Quantitative examples of safety assessment using logical-probabilistic methods

Igor A. Ryabinin*

N.G. Kuznetsov Naval Academy,
Ushakovskaya naberezhnaya, 17/1,
Sankt-Petersburg, Russia
Email: tatiana.migai@mail.ru
*Corresponding author

Alexander V. Strukov

JSC ‘Specialized Engineering Company
SEVZAPMONTAGEAUTOMATICA’,
(JSC SPIK SZMA), St.Petersburg, Russia
Email: alexander_strukov@szma.com

Abstract: The article presents examples of solving the tasks of analysis of safety of complex technical systems by using logical-probabilistic methods (LPM). LPM are characterised by sufficient visualisation and simplicity of formalisation of the hazardous state of the object in the form of the shortest paths of hazardous state or hazardous state scenario. Parametric representation of logical functions (Boolean sum and products of initiating events and initiating conditions) is carried out using the methods of orthogonalisation. Determination of individual and total contribution of events in probability of realisation of a dangerous condition can allow you to plan the activities to ensure the safety state of the object. In this article the examples are being solved with the use of ARBITR software.

Keywords: dangerous state; the shortest path of the dangerous state; an initiating event; an initiating condition; risk assessment; functional integrity schemes; FIS.


Biographical notes: Igor A. Ryabinin is Doctor of Technical Science, Professor, and Professor Emeritus of N.G. Kuznetsov Naval Academy. He is an Honorary Person of Russian Higher Education. He is the Founder of the Logical-Probabilistic Methods of the Structural Complex Systems Reliability. He is a Laureate of the USSR State Prize. He is a Rear Admiral of the Naval Forces, Academician of the Russian Academy of Natural Sciences and New York Academy of Sciences, the International Man of the Year 1993. His research interests include reliability and safety analysis of structurally complex systems, logical-probabilistic interpretation of relations between the mathematical logic and the probability theory.
Quantitative examples of safety assessment

Alexander V. Strukov holds a PhD and he is an Assistant Professor, and Senior Engineer in Research Department, JSC Specialized Engineering Company Sevzapmontageautomatica (SPIK SZMA) St. Petersburg, Russia. His current research includes data analysis, analysis of systems, reliability theory, mathematical models and methods of decision-making support in complex technical-organisational systems.

This paper is a revised and expanded version of a paper entitled ‘Guide in logical and probabilistic calculation’ presented at International Scientific School ‘Modeling and Analysis of Safety and Risk in Complex Systems’, Saint Petersburg, Russia, 25–28 October 2016.

1 Introduction

“There are theories coming and fading away, while the examples remain.”
I.M. Gelfand

A fundamental concept in logical-probabilistic theory of safety (LPTS) is the concept of the system hazardous state (SHS), characterised by large-scale damage (i.e., collapse), and hazards, which can bring the system to hazardous state.

In each case it is necessary to give an analytical description of SHS, which could lead to a collapse. In LPTS this description starts with making a hazardous state scenario, which is carried out by means of sum and products of initiating events (IE) and initiating conditions (IC). IE and IC stand for various internal and external impacts, equipment failures, breach of the rules of operation, transportation, storage, and so on. The main difficulties in LPTS arise when hazardous state scenario (HSS) is prepared by trying all possible system states from top downward: from specific SHS under investigation to the reasons (IE and IC), which are able to cause it.

In LPTS they are interested only in the truth values of statements (true or false), they study the question of the truth values of a complex statement depending on the truth values of its components i.e. simple statements, which are indicated as 1 (true) and 0 (false).

Quantitative safety assessment examples for certain systems published in (Ryabinin, 2000, 2007) are unlikely to be commonly known to international audience due to both the small number of the published books and language barrier.

Risk assessment that system will get into hazardous state can be approached by two sides:

• by developing a model of reliability towards the consideration of possible IE and IC
• by developing an independent safety model that considers possible failures of equipment and personnel.

Without denying that in some cases it’s useful to develop the reliability model towards safety, let’s consider the following examples of the development of independent safety models, taking into account the reliability of its components.

Considering 50-year history of logical-probabilistic methods (LPM) (Ryabinin, 2011, 2015) and the opinion that sometimes the specific examples can teach quicker and more deeply, let us view several such examples.
2 Examples

2.1 Example 1: Risk of the submarine flooding

A hazardous event will be the submarine flooding. The hazardous state scenario with all possible states is shown on Figure 1.1.

