doi:10.3969/j.issn.1671-637X.2015.08.013

基于漏洞属性分析的软件安全评估方法

韦 涛, 彭 武, 王冬海
(中国电子科技集团公司电子科学研究院,北京 100041)

摘 要: 软件漏洞存在于软件生命周期的各个阶段。目前已有的软件漏洞评估方法所涉及的属性较少,且大多数只是对软件采取定性的评估。首先分析了现在比较权威的漏洞库,通过相关漏洞库找到对软件安全影响比较大的属性,在此基础之上利用专家经验法来量化相关属性,并提出对软件安全进行量化评估的方法,为后续的软件漏洞修复工作提供有效依据。

关键词: 软件安全评估; 漏洞库; 量化评估; 漏洞修复
中图分类号: V271.4; TP393.08 **文献标志码**: A **文章编号**: 1671-637X(2015)08-0066-05

A Method for Software Security Assessment Based on Analysis of Software Defects

WEI Tao, PENG Wu, WANG Dong-hai
(China Academy of Electronics and Information Technology, CETC, Beijing 100041, China)

Abstract: Software defects exist in all stages of the software life cycle. The current software defect assessment methods generally investigate only a few kinds of properties, most of which just make a qualitative assessment. In this paper, the authoritative defect databases are introduced. By the relevant databases, the corresponding properties that have comparatively great impact on the software defect are identified. Based on the analysis, the corresponding properties are quantified by applying the method of expertise, and a quantitative software assessment method is presented, which provides an effective reference for subsequent software repair.

Key words: software security assessment; vulnerability database; quantitative assessment; vulnerability fix

0 引言

随着社会信息化程度的提升,各行业的发展也越来越智能化、自动化,而这一切都与软件行业的快速发展息息相关。软件漏洞的分析、发现、修复问题日益突现。

首先,软件中的漏洞具有不可避免性。国际知名气动设备供应商Humphrey的数据表明[1],没有经过个人软件过程(PSP)培训的有经验的软件工程师漏洞的引入率一般在每千行代码50~250个,经过PSP培训者平均漏洞引入率为每千行代码50个,而且这个数据一般和工程师的经验没什么关系。目前,一般软件的漏洞密度为每千行代码4~40个,高水平的软件研制组织所研制的软件,可以达到的软件漏洞密度为每千行代码2个。但并不是所有漏洞都必须修复,某些漏洞对软件的正常使用影响不大,修复这些漏洞需要投入大量的人力和财力[2],所以没有必要对所有漏洞进行修复。

其次,软件漏洞评估技术是软件漏洞修复的前提条件。软件中存在各种类型的漏洞,而软件漏洞评估技术通过科学合理的计算方法得出漏洞对软件的危害程度,从而能够为漏洞是否需要修复提供有效的判断依据。

本文首先介绍了一些国内外知名漏洞库,并对各漏洞库属性的特点进行分析,提出与漏洞评估相关的属性并进行量化,接下来利用相关漏洞评估方法对具体的软件漏洞进行安全评估。

1 国内外漏洞数据库

1.1 CVE

CVE(Common Vulnerabilities & Exposures)即"公

收稿日期:2014-06-26 修回日期:2015-02-01
基金项目:国防基础科研项目(B1120132031)
作者简介:韦 涛(1989—),男,湖北黄冈人,硕士生,研究方向为信息安全。

共漏洞和暴露”，是目前最具权威的漏洞数据库，为广泛认同的信息安全漏洞或者已经暴露出来的漏洞给出一个公共的名称。使用一个共同的名字，可以帮助用户在各自独立的各种漏洞数据库中和漏洞评估工具中共享数据（虽然这些工具很难整合在一起），这样就使得 CVE 成为了安全信息共享的“关键字”。

CVE 提供的内容主要包括漏洞名称、简单描述和参考这 3 部分。其中，漏洞名称是漏洞的 CVE 标准化命名，CVE 命名的产生要通过该组织编委会严格审查。首先，CNA（Candidate Numbering Authority）机构为一个新的安全漏洞分配一个被称为 CAN（CVE Candidate）的 CVE 候选号，然后，由编委会研究讨论是否批准一个 CAN 成为 CVE。因此，CVE 漏洞命名通常包括 CVE 和 CAN 两种形式。但是，为了便于用户维护和使用 CVE 命名，MITRE 已将 CAN 统一改为 CVE。

CVE 中关于具体的属性介绍的比较少，根据 CVE 官方网站统计，截止到 2014 年 1 月 4 日，记载的漏洞条数为 59110 条。

1.2　Bugtraq

Bugtraq[3] 库是 Symantec 公司的 SecurityFocus 组织根据收集的漏洞公布邮件而发布的漏洞数据库，描述的漏洞属性包括名称、BID 编号、类别（按起因）、CVE、攻击源、公布时间、可信度、受影响的软件或系统以及讨论、攻击方法、解决方案、参考等。该漏洞库最大的特点是提供了较详细的攻击方法或脚本，用户可以应用这些方法测试或识别该漏洞，该漏洞数据库描述的漏洞属性较完备且漏洞更新及时。

