文章编号:1671-4598(2020)03-0255-05 DOI:10.16526/j.cnki.11—4762/tp.2020.03.053 中图分类号:TP311.5 文献标识码:A

一种航空机载嵌入式软件安全性评价方法研究

刘玉军[1],冯 飞[1],曹 乐[2]
(1.西南电子技术研究所 天奥软件测评中心,成都 610036;
2.成都中电锦江信息产业有限公司,成都 610051)

摘要:机载嵌入式软件是航空电子系统的重要组成部分,其安全性直接关系到飞行安全;由于软件安全性包含的范围较广,对安全性的评价往往周期长、结果不明确;针对嵌入式软件安全性评价的难题,在软件的整个生命周期采用分类模糊综合评价方法,建立了评价模型,提出了一种嵌入式软件安全性评价方法,在软件生命周期的5个阶段提出了59种评价元素,每种评价元素均反应出软件在每个阶段的关键活动;在各个阶段选择相关项目人员对每个元素进行评价,并依据计算公式得出软件安全分值;通过工程实践证明,该方法切实可用,评价过程相比传统的方法节约了时间,评价结果准确、直观,为航空机载嵌入式软件尤其是型号软件的安全性评价提供了一种新方法,为软件总体质量的评价和软件安全性的改进方向提供支撑。

关键词:机载软件;嵌入式;安全性;评价方法

Research on Security Evaluation Method of Airborne Embedded Software

Liu Yujun[1], Feng Fei[1], Cao Le[2]
(1. Dept. of Software testing, Southwest China Institute of Electronic Technology, Chengdu 610036, China;
2. CEC Jinjiang Information Industrial Company, Ltd., Chengdu 610051, China)

Abstract: Airborne embedded software is an important part of avionics systems and its safety is directly related to flight safety. Because software security covers a wide range, the evaluation of security tends to be long-term and the results are not clear. Aiming at the difficulty of embedded software security evaluation, the classification fuzzy comprehensive evaluation method was adopted in the whole life cycle of the software, and the evaluation model was established. An embedded software security evaluation method was proposed, and fifty-nine evaluation elements were proposed in five stages of its life cycle. Each evaluation element reflects the key activities of the software in each stage. The relevant project personnel are selected to evaluate each element, and the software safety value is obtained according to the calculation formula. Proved by engineering practice, the method is practical, the evaluation process saves time compared with the traditional method, and the evaluation result is accurate and intuitive. It provides a new method for the safety evaluation of aviation airborne embedded software, especially model software. Providing support for the overall quality of the software and the improvement direction of software security.

Keywords: airborne software; embedded software; security; evaluation method

0 引言

嵌入式软件以其专用性强、高实时性、可裁剪、重量轻、体积小等特点广泛应用于生产、生活乃至军用航空领域[1]。嵌入式软件作为嵌入式系统的控制中心,其安全性直接关系到系统的使用和人、机安全。由于嵌入式软件的失效引起的安全事故对国家会造成严重的经济和军事影响[2]。随着航空电子技术不断发展,现代飞机的体系架构已由分离式、联合式逐渐向模块化、高度综合化方向发展,系统功能越来越复杂软件实现的功能在航空电子系统中所占的比重越来越大[3]。航空机载软件具有嵌入式、实时性、结构复杂、高关键等级等特点[4]。近年来,由于航空机载软件安全性问题所造成的事故也成逐年上升趋势。2018年10月印尼狮航和2019年3月埃塞俄比亚航空两架波音737 MAX8客机坠毁,造成重大财产损失和人员伤亡。失事原因主要是由于AOA(飞机高迎角传感器)将错误的数据传输给MCAS(操纵辅助系统),MCAS软件未对异常的AOA数据做正确的处理导致的。软件安全性包含很广,既包含软件失效对系统造成故障、危及飞行安全,也包括软件内部数据保护,防止非授权的用户使用、篡改、分析和从中挖掘信息[5]。例如本身涉及国家秘密或商业秘密的数据被破解泄露,软件的程序被逆向,架构被再工程利用。

