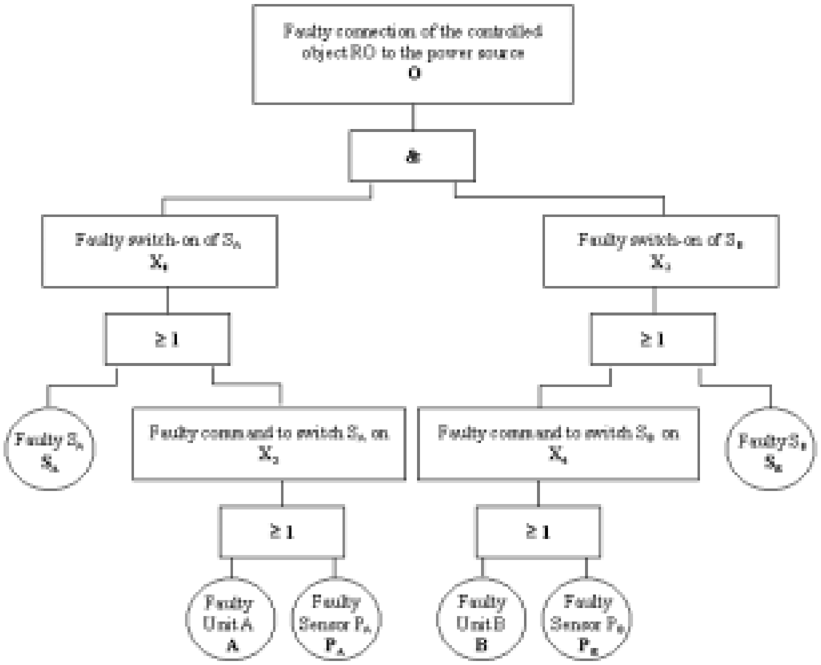

Faulty connection of the controlled object RO to the power source
O
&
Faulty switch-on of S_A
X_1
Faulty switch-on of S_B
X_2
≥ 1
≥ 1
Faulty S_A
S_A
Faulty command to switch S_A on
X_3
Faulty command to switch S_B on
X_4
Faulty S_B
S_B
≥ 1
≥ 1
Faulty Unit A
A
Faulty Sensor P_A
P_A
Faulty Unit B
B
Faulty Sensor P_B
P_B

Fig. 3. Fault tree of the two-channel system with two switching points and feedback

On the base of known logical function (5), in accordance with the standard ENV 50 129, the following facts can be declared:

1. All system elements are safety related.
2. System safety can be based on technique of composite fail-safety provided that:
   - The element A is independent of elements B, S_B, P_B.
   - The element B is independent of elements A, S_A, P_A.
   - The element S_A is independent of elements B, S_B, P_B.
   - The element S_B is independent of elements A, S_A, P_A.
   - The element P_A is independent of elements B, S_B, P_B.
   - The element P_B is independent of elements A, S_A, P_A.
   - Under faulty conditions of the element A the system will get to the safe state within the time

$$t_{OA} = \frac{1}{1000 \cdot (\lambda_A + \lambda_B + \lambda_{SB} + \lambda_{PB})}.$$

- Under faulty conditions of the element S_A the system will get to the safe state within the time

$$t_{OSA} = \frac{1}{1000 \cdot (\lambda_{SA} + \lambda_B + \lambda_{SB} + \lambda_{PB})}.$$

- Under faulty conditions of the element P_A the system will get to the safe state within the time

$$t_{OPA} = \frac{1}{1000 \cdot (\lambda_{PA} + \lambda_B + \lambda_{SB} + \lambda_{PB})}.$$

- Under faulty conditions of the element B the system will get to the safe state within the time

$$t_{OB} = \frac{1}{1000 \cdot (\lambda_B + \lambda_A + \lambda_{SA} + \lambda_{PA})}.$$

- Under faulty conditions of the element S_B the system will get to the safe state within the time

$$t_{OSB} = \frac{1}{1000 \cdot (\lambda_{SB} + \lambda_A + \lambda_{SA} + \lambda_{PA})}.$$

- Under faulty conditions of the element P_B the system will get to the safe state within the time