截止 2014 年 1 月 4 日，收录的漏洞数近 45270 个。

1.3　CVSS

CVSS（Common Vulnerability Scoring System）即通用缺陷评分系统，是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。

CVSS 是安全内容自动化协议（SCAP）的一部分，通常 CVSS 和 CVE 由美国国家漏洞库（NVD）一同发布并保持数据的更新。

漏洞是网络安全中的一个重要因素，在多种安全产品（如漏洞扫描、入侵检测、防病毒、补丁管理等）中涉及到对漏洞及其可能造成影响的评价，但目前业界并没有统一通用的评价体系标准。通用漏洞评价体系（CVSS）是由 NIAC 开发、FIRST 维护的一个开放并且能够被产品厂商免费采用的标准，利用该标准，可以对漏洞进行评分，进而帮助判断修复不同缺陷的优先等级。CVSS 评价系统如表 1 所示。

表 1　CVSS 评价系统

Table 1　CVSS evaluation system

	要素	可选值	评份标准
Base Metrics（基本评价）	攻击途径（AV）	远程/本地	0.7/1.0
	攻击复杂度（AC）	高/中/低	0.6/0.8/1.0
	认证（Au）	需要/不需要	0.6/1.0
	机密性（c_I）	不受影响/部分地/完全	0/0.7/1.0
	完整性（I_I）	不受影响/部分地/完全	0/0.7/1.0
	可用性（A_I）	不受影响/部分地/完全	0/0.7/1.0
Temporal Metrics（生命周期评价）	利用代码（TE）	未提供/验证方法/功能性代码/无需代码	0.85/0.90/0.95/1.00
	修正程度（RL）	官方补丁/临时补丁/临时解决方案/无	0.87/0.90/0.95/1.00
	确认程度（RC）	传言/未经确认/已经确认	0.90/0.95/1.00
Environment Metric（环境评价）	影响（CDP）	无/低/中/高	0/0.1/0.3/0.5
	目标分布（TD）	无/低/中/高（0/1% ~15%/16%~49%/50% ~100%）	0/0.25/0.75/1.00

具体的算法为 BaseScore = round_to_1_decimal(10 * AV * AC * Au * ((c_I * ConfImpactBias + (I_I * IntegImpactBi + (A_I * AvailImpactBias)))；TemporalScore = round_to_1_decimal(BaseScore * TE * RL * RC)；EnvironmentalScore = round_to_1_decimal((TemporalScore + ((10 - TemporalScore) * CDP) * TD)。

1.4　国家信息安全漏洞共享平台

我国的国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，英文简称 CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

建立 CNVD 的主要目标即与国家政府部门、重要信息系统用户、运营商、主要安全厂商、软件厂商、科研机构、公共互联网用户等共同建立软件安全漏洞统一收集验证、预警发布及应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，进而提高我国信息系统及国产软件的安全性，带动国内相关安全产品的发展。

CNVD 将漏洞分为应用漏洞和行业漏洞两大类。其中：应用漏洞包括 WEB 应用漏洞、安全产品漏洞、应用程序漏洞、操作系统漏洞、数据库漏洞和网络设备漏洞六大类；而行业漏洞则细分为电信、移动互联网和工

控系统等三类。

截止 2013 年 12 月 23 日，收录漏洞总数为 57 716 条，其中：WEB 应用漏洞记录 7842 条；安全产品漏洞记录 504 条；应用程序漏洞记录 18 804 条；操作系统漏洞记录 2412 条；数据库漏洞记录 988 条；网络设备漏洞 1199 条。具体如图 1 所示。

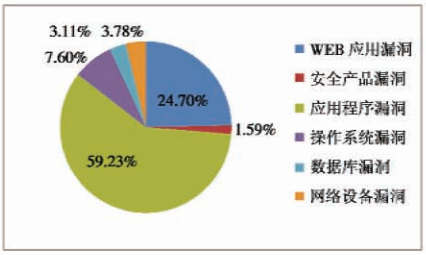

图 1 信息安全漏洞库中各类漏洞数

Fig. 1 All kinds of loopholes in CNVD

漏洞种类分为软件漏洞和非软件漏洞。其中：软件漏洞包括 WEB 应用漏洞、应用程序漏洞、操作系统漏洞、数据库漏洞；非软件漏洞包括安全产品漏洞和网络设备漏洞。统计结果显示软件漏洞占据总漏洞的 94.6%，可见软件漏洞在所有漏洞中所占比重之大。

