

面向产品综合设计的故障知识本体研究

任 羿, 曾声奎, 王子寅, 冯 强

(北京航空航天大学工程系统工程系, 北京 100191)

摘 要: 以满足产品的性能与可靠性维修性保障性(RMS)综合设计需求为目标,对产品设计过程中如何预防故障,定位故障及故障维修的相关概念进行分析、总结和归纳,提出了以故障知识为核心,面向产品综合设计的知识本体框架,该框架将相关概念划分为四层进行描述,即产品层、故障基本概念层、故障扩展层、故障应对层。利用本体论方法对相关的核心概念进行了形式化的定义,并给出了基本的故障知识本体和设计应对本体结构。最后以挑战者号航天飞机的失事为例,应用本文建立的故障本体较好地表达了航天飞机故障过程及应对的改进措施,验证了该方法的可行性。

关键词: 故障; 知识; 本体; 综合设计; 故障扩展

中图分类号: TP391 **文献标识码:** A **文章编号:** 1000-1328(2010)02-0615-06

DOI:10.3873/j.issn.1000-1328.2010.02.049

0 引言

产品设计是综合运用多种知识的创造性活动,设计质量的高低依赖于产品设计过程中知识的应用水平,因此获取足够的知识并建立相应的知识模型对产品设计系统至关重要^[1]。国内外产品设计知识建模领域已开展了广泛的研究^[2-4],这些知识建模方法主要是从产品功能实现的角度出发来描述设计知识。可靠性维修性保障性(RMS)是产品固有的设计属性,近年来正逐渐成为并行工程考虑的重点^[5],需要在产品寿命周期建模中给予充分的考虑。与性能设计不同,RMS设计都是围绕产品不能正常工作开展的,都与产品的故障直接或间接的相关,已有的产品设计知识模型没有系统地考虑故障及其相关活动。

本文以故障维修保障信息和 RMS 设计经验知识的共享为目的,利用本体对产品设计中故障相关的核心概念及其关系进行描述,构造出面向性能与 RMS 综合设计的产品故障知识本体框架,包括两方面的内容,(1) 通过一组形式化的本体来定义产品的故障及其相关行为,(2) 利用故障及其相关本体表达产品可靠性维修性保障性设计知识。

1 面向综合设计的故障本体概述

1.1 故障本体

按照 Borst 的定义,本体是一套得到大多数人认同的、关于概念体系的明确的、形式化的规范说明^[6]。国外目前已开展了故障知识建模的研究工作,如 Yoshinobu 等给出了故障过程和故障分类的本体,Lars Dittmann 给出了基于本体的 FMECA 知识重用方法^[7,8],但这些研究是从故障分析的角度出发,主要为故障诊断和局部的可靠性分析服务。本文所建立的故障本体是面向工程设计领域的,其目标是在产品研制和使用过程中,捕获与产品故障相关的知识,并对故障相关的知识进行精确的形式化表达,实现对故障知识明确的理解,并以此为基础,对产品功能设计与可靠性、维修性和保障性设计进行本体建模,获取性能与 RMS 设计知识,为实现综合设计共同的产品模型和知识共享奠定基础。限于篇幅,本文内容仅限于故障本体中最核心的概念及其关系,并重点研究产品的可靠性设计。

1.2 故障本体的结构

故障通常定义为产品或产品的一部分不能或将不能完成预定功能的事件或状态^[9]。由于应用目的的不同,与故障相关的概念非常多,本文重点从产品

的设计角度出发,关注故障的描述,故障在系统中扩展(extend)的规律以及对故障应对的方法途径几个方面。为了清晰地描述产品故障本体,本文分四层来建立故障本体的结构,如图 1 所示。

