

# Safety analysis for integrated modular avionics based on blueprints

Jiayun Chu, Xiaohong Bao, Tingdi Zhao<sup>a</sup> and Fuchun ren

*School of Reliability and Systems Engineering, Beihang University, China*

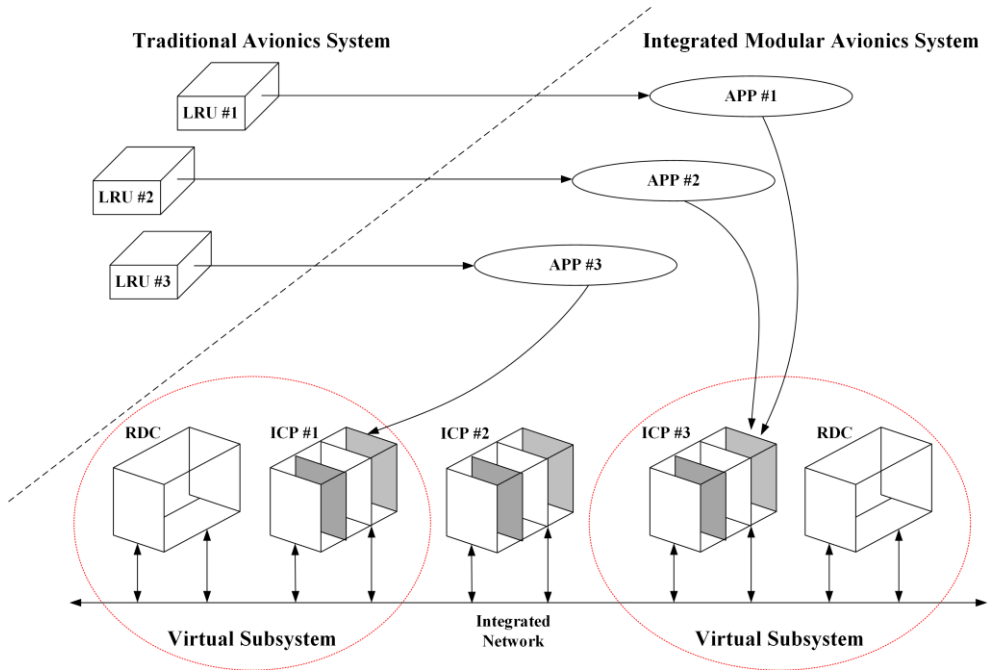
**Abstract.** The Integrated Modular Avionics System (IMA) has been a core technology for the new generation of aircrafts in recent years. It consists of a set of reusable and interoperable common functional modules. However, the highly coupled relationship of resources makes it difficult to identify and control dangers. As an effective and efficient way, the blueprints are used to describe and manage the IMA system. Owing to the system management functions provided by the blueprints, we can accurately determine the system resources configuration status, which is very crucial for safety analysis. In this paper, we explore the possibilities to conduct safety analysis based on blueprints. A safety analysis method based on blueprints is proposed, which applies mathematical logic to describe the logical relationship between targets and resources provided by the blueprints and uses semi-tensor product of matrix theory to simplify the logical expressions. Based on the mathematical model, we can conduct the fail safety analysis and identify resources failures that may undermine the IMA system safety.

## 1 Introduction

The avionics system is a comprehensive control information-intensive system consisting of hardware and software such as mission management, display control, detection sensors and weapons [1]. From the end of the last century, the integrated modular avionics system is gradually applying to the modern aircraft design process, such as F22, A380. Different from the original discrete or federated avionics system, the IMA system implements a wide range of physical synthesis and functional integration. As shown in Figure 1, each function is not located within special processor or line replacement unit (LRUs) in the IMA system [2]. While the system is running, the resources are dynamically allocated to different targets, and it can be regarded that there are many variable virtual subsystems. Although there are many benefits offered by the resources sharing mechanism, such as improving the mission performance and operational performance, reducing the life cycle cost [3], several problems need to be solved urgently. One of the most important problem is how to conduct safety analysis after sharing resources widely. And the allocation of the applications to hardware in an effective and efficient way is also a critical issue. In order to solve the problems above, a concept called “blueprints” is used to describe the IMA system.

