doi:10.3969/j.issn.1671-637X.2015.10.013

# 综合模块化航空电子系统可靠性评估方法研究

王 鹏[1], 刘 锐[2], 刘万和[2], 阎 芳[1]
(1. 中国民航大学天津市民用航空器适航与维修重点实验室,天津 300300;
2. 中国民航大学安全科学与工程学院,天津 300300)

**摘 要**: 综合模块化航空电子(IMA)系统采用资源共享的系统架构,在提供更加复杂强大的航电功能的同时也带来了更复杂的故障增殖模式,针对此问题提出了基于AADL和GSPN的可靠性评估方法。首先采用AADL语言对系统的架构及故障信息进行描述,建立其AADL可靠性模型,为了进一步分析其故障动态行为,研究了AADL可靠性模型向GSPN模型转化规则,通过对GSPN模型的分析来评估IMA系统可靠性。最后以IMA系统显示功能为例进行了可靠性评估,验证了该方法的有效性,并且通过实验对比的方式给出了显示功能架构的选择建议。

**关键词**: 综合模块化航空电子; 体系结构分析及设计语言; 广义随机Petri网; 可靠性
**中图分类号**: V243 **文献标志码**: A **文章编号**: 1671-637X(2015)10-0056-06

# On Reliability Assessment Method of Integrated Modular Avionics System

WANG Peng[1], LIU Rui[2], LIU Wan-he[2], YAN Fang[1]
(1. Civil Aircraft Airworthiness and Repair Key Laboratory of Tianjin, Civil Aviation University of China, Tianjin 300300, China; 2. College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China)

**Abstract**: Integrated Modular Avionics (IMA) system adopts a resource sharing architecture, which provides a more sophisticated and powerful avionics functionality, but also brings a more complex fault proliferation model at the same time. To solve this problem, we proposed a reliability assessment method based on Architecture Analysis and Design Language (AADL) and Generalized Stochastic Petri Nets (GSPN). Firstly, the system's architecture and fault information were described with AADL language, and its AADL reliability model was established. To further analyze the dynamic behavior of its faults, the rule for transformation from AADL reliability model to GSPN model was studied, and IMA system reliability was assessed by analyzing the GSPN model. Finally, the effectiveness of this method was validated by reliability assessment of the display function of IMA system, and suggestions for selecting the architecture of display function were given via experimental comparison.

**Key words**: Integrated Modular Avionics (IMA); Architecture Analysis and Design Language (AADL); Generalized Stochastic Petri Nets (GSPN); reliability

## 0 引言

IMA系统是当前航空电子系统体系结构发展的最高阶段,解决了由于功能需求增加而导致的系统尺寸、重量、能耗以及通信复杂度增加等问题,克服了联合式体系结构的固有缺陷[1]。同时IMA系统架构简化了航电软件与硬件的开发和验证,增强了系统的处理能力与可靠性,因而被广泛应用于A380,B787,C919,F-35等新一代民用与军用飞机的系统设计中[2]。然而,IMA系统各单元之间由于相互联网通信、资源高度共享、数据高度融合,造成IMA系统故障传播机制渐趋复杂,对其安全性、可靠性评估带来了挑战。因而研究一种与之相适应的可靠性评估方法,具有一定的研究意义和工程实用价值。可靠性评估方法一直是航空、航天领域的研究热点,国内外学者在可靠性研究领域

**收稿日期**:2014-10-29 **修回日期**:2014-12-08
**基金项目**:国家重点基础研究发展计划(2014CB744902);2014民航科技项目;中央高校基本科研业务费资助项目(SY-1448)
**作者简介**:王 鹏(1982—),男,天津人,硕士,副研究员,研究方向为民机系统安全性设计与评估、机载电子硬件适航技术。

取得了丰硕的研究成果。文献[3]针对航天电子设备提出了基于 Bayes 的可靠性评估方法；文献[4]针对飞船降落伞系统提出了基于事件树的系统可靠性评估方法；文献[5]针对飞机姿态确定与控制系统提出了通过 RAMSAS 的方法来评估其可靠性，但是上述研究成果几乎没有适用于 IMA 系统体系结构的可靠性评估方法。针对 IMA 系统，本文提出一种基于 AADL[6] 和 GSPN[7] 的可靠性评估方法。