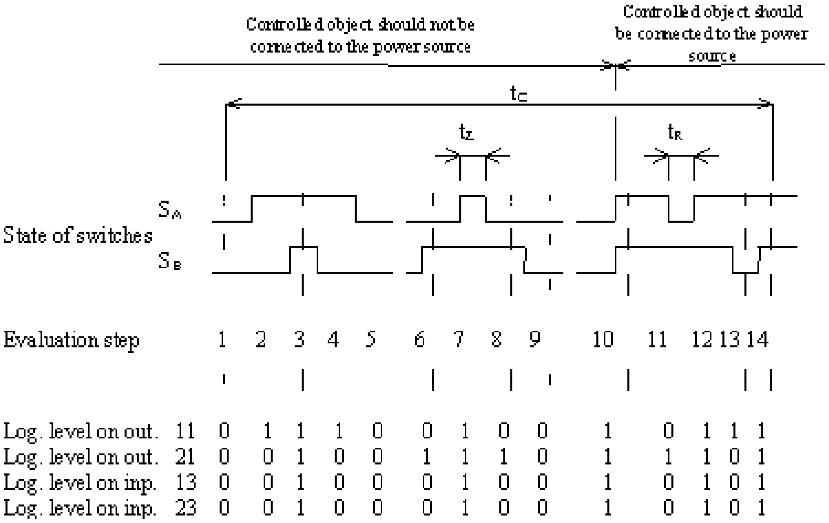
$$t_{OPB} = \frac{1}{1000 \cdot (\lambda_{PB} + \lambda_A + \lambda_{SA} + \lambda_{PA})}.$$

  where λ_A is the failure rate of the element A, λ_B is the failure rate of the element B, λ_{SA} is the failure rate of the element S_A, λ_{SB} is the failure rate of the element S_B, λ_{PA} is the failure rate of the element P_A and λ_{PB} is the failure rate of the element P_B.

From the analysis of the scheme in *Fig. 2* it is clear that the fault of the element leading to the faulty switching the switch $S_A(S_B)$ on has no direct effect on system operation. On the other hand, if occurring simultaneously with a fault of other system element this fault can be hazardous. For that reason the system must have a mechanism for fault detection. To get probability of faulty switching the switches on lower or equal to the acceptable value, in the scheme according to *Fig. 2* the switches S_A, S_B must be checked for:

- Their ability to operate within the time period when the controlled object RO is connected to the power source.
- Their operation free of faults (especially faults of the 'switch-on' type) during the time period when the controlled object RO is disconnected from the power source.

Reliable check of switches is conditional on correct operation of the sensors P_A and P_B. Mutual independence of sensors and dynamic mode of their operation is the premise for trustworthiness of provided information. Testing the sensors is associated with a change of the provided signal. To show an example of checking the sensors the test procedure is given in *Fig. 4*.


Controlled object should not be connected to the power source
Controlled object should be connected to the power source
tC
tZ
tR
SA
State of switches
SB
Evaluation step

Evaluation step		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Log. level on out.	11	0	1	1	1	0	0	1	0	0	1	0	1	1	1
Log. level on out.	21	0	0	1	0	0	1	1	1	0	1	1	1	0	1
Log. level on inp.	13	0	0	1	0	0	0	1	0	0	1	0	1	0	1
Log. level on inp.	23	0	0	1	0	0	0	1	0	0	1	0	1	0	1

Fig. 4. Test procedure

In *Fig. 4* operation of the system according to *Fig. 2* is demonstrated during testing it by time-limited commands issued to switch S_A or S_B on during the time when the controlled object RO should be disconnected from the power source and by time-limited commands issued to switch S_A or S_B off during the time when the controlled object RO should be connected to the power source. Given values of logical levels (expected values) characterise the operation of the output circuit being free of fault and stable. Other values of logical levels (different from those given) are evaluated by units A, B and specified as products of faulty output circuit, possibly with more detailed specification. During one test cycle t_C the state of sensors is changed several times (including the time when no controlled object is to be connected to the power source) and ability of both switches to switch off is tested. In the process of testing the sensors the following conditions should be fulfilled:

$$\begin{gathered} t_C < t_0, \\ t_V < t_R < t_{PR}, \\ t_V < t_Z < t_{PZ}, \end{gathered} \tag{6}$$

where

- t_C is the time of test cycle,
- t_0 is the maximum detection-plus-negation time of a fault, calculated on the base of information about failure rates of individual system elements,
- t_V is the time necessary for evaluation of the sensor state,
- t_R is the time necessary for switching the switch off,
- t_Z is the time necessary for switching the switch on,
- t_{PR} is the response time of the controlled object to switching the power off,
- t_{PZ} is the response time of the controlled object to switching the power on.