---

<sup>a</sup> Corresponding author : [ztd@buaa.edu.cn](mailto:ztd@buaa.edu.cn)



**Figure 1.** The Basic Schematic Graph of IMA System

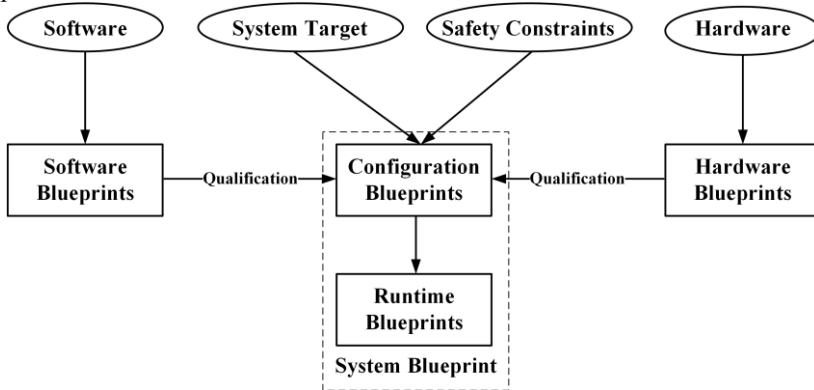
In 1997, A. Marchetto [4] proposed an IMA system management methods using blueprints. He described blueprints as a means of centralizing and organizing the system definition information in such a way that changes of system integration decisions can be transferred, in a controlled and automatic or semi-automatic way, to the target system, simply altering the appropriate blueprints. Allied Standards Avionics Architecture Council (ASAAC) incorporated the blueprints into the recommended technology for IMA system management in its guidelines, and fault monitoring and management functions were added to the blueprints. In the same year, Graham Jolliffe and DM Nicholans [2] explored the possibilities towards a preliminary safety case for IMA blueprints. Li Qian etc. [5] applied the blueprints technology to TV-command-guided system in 2009. Furthermore, there are also many researches on the IMA system blueprints design internationally. Shen Y [6] proposed a method for the design and implementation of IMA system blueprints using AADL in 2008, while Haotian Wang etc. [7] modelled the IMA system blueprints based GSPN and LP in 2013.

Recently, the blueprints technology is widely regarded as a method to centrally organize and manage the system definition information. And the blueprints are implemented by one or a group of management software located in the operating system. Except the system management functions, blueprints can also provide support for the safety analysis due to the definition of system information. In this paper, we apply mathematical logic to describe the logical relationship between targets and resources provided by the blueprints. And semi-tensor product of matrix theory is used to simplify the logical expressions. Based on the mathematical model, we can conduct the fail safety analysis and identify resources failures that may undermine system safety.

The rest of the paper is organized as follows. In Section 2, a brief introduction of the IMA blueprints is given. Section 3 discusses some basic concepts and related properties of matrix algebra at first. And then according to the semi-tensor product theory, the IMA systems model based on blueprints is proposed. In Section 4, we apply the method proposed above to a simple IMA system case. Section 5 is the concluding remarks.

## 2 IMA blueprints

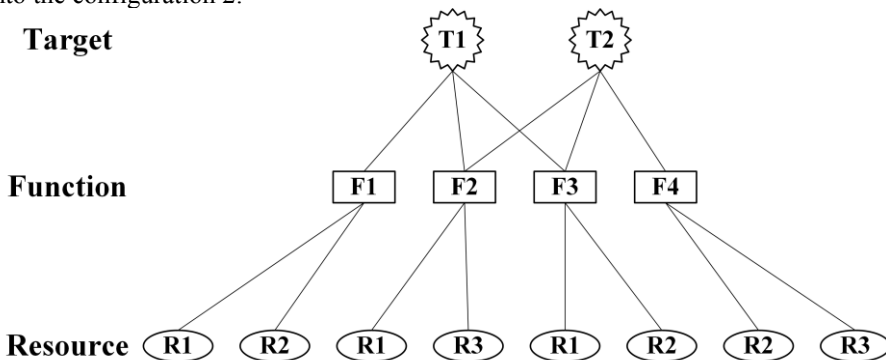
Blueprints technology is a method to centrally organize and manage the system definition information. And they are implemented by one or a group of management software located in the operating system. The blueprints can implement the resources configuration and reconfiguration automatically or semi-automatically, which means the deterministic management of system resources. The IMA blueprints can be designed by AADL or ADA tools. As shown in Figure 2, the blueprints are usually subdivided into three parts recently, including software blueprints, hardware blueprints and system blueprints. And the system blueprints can be further divided into static configuration blueprints and dynamic runtime blueprints.