## 1　评估方法研究

基于 AADL 和 GSPN 的 IMA 系统可靠性评估过程中，首先评估人员应该根据 IMA 系统功能模块确定其体系结构，同时分析每一个功能模块的故障信息，建立 IMA 系统的 AADL 可靠性模型，然后根据转化规则将 AADL 可靠性模型转化为 GSPN 模型，通过对 GSPN 模型的分析，来评估 IMA 系统的可靠性，具体实现路径见图 1。

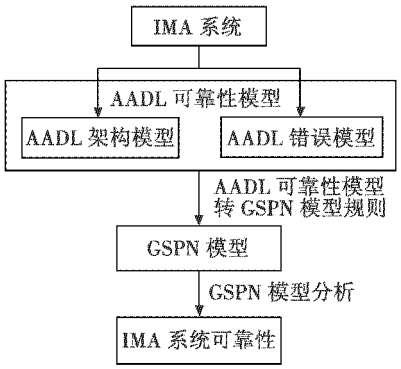


图 1　IMA 系统可靠性评估实现路径

Fig. 1　The process to implement IMA system reliability assessment

### 1.1　系统建模

#### 1.1.1　AADL 架构模型

AADL 架构模型以构件为基本单位，从软件、硬件两个方面综合描述一个系统。在 AADL 中，构件可以划分为 3 类：软件构件（数据、子程序、线程、线程组、进程）、平台构件（处理器、存储器、外设、总线）、系统构件。软件构件通过其属性绑定到平台构件，而为了体现整个系统的层次关系，系统构件应运而生。

每一个 AADL 构件又包含两个层级的描述：构件类型、构件实现。在构件类型中定义了构件的属性、端口、子程序、参数值等，构件类型是对构件的外部描述，典型的构件类型描述如输入、输出端口描述。构件实现中定义了构件的子构件、子程序调用、运行模式等，构件实现是对构件的内部描述。

#### 1.1.2　AADL 错误模型

AADL 错误模型[8] 是对 AADL 架构模型中构件故障信息的描述。AADL 错误模型主要包括错误状态、错误事件、错误变迁及相关的可靠性参数，与 AADL 架构模型类似，错误模型描述也分为错误模型类型，错误模型实现两个层级。典型简单错误模型如下所示。

```
error model General
    features
        error_free:initial error state;
        failed:error state;
        repair,fail:error event;
end General;
error model implementation General.Error
    transitions
        error_free-[fail]->failed;
        failed-[repair]->error_free;
    properties
        occurrence =>poisson 2.0e-3 applies to fail;
        occurrence =>poisson 1.0 applies to repair;
end General.Error;
```

#### 1.1.3　AADL 可靠性模型

AADL 可靠性模型是对系统的构件组成、连接关系及构件故障行为等的综合描述，为了获得系统的 AADL 可靠性模型，需要在 AADL 架构模型的基础上实现构件与相应错误模型的绑定，通过绑定得到 AADL 可靠性模型。AADL 可靠性模型见图 2。

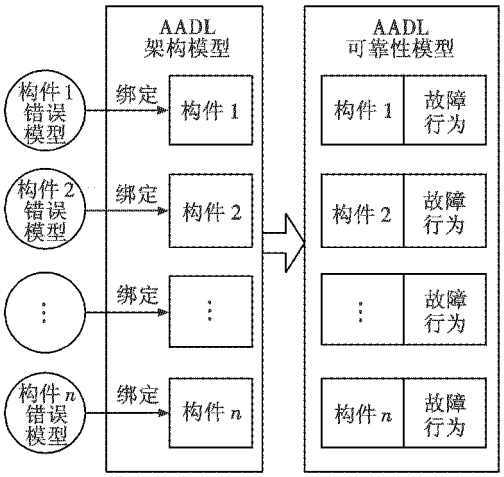


图 2　AADL 可靠性模型

Fig. 2　AADL reliability model

### 1.2　转化规则

由于 AADL 可靠性模型只是一个“静态模型”，不能对系统的架构进行可靠性评估，所以需要将 AADL 可靠性模型进行必要的转化。鉴于 GSPN 良好的动态特性及对时间因素的支持[9]，在可靠性分析方面显现出了巨大的优势，因此考虑将 AADL 可靠性模型转化为 GSPN 模型。AADL 可靠性模型向 GSPN 模型转化时的规则有孤立构件转化规则、Out-In 转化规则和热备份转化规则。