If for any reason the defined conditions could not be fulfilled during realisation of the system, possible increase of number of switching points should be considered.

2.2. System with Three Switching Points and Feedback

The units A and B connect the controlled object RO to the power source. Connecting and disconnecting the controlled object RO to/from the power source (terminals $Z1$, $Z2$) are realised through the switches S_A, S_B and S_{AB} , directly controlled by commands from the units A, B (*Fig. 5*). The switch S_{AB} is controlled by the AND gate H and switches on provided that both of units have issued commands to switch on. The current sensors P_A and P_B give information to the units A and B only on whether the electric current flows through the controlled object or not. Individual states of the switches S_A and S_B are monitored by an appropriate test procedure. Voltage sensors P_{AA} and P_{BB} give information about the state of the switch S_{AB}.

In *Fig. 4* operation of the system according to *Fig. 2* is demonstrated during testing it by time-limited commands issued to switch S_A or S_B on during the time when the controlled object RO should be disconnected from the power source and by time-limited commands issued to switch S_A or S_B off during the time when the controlled object RO should be connected to the power source. Given values of logical levels (expected values) characterise the operation of the output circuit being free of fault and stable. Other values of logical levels (different from those given) are evaluated by units A, B and specified as products of faulty output circuit, possibly with more detailed specification. During one test cycle t_C the state of sensors is changed several times (including the time when no controlled object is to be connected to the power source) and ability of both switches to switch off is tested. In the process of testing the sensors the following conditions should be fulfilled:

$$\begin{aligned} t_C &< t_0, \\ t_V < t_R &< t_{PR}, \\ t_V < t_Z &< t_{PZ}, \end{aligned} \qquad (7)$$

where

- t_C is the time of test cycle,

- t_0 is the maximum detection-plus-negation time of a fault, calculated on the base of information about failure rates of individual system elements,
- t_V is the time necessary for evaluation of the sensor state,
- t_R is the time necessary for switching the switch off,
- t_Z is the time necessary for switching the switch on,
- t_{PR} is the response time of the controlled object to switching the power off,
- t_{PZ} is the response time of the controlled object to switching the power on.

If for any reason the defined conditions could not be fulfilled during realisation of the system, possible increase of number of switching points should be considered.

2.3. System with Three Switching Points and Feedback

The units A and B connect the controlled object RO to the power source. Connecting and disconnecting the controlled object RO to/from the power source (terminals $Z1$, $Z2$) are realised through the switches S_A, S_B and S_{AB} , directly controlled by commands from the units A, B (*Fig. 5*). The switch S_{AB} is controlled by the AND gate H and switches on provided that both of units have issued commands to switch on. The current sensors P_A and P_B give information to the units A and B only on whether the electric current flows through the controlled object or not. Individual states of the switches S_A and S_B are monitored by an appropriate test procedure. Voltage sensors P_{AA} and P_{BB} give information about the state of the switch S_{AB}.

If the faulty connection of the controlled object RO to the power source (top event $\boldsymbol{O}$) at time when it should be disconnected is considered hazardous then the fault tree describing behaviour of the structure shown in *Fig. 5* with faulty conditions of individual elements can be built (*Fig. 6*).