Figure 1.1 Hazardous state scenario: flooding of submarine

The initiating events are $z_1$ and $z_2$ – holes in the sections 1 and 2, and the initiating conditions are $z_3$ and $z_4$ – failures (unavailability due to disassembly, etc.) of the pumps P1, P2; $z_5$ – impossibility to access the barrier value of the emergency section.

Let us make a hazardous state function (HSF) using the shortest paths of hazardous operation (SPHO):

$$SPHO_1 = z_1 z_2 z_4, \quad SPHO_2 = z_1 z_3 z_5, \quad SPHO_3 = z_2 z_3 z_5, \quad SPHO_4 = z_2 z_4 z_5;$$

$$y(z_1, \ldots, z_5) = \begin{vmatrix} z_1 & z_3 & z_4 \\ z_1 & z_3 & z_5 \\ z_2 & z_4 & z_5 \end{vmatrix},$$

Let us apply the orthogonalisation algorithm and represent the HSF (1.1) as a sum of disjoint products (SDP)
Quantitative examples of safety assessment

\[ y(z_1, \ldots, z_5) = \begin{bmatrix}
  z_1z_2z_4 \\
  z_1z_3 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4
\end{bmatrix} \]  

(1.2)

Applying to (1.2) De Morgan's theorem we get

\[ y(z_1, \ldots, z_5) = \begin{bmatrix}
  z_1z_2z_4 \\
  z_1z_3 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4
\end{bmatrix} \]  

(1.3)

The result of the inner loop procedure is the disjoint form of matrix (1.3):

\[ y(z_1, \ldots, z_5) = \begin{bmatrix}
  z_1z_2z_4 \\
  z_1z_3 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4 \\
  z_1z_2z_4 \\
  z_1z_3z_5 \\
  z_2z_3z_4
\end{bmatrix} \]  

(1.4)

Now we may define the expression for calculating the submarine submersion risk using notes:

- \( D_i \) probability of dangerous initiating event \( i \)
- \( S_i \) probability of safety initiating event \( i \).

Then

\[ D_c = D_1D_2D_3 + D_1D_3S_4D_5 + S_1D_2D_3D_4 + D_2S_1D_4D_5. \]  

(1.5)
This example is interesting due to the following reasons:

1. it is not possible to formalise the performance of two sections of the submarine
2. it is very easy to formalise the hazardous state of the submarine due to the initiating events \( z_1 \) and \( z_2 \).

Let us consider the weights of the arguments in the functions defined using the Boolean differences of HSF (1.1):

\[
\Delta_{z_1} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_2 & z_1 & z_3 \\
\varphi_2 & z_3 & z_4 \\
\varphi_3 & z_4 & z_5 \\
\end{vmatrix},
\quad (1.6)
\]

\[
\Delta_{z_2} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_1 & z_1 & z_3 \\
\varphi_1 & z_3 & z_4 \\
\varphi_3 & z_4 & z_5 \\
\end{vmatrix},
\quad (1.7)
\]

\[
\Delta_{z_3} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_1 & z_1 & z_2 \\
\varphi_2 & z_2 & z_3 \\
\varphi_3 & z_3 & z_4 \\
\end{vmatrix},
\quad (1.8)
\]

\[
\Delta_{z_4} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_1 & z_1 & z_2 \\
\varphi_2 & z_2 & z_3 \\
\varphi_3 & z_3 & z_4 \\
\end{vmatrix},
\quad (1.9)
\]

\[
\Delta_{z_5} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_2 & z_1 & z_3 \\
\varphi_3 & z_3 & z_4 \\
\varphi_4 & z_4 & z_5 \\
\end{vmatrix},
\quad (1.10)
\]

We may represent the expressions (1.6) to (1.10) as SDP:

\[
\Delta_{z_1} y_i (z_1, \ldots, z_s) = \begin{vmatrix}
\varphi_2 & z_1 & z_3 \\
\varphi_2 & z_3 & z_4 \\
\varphi_3 & z_4 & z_5 \\
\end{vmatrix},
\quad (1.11)
\]
Quantitative examples of safety assessment

Substituting the probabilities 0.5 in the expressions (1.10) and (1.11) provided that

\[ S_i = D_j = 0.5, \ i = 1, m, \]

we will receive the weights \( g_{z_j} \), shown in the Table 1.1.