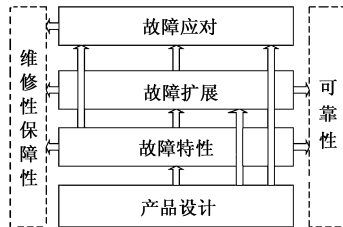


图 1 故障本体的结构

Fig.1 The constructs of failure ontology

2 产品故障本体核心概念

这里采用形式化的方式表达故障本体,故障是一个抽象的概念,不能独立存在,必须依附于一个人造物,即产品,故障是产品的一个外在状态,故障状态与产品自身的组成、结构和功能密切相关,同时产品功能的发挥和保持受所处环境的制约。因此对故障本体的分析必然包含对产品结构和功能设计的分析以及环境条件的分析。本文关于产品和设计相关部分本体借鉴了 M. Bunge 关于实体和系统的表达形式^[10]。

2.1 产品设计层本体定义

从设计的角度看产品,产品总是由基本的物理部件构成的,在这里将其定义为产品元素。

定义 1:产品元素,产品设计中,包含在系统内,不考虑其内部设计的产品物理组成部分,称为产品元素 c_i , 产品由全部产品元素的集合

$$C = \{(c_1, c_2, \dots, c_n \mid \forall c_i, 0 \leq i < n, c_j \subset c_i)\} \quad (1)$$

构成

定义 2:结构体,令 C 为一组产品元素,令

$$B_C = \{(X, Y) \mid X, Y \in C, X \wedge Y\} \quad (2)$$

其中 $B(X, Y)$ 表示产品元素 X, Y 相互耦合。令 $\sigma(C, B_C)$ 为一个图,当且仅当 σ 为联通图时, σ 为结构体,即结构体为相互关联的产品元素构成的集合。

产品设计由多个产品主题构成,产品设计主题 Z 是当前视角下的设计对象,体现为在设计域中,包含当前设计所能反映的全部功能。功能 F 是产品

元素外在状态的全集,既包含期望的正常的功能状态,也包括非期望的非法的功能状态。

定义 3:产品设计主题,产品的设计主题 Z_m 由外在功能模式来表达:

$$Z_m = \langle T, \tilde{F} \rangle \quad (3)$$

其中 $\tilde{F} = \langle F_1, \dots, F_n \rangle: T \rightarrow V_1 \otimes \dots \otimes V_n$

F_i 称为 Z 的第 i 种可能的状态功能, \tilde{F} 称为 Z 的全部状态功能。 T 是一组时刻,蕴含着状态变量的笛卡积。

$$S(Z) = \{\langle z_1, \dots, z_n \rangle \in V_1 \otimes \dots \otimes V_n \mid z_i = F_i(T)\} \quad (4)$$

称为 Z 可能的状态空间,对于产品设计来说,仅考虑符合物理规律的状态变量及其组合关系,因此可令

$$\hat{S} = \{S(Z) \mid \langle z_1, \dots, z_n \rangle \text{ 符合物理规律}\} \quad (5)$$

为合法的状态空间。本文仅考虑合法的状态空间,为了表达方便, $S(Z)$ 代表合法的状态空间。

产品设计主题通过设计元素、结构体等物理元素来实现。

2.2 故障特性层本体定义

故障的定义是建立在产品功能状态的基础上的。这里仅考虑由于产品元素至少有一项状态变量的参数不满足设计要求时而引起的故障,包括产品元素自身的故障和产品元素故障的扩展而引起产品功能结构的故障。

定义 4:若设计主题的功能模式为 $Z_m = \langle D, \tilde{F} \rangle$, $fa(z) \in Fa(z)$ 为故障的判定规则,那么产品元素的故障空间为

$$S_{fa}(Z) = \{\langle z_1, \dots, z_n \rangle \in V_1 \otimes \dots \otimes V_n \mid \tilde{F}\} \quad (6)$$

其中 $\tilde{F} = \{\tilde{F} \text{ 满足于每个 } l(Z) \in L(Z)\}$

称 $Z_{fm} = \langle D, \tilde{F} \rangle$ 为故障功能模式。

定义 5:故障事件,一个序列偶

$$Ft = \langle s', s \rangle \quad (7)$$

称为一个故障事件,其中, $s \in S_{fa}(Z)$, $s' \in \overline{S_{fa}(Z)}$, 即产品从正常状态到故障状态的转换。若触发故障发生的条件丧失,产品能够从故障状态转换为正常状态称为可逆故障事件,反之称为不可逆故障事件。