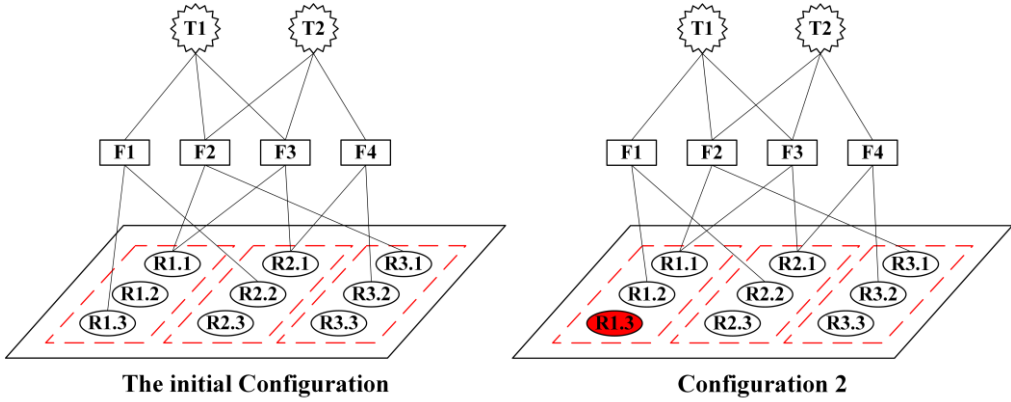
**Figure 2.** The IMA System Blueprints

The software blueprints describe the function software resources in terms of runtime requirements, processing and memory requirements and communication requirements. And the hardware blueprints describe the physical system [8]. The software blueprints and hardware blueprints together describe the resources set of the IMA system, which can be also called as resources pool [9].

The system blueprints guaranteed the safe operation of the IMA system. System designers make decomposition of system targets and determine the resources needed to complete the targets. The decomposition result can be given in the form of a tree as shown in Figure 3. According to the decomposition result and the resources capacity in the resources pool, the initial resources configuration plan is determined, and designers record it in the configuration blueprints. System designers also record the reconfiguration plans when some resources fail in the configuration blueprints. The monitoring and management of the running process are completed by the running blueprints. For example, while the resources R1.3 fails in the Figure 4, the system configuration changes into the configuration 2.



**Figure 3.** Target Decomposition Diagram



**Figure 4.** The Configuration Blueprints

### 3 The IMA system model based on blueprints

#### 3.1 Matrix algebra

This paper is aimed at the logical relationship between targets and resources provided by the blueprints, and tries to simply the logic expressions using semi-tensor product of matrix theory. In this section, we present some basic concepts and related properties of matrix algebra first [10-12].

Definition 1: Assume that  $A = (a_{ij}) \in M_{m \times n}$  and  $B = (b_{ij}) \in M_{p \times q}$ . Then the Kronecker product of  $A$  and  $B$  is represented as  $A \otimes B$  and defined by

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \in M_{mp \times nq} \quad (1)$$

Definition 2: Assume that  $A = (a_{ij}) \in M_{m \times r}$  and  $B = (b_{ij}) \in M_{n \times r}$ . Then the Khatri-Rao product of  $A$  and  $B$  is represented as  $A * B$  and defined by

$$A * B = (Col_1(A) \otimes Col_1(B) \quad Col_2(A) \otimes Col_2(B) \quad \cdots \quad Col_r(A) \otimes Col_r(B)) \in M_{mp \times nq} \quad (2)$$

Definition 3: Assume that  $A = (a_{ij}) \in M_{m \times r}$  and  $B = (b_{ij}) \in M_{n \times r}$ . then the left semi-tensor product  $A$  and  $B$  is represented as  $A \bowtie B$  and defined by

$$A \bowtie B = (A \otimes I_{t/n}) (B \otimes I_{t/p}) \in M_{(mt/n) \times (tq/p)} \quad (3)$$

While  $t = lcm(n, p)$  is the least common multiple of  $n$  and  $p$ , and  $I_k$  is the  $k$  degree identity matrix.