Using the transformation [2, (6.79), (6.80) and (6.85)], we receive:

\[ D_c = D_{c1}^{(i)} + S_i D_{c,o}^{(i)}, \]

\[ \bar{s}_i = D_{c1}^{(i)} - D_{c,o}^{(i)} \]

\[ B_{zi} = D_c - D_{c,o}^{(i)}, \]

where

\[ D_{c1}^{(i)} = P \{ Y_{c1}^{(i)} (z_1, \ldots, z_m) = 1 \}, \]

\[ D_{c,o}^{(i)} = P \{ Y_{c,o}^{(i)} (z_1, \ldots, z_m) = 1 \}, \]

are the system danger probabilities in case of presence (c1) or absence (c.o) of the \( i \)th initiating event (or condition).

Table 1.1  Weights of the arguments \( z_i \) in the function (1.1)

<table>
<thead>
<tr>
<th>( i )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g_{z_i} )</td>
<td>0.250</td>
<td>0.250</td>
<td>0.375</td>
<td>0.375</td>
<td>0.250</td>
</tr>
</tbody>
</table>

Based on HSF (1.1) in ARBITR software using repeated events the functional integrity scheme (FIS) is built as a compact design model [Figure 1.2(a)]. Figure 1.2(b) shows the results of the analysis of a hazardous state by means of a diagram of initiating events’ importance, the numerical values of which agree with the data in Table 1.1.

Figure 1.2  ARBITR screenshots, (a) FIS (b) diagram of initiating events and conditions

(see online version for colours)

We may define the individual impacts \( B_{zi} \) of initiating event or condition \( z_i \) in the system danger using the formula (1.15), by defining \( D_{c,o}^{(i)} \) and substituting in the expression (1.5) \( D_{zi} = 0 \) and \( S_{zi} = 1 \):
Let us assume that $D_1 = D_2 = 10^{-5}$; $D_3 = 2 \cdot 10^{-3}$; $D_4 = 10^{-3}$. Thus, we will receive the data shown in Table 1.2.

**Table 1.2** Impact of the initiating events $z_i$ in the system danger (1.1)

<table>
<thead>
<tr>
<th>$i$</th>
<th>$B_z \cdot 10^{-10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.198</td>
</tr>
<tr>
<td>2</td>
<td>1.198</td>
</tr>
<tr>
<td>3</td>
<td>2.396</td>
</tr>
<tr>
<td>4</td>
<td>1.396</td>
</tr>
<tr>
<td>5</td>
<td>2.996</td>
</tr>
</tbody>
</table>

$$B_{z5} > B_{z3} > B_{z1} > B_{z4} > B_{z2}, \quad D_c = 3 \cdot 4 \cdot 10^{-10}$$  \hspace{1cm} (1.18)

These results show that the main impact in the system danger is made by the initiating conditions $z_5$ and $z_3$. This could be assumed without making any calculations just based on the initial data

$$D_{z5} > D_{z3} > D_{z4} > D_{z2} = D_{z1}.$$  \hspace{1cm} (1.19)

However, it would be much more difficult to assume that

$$B_{z4} < B_{z1}, \text{ when } D_{z4} \gg D_{z1} \| g_{z4} > g_{z2}.$$  \hspace{1cm} (1.20)

Similar to [2, (6.118)], we receive

$$B_{z4}v_{z4} = D_c - D_{c, z4}^{(i,j)},$$  \hspace{1cm} (1.21)

where

$$D_{c, z4}^{(i,j)} = P\left(Y_{c, z4}^{(i,j)}(z_1, \ldots, z_n) = 1\right)$$  \hspace{1cm} (1.22)

is a probability of the system danger if the 1st and $i$th initiating conditions are missing. Without going into particulars, let us show the calculated total impacts of all ten possible couples (Table 1.3).

**Table 1.3** Consolidated impacts of arguments $z_i$ and $z_j$ in the system danger

<table>
<thead>
<tr>
<th>$i$</th>
<th>$j$</th>
<th>$B_{zij} \cdot 10^{-10}$</th>
<th>$B_{zij}/O_c$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2.3</td>
<td>0.71</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>3.4</td>
<td>1.00</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2.4</td>
<td>0.94</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>3.2</td>
<td>0.94</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>3.4</td>
<td>1.00</td>
</tr>
</tbody>
</table>

In this clear case, the results shown in Table 1.3 might be explained using powers of reason. However, in real systems with a large number of initiating conditions and complex logical connections, it is not possible to define the overall system risk and
Quantitative examples of safety assessment

Impacts of individual initiating conditions and their combinations without using a special theory.