### 1.2.1 孤立构件转化规则

孤立构件转化规则[10]是研究孤立构件 AADL 错误模型中错误状态、错误事件等故障信息向 GSPN 模型中元素转化的规则，如表 1 所示。

**表 1 孤立构件转化规则**

**Table 1 Transformation rule of isolated component**

| AADL 错误模型元素 | GSPN 模型 | |
|---|---|---|
| | 元素 | 符号 |
| Error State | 位置 | ○ |
| Initial Error State | 带托肯的位置 | ◉ |
| Error Event | 变迁 | 瞬时变迁 |
| Transition | 连接弧 | ○→▮→○ |
| Occurrence Property | 变迁类别 | 瞬时变迁 ▯ 时间变迁 |

对于一个或多个相互孤立的构件而言，因为一个错误模型相当于一个随机状态机，其 AADL 错误模型向 GSPN 模型转化是十分容易的，只需要使用孤立构件转化规则即可。上文所述简单错误模型转化为 GSPN 模型见图 3。

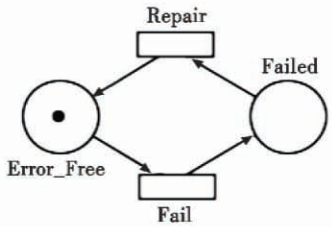


图 3 简单错误模型转化为 GSPN 模型

Fig. 3 The GSPN model of simple error model

### 1.2.2 Out-In 转化规则

由于构件间连接存在结构依赖关系，当一个构件发生故障后，故障会沿着数据流的方向，以一定的概率传出，进而对直接相连的构件产生影响，这种情况下的转化规则称为 Out-In 转化规则[11]。

1）符号定义。

符号定义如表 2 所示。

**表 2 符号定义**

**Table 2 Symbol definition**

| 符号 | 定义 |
|---|---|
| Out_src | 构件发生故障后，未传出故障前状态 |
| Out_dst | 构件发生故障后，传出故障后状态 |
| In_src | 直接相连构件，未引入故障前状态 |
| In_dst | 直接相连构件，引入故障后状态 |
| Outprop | 构件故障传出后，故障暂存位置 |
| Out_error | 使得故障传出的事件 |
| Inprop | 使得故障引入的事件 |
| Empty | 使得故障清除的事件 |
| $C \times D$ | 集合 $C$ 中元素指向集合 $D$ 中元素的连接弧的集合 |
| *EMA_GSPN* | AADL 错误模型元素向 GSPN 模型元素转化函数 |

2）Out-In 转化规则形式化[12]描述。

$$EMA\_GSPN(Out) = Out\_S \cup Out\_T \cup Out\_A_{TS} \cup Out\_A_{ST}^{!} \quad (1)$$

式中：位置集合 $Out\_S = \{Outprop\}$；变迁集合 $Out\_T = \{Out\_error\}$；弧线集合 $Out\_A_{TS} = Out\_T \times Out\_S$；禁止弧集合 $Out\_A_{ST}^{!} = Out\_S \times Out\_T$。

$$EMA\_GSPN(Out - Self) = OS\_S \cup OS\_A_{ST} \cup OS\_A_{TS} \quad (2)$$

式中：位置集合 $OS\_S = \{Out\_src, Out\_dst\}$；弧线集合 $OS\_A_{ST} = \{Out\_src\} \times Out\_T$；弧线集合 $OS\_A_{TS} = Out\_T \times \{Out\_dst\}$。

$$EMA\_GSPN(Out - In) = OI\_T \cup OI\_A_{ST} \cup OI\_A_{TS} \quad (3)$$

式中：变迁集合 $OI\_T = \{Inprop\}$；弧线集合 $OI\_A_{ST} = Out\_S \times OI\_T$；弧线集合 $OI\_A_{TS} = OI\_T \times Out\_S$。

$$EMA\_GSPN(In - Self) = IS\_S \cup IS\_A_{ST} \cup IS\_A_{TS} \quad (4)$$

式中：位置集合 $IS\_S = \{In\_src, In\_dst\}$；弧线集合 $IS\_A_{ST} = \{In\_src\} \times OI\_T$；弧线集合 $IS\_A_{TS} = OI\_T \times \{In\_dst\}$。

$$EMA\_GSPN(Empty) = E\_T \cup E\_A_{ST}^{!} \cup E\_A_{ST} \quad (5)$$

式中：变迁集合 $E\_T = \{Empty\}$；禁止弧集合 $E\_A_{ST}^{!} = \{In\_src, Out\_src\} \times E\_T$；弧线集合 $E\_A_{ST} = Out\_S \times E\_T$。