$A \otimes B$ ,  $A * B$  and  $A \bowtie B$  testify the associative law and the distributive law. Furthermore, because the point product is a special case of the left semi-tensor product, this paper makes the following assumption:

$$A \bowtie B = AB \quad (4)$$

Theorem 1: Assume that  $X \in R^r$  is a column vector,  $Y \in R^r$  is a row vector, and,  $A$  is an arbitrary matrix. Then we have

$$XA = (I_t \otimes A)X, AY = Y(I_t \otimes A) \tag{5}$$

Definition 4: Assume that  $W \in M_{m \times mn}$ , and it ranks with double index mark in turn. We define  $W$  as transposition matrix if it safeties

$$W_{(I,J),(i,j)} = \begin{cases} 1 & I = i \text{ and } J = j \\ 0 & \text{else} \end{cases} \tag{6}$$

Theorem 2: Assume that  $X \in R^m, Y \in R^n$  are two column vectors, and  $A \in R^m, B \in R^n$  are two row vectors. Then we have

$$W_{[m,n]}XY = YX, ABW_{[m,n]} = BA \tag{7}$$

Definition 5: Assume that  $D = \{1, 0\}$ , and  $x_i (i = 1, 2, \dots, k) \in D$  is a group of logic variable. A mapping  $f : D^n \rightarrow D$  is defined as a logic function below

$$y = f(x_1, x_2, \dots, x_n) = Mx \tag{8}$$

While  $M$  is defined as structure matrix,  $x = x_1, x_2, \dots, x_n$ . And  $M$  is called as logic operator when  $n \leq 2$ .

Definition 6: Assume that  $M_c, M_d$  and  $M_n$  respectively represent  $\text{and}(\wedge), \text{or}(\vee)$  and  $\text{not}(\neg)$ . Then we have

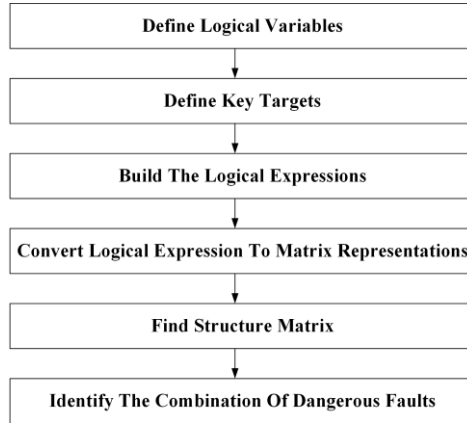
$$M_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, M_d = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, M_n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{9}$$

Definition 7: Assume that  $R_k^P = \text{diag}(\delta_k^1, \delta_k^2, \dots, \delta_k^k)$  with  $\delta_k^i = \left( \underbrace{0, 0, \dots, 1 \dots, 0}_i \right)$ . Then we define  $R_k^P$  as reduction matrix if it safeties

$$x^k = R_k^P x \tag{10}$$

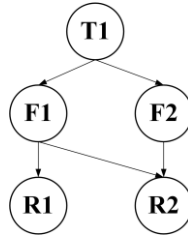
### 3.2 IMA blueprints model and safety analysis

Based on the matrix algebra theory shown in Section 3.1, we propose a method to model the IMA blueprints. And with the IMA blueprints model, we can find the combination of dangerous faults which may influence the system safety. Refer to definition 5, we represent the logical nodes (targets, functions and resources) as binary logical variables. According to the logical relationship between the nodes provided by the blueprints, we build the logical expressions, and simply them with the help of semi-tensor product of matrix theory. As long as we identify the structure matrix of the key targets which may influence the system safety, we can discuss the combination of dangerous failures by solving the logical equations. The flow chart of modelling and analysing is shown in Figure 5.



**Figure 5.** The Flow Chart of Modelling and Analysing

Taking a simply example shown in Figure 6 to present the process of finding structure matrix, we represent the logical nodes as  $t_1, f_1, f_2, r_1, r_2$ .



**Figure 6.** A Simple Example of Logical Graph

Then we can describe the logical relationship as follows.

$$t_1 = f_1 \wedge f_2 = (r_1 \wedge r_2) \wedge r_2 \tag{11}$$

According to the theory introduced in Section 3.1, we can convert formula 11 to formula 12.

$$t_1 = f_1 \wedge f_2 = M_c (M_c r_1 r_2) r_2 = M_c^2 r_1 r_2^2 = M_c^2 r_1 R_2^p r_2 = M_c^2 (I_2 \otimes R_2^p) r_1 r_2 \tag{12}$$