For instance, the theory helps to substantiate the following equations

\[ B_{z_1z_2} = B_{z_1z_4} = B_{z_2z_5} = B_{z_3z_5} = B_{z_4z_5} = D_v \]  

(1.23)

At the logical transformation stage, without using the formula (1.21). In fact, by inverting the HSF (1.1), we will receive a safety state function (SSF)

\[
\overline{y}(\overline{z}_1, \ldots, \overline{z}_5) = \begin{vmatrix}
\overline{z}_1 \overline{z}_2 \\
\overline{z}_1 \overline{z}_4 \\
\overline{z}_2 \overline{z}_4 \\
\overline{z}_3 \overline{z}_5 \\
\overline{z}_4 \overline{z}_5 \\
\end{vmatrix}
\]

(1.24)

Where six minimum cuts of the danger prevention show the products which completely protect the system from any dangers (1.23).

2.2 Example 2: Risk assessment for explosion in the submarine section

It is known that special measures are taken to prevent explosion of the mixture of the hydrogen emissions from batteries and the air. The intensity of the battery gas emissions depends on the battery operation mode, life time, environmental temperature, etc. The hydrogen is discharged using the ventilation system or fired in special chambers. The hydrogen content in the room is continuously controlled by automatic and portable gas analysers.

The explosion will unavoidably occur (Figure 2.1) when the explosive hydrogen content is achieved due to the absence of ventilation (IC: \( z_4 - z_7 \)) or hydrogen control (IC: \( z_1 - z_3 \)), and due to the mixture firing source (IE: \( z_8 - z_{10} \)), \( zi \) - is a logical variable.

Figure 2.1 shows the hazardous state scenario. Generation of this scenario is a creative, the most difficult and non-algorithmic part of the safety analysis. In this case, the hazardous state is hydrogen explosion in the battery room. Such explosion can result (and did it many times) in destruction of personnel and objects, that is, in a damage of big scale.

The philosophical problem of uniqueness and completeness of safety research raises two main questions:

1. Will all specialists give uniqueness of ways the system gets to the hazardous state?
2. Will all circumstances, leading to the explosion, be taken into consideration?

We believe, that we may answer positively to these questions by using mathematical apparatus (LPM) and pragmatic assessment of the scale of the system under consideration (i.e. considering all conditions and assumptions only within the limited volume and limited resources). Wishing to obtain as many as possible concrete recommendations on active protection of the system to avoid getting in a hazardous state, you should not think that the purpose can be reached only by searching of as many as possible initiating events. It would be more correct to move from small to big, i.e. from minimal number of taken into account conditions, added to this core.
In our case, the system ‘core’ would initially cover only events $z_4$, $z_5$, $z_6$, and $z_8$, and secondly we would find other events $z_i$. Broader interpretation is possible for both human errors ($z_1$) and instructions violation cases ($z_7$). However, one should sometimes stop to miss the trees for the wood.

Figure 2.1 Hazardous state scenario: hydrogen explosion

Let us consider the organisational role of mathematical apparatus by generating HSF. If the scenario of the hazardous state was created (Figure 2.1), then the HSF may be shown as a logical matrix of $z_i$ events:

$$y_1(z_1, \ldots, z_{10}) = \begin{vmatrix} z_1 & z_4 & z_5 & z_6 \\ z_2 & z_3 & z_6 & z_9 \\ z_6 & z_{10} \end{vmatrix} \quad (2.1)$$

After opening the brackets (logical multiplication), the HSF will become a disjunction of 12 MPDO:
Quantitative examples of safety assessment

Therefore, the singularity of hydrogen explosion in mixture with the air will comprise 12 event cases.

HSF inversion (2.2) will result in a sum of six minimal cuts sets (MCS):