Out-In 转化规则对应的 GSPN 模型见图 4。

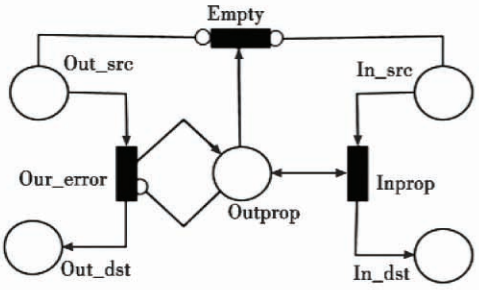


图 4 Out-In 转化规则对应的 GSPN 模型

Fig. 4 The GSPN model of Out-In transformation rule

### 1.2.3 热备份转化规则

在 AADL 中，Guard_Transition 属性将构件的逻辑错误状态与系统的模式转换联系起来了，本文对热备份情况下的双模式系统进行转化规则研究。

图 5 中，Error_free_P，Failed_P 位置分别表示主构件处于正常、故障状态；Error_free_B，Failed_B 位置分别表示备份构件处于正常、故障状态；Primary，Backup 位置分别表示系统工作于初始模式、备份模式；To_modeP 表示使得系统切换到初始模式的变迁，To_modeB 表示使得系统切换到备份模式的变迁。

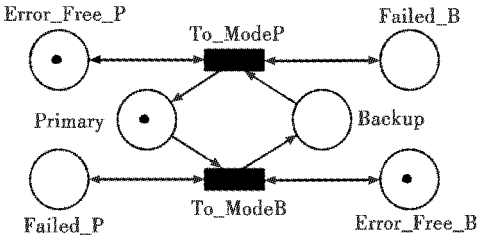


图 5　热备份转化规则对应的 GSPN 模型

Fig. 5　The GSPN model of hot-standby transformation rule

对热备份转化规则简要说明：

1）系统刚运行时，工作于初始模式，主构件、备份构件均正常；

2）当主构件故障且备份构件正常时，系统通过 To_ModeB 瞬时变迁切换到备份模式；

3）当主构件恢复正常且备份构件故障时，系统通过 To_ModeP 瞬时变迁又切换到初始模式。

### 1.3　GSPN 模型分析

将 AADL 可靠性模型通过上述规则转化为 GSPN 模型后，需要对 GSPN 模型进行分析，以评估系统可靠性。目前 GSPN 的分析工具较多，如 Pipe2[13]，TimeNet[14] 等。

## 2　实例验证

为了验证评估方法的有效性，本章以 IMA 系统的显示功能为例进行分析。

### 2.1　显示功能模型建立

IMA 系统的显示功能用于实现飞机飞行姿态、航向、高度等参数信息的显示。为了实现显示功能，首先传感器将采集到的数据传送给相应的数据处理（DP）单元，数据经过处理后传给图像处理（IP）单元，图像处理单元将相关的数据处理后生成要求的图形显示在显示屏，供飞行员参考，本文称显示屏为综合显示（ID），其体系结构见图 6。

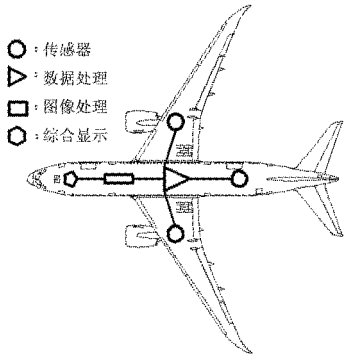


图 6　显示功能体系结构

Fig. 6　The architecture of display function

根据上文的描述，建立 IMA 系统显示功能 AADL 可靠性模型，见图 7。

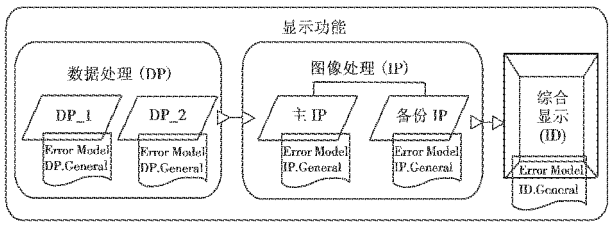


图 7　显示功能 AADL 可靠性模型

Fig. 7　AADL reliability model of display function

在图 7 中，数据处理单元包含两个构件：DP_1，DP_2，且它们互为运行备份。图像处理单元包含两个构件：主 IP，备份 IP，它们互为热备份，可以根据运行状态进行模式转化。综合显示单元包含一个外设构件。