传统的软件安全性和可靠性利用各种方法去验证满足"安全关键失效率"(λ)。例如在需求分析阶段,一般有失效模式分析(FMEA)、故障树FTA分析等方法,编码阶段使用审查、走查等方法验证。然而航空软件对λ要求很高,一般为10^{-6}到10^{-9},而可靠性指标一般也为10^{-3}以上,按照理论测试模型推算,收集到足够的失效数据用于参数估计的时间短则一年半载,长则几十年,周期较长,并且"安全关键失效率"λ也不能当做量化指标去测试评估。现有的对嵌入式软件的安全性评估方法较为分散,缺少一种快速并可以量化的安全性评估方法。

本文针对嵌入式软件安全性评价的难题,在软件的全

收稿日期:2019-10-18; **修回日期**:2019-11-07。

作者简介:刘玉军(1988-),男,山东聊城人,工程师,主要从事软件测试技术方向的研究。

生命周期基于分类模糊综合评价理论，建立了评价模型，提出了一种评价方法，能快速、准确、客观的对嵌入式软件的安全性进行评价。

1 软件生命周期模型

软件开发模型有多种，目前常见的开发模型有增量模型、瀑布模型、螺旋模型、瀑布模型、智能模型等。增量模型的开发过程如图 1 所示。瀑布模型的开发过程如图 2 所示。根据实际项目的复杂程度、周期要求等选取不同的模型进行开发。虽然瀑布模型有其缺点，但它有利于大型软件开发过程中人员的组织管理，有利于软件开发方法和工具的研究与使用从而提高了大型软件项目开发的质量和效率[6]。为保证软件质量，软件开发过程和交付过程通常伴随软件测试。结合软件开发的升级瀑布模型形成 V 模型。由于军用航空软件的特殊性，航空航天领域的机载嵌入式软件开发广泛使用 V 模型[7]。

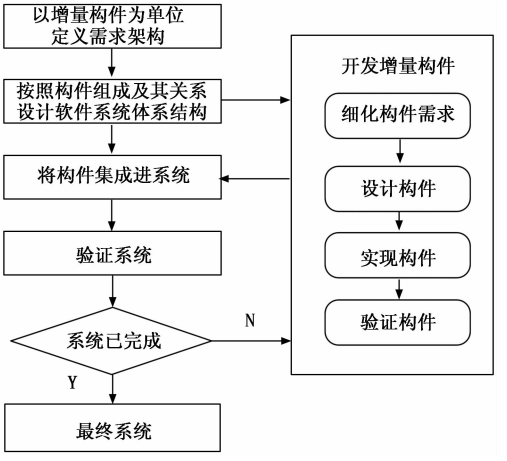

图 1 软件开发增量模型图

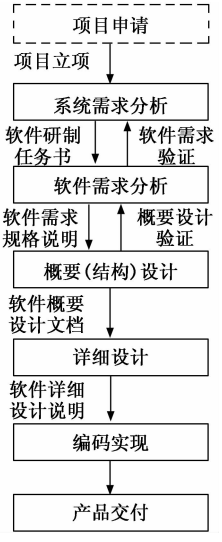

图 2 软件开发瀑布模型

软件生命周期 V 型关系[8]如图 3 所示。

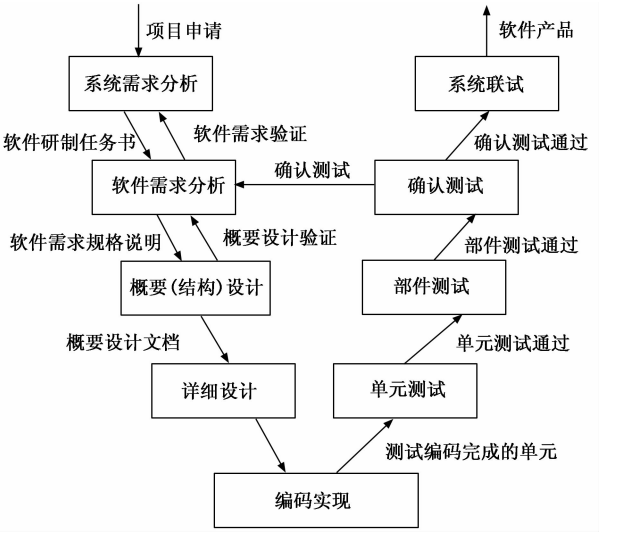

图 3 软件生命周期 V 型关系图

2 嵌入式软件等级划分

根据软件失效或发生安全性问题可能导致的后果和相关军用标准[9]，将嵌入式软件重要性等级分为Ⅰ、Ⅱ、Ⅲ、Ⅳ四个等级。软件等级划分如表 1 所示。

表 1 软件等级划分

软件重要等级	危险程度	软件失效可能的后果
Ⅰ	灾难性危害	人员死亡、系统报废、任务失败、环境严重破坏。
Ⅱ	严重危害	人员严重受伤、系统严重损坏、任务受到严重影响。
Ⅲ	轻度危害	人员轻度受伤，系统轻度损坏、任务受到影响。
Ⅳ	轻微危害	轻微危害，不影响任务及人员安全。