定义 6:故障演变,若产品元素的故障功能模式

为 $Z_{fm} = \langle D, \bar{F} \rangle$, 令 $t \in D$, 若产品元素的功能故障演变可以表达为时间的函数 $f_i(E, t) (t \leq t_{故障})$, 则 Z 的故障演变为

$$hf(Z) = \{ \langle t, \bar{F}(t) \rangle \} \quad (8)$$

根据 t 的不同, 故障演变可以分为不同的种类, 若 $t \rightarrow 0$, 成为瞬时故障, 故障演变过程为时间连续的, 称为渐变故障, 故障演变过程为时间离散的, 称为间歇故障。产品元素的故障演变有其内在的机理作用。

2.3 故障扩展层本体定义

定义 7: 故障关联, 产品元素的故障功能模式关联 $B(X, Y)$, 当且仅当 $(X \triangleright Y) \vee (Y \triangleright X)$, 其中

$$(X \triangleright Y) \leftrightarrow hf(Y | X) \neq hf(Y) \quad (9)$$

表示故障功能模式 X 作用于故障功能模式 Y 。即若两个故障功能模式的演变是独立的, 则两项故障功能模式之间没有关联。

定义 8: 故障扩展, 若 X 为产品元素 c 的故障功能模式, Y 为包含产品元素 c 的结构体 σ 的故障功能模式, 若 $(X \nabla Y) \leftrightarrow (Y | X) \neq hf(Y)$ 则称为 c 向 σ 的故障扩展。

故障扩展包括两类, 分别为拓扑扩展和逻辑扩展, 拓扑扩展是指故障沿着系统实际的物理结构, 从一个产品元素向其它产品元素传播, 拓扑扩展是时间的函数。逻辑扩展是指系统中的一个产品元素的故障导致系统内的结构体的功能不能实现。故障扩展将导致一定的后果, 如是否会导致周围产品元素的故障, 是否会导致结构体的故障, 是否会导致系统的最终故障等。扩展后果可根据严重程度分级。

故障扩展是造成产品故障的主要内因, FMECA 就是一种对产品元素故障扩展的影响和后果进行分析的工程方法。

2.4 故障应对层本体定义

故障应对指产品在使用过程中, 如何预防故障、发现故障和恢复故障的活动, 但产品故障应对的能力也与自身的设计特性有着密切的关系, 产品的测试性、维修性和保障性设计就是主要的故障应对设计活动。由于测试、维修和保障涉及的概念较多, 因此相关形式化本体的定义比较复杂, 限于篇幅本文不作形式化的定义。

定义 9: 隔离故障, 若结构体 σ 具备的故障功能

Y 与一组产品元素 C 的故障功能的形成故障关联, 发现产品的故障或潜在故障, 并将故障定位到一个或一组元素。

定义 10: 故障维修, 将结构体 σ 从故障功能状态恢复到正常功能状态的活动集合。

定义 11: 维修保障, 支持故障维修的活动集合, 以及这些活动所依赖的各类资源实体的集合。

2.5 故障本体的关系

本体的 4 种基本关系^[11], 即 part-of、kind-of、instance-of、attribute-of 在故障本体的描述中仍然是适用的。

part-of 表达概念之间部分与整体的关系; kind-of 表达概念之间的继承关系; instance-of 表达概念的实例和概念之间的关系; attribute-of 表达某个概念是另外一个概念的属性。这四种关系在故障本体中依然存在, 除此之外, 故障本体还存在如下的关系:

(1) 产品元素或结构体的故障状态之间故障的相互影响关系称为“关联到”关系 (Causation-of), 关联关系可分为单向关联 (Unidirectional Causation-of) 和双向关联 (Bidirectional Causation-of), 代表着故障状态影响的方向。