\[ y_e (z_1, \ldots, z_{10}) = \begin{vmatrix}
    z_1 z_6 z_7 z_8 \\
    z_1 z_8 z_7 z_9 \\
    z_1 z_6 z_7 z_{10} \\
    z_1 z_7 z_8 z_9 \\
    z_1 z_7 z_8 z_{10} \\
    z_1 z_7 z_9 z_{10} \\
    z_2 z_{10} z_8 z_9 \\
    z_2 z_7 z_8 z_{10} \\
    z_2 z_7 z_9 z_{10} \\
    z_2 z_8 z_7 z_9 \\
    z_2 z_8 z_7 z_{10} \\
    z_2 z_8 z_9 z_{10} \\
    z_2 z_9 z_7 z_{10} \\
    z_2 z_9 z_8 z_{10} \\
    z_2 z_9 z_8 z_{10} \\
    z_2 z_9 z_9 z_{10} \\
    z_3 z_{10} z_8 z_9 \\
    z_3 z_7 z_8 z_{10} \\
    z_3 z_7 z_9 z_{10} \\
    z_3 z_8 z_7 z_{10} \\
    z_3 z_8 z_8 z_{10} \\
    z_3 z_9 z_7 z_{10} \\
    z_3 z_9 z_8 z_{10} \\
    z_3 z_9 z_9 z_{10} \\
    z_4 z_{10} z_8 z_9 \\
    z_4 z_7 z_8 z_{10} \\
    z_4 z_7 z_9 z_{10} \\
    z_4 z_8 z_7 z_{10} \\
    z_4 z_8 z_8 z_{10} \\
    z_4 z_9 z_7 z_{10} \\
    z_4 z_9 z_8 z_{10} \\
    z_4 z_9 z_9 z_{10} \\
    z_5 z_{10} z_8 z_9 \\
    z_5 z_7 z_8 z_{10} \\
    z_5 z_7 z_9 z_{10} \\
    z_5 z_8 z_7 z_{10} \\
    z_5 z_8 z_8 z_{10} \\
    z_5 z_9 z_7 z_{10} \\
    z_5 z_9 z_8 z_{10} \\
    z_5 z_9 z_9 z_{10} \\
    z_6 z_{10} z_8 z_9 \\
    z_6 z_7 z_8 z_{10} \\
    z_6 z_7 z_9 z_{10} \\
    z_6 z_8 z_7 z_{10} \\
    z_6 z_8 z_8 z_{10} \\
    z_6 z_9 z_7 z_{10} \\
    z_6 z_9 z_8 z_{10} \\
    z_6 z_9 z_9 z_{10} \\
    z_7 z_{10} z_8 z_9 \\
    z_7 z_7 z_8 z_{10} \\
    z_7 z_7 z_9 z_{10} \\
    z_7 z_8 z_7 z_{10} \\
    z_7 z_8 z_8 z_{10} \\
    z_7 z_9 z_7 z_{10} \\
    z_7 z_9 z_8 z_{10} \\
    z_7 z_9 z_9 z_{10} \\
    z_8 z_{10} z_8 z_9 \\
    z_8 z_7 z_8 z_{10} \\
    z_8 z_7 z_9 z_{10} \\
    z_8 z_8 z_7 z_{10} \\
    z_8 z_8 z_8 z_{10} \\
    z_8 z_9 z_7 z_{10} \\
    z_8 z_9 z_8 z_{10} \\
    z_8 z_9 z_9 z_{10} \\
    z_9 z_{10} z_8 z_9 \\
    z_9 z_7 z_8 z_{10} \\
    z_9 z_7 z_9 z_{10} \\
    z_9 z_8 z_7 z_{10} \\
    z_9 z_8 z_8 z_{10} \\
    z_9 z_9 z_7 z_{10} \\
    z_9 z_9 z_8 z_{10} \\
    z_9 z_9 z_9 z_{10} \\
    z_{10} z_{10} z_8 z_9 \\
    z_{10} z_7 z_8 z_{10} \\
    z_{10} z_7 z_9 z_{10} \\
    z_{10} z_8 z_7 z_{10} \\
    z_{10} z_8 z_8 z_{10} \\
    z_{10} z_9 z_7 z_{10} \\
    z_{10} z_9 z_8 z_{10} \\
    z_{10} z_9 z_9 z_{10} \\
\end{vmatrix} \quad (2.2)

\[ \bar{y}_e (z_1, \ldots, z_{10}) = \begin{vmatrix}
    z_1 \\
    z_2 \\
    z_3 \\
    z_4 \\
    z_5 \\
    z_6 \\
    z_7 \\
    z_8 \\
    z_9 \\
    z_{10} \\
\end{vmatrix}, \quad (2.3)

where \( z_i \) is inversion of \( z_i \).

Table 2.1  Weights of arguments in the function (2.1)

<table>
<thead>
<tr>
<th>( z_i )</th>
<th>( g_{i0} )</th>
<th>( g_{i1} )</th>
<th>( g_{i2} )</th>
<th>( g_{i3} )</th>
<th>( g_{i4} )</th>
<th>( g_{i5} )</th>
<th>( g_{i6} )</th>
<th>( g_{i7} )</th>
<th>( g_{i8} )</th>
<th>( g_{i9} )</th>
<th>( g_{i10} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( z_1 )</td>
<td>0.205</td>
<td>0.068</td>
<td>0.068</td>
<td>0.068</td>
<td>0.068</td>
<td>0.205</td>
<td>0.342</td>
<td>0.049</td>
<td>0.049</td>
<td>0.049</td>
<td>0.049</td>
</tr>
</tbody>
</table>

In this context, the singularity is an opportunity to prevent the explosion by only six minimum sets \( \bar{z}_i \).