Following states of the top and primary events according to (2) the logical function for faulty conditions of the two-channel system with three switching points can be expressed as:

$$\begin{aligned}\boldsymbol{O} = \boldsymbol{A}\cdot\boldsymbol{B} + \boldsymbol{A}\cdot\boldsymbol{S}_B\cdot\boldsymbol{H} + \boldsymbol{B}\cdot\boldsymbol{S}_A\cdot\boldsymbol{H} + \boldsymbol{A}\cdot\boldsymbol{S}_B\cdot\boldsymbol{S}_{AB}\\ +\boldsymbol{B}\cdot\boldsymbol{S}_A\cdot\boldsymbol{S}_{AB} + \boldsymbol{S}_A\cdot\boldsymbol{S}_B\cdot\boldsymbol{H} + \boldsymbol{A}\cdot\boldsymbol{P}_B\cdot\boldsymbol{P}_{BB} + \boldsymbol{B}\cdot\boldsymbol{P}_A\cdot\boldsymbol{P}_{AA}\\ +\boldsymbol{S}_A\cdot\boldsymbol{H}\cdot\boldsymbol{P}_B\cdot\boldsymbol{P}_{BB} + \boldsymbol{S}_B\cdot\boldsymbol{H}\cdot\boldsymbol{P}_A\cdot\boldsymbol{P}_{AA} + \boldsymbol{S}_A\cdot\boldsymbol{S}_B\cdot\boldsymbol{S}_{AB}\\ +\boldsymbol{S}_A\cdot\boldsymbol{S}_{AB}\cdot\boldsymbol{P}_B\cdot\boldsymbol{P}_{BB} + \boldsymbol{S}_B\cdot\boldsymbol{S}_{AB}\cdot\boldsymbol{P}_A\cdot\boldsymbol{P}_{AA} + \boldsymbol{P}_A\cdot\boldsymbol{P}_B\cdot\boldsymbol{P}_{AA}\cdot\boldsymbol{P}_{BB},\end{aligned} \tag{8}$$

where $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{S}_A$, $\boldsymbol{S}_B$, $\boldsymbol{S}_{AB}$, $\boldsymbol{H}$, $\boldsymbol{P}_A$, $\boldsymbol{P}_B$, $\boldsymbol{P}_{AA}$ and $\boldsymbol{P}_{BB}$ are the primary events of the elements (unit A, unit B, switch S_A, switch S_B, switch S_{AB}, gate H, sensor P_A, sensor P_B, sensor P_{AA}, sensor P_{BB}) of the structure under consideration.

On the base of the known logical function (7), in accordance with the standard ENV 50 129, the following facts can be declared:

1. All system elements are safety related.
2. System safety can be based on technique of composite fail-safety provided that:

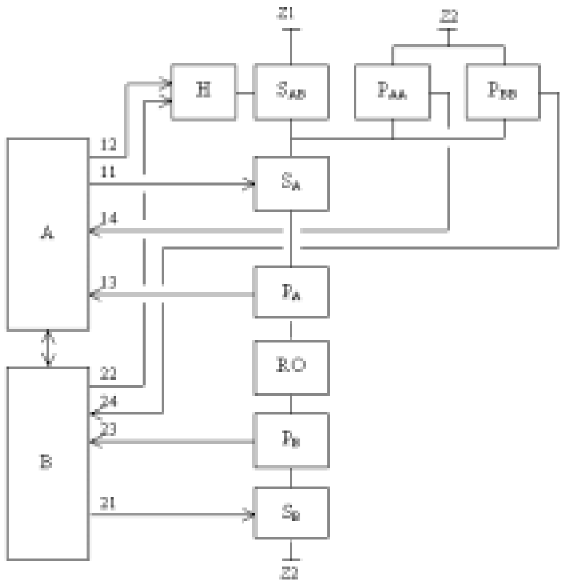


Fig. 5. Two-channel system with three switching points and feedback

- The element A is independent of elements B, S_B, S_{AB}, H, P_B, P_{BB}.
- The element B is independent of elements A, S_A, S_{AB}, H, P_A, P_{AA}.
- The element H is independent of elements A, B, S_A, S_B, P_A, P_{AA}, P_B, P_{BB}.
- The element S_A is independent of elements B, S_B, S_{AB}, H, P_B, P_{BB}.
- The element S_B is independent of elements A, S_A, S_{AB}, H, P_A, P_{AA}.
- The element S_{AB} is independent of elements A, B, S_A, S_B, P_A, P_{AA}, P_B, P_{BB}.
- The element P_A is independent of elements B, S_B, S_{AB}, H, P_B, P_{BB}, P_{AA}.
- The element P_B is independent of elements A, S_A, S_{AB}, H, P_A, P_{AA}, P_{BB}.
- The element P_{AA} is independent of elements B, S_B, S_{AB}, H, P_B, P_{BB}, P_A.
- The element P_{BB} is independent of elements A, S_A, S_{AB}, H, P_A, P_{AA}, P_B.
- Under faulty conditions of the element A or B the system will get to the safe state within the time