(2) 产品元素的故障向产品结构体传播的关系称为“扩展到”关系 (Proliferation-of), 该关系同时与“故障状态”、“故障扩展”、“产品元素”和“结构体”等概念相对应, 该关系的实质是表达产品元素的故障状态通过某种故障扩展方式, 向结构体传播, 形成了结构体的故障状态。

产品元素故障向结构体的扩展关系又可分为两类子关系, 即拓扑扩展关系 (Topological Proliferation-of) 和逻辑扩展关系 (Logical Proliferation-of)。

(3) 产品故障状态与正常状态之间的转移称为“转换为”关系 (Change-of)。该关系同时与故障应对概念相对应。

(4) 针对故障的状态和扩展路径采用的设计措施称为“设计应对” (Redesign-of)。该关系包括对故障源的监测, 对故障扩展路径的阻断和监测等。

3 故障本体的应用

产品设计过程是利用知识和产生知识的过程, 基于本体的故障知识描述为产品性能设计和 RMS

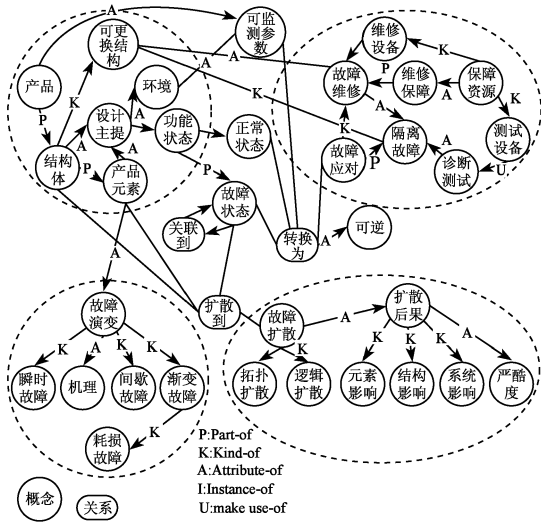


图 2 面向综合设计的故障本体框架

Fig.2 Failure ontology framework for IPRMS

设计知识的联系建立了桥梁。基于知识的产品性能与 RMS 综合设计是将实现规定功能的知识和如何防止和减低故障的知识有机结合起来,共同实现高效能产品的设计过程。

3.1 基于本体的故障案例描述

利用本体可以将故障案例的发生发展过程以及故障与产品设计之间的关系进行形式化的描述,为这些知识的重用奠定基础。其建立的主要过程包括产品、故障等相关概念的实例化,构建实例对象关系等内容,由于对故障过程的认识程度的不同,故障案例的内容不一定涵盖全部的故障本体概念,是故障本体概念的子集。

3.2 基于本体的故障应对措施描述

在故障知识描述的基础上,可进一步描述如何在设计中“阻止”故障发生的知识。针对产品可能发生的各类故障,产品设计要从多个角度来采取应对措施,可以对各类应对措施建立本体,描述设计应对措施的相关概念以及与故障概念之间的关系,初步建立的设计应对措施本体如图 3 所示。其主要部分包括:

(1) 产品元素和环境的控制。设计中如何优选元器件原材料,以减少缺陷。如何进行耐环境设计,使缺陷对环境的敏感程度降低。

(2) 故障扩展的控制。设计中如何对拓扑故障扩展进行封闭,对逻辑扩展采用何种冗余设计技术,阻止故障的逻辑传播,同时对故障源采取何种故障

补偿措施等;