The HSF (2.2) and SSF (2.3) show that the event \( z_7 \) (the fan was not started manually) is a part of all 12 MDPO and, at the same time, is the most ‘efficient’ MCS, i.e. \( z_7 \) is absolutely required to create explosive environment, and it will be enough to start the fan at least in manual mode to prevent the explosion (\( \bar{z}_7 \)). Weights of the arguments \( z_i \) are shown in Table 2.1.

Figures 2.2 and 2.3 show sample ARBITR screenshots for the solution of the problem about hydrogen explosion at submarine compartment with the use of ARBITR software (Strukov, 2015; Mozhaev et al., 2013). Hazardous state scenario is shown in Figure 2.2 as a FIS and the results of Birnbaum’s structure importance analysis (Table 2.1) are shown as a diagram in Figure 2.3.
Weighing the initiating events $z_i$ separately, by two, three, etc. allows to evaluate their impact on the hazardous system state occurrence based on their position in HSF (SSF), thus only with consideration of the potential events development logic, which is also important though. The system developers receive a single, unambiguous and easy-explainable result. However, we should remember about huge difference between $O_i$ values — a potential danger from possible occurrence of the initiating event $z_i$ (the values may differ by several orders!).

The efforts to get a more objective evaluation of the initial probabilities of the initiating events $z_i$ are very useful and productive. If these information difficulties are overcome, further development of the structurally complex system safety theory shall be aimed at specifying and précising the actual impact of certain events in SHS (or its prevention).

Let us consider several simple initial data showing our possible perception of their values (Table 2.2).
It is expedient to consider this simple example of the HSF with no argument repetitions without using the orthogonalisation, i.e. identify the explosion risks directly in the following expression (2.1):

\[
D_c = P\left(\begin{array}{c} z_7 \\ z_3 \\ z_4 \\ z_8 \\ z_9 \end{array}\right) = 1 \\
= D_1[1-S_1(1-D_2D_3)]\cdot[1-S_6(1-D_4D_5)]\cdot[1-S_9S_8S_{10}],
\]

where

- \(D_c\)  system danger probability
- \(D_i\)  event \(i\) danger probability
- \(S_i\)  event \(i\) safety probability, \(S_i = 1 - D_i\).

**Table 2.2** Initial hazardous events in the system (2.1)

<table>
<thead>
<tr>
<th>(z_i)</th>
<th>(D_1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(z_1)</td>
<td>(10^{-2})</td>
</tr>
<tr>
<td>(z_2)</td>
<td>(10^{-3})</td>
</tr>
<tr>
<td>(z_3)</td>
<td>(10^{-3})</td>
</tr>
<tr>
<td>(z_4)</td>
<td>(10^{-3})</td>
</tr>
<tr>
<td>(z_5)</td>
<td>(10^{-1})</td>
</tr>
<tr>
<td>(z_6)</td>
<td>(10^{-4})</td>
</tr>
<tr>
<td>(z_7)</td>
<td>(10^{-2})</td>
</tr>
<tr>
<td>(z_8)</td>
<td>(10^{-2})</td>
</tr>
<tr>
<td>(z_9)</td>
<td>(10^{-1})</td>
</tr>
<tr>
<td>(z_{10})</td>
<td>(10^{-1})</td>
</tr>
</tbody>
</table>

By substituting the initial data from Table 2.2 in the expression (2.4):

\[
D_c = 10^{-4}\left[1 - 0.99\left(1 - 10^{-6}\right)\right]\left[1 - 0.999\left(1 - 10^{-6}\right)\right]\left[1 - 0.99\times0.9\right] = 0.118039 \times 10^{-9}.
\]

Individual impacts \(B_{zi}\) as a share in the system risk \(D_c\) are shown in Table 2.3.