根据 IMA 系统 AADL 可靠性模型向 GSPN 模型转化规则，将显示功能 AADL 可靠性模型转化为 GSPN 模型，见图 8。

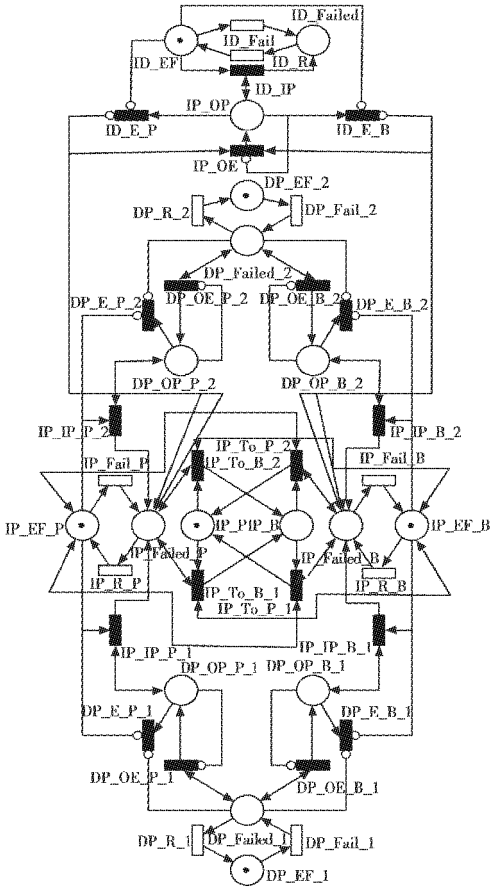


图 8　显示功能 GSPN 模型

Fig. 8　The GSPN model of display function

图 8 中，初始时数据处理单元的构件 DP_1，DP_2 均正常；图像处理单元工作在初始模式下，同时主 IP 和备份 IP 构件均正常；综合显示单元正常。

经过一段时间的运行后，各单元均有可能发生故障，如果数据处理单元发生故障，那么故障将以一定的概率传出，同时被图像处理单元引入，造成图像处理单

元故障,当主 IP 和备份 IP 均发生故障后,故障将会以一定的概率传出,同时被综合显示单元引入,造成综合显示单元故障,一旦综合显示单元发生故障,则认为显示功能丧失。

由于各单元都具有自恢复能力,经过一段时间后,如果综合显示单元恢复正常,则认为显示功能得到了恢复。

本文通过对 IMA 系统显示功能 GSPN 模型的分析,获得其达到稳态时各单元托肯的分布情况及对应的概率,从而评估显示功能的可靠性。

### 2.2 可靠性分析

将 IMA 系统显示功能 GSPN 模型在 Pipe2 建立后,设置好相关变迁、位置的参数,调用 GSPN Analysis 分析模块,即可得到分析结果。由于结果中可能的稳定状态有 16 个,并且每个稳定状态下有 17 个位置的托肯分布情况,所以本文只展示出显示功能正常下的 3 个单元托肯分布情况,见表 3。

**表 3 显示功能正常下分析结果**

**Table 3 The analytical result of display function under normal conditions**

| | M0 | M4 | M5 | M14 |
|---|---|---|---|---|
| DP_EF_1 | 1 | 1 | 1 | 1 |
| DP_EF_2 | 1 | 1 | 1 | 1 |
| IP_EF_P | 1 | 0 | 1 | 1 |
| IP_EF_B | 1 | 1 | 0 | 1 |
| IP_P | 1 | 1 | 0 | 0 |
| IP_B | 0 | 0 | 1 | 1 |
| ID_EF | 1 | 1 | 1 | 1 |
| 稳态概率 | 0.491 10 | 0.002 94 | 0.002 94 | 0.491 10 |