(3) 采取的故障应对设计。如何进行测试性设计、维修性设计和保障性设计。

(4) 对灾难性故障后果的控制。如何通过安全性设计来阻止故障造成灾难性后果。

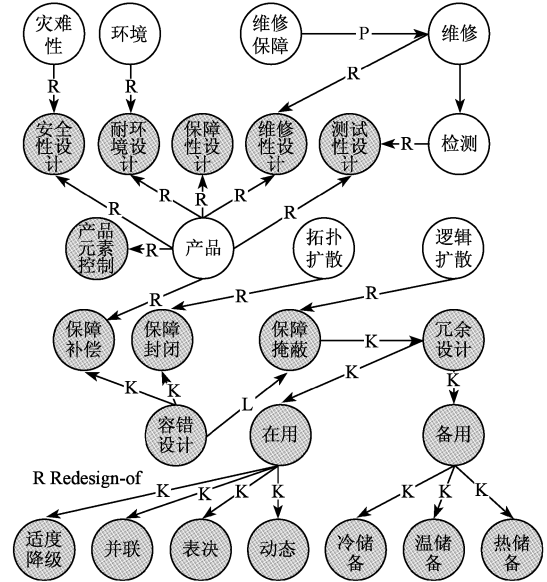


图 3 设计应对措施本体

Fig.3 Design response action ontology

设计应对措施本体形式化地记录了产品进行性能设计与可靠性维修性保障性的关系,以及蕴涵在设计过程中的设计知识。

3.3 故障及其应对措施的本体描述案例

以美国 1986 年挑战者号航天飞机失事事故为例,利用故障本体对其进行描述。

根据事故调查的情况^[12],可以利用故障本体对这一过程进行描述,如图 4 所示。需要考察的产品元素为固体火箭助推器的 O 型环,其设计主题为 <工作状态,连接处密封>,所处的环境为低温,其功能状态为 <封闭燃气,泄漏燃气>,其中“泄漏燃气”为故障功能状态,该功能故障在低温环境和燃气高压的双重作用下产生,并通过物理路径逐步向助推器外壁、助推器支柱、主燃料箱传播,直至航天飞机,最终导致航天飞机的爆炸。挑战者号的助推器连接如图 5a 所示。

基于该故障案例本体,可利用设计应对措施本体对航天飞机火箭助推器的改进设计进行描述。

改进后的火箭助推器连接如图 5b 所示,利用本

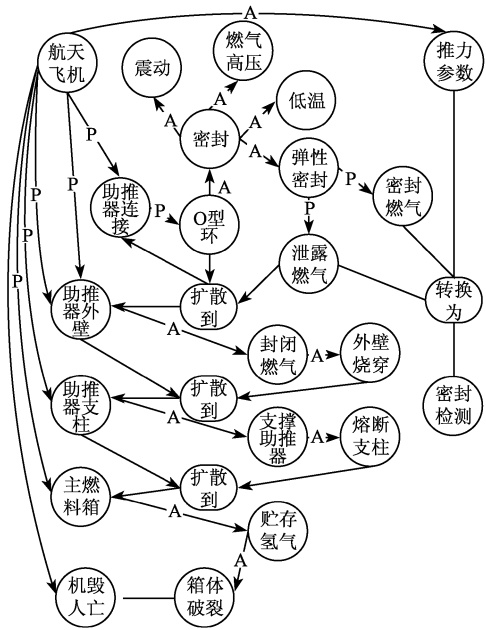
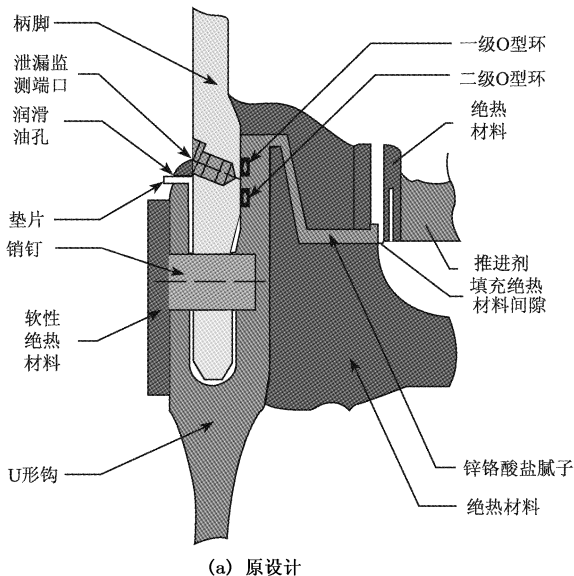