**Table 2.3** Impacts of the initiating events \(z_i\) in the system danger (2.1)

<table>
<thead>
<tr>
<th>(z_i)</th>
<th>(B_{zi}/Q_c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(z_1)</td>
<td>0.9999</td>
</tr>
<tr>
<td>(z_2, z_3)</td>
<td>0.000099</td>
</tr>
<tr>
<td>(z_4, z_5)</td>
<td>0.00099</td>
</tr>
<tr>
<td>(z_6)</td>
<td>0.999</td>
</tr>
<tr>
<td>(z_7)</td>
<td>1.00000</td>
</tr>
<tr>
<td>(z_8, z_9)</td>
<td>0.07566</td>
</tr>
<tr>
<td>(z_{10})</td>
<td>0.83123</td>
</tr>
</tbody>
</table>

Comparison of the data shown in Tables 2.1 and 2.3 generally confirms the allocation of ranks which was made based on the HSF structure, namely:

- \(g_{z_7} > g_{z_1} > g_{z_6} > g_{z_3} = g_{z_4} = g_{z_5} > g_{z_8} = g_{z_{10}}\); \(g\) (2.5)

- \(B_{z_7} > B_{z_1} > B_{z_6}B_{z_8} > B_{z_2} = B_{z_3} > B_{z_4} = B_{z_5} > B_{z_2} > B_{z_3}\) \(B\) (2.6)

Only events \(z_2 \ldots z_5\), became less important which is due to a significant difference in initial data (probabilities \(z_8 \ldots z_{10}\) are ten times greater than probabilities \(z_2 \ldots z_5\)), which was intentionally assigned in this way.
As indicated above while the safety investigating the problem of the uniqueness and completeness is in various specialists’ interpretations of conditions of emergency situation development. For example, let us consider the following algorithm of batteries explosion safety system operation. Let us assume that the main tool reducing hydrogen concentration is afterburning equipment. In the case of its failure automatic equipment turning the fans on activates according to the signals of stationary gas analysers. In case of stationary gas analysers failure the fact of hydrogen concentration increasing is observed by operators using portable gas analysers. In this case, the fans are started manually. In case of fan failure and ignition source available an explosion can occur.

Figure 2.4 shows a fragment of ARBITR display with developed event tree upon the above mentioned scenario of hazardous state development.

Figure 2.4 ARBITR screenshot, event tree (see online version for colours)

In Figure 2.4 the function vertices (X4, X6 and X10) show the conditions for the simple events’ instance (failure of afterburning equipment, fan, and ignition source available). The triangles are for the function vertices showing the conditions for complex events’ instance. For example, vertex X35 shows the condition of the simultaneous failure of stationary gas analysers and automation equipment. Vertex X12 shows the failure of portable gas analysers and incorrect operators’ actions.

Event tree solution is shown by means of nine scenarios of the accident development; three of them (y1, y3 and y6) may cause an explosion. Analysis of events’ importance indicates that the most sensitive elements of the scenarios are event X4 and X6. They are the failure of afterburning equipment and fan failure. From a practical perspective, such a conclusion is quite reasonable and assumes the implementation of commonly used safety precautions, i.e. increasing the reliability of afterburning equipment and fan.
2.3 Example 3: Safety analysis of railway section

Let us consider the mathematical model building and railway accident probability calculation at a hypothetic railway section. The task solution will be explained using LPM. The initiating events are: $z_1$ – gage widening, $z_2$ – rail break, $z_3$ – explosive gas content of the area where railway bed is located, $z_4$ – foreign object on rails. We can name the following actions as IC: $z_5$ – late detection by technical means IE $z_1$ and $z_2$ and the information about it wasn’t provided to driver or dispatcher; $z_6$ – incorrect dispatcher’s function execution (dispatcher’s failure); $z_8$ – traffic lights malfunction about track occupancy; $z_7$ – driver’s failure; $z_{10}$ – breaking system failure (task element no. 9 is missing).

We will make a HSF for hazardous state scenario represented at Figure 3.1:

$$y_e (z_1, \ldots, z_{10}) = \begin{vmatrix} z_1 & z_{10} \\ z_2 & z_5 z_6 \\ z_3 & z_5 z_6 \\ z_4 & z_7 z_8 \end{vmatrix}$$

(3.1)

By inverting the HSF (3.1), we will receive a SSF

$$y_i (z_1, \ldots, z_{10}) = \begin{vmatrix} z_1 z_2 z_3 z_4 \\ z_{10} z_5 z_6 z_7 \\ z_4 z_5 z_6 z_7 \\ z_6 z_7 \end{vmatrix}$$

(3.2)

Figure 3.1 Dangerous state scenario (3.1)
Boolean functions (3.1) and (3.2) are monotonous and repeated. To convert them into SDP we will make the corresponding disjointness:

\[
y_c(z_1, \ldots, z_{10}) = \begin{vmatrix}
    z_1 & z_{10} \\
    z_2 & \overline{z_1} \overline{z_0} z_5 z_6 \\
    z_3 & \overline{z_1} \overline{z_0} z_2 z_9 \\
    z_4 & \overline{z_1} \overline{z_6} z_7 z_8 \\
\end{vmatrix}
\]