3 软件安全性评价过程

3.1 评价方法

对嵌入式软件安全评价采用分类模糊综合评价方法[10]，即将评价指标分类，分别有相对的评价人员进行评价，分类评价中又采用模糊综合评价方法进行，最后加权得到总体评价。模糊综合评价法是基于模糊数学模糊集理论，对评价对象作以综合评价的一种方法，它以模糊数学为基础，应用模糊关系合成定理，将一些边界不清、不一定量的因素定量化，符合嵌入式软件安全性评价的特点。

3.2 评价元素

依据软件开发周期的 V 模型，将嵌入式软件安全评价分为 5 个阶段，即软件需求阶段、软件设计阶段、软件编码阶段、软件测试阶段，软件使用阶段，对应为 A、B、C、D、E 五个阶段。每个阶段对应一个评价元素集合 $\{a_1, a_2, \cdots. a_n\}$，$n=11$、$\{b_1, b_2, \cdots. b_n\}$，$n=12$、$\{c_1, c_2, \cdots. c_n\}$，$n=8$、$\{d_1, d_2, \cdots. d_n\}$，$n=26$、$\{e_1 \cdots e_n\}$，$n=2$，共 59 个评价活动元素。

软件需求阶段评价元素如表 2 所示。

表 2　软件需求阶段评价元素

阶段	评价元素	元素符号
软件需求阶段	明确嵌入式软件的安全等级	a_1
	明确系统安全设计需求	a_2
	是否明确系统向软件分配的安全需求，可结合 BDA 分析技术对软件安全需求进行分析	a_3
	明确软件设计与开发过程需求	a_4
	明确软件配置管理需求，包括需求的变更等	a_5
	明确软件分析与测试需求	a_6
	明确用户对软件的特殊安全性需求，如软件中数据是否涉及国家或商业秘密的保密需求	a_7
	明确常规安全需求例如软件跑飞的机制、中断初始化和开关中断的时机	a_8
	明确软件失效异常时处理需求	a_9
	安全性需求经过评审	a_{10}
	明确系统其他安全需求	a_{11}

软件设计阶段评价元素如表 3 所示。

表 3　软件设计阶段评价元素

阶段	评价元素	元素符号
软件设计阶段	需求阶段的安全性需求设计了相应的模块或函数实现	b_1
	代码保护设计，对进行加壳、混淆等保护，防止被逆向	b_2
	对软件传输和存储的敏感信息进行加密	b_3
	对软件进行了容错设计	b_4
	对软件进行了过载设计	b_5
	对软件的接口缓冲等进行了余量设计	b_6
	对 CPU 使用率进行了余量设计	b_7
	对嵌入式系统芯片 Flash 进行了余量设计	b_8
	对数据的计算进行了安全设计	b_9
	对软件的中断进行了分析与设计	b_{10}
	进行通信安全的设计，如超时处理、出错处理、校验方式、通信缓冲防溢出等设计	b_{11}
	完成其他安全设计	b_{12}

软件编码阶段评价元素如表 4 所示。

在软件测试阶段，根据嵌入式软件的等级不同可选择不同的测试级别。软件测试阶段评价元素如表 5 所示。

软件使用阶段评价元素如表 6 所示。

嵌入式软件在生命周期的不同阶段对应不同的评价元素，每个评价元素对应的安全分值为 [0，100]，在 5 个阶段中选择不同的人员进行评价，在软件需求阶段和软件设计阶段选择项目总体技术人员，软件编码阶段选择编程人员，软件测试阶段选择软件测试人员，软件使用阶段选择使用总体人员。

其中，软件需求阶段、软件设计阶段、软件编码阶段、软件测试阶段对应的评分数值 S_{ij}，其中 $i=\{a, b, c, d, e\}$，$j=\{1, 2\cdots n\}$。S_i 乘以相应的权重 Q_{ij} 后相加，得出在