$$t_{OA} = t_{OB} = \frac{1}{1000 \cdot (\lambda_A + \lambda_B)}.$$

- Under faulty conditions of the element H the system will get to the safe state within the time

$$t_{OH} = \frac{2}{\lambda_H + \lambda_A + \lambda_B + \lambda_{SA} + \lambda_{SB}}.$$

- Under faulty conditions of the element S_A the system will get to the safe state within the time

$$t_{OSA} = \frac{2}{\lambda_{SA} + \lambda_B + \lambda_H + \lambda_{SAB} + \lambda_{SB}}.$$

- Under faulty conditions of the element S_{AB} the system will get to the safe state within the time

$$t_{OSAB} = \frac{2}{\lambda_{SAB} + \lambda_B + \lambda_A + \lambda_{SA} + \lambda_{SB}}.$$

- Under faulty conditions of the element P_A or P_{AA} the system will get to the safe state within the time

$$t_{OPA} = t_{OPAA} = \frac{2}{\lambda_{PAA} + \lambda_B + \lambda_{PA}}.$$

- Under faulty conditions of the element S_B the system will get to the safe state within the time

$$t_{OSB} = \frac{2}{\lambda_{SB} + \lambda_A + \lambda_H + \lambda_{SAB} + \lambda_{SA}}.$$

- Under faulty conditions of the element P_B or P_{BB} the system will get to the safe state within the time

$$t_{OPB} = t_{OPBB} = \frac{2}{\lambda_{PBB} + \lambda_B + \lambda_{PB}},$$

where λ_A is the failure rate of the element A, λ_B is the failure rate of the element B, λ_H is the failure rate of the element H, λ_{SA} is the failure rate of the element S_A, λ_{SB} is the failure rate of the element S_B, λ_{SAB} is the failure rate of the element S_{AB}, λ_{PA} is the failure rate of the element P_A, λ_{PB} is the failure rate of the element P_B, λ_{PAA} is the failure rate of the element P_{AA} and λ_{PBB} is the failure rate of the element P_{BB}.