(3.3)

\[
\overline{y}_c(z_1, \ldots, z_{10}) = \begin{vmatrix}
    z_2 & z_3 & z_4 & \overline{z}_1 & \overline{z}_0 & \overline{z}_5 & \overline{z}_6 & \overline{z}_7 & \overline{z}_8 \\
    z_5 & z_6 & z_7 & \overline{z}_1 & \overline{z}_0 & \overline{z}_2 & \overline{z}_3 & \overline{z}_4 & \overline{z}_8 \\
    z_8 & z_9 & \overline{z}_6 & \overline{z}_5 & \overline{z}_7 & \overline{z}_8 \\
\end{vmatrix}
\]

(3.4)

Going to probabilistic functions we will get:

\[
D_c = (1 - S_1 S_2 S_3 S_4)[D_{10} + S_{10} (D_1 D_6 + S_1 D_1 D_8 + S_6 D_7 D_8)]
\]

(3.5)

\[
S_c = 1 - D_c
\]

(3.6)

Let us take the values shown in the Table 3.1 as the initial data.

Table 3.1  The data for the system (3.1)

<table>
<thead>
<tr>
<th>z_i</th>
<th>O_i</th>
<th>n_i</th>
<th>z_i</th>
<th>O_i</th>
<th>n_i</th>
</tr>
</thead>
<tbody>
<tr>
<td>z_1</td>
<td>0.1</td>
<td>0.9</td>
<td>z_5</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>z_2</td>
<td>0.1</td>
<td>0.9</td>
<td>z_6</td>
<td>0.0001</td>
<td>0.9999</td>
</tr>
<tr>
<td>z_3</td>
<td>0.1</td>
<td>0.9</td>
<td>z_7</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>z_4</td>
<td>0.1</td>
<td>0.9</td>
<td>z_8</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>z_{10}</td>
<td>0.0000001</td>
<td>0.999999</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Substituting the probabilities from the Table 3.1 in the expressions (3.5) and (3.6) we’ll receive

\[
D_c = 0.00344522, \quad S_c = 0.99655478
\]

(3.7)

Let us briefly analyse the results received.

1. Assessment of the risk of railway accident when a high speed train goes on a dangerous section of the railway with the initial data from Table 3.1 was equal 0.00344522.

2. If to consider non-simultaneous presence of four IC \((1 - S_1 S_5 S_6 S_8) = 0.3439\), but to consider them one by one, then the risk shall be decreased to

\[
D_{c2} = \frac{0.1}{0.3439}, \quad D_c = 0.00100181.
\]

(3.8)
3 It is interesting to note that in this task the safety calculation would be easier to maintain by SSF (3.2), and not by the HSF (3.1), as only 4 MCS are there in formula (3.2), and 16 SPHO – in the formula (3.1).

4 It is useful to highlight that it’s impossible to stop the train at high speed even when a driver visually detects a foreign object on the tracks what can be proved by numerous catastrophes associated with such crashes (when moving buses, vans, etc. appear on the tracks).

3 Conclusions

LPTS is attractive for engineers owing to exceptional clarity, uniqueness and great possibilities in the analysis of any argument affecting system safety.

We agree with a certain idealisation of the subject of research by contradictory oppositions (‘white’ – ‘non white’) which provides high accuracy and transparency of manual and machine calculations.

Safety specialists must have the psychology of ‘saboteur’, i.e. find the easiest way how to bring the system to a hazardous state, which is opposed to reliability specialists thinking about saving its performance.

References


## Appendix

### Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSF</td>
<td>Hazardous state function</td>
</tr>
<tr>
<td>IC</td>
<td>Initiating conditions</td>
</tr>
<tr>
<td>IE</td>
<td>Initiating events</td>
</tr>
<tr>
<td>LPM</td>
<td>Logic-probabilistic methods</td>
</tr>
<tr>
<td>LPTS</td>
<td>Logical-probabilistic theory of safety</td>
</tr>
<tr>
<td>MCS</td>
<td>Minimal cut sets</td>
</tr>
<tr>
<td>SPHO</td>
<td>Shortest path of hazardous operation</td>
</tr>
<tr>
<td>SCS</td>
<td>Structurally complex system</td>
</tr>
<tr>
<td>SDP</td>
<td>Sum of disjoint products</td>
</tr>
<tr>
<td>SHS</td>
<td>System hazardous state</td>
</tr>
</tbody>
</table>