表 4　软件编码阶段评价元素

阶段	评价元素	元素符号
软件编程阶段	编程方法和编程规范是否符合编程语言通用要求和行业要求；例如 GJB 8114 等，包含数据、表达式、控制结构、函数、指针与数组、类型转换、结构体与联合体、声明与定义、预处理与标准库、内存管理、注释等要求	c_1
	软件程序复杂性控制程度符合要求；例如每个模块的圈复杂度一般不大于 10，扇入、扇出数一般不大于 7，程序的入口、出口是否进行了限制，传递的参数一般不超过 6 个等[11]	c_2
	代码的效率保证，例如程序的运行时间，存储效率，输入/输出效率	c_3
	对影响飞行安全的关键数据，对精度等进行检查	c_4
	对外部通信传输的数据进行格式匹配和数值合理性检查	c_5
	中断处理、硬件初始化参数配置符合要求和安全性需求	c_6
	软件代码版本控制符合规范	c_7
	完成其他安全编码要求	c_8

A、B、C、D 四个阶段的安全分值，安全分值总分为 100 分。得出 A、B、C、D 四个阶段的安全分值计算公式为 $S_1=\sum_{i=a}^{d}\sum_{j=1}^{n}S_{ij}*Q_{ij}$。

在 E 阶段，若 MTTF 值大于设计使用时间的 20%，e_1 值为 −10；满足设计时间但小于 20%时，分值为 0；若不满足设计时间，e_1 值为 10。试用阶段发现的安全问题数按照严重等级计算分值，发现严重安全问题为 −5 分/个，一般安全问题为 −3 分/个，轻微安全问题为 −2 分/个。E 阶段的安全分值 $S_2=Se_1+Se_2$，得出嵌入式软件安全分值 S 的计算公式为：

$$S=\sum_{i=a}^{d}\sum_{j=1}^{n}S_{ij}*Q_{ij}+Se_1+Se_2$$

为降低评价人员的主观性，每个阶段选取 k 个评价人员，将评价值相加后取平均值，继而得到计算评价结果公式：

$$S=\frac{1}{k}\sum_{i=1}^{k}S(i)$$

3.3　权重的确定

依据行业经验和专家知识，结合航空嵌入式软件的特点，确定 A、B、C、D 对应的权重值为 30%，25%，25%，20%。依据每个评价元素的重要程度和对软件安全性产生的影响，进而明确评价权重矩阵：$\{Qa_1, Qa_2, \cdots. Qa_{11}\}=\{0.02, 0.04, 0.04, 0.02, 0.04, 0.02, 0.02, 0.02, 0.03, 0.03, 0.02\}$；

$\{Qb_1, Qb_2, \cdots. Qb_{12}\}=\{0.04, 0.02, 0.02, 0.02, 0.02, 0.02, 0.02, 0.02, 0.02, 0.02, 0.02, 0.01\}$；

$\{Qc_1, Qc_2, \cdots. Qc_8\}=\{0.04, 0.03, 0.02, 0.03, 0.02, 0.02, 0.02, 0.02\}$；

表 5 软件测试阶段评价元素

阶段		评价元素	元素符号
软件测试阶段	单元测试	使用代码走查的方式测试软件编码是否与安全详细设计一致	d_1
		使用工具对软件进行静态安全测试,包括代码逻辑分析,接口分析,中断使用分析,代码数据分析	d_2
		语句覆盖率、分支覆盖率、MC/DC 覆盖率到达 100%	d_3
		软件的资源消耗测试,例如 CPU 余量、内部存储空间余量在需求的基础上留有 20%余量	d_4
		使用工具对软件源代码进行静态安全分析	d_5
	部件测试	需求覆盖性,检查软件单元和软件部件之间的接口关系,是否符合安全设计需求	d_6
		准确性,对软件部件中具有准确性要求的功能和精度要求的项进行测试,例如数据处理精度,时间测量精度等	d_7
		互操作性,对部件和支持部件运行的其他部件例如程序和硬件设备件进行测试,对接口的输入输出格式、内容、传递方式进行测试	d_8
		容错性,测试软件部件对错误中断、错误输入、性能降级等情况下的容错能力	d_9
		时间特性;测试软件部件最长路径下的运行时间。是否满足设计要求	d_{10}
		资源使用性,测试软件部件运行时所占用的内存空间是否符合要求	d_{11}
		调用性,软件单元和软件部件的所有调用达到 100%调用	d_{12}
		明确软件的危险状态和可能导致危险状态的原因并进行测试	d_{13}
	配置项测试	测试环境是否与真实实装环境一致	d_{14}
		对软件配置项测试输入包含有效等价类、无效等价类和边界数据值	d_{15}
		软件运行条件在边界状态和异常条件下	d_{16}
		测试敏感数据访问权限的可控制性,以及是否进行了在存储或传输时进行了加密处理	d_{17}
		异常或非法操作测试,包括非授权的删增加、修改、删除程序信息	d_{18}
	系统测试	完成安全需求的验证,异常操作	d_{19}
		对软件进行强度测试,包括规定负载和最大负载性情况下长时间运行的强度测试	d_{20}
		与上层应用软件交互的敏感数据的传输、存储加密的测试	d_{21}
		完成误操作测试	d_{22}
		完成故障注入测试	d_{23}
		故障恢复能力及故障恢复时间满足要求	d_{24}
		多种环境下软件的测试	d_{25}
		系统其他需要完成的安全测试	d_{26}