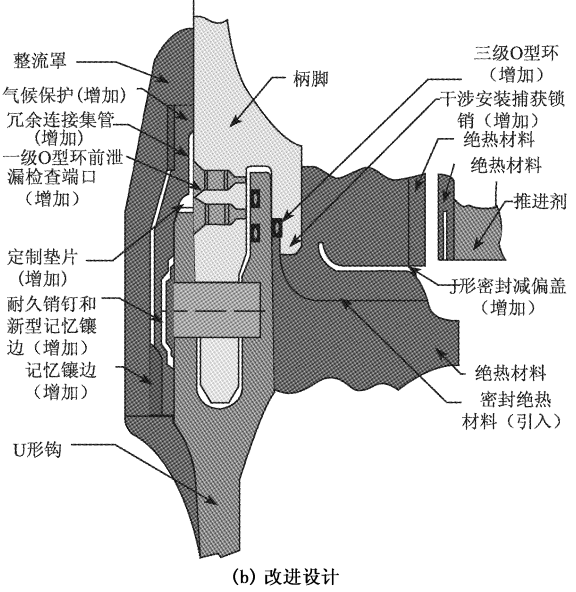
图 4 航天飞机故障案例本体描述

Fig.4 The ontology based description of the disaster

体可以将这些改进与应对措施与故障之间建立联系,如图 6 所示。从产品的可靠性角度出发,重点在于防止拓扑扩展,因此增加了第三级 O 型环,使 O 型环始终处于受压密封的状态。阻断了一二级 O 型环失效可能带来的故障拓扑扩展,同时重新设计连接销钉,使连接更加牢固,提高了结构体的可靠裕度。进行了耐环境设计,增加了气候保护,可以将温度维持在 75 华氏度之上,也可以防止水的进入。由于火箭助推器是一次性使用产品,没有进行维修性



(a) 原设计



(b) 改进设计

图 5 助推器连接的原设计和改进设计^[12]

Fig.5 Field joint's original design and redesign^[12]

方面的设计。在保障设计方面,设计了安装捕获锁(同时起到减少震动影响的作用),重新设计了地面装配支持设备,减少了安装变形,同时对运输和搬运设备也进行了改进。在测试性设计方面,增加了一级 O 型环前泄漏检查端口,提高了故障监测的能力。针对可能发生的灾难性后果,NASA 考虑为航天飞机设计安全逃逸装备,但由于技术和经济条件的限制,没有实现这方面的改进。

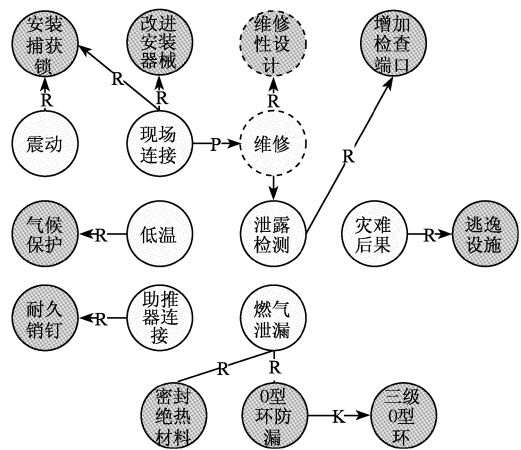


图 6 航天飞机改进设计本体描述

Fig.6 The redesign ontology structure of space shuttle

4 结束语

针对当前产品设计领域已建立的故障本体的局

限性,本文从产品的整体性及其同外界环境的辩证关系出发,分析了产品故障的发生、扩展及其预防和维修保障的基本规律,给出了面向综合设计的故障本体的形式化基本概念。利用这些概念以及概念间的关系建立了面向综合设计的故障本体框架,并给出了基于故障本体实现产品性能设计和 RMS 设计有机联系的方法,可以指导基于知识的性能与 RMS 的综合设计体系的建立。