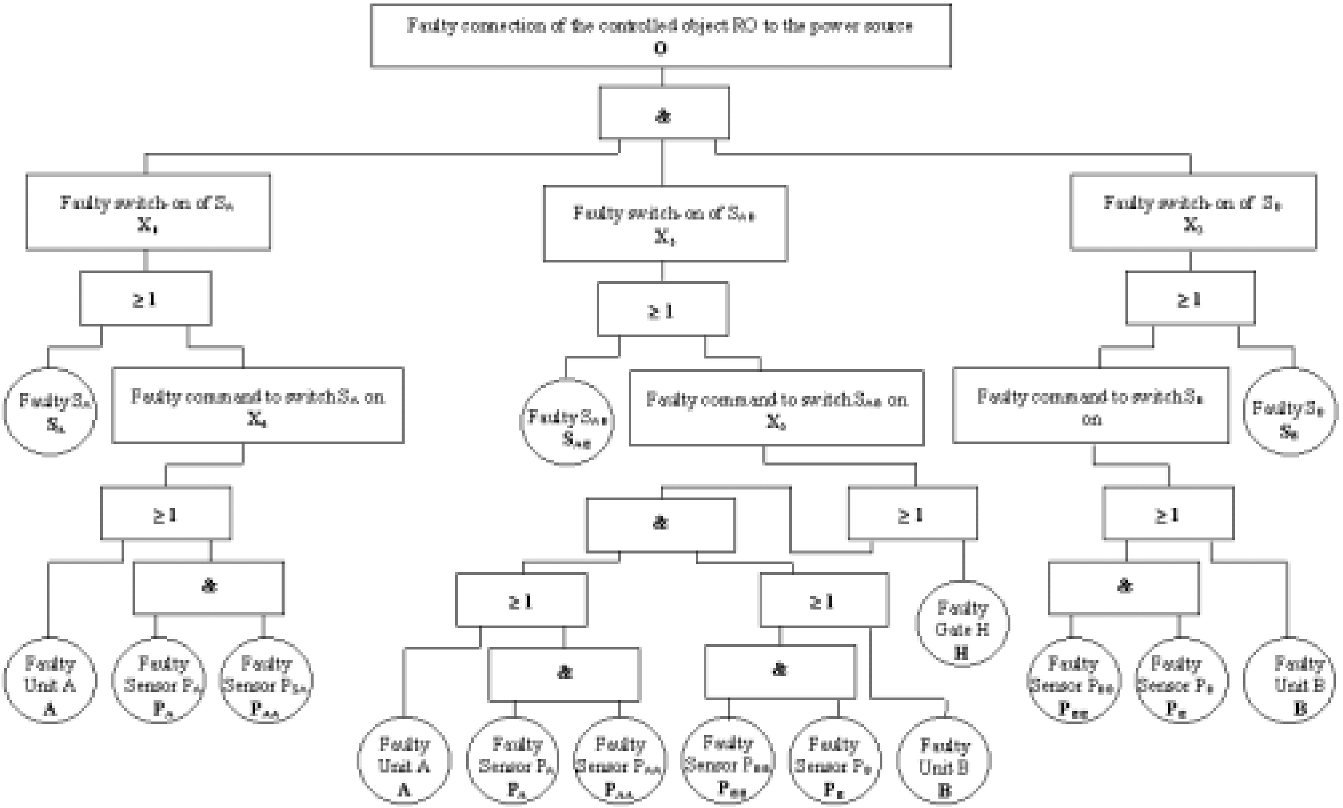


Fig. 6. Fault tree of the two-channel system with three switching points and feedback

3. Conclusions

For better understanding in the *Table 1* there are given values of maximum detection-plus-negation times for element faults of considered systems (*Fig. 2*, *Fig. 5*) calculated on the base of given considerations and the simplifying premise $\lambda_A = \lambda_B = 5E - 5h^{-1}$, $\lambda_{SA} = \lambda_{SB} = \lambda_{SAB} = 1E - 5h^{-1}$, $\lambda_H = 1E - 7h^{-1}$, $\lambda_{PA} = \lambda_{PB} = \lambda_{PAA} = \lambda_{PBB} = 1E - 6h^{-1}$.

Table 1. Maximum detection-plus-negation times for system elements

	Maximum detection-plus-negation time of the element t_0 [h]					
	A, B	S_A, S_B	S_{AB}	H	P_A, P_B	P_{AA}, P_{BB}
System with 2 switching points	9	14	–	–	16	–
System with 3 switching points	10	24752	15384	16638	39840	39840

In the development phase of the system it is necessary to define maximum detection-plus-negation times on the base of known reliability parameters and to design appropriate test diagnostics.

Thanks to a change of the structure better prerequisites for ensuring required system integrity can be created but integrity is one of the system safety attributes only. The other attribute of equal importance is availability of the system. The effect of a change of the structure on availability of the system and its evaluation is not a subject of this paper.

References

[1] Lee, W. S. – Grosh, D. L. – Tillman, F. A. – Lie, C. H. (1985): Fault Tree Analysis, Methods and Applications – A Review, *IEEE Transactions on Reliability*, Vol. R-34, No. 3, pp. 194–203.

[2] Sabó, G. – Tarnai, G. (1999): Dependability Analysis of Interlocking Systems – a Comparison of the Probabilistic and the Deterministic Approaches. *Proc. International Scientific Conference ELEKTRO 99*, Žilina, May 25-26, 1999. Slovak Republic, EDIS Žilina, pp. 7–12.

[3] Rastočný, K. (1998): Models for Safety Analysis of Computer-based Interlocking Systems. *Habilitation thesis*. Žilina, Slovak Republic, 1998. (In Slovak).

[4] ENV 50 129 (1998): Railway Applications: Safety Related Electronic Systems.