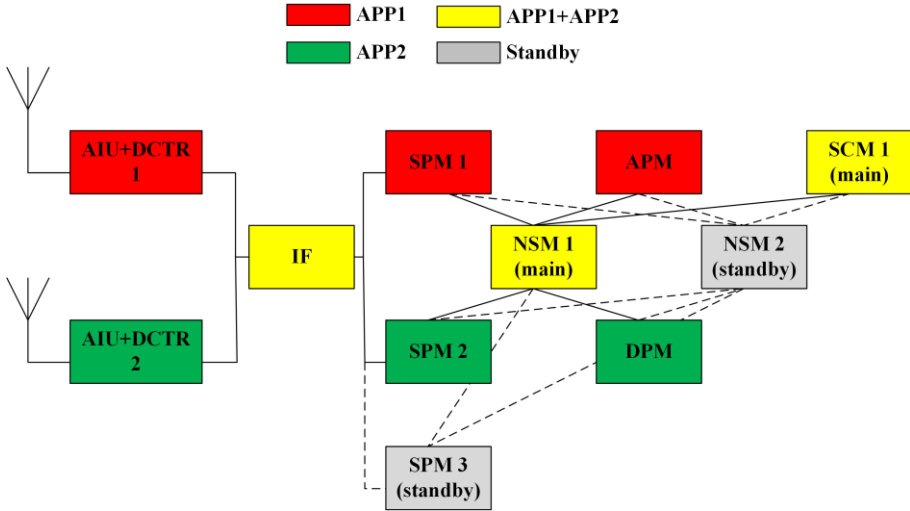
While  $M_c, R_2^p$  are defined in definition 6 and 7, and  $I_2$  is an identity matrix.

The structure matrix of  $t_1$  is represented as  $M_{t_1}$ , and then we have

$$M_{t_1} = M_c^2 (I_2 \otimes R_2^p) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \tag{13}$$

### 4 A simple IMA system case

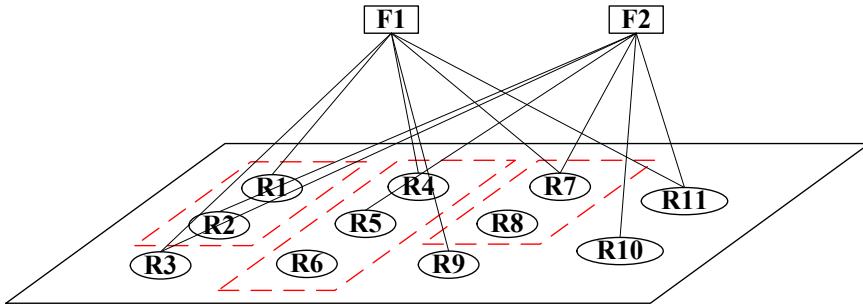
In this section, we take the radio data processing function as an example. As shown in Figure 7, the AAP1 represents voice data processing function while the APP2 represents general data processing function. And the APP1 has a higher priority than the APP2. And we consider the APP1 as the key target.



**Figure 7.** A Simple IMA System Case

According to the order of functions priority, the pre-set reconfiguration strategies which are record in the blueprints are as follows:

- 1) The APP1 has a higher priority than the APP2;
  - 2) While the AIU+DCTR1 fails, stop the APP2 and reallocate the AIU+DCRT2 to APP1;
  - 3) While the SPM1 fails and the SPM2 doesn't fail, use the SPM3 to replace the SPM1; While the SPM1 doesn't fail and the SPM2 fails, use the SPM3 to replace the SPM2; while the SPM1 and the SPM2 fail together, there isn't any change;
  - 4) While the NSM1 fails, use the NSM2 to replace the NSM1;
- Similar to Figure 4, we describe the initial configuration plan as follows.



**Figure 8.** Initial Configuration Plan

While the meanings of each node in Figure 8 are shown in Table 1.

**Table 1.** The Meanings of Nodes

Number	Item	Number	Item
$f_1$	APP 1	$r_6$	SPM 3
$f_2$	APP 2	$r_7$	NSM 1
$r_1$	AIU+DCTR 1	$r_8$	NSM 2
$r_2$	AIU+DCTR 2	$r_9$	APM
$r_3$	IF	$r_{10}$	DPM
$r_4$	SPM 1	$r_{11}$	SCM 1
$r_5$	SPM 2		

Because we only consider the APP1 as the key target, we can build the following logical expression according to the initial configuration plan.

$$f_1 = r_1 \wedge r_3 \wedge r_4 \wedge r_7 \wedge r_9 \wedge r_{11} \tag{14}$$

As we consider the pre-set reconfiguration strategies, we can modify formula 14 to formula 15.