表 3 中,第一行表示在显示功能正常时有 4 种可能的稳定状态。在 M0 列下,DP_EF_1,DP_EF_2 数值为 1,表示数据处理单元的构件 DP_1,DP_2 均正常;IP_EF_P,IP_EF_B 数值为 1,表示主 IP 和备份 IP 均正常,由于 IP_P 数值为 1, IP_B 数值为 0,故图像处理单元工作在初始模式下;ID_EF 数值为 1 表示综合显示单元正常。通过以上分析可知,IMA 系统显示功能在 M0 稳定状态下各单元均正常,并且图像处理单元工作在初始模式下,此稳定状态概率为 0.491 1。其余列分析不再赘述。通过将表 3 中每一列对应的稳态概率相加即可得到 IMA 系统显示功能的可靠性,相加结果为 0.988 08。

综上可知,IMA 系统显示功能在数据处理单元不含故障限制域、图像处理单元热备份的情况下(记为 A)系统可靠性为 0.988 08。

## 3 实验对比

在系统运行过程中,常常会出现以下情况:个别子系统或构件由于各种原因出现故障时,不仅会对自身造成影响,而且故障会沿着数据流方向进行传播,造成与之相关联的子系统或构件也发生故障。这样,单个子系统或构件的故障往往会波及到与其相关的若干子系统或构件,进而对整个系统构成巨大影响,所以在 IMA 系统的设计中提出了故障限制域的概念。故障限制域的实质是指将故障限定在特定区域内,而不向该区域以外的区域传播[15]。故障限制域分为完全故障限制域和条件性故障限制域:完全故障限制域即是将子系统或构件的所有故障均限制在一定区域内而不向区域以外区域传播;条件性故障限制域是将子系统或构件部分故障限制在一定区域内而不向区域以外区域传播。

为了进一步提高 IMA 系统显示功能的可靠性,同时研究数据处理单元、图像处理单元不同配置下对 IMA 系统显示功能的可靠性产生的影响,本文又研究了 3 种不同情况下的 IMA 系统显示功能的可靠性:

1) IMA 系统显示功能的数据处理单元采用条件性故障限制域(即 DP_2 的故障不会向图像处理单元传播)、图像处理单元采用热备份,综合显示单元保持不变,记为 B;

2) IMA 系统显示功能的数据处理单元采用条件性故障限制域、图像处理单元没有备份,综合显示单元保持不变,记为 C;

3) IMA 系统显示功能的数据处理单元不含故障限制域、图像处理单元没有备份,综合显示单元保持不变,记为 D。

通过对上述 3 种情况下的 IMA 系统显示功能 GSPN 模型进行分析可得 3 种情况下的 IMA 系统显示功能可靠性,分析结果见表 4。

**表 4 不同情况下 IMA 系统显示功能可靠性**

**Table 4 The reliability of display function of IMA system under different condition**

| | 热备份 | 未备份 |
|---|---|---|
| 条件性故障限制域 | 0.993 02(B) | 0.984 18(C) |
| 不含故障限制域 | 0.988 08(A) | 0.982 21(D) |

根据上述分析结果,可以得出以下结论。

1) 在数据处理单元采用同样的配置策略条件下,图像处理单元热备份下 IMA 系统显示功能可靠性比未备份下的可靠性显著提高。这是因为在热备份下,一个构件发生故障后,系统可以通过模式切换让备份的构件来接替主构件的工作,因而可以使得系统的可靠性得到显著提高。

2) 在图像处理单元采用同样的配置策略条件下,数据处理单元条件性故障限制域下的 IMA 系统显示

功能可靠性比数据处理单元不含故障限制域下的系统显示功能可靠性得到了提高。这是因为在条件性故障限制域下，构件发生故障后，由于故障限制域的存在，使得故障并不会沿着数据流的方向传播，所以不会对后续的构件产生任何的影响。

综上分析可以得出：对于 IMA 系统显示功能，在考虑经济性与可靠性的条件下，数据处理单元采用条件性故障限制域、图像处理单元采用热备份的方式可以明显地提高可靠性。

## 4　结论

本文针对 IMA 系统各单元之间由于相互联网通信、资源高度共享等造成的 IMA 系统错误传播机制渐趋复杂的特性提出了基于 AADL 和 GSPN 的可靠性评估方法。该评估方法在嵌入式系统设计初期对系统可靠性评估具有较好的参考价值，方便设计人员根据系统可靠性要求及时调整系统架构。由于大型嵌入式系统组成单元众多，并且单元之间连接关系也比较复杂，再手动将 AADL 可靠性模型转化为 GSPN 模型则会十分耗时费力，接下来考虑开发转化接口软件用于自动将 AADL 可靠性模型转化为 GSPN 模型。