表 6 软件使用阶段评价元素

阶段	评价元素	元素符号
软件使用阶段	软件使用平均无安全故障使用时间 MTTF	e_1
	试用阶段内发现安全问题	e_2

$\{Qd_1, Qd_2, \cdots . Qd_{26}\}$ = {0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.005,0.005,0.005,0.005,0.005,0.005,0.01,0.02,0.02,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01}。

3.4 评判标准

在评价活动中，根据 A、B、C、D、E 五个阶段计算出的安全分值应约大越好，但由于项目实际的时间进度限制、人员水平限制、经费限制等因素，软件的安全性往往受到影响。依据航空产品相关标准和不同等级嵌入式软件必须进行和推荐进行的活动划分出不同等级软件的安全分值符合标准，不同重要等级的软件对应的安全分值如表 7 所示。

表 7 软件安全分值评价对照表

软件重要等级	安全分值合格标准
Ⅰ	≥90
Ⅱ	≥86
Ⅲ	≥81
Ⅳ	≥72

4 实验结果与分析

某航空机载设备研制单位采用以上评价模型对 3 款嵌入式软件产品安全性进行评价，3 款嵌入式软件均为某型飞机通信导航识别系统内的嵌入式软件，分别为 CNI（Communication Navigation Identification，CNI）主控软件、通用平台管理软件、音频告警软件。其中 CNI 主控软件、通用平台管理软件运行在 PowerPC 芯片上，音频告警软件运行在 DSP 芯片上，分别记为 α、β、γ，其对应的软件重要等级为分别为Ⅰ、Ⅱ、Ⅲ级。

步骤一：

A、B、C、D 阶段评价：每个项目在每个阶段分别选择 3 名负责该项目的项目总体技术人员、软件编程人员、软件测试人员、使用总体人员进行评分。每个评价元素的分值为 [0，100]，参与评价的人员依照项目的实际情况进行评分后依据安全分值公式计算出 3 款软件的安全分值 S；

步骤二：

E 阶段评价：嵌入式软件 α 在 E 阶段平均无故障时间满足设计要求但不超过设计时间的 20%，并在使用中发现 1 个轻微安全性问题，E 阶段安全分值为－2；嵌入式软件 β 在 E 阶段平均无故障时间未达到设计要求，并在使用中发现 2 个严重安全性问题，E 阶段安全分值为－12；嵌入式软件 γ 在 E 阶段平均无故障时间超过设计要求的 20%，在使用中发现 1 个轻微安全性问题，E 阶段安全分值为 8；

步骤三：

将各阶段每个评价元素的评分，利用嵌入式软件安全分值 S 的计算公式计算出嵌入式软件 α、β、γ 的安全分值，再对每个阶段 3 名评价人员总评价分值取平均，得出最总软件的安全分值如表 8 所示。

表 8　阶段评价安全分值表

软件	关键等级	A 阶段	B 阶段	C 阶段	D 阶段	E 阶段	安全分值
α	Ⅰ	27.8	23.6	24.4	23.2	－2	92.0
β	Ⅱ	27.2	22.5	18.4	18.5	－12	74.6
γ	Ⅱ	26.3	19.2	16.1	18.6	8	88.2