$$f_1 = (r_1 \vee (\neg r_1 \wedge r_2)) \wedge r_3 \wedge (r_4 \vee (\neg r_4 \wedge r_5 \wedge r_6)) \wedge (r_7 \vee (\neg r_7 \wedge r_8)) \wedge r_9 \wedge r_{11} \tag{15}$$

And then we convert the logical expression to matrix representation.

$$f_1 = M_c^5 (M_d r_1 M_c M_n r_1 r_2) r_3 (M_d r_4 M_c^2 M_n r_4 r_5 r_6) (M_d r_7 M_c M_n r_7 r_8) r_9 r_{11} \tag{16}$$

The simplification process is as follows.

$$M_d r_1 M_c M_n r_1 r_2 = M_d (I_2 \otimes M_c M_n) R_2^p r_1 r_2 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} r_1 r_2 = M_1 r_1 r_2 \tag{17}$$

$$M_d r_4 M_c^2 M_n r_4 r_5 r_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} r_4 r_5 r_6 = M_2 r_4 r_5 r_6 \tag{18}$$

$$M_c r_7 M_d M_n r_7 r_8 = M_c r_7 r_8 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} r_7 r_8 = M_3 r_7 r_8 \tag{19}$$

The final simplification result is shown as formula 20.

$$f_1 = M_c^5 M_1 r_1 r_2 r_3 M_2 r_4 r_5 r_6 M_3 r_7 r_8 r_9 r_{11} = M_c^5 M_1 (I_8 \otimes M_2) (I_{64} \otimes M_3) r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{11} \tag{20}$$

The structure matrix of  $f_1$  is represented as  $M_{f_1}$ , and then we have

$$M_{f_1} = M_c^5 M_1 (I_8 \otimes M_2) (I_{64} \otimes M_3) \tag{21}$$

If we only consider the possible safety problems caused by SPM resources failures, we make  $r_1 = r_2 = r_3 = r_7 = r_8 = r_9 = r_{11} = (1 \ 0)^T$ , and solve the equation  $f_1 = (0 \ 1)^T$ , that is

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} r_4 r_5 r_6 \tag{22}$$

According to the equation solution, we can find that only when  $r_4 = (0 \ 1)^T$ , and at least one of  $r_5 = (0 \ 1)^T$  and  $r_6 = (0 \ 1)^T$  holds, then the  $f_1$  fails. The analysis result is in line with expectations.

## 5 Conclusions

In this paper, we propose a method of safety analysis for the IMA system based on blueprints, which applies mathematical logic to describe the logical relationship between targets and resources provided

by the blueprints and uses semi-tensor product of matrix theory to simplify the logical expressions. Based on the mathematical model, we can conduct the fail safety analysis and identify resources failures that may undermine system safety. Adopting the method proposed above, the value of the blueprints is further tapped. Owing to the system management functions provided by the blueprints, we can accurately determine the system resources configuration status, which is very crucial for safety analysis.

## References

1. I. Moir, A. Seabridge and M. Jukes, *Civil Avionics Systems* (West Sussex, UK, 2013)
2. G. Jolliffe and DM. Nicholson, *Constituents of Modern System-safety Thinking*, 163-181 (2005)
3. C. Yin, Y. Renliang and Z. Li, *Integrated Technology of Avionics Modular Integrated System* (Beijing, China, 2013)
4. A. Marchetto, *Dasc. Aiaa/iee. IEEE*, **18**, 3.2-24-31 (1997)
5. L. Qian, F. Jinfu, P. Bo and Z. Jiaqiang, *Computer Engineering*, **35**, 225-227 (2009)
6. Y. Shen, *Computer Engineering*, **34**, 66-71 (2008)
7. W. Haotian, H. Feng and X. Huagang, *Aerosp. Sci. Technol.*, **26**, 111-119 (2013)
8. D. Suo, J. An and J. Zhu, *Digital Avionics Systems Conference. IEEE*, 1C4-1-1C4-12 (2011)
9. Y. Wonkeun and Y. Baeck-jun, *Computer Standards & Interfaces*, **36**(6), 889-898 (2014)
10. C. Daizhan, X. Yuanqing, M. Hongbin, Y. liping, *Matrix Algebra, Control and Game* (Beijing, China, 2016)
11. C Daizhan, Q Hongsheng and X Ancheng, *Journal of Systems Science & Complexity*, **20**, 304-322 (2007)
12. C Daizhan and Q Hongsheng, *IEEE Trans. Autom. Control*, **55**, 2251-2258 (2010)