## 参考文献


[1] 熊华钢，王中华. 先进航空电子综合技术[M]. 北京：国防工业出版社，2009.（XIONG H G, WANG Z H. Advanced avionics integration techniques[M]. Beijing: National Defense Industry Press, 2009.）

[2] 丁全心. 综合模块化航空电子系统标准述评[J]. 电光与控制，2013，20（6）：1-3.（DING Q X. Remarks on standards of integrated module avionic system[J]. Electronics Optics & Control, 2013, 20(6): 1-3.）

[3] 孙鹏，赵阳，董海平. 航天电子设备可靠性评估方法研究[J]. 空间科学学报，2012，32（2）：265-269.（SUN P, ZHAO Y, DONG H P. Study on assessment method of reliability of spaceflight electronic device[J]. Chinese Journal of Space Science, 2012, 32(2): 265-269.）

[4] 王学，高普云，冯志刚，等. 飞船降落伞系统的可靠性建模[J]. 宇航学报，2011，32（7）：1645-1649.（WANG X, GAO P Y, FENG Z G, et al. Reliability modeling for parachute system of spacecraft[J]. Journal of Astronautics, 2011, 32(7): 1645-1649.）

[5] GARRO A, GROB J, RICHTER M R, et al. Reliability analysis of an Attitude Determination and Control System (ADCS) through the RAMSAS method[J]. Journal of Computational Science, 2014, 5(3): 439-449.

[6] TU X J, XU J R, WU Q, et al. Modeling and reliability evaluation of avionics clouds based on AADL and GSPN[C]//Digital Avionics Systems Conference (DASC), 2013 IEEE/AIAA 32nd. New York: IEEE, 2013: 8C1-1-8C1-11.

[7] REISIG W. Understanding Petri nets: modeling techniques, analysis methods, case studies hardcover[M]. Berlin: Springer, 2013.

[8] LARS G, HAN J. A comparative study into architecture-based safety evaluation methodologies using AADL's error annex and failure propagation models[C]//High Assurance Systems Engineering Symposium, New York: IEEE, 2008: 283-292.

[9] 董世良，刘海港，石健，等. 容错计算机网络综合可用性建模与仿真分析[J]. 系统仿真学报，2011，23（s1）：75-82.（DONG S L, LIU H G, SHI J, et al. Integrated availability modeling and simulation for fault-tolerant network system[J]. Journal of System Simulation, 2011, 23(s1): 75-82.）

[10] RUGINA A E, KANOUN K, KA-ÂNICHE M. A system dependability modeling framework using AADL and GSPNs[C]//LNCS 4615: Architecture Dependable System IV. Berlin, Heidelberg: Springer-Verlag, 2007: 14-38.

[11] 董云卫，王广仁，张凡，等. AADL 模型可靠性分析评估工具[J]. 软件学报，2011，22（6）：1252-1266.（DONG Y W, WANG G R, ZHANG F, et al. Reliability analysis and assessment tool for AADL model[J]. Journal of Software, 2011, 22(6): 1252-1266.）

[12] 李莹，吴江琴. 软件工程形式化方法与语言[M]. 杭州：浙江大学出版社，2010.（LI Y, WU J Q. Formal methods and language of software engineering[M]. Hangzhou: Zhejiang University Press, 2010.）

[13] DINGLE N, KNOTTLT W J, SUTO T. PIPE2: a tool for the performance evaluation of generalised stochastic Petri nets[J]. ACM Sigmetrics Performance Evaluation Review, 2009, 36(4): 34-39.

[14] ZIMMERMANN A. Modeling and evaluation of stochastic Petri nets with TimeNET 4.1[C]//The 6th International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS), New York: IEEE, 2012: 54-63.

[15] KOPETZ H. Fault containment and error detection in the time-triggered architecture[C]//The 6th International Symposium on Autonomous Decentralized Systems, New York: IEEE, 2003: 139-146.