3 款航空嵌入式软件的评价活动结束后获得安全分值 S，按照其关键等级依据表 7 中的评判标准可以得出安全性评价结果为软件 α 合格，软件 β 不合格，软件 γ 合格。

3 款软件采用以上评价模型对软件安全性进行了评价，在不同软件阶段均有相对应的安全分值，通过评价结果更易于发现各阶段中的安全性问题，相比传统的安全性评价方法评价过程更加全面，评价结果更准确、直观。

5　结束语

嵌入式软件安全是保证航空机载电子系统安全的重要因素，本文基于嵌入式软件开发 V 模型在软件整个生命周期提出了一种嵌入式软件安全性评价方法。通过工程实际应用证明，该方法具有评价过程简单、评价元素全面、评价结果直观的特点。由于软件安全性包含的范围较广，评价元素不可能穷举，实际应用中可在该评价模型的基础上对评价元素进行适当增加、修改或删除，权重参考同等重要的评价元素的权重，在后续的研究中也会持续改进。文中的评价方法主要创新点在于：一是采用分类模糊综合评价法将与安全性相关的元素分析、归纳、整理形成每个阶段的评价元素，再结合工程实践经验赋予权重；根据软件的重要性进行分类，制定不同的评价标准；二是评价不单单是软件使用阶段出现安全问题反馈，而是贯穿软件全生命周期，评价更加完整，对航空机载电子系统型号延续的安全性改进提供了帮助。

参考文献：

[1] 刘维维. 基于 AADL 的嵌入式软件可靠性建模与评估技术研究 [D]. 南京：南京航空航天大学，2017.

[2] Jay Abraham. Improve the quality of embedded software [J]. world Electronic Components，2010 (12)：46－47.

[3] 刘　涛，李　娜. 航空机载软件测试质量评价方法研究 [J]. 计算机测量与技术，2018，26 (11)：285－286.

[4] 张义德，王国庆，杨　平，等. 基于需求的航空嵌入式软件测试技术研究 [J]. 计算机工程与设计 2002，23 (10)：4－5.

[5] 鲁晓成. 嵌入式软件保护关键技术与应用 [D]. 武汉：武汉理工大学，2011.

[6] 张友生，李　雄. 软件开发模型研究综述 [J]. 计算机工程应用，2006，3：109－110.

[7] 姜　磊，张天宏. 基于全数字仿真的航空机载软件验证技术研究 [J]. 航空制造技术，2014，5 (16)：109－109.

[8] 王崑声、经小传. 嵌入式软件安全保证技术 [M]. 北京：国防工业出版社，2015.

[9] 许聚常、朱国庆，等. GJB/Z 141－2004，军用软件测试指南 [S]. 北京：总装备部军标出版发行部，2004.

[10] 吴　炎，王周文，杜　栋. 模糊综合评价软件设计与实证 [J]. 2011，20 (4)：64－65.

[11] 王　纬、潘　华，等. GJB/Z 102A－2012，军用软件安全性设计指南 [S]. 北京：总装备部军标出版发行部，2012.

(上接第 254 页)

[2] 中华人民共和国教育部. 教育部关于公布 2018 年度普通高等学校本科专业备案和审批结果的通知 [EB/OL]. http://www.moe.edu.cn/srcsite/A08/moe_1034/s4930/201903/t20190329_376012.html,2019.

[3] Harrington P. Machine Learning in Action [M]. 2012.

[4] Wang C C，Tan K L，Lin C J. Newton Methods for Convolutional Neural Networks [Z]. 2018.

[5] Guo G，Hui W，Bell D，et al. KNN Model－Based Approach in Classification [M]. On The Move to Meaningful Internet Systems 2003：CoopIS，DOA，and ODBASE. 2003.

[6] 丁世飞，齐丙娟，谭红艳. 支持向量机理论与算法研究综述 [J]. 电子科技大学学报，2011，40 (1)：2－10.

[7] 张宗梅. 利用神经网络求解组合优化问题 [D]. 济南：山东大学，2006.

[8] 尹春林，王　炜，李　彤，等. 基于 RNN 进行面向主题的特征定位方法 [J]. 计算机应用与软件，2017 (6)：12－17.

[9] 中国政府网. 国务院印发《新一代人工智能发展规划》[J]. 广播电视信息，2017 (8)：8.