参考文献:

- [1] Yoshinobu Kitamura. Roles of ontologies of engineering artifacts for design knowledge modeling[C]. EDIProD 2006.
- [2] 胡玉杰,李善平,郭鸣.基于本体的产品知识表达[J].计算机辅助设计与图形学学报,2003,15(12):1531-1537.[HU Yujie, LI Shan-ping, GUO Ming. Ontology-based product knowledge representation[J]. Journal of Computer-Aided Design & Computer Graphics, 2003,15(12):1531-1537(in Chinese).]
- [3] 应杭,李善平,郭鸣,等.本体在产品知识 S-B-F 表达模型中的应用研究[J].计算机集成制造系统,2004,10(12):30-38.[YING Hang, LI Shan-ping, GUO Ming, et al. Research on ontology-based product knowledge S-B-F representation model[J]. Computer Integrated Manufacturing Systems, 2004,10(12):30-38(in Chinese).]
- [4] Yoshinobu Kitamura, Riichiro Mizoguchi. Ontology-based Functional-Knowledge Modeling Methodology and its Deployment[C]. KAW 2004.
- [5] Clifton B, Robert R. Integrating Reliability and Maintainability into a Concurrent Engineering environment[R]. AIAA-93-1021,1993.
- [6] 邓志鸿,唐世渭,张铭,等. Ontology 研究综述[J]. 北京大学学报(自然科学版), 2002, 38(3): 730-738. [DENG Zhi-hong, TANG Shi-wei, ZHANG Ming, et al. Overview of ontology[J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2002, 38(3): 730-738(in Chinese).]
- [7] Yoshinobu Kitamura and Riichiro Mizoguchi. An ontological analysis of fault process and category of faults[C]. Proc. of Tenth International Workshop on Principles of Diagnosis (DX-99), 1999, 8(11): 118-128.
- [8] Lars Dittmann. Performing FMEA using ontologies[C]. Eighteenth International Workshop on Qualitative Reasoning, 2004.
- [9] GJB451A, 可靠性维修性保障性术语[S]. [GJB 451A, Reliability, Maintainability & Supportability Terms[S](in Chinese).]
- [10] Borst W N. Construction of engineering ontologies for knowledge sharing and reuse[D]. CTIT Ph.D-thesis series No.97-14, University of Twente(NL), Enschede, 1997.
- [11] Yair Wand, Ron Weber. An Ontological Model of an Information System[J]. IEEE Transactions on Software Engineering, 1990, 16(11).
- [12] The Presidential Commission on the Space Shuttle Challenger Accident [R/OL]. <http://history.nasa.gov/rogersrep>.

作者简介:任羿(1973-),男,高级工程师,研究方向为可靠性系统工程和质量特性综合设计。
通信地址:北京航空航天大学工程系统工程系(100191)
电话:13911368830
E-mail:renyi@buaa.edu.cn

Ontology-based Failure Knowledge Modeling for Integrated Product Design

REN Yi, ZENG Sheng-kui, WANG Zi-yin, FENG Qiang

(Department of System Engineering of Engineering Technology, Beihang University, Beijing 100083, China)

Abstract: In view of the integration design of performance, reliability, maintainability and supportability (IPRMS), the concepts concerning on failure prevention, fault localization and failure maintenance were analyzed and summarized. Then an ontology-based knowledge framework for IPRMS was proposed based on the kernel of failure knowledge, and related concepts were divided into four layers, that is products level, essential fault/failure concepts level, failure extendibility level and failure response level. Related essential concepts were defined in formalized style, and the basic framework of failure knowledge ontology and design response ontology were presented. Finally, a case study of the Space Shuttle Challenger Accident was presented to demonstrate the ability of failure ontology to depict knowledge of product failure and design improving, which shows that our methods are feasible and satisfactory.

Key words: Fault/failure; Knowledge; Ontology; IPRMS; Failure extendibility