危险级别从攻击途径、攻击复杂度、是否需要认证、机密性、完整性、可用性等六方面综合考虑，然后得出一个系统的综合漏洞评分。

CNVD 将漏洞产生的原因分为：输入验证错误、访问验证错误、意外情况处理错误、边界条件错误、配置错误、竞争条件、环境错误、设计错误、其他错误、未知错误。截止 2013 年 12 月 28 日，各种错误占比如图 2 所示。

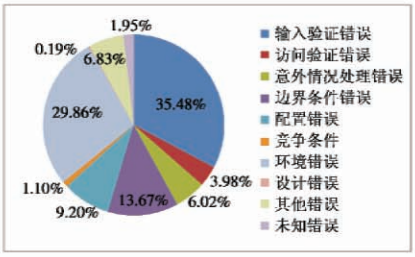

图 2 信息安全漏洞库中缺陷产生原因占比图

Fig. 2 Pie chart of defect causes in CNVD

漏洞引发的威胁包括：其他、拒绝服务、普通用户访问权限获取、未授权的信息修改、未授权的信息泄露、未知、管理员访问权限获取。漏洞严重程度包括：高、中、低。漏洞利用的攻击位置包括：其他、本地、远程。综上所述，国家信息安全漏洞共享平台中包括的基本属性有：CNVD 标识号、攻击途径、攻击复杂度、是否需要认证、机密性、完整性、可用性、漏洞产生原因、漏洞引发的威胁、漏洞严重程度和漏洞利用的位置[4]。

1.5 中国国家信息安全漏洞库

中国国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD），是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设、运行维护的国家信息安全漏洞库，为我国信息安全保障提供基础服务。

截止 2013 年 12 月 28 日，中国国家信息安全漏洞库中共收录了 63 692 条漏洞记录，而且上面能查询到的信息远没有国家信息安全漏洞共享平台那么多。它发布的漏洞信息详情中包括：漏洞名称、CNNVD 编号、发布时间、更新时间、危害等级、漏洞类型、威胁类型、CVE 编号和漏洞来源。

CNNVD 将漏洞类型分为 6 大类。分别为跨站脚本漏洞（8033）、缓冲区溢出漏洞（7336）、SQL 注入漏洞（6189）、未知漏洞（5915）、输入验证漏洞（5774）和资料不足漏洞（4004）。各类型漏洞占比如图 3 所示。

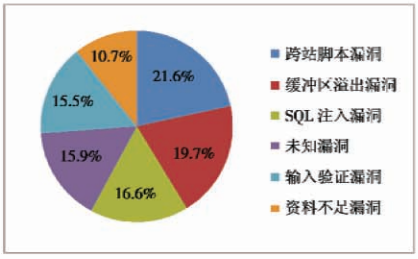

图 3 中国国家信息安全漏洞库类型统计图

Fig. 3 Vulnerability database types in CNNVD

1.6 综合比较

国内外关于软件漏洞方面的数据库还有很多，而且各有其特点，为了能够对这些数据库有一个更为直观的了解和比较，现从收录漏洞数目、记录属性多少、更新速度以及其独有特点等 4 个方面对上述 5 个库进行综合比较，如表 2 所示。

表 2 漏洞库综合比较表

Table 2 Comparison of comprehensive vulnerability databases

漏洞库名称	收录漏洞数量	记录属性多少	更新速度	独有特点
CVE	59 110	少于 10	一般	标准弱点命名
Bugtraq	45 270	多于 20	快	突出脚本攻击代码
CVSS	——	10～20	快	简单的通用评分
国家信息安全漏洞共享平台	57 716	10～20	较慢	将漏洞按应用和行业分类
中国国家信息安全漏洞库	63 693	少于 10	较慢	漏洞类型分类很细

表 2 中国家信息安全漏洞共享平台和中国国家信息安全漏洞库数据是截止到 2013 年 12 月 28 日，其他数据库是截止到 2014 年 1 月 4 日。

2　相关漏洞属性的量化方法与整体评估

2.1　软件漏洞属性综合

CVE、Bugtraq、CVSS(通用漏洞评分系统)、国家信息安全漏洞共享平台和国家信息安全漏洞库主要是从信息安全这个大的方面阐述了信息安全方面的漏洞，而软件是信息安全系统中的重要组成部分，所以对于软件漏洞的属性必须要考察得更细致。

软件包括系统软件、应用软件和介于这两者之间的中间件[2]。系统软件是负责管理计算机系统中各种独立的硬件，使得它们可以协调工作，一般系统软件包括操作系统和一系列基本的工具(如编译器、数据库管理、存储器格式化、文件系统管理、用户身份验证、驱动管理、网络连接等方面的工具)；而应用软件是为了某种特定的用途而被开发的软件，它可以是一个特定的程序，也可以是一个由众多独立应用程序组成的庞大的软件系统，比如数据库管理系统。

通过对相关漏洞库的分析了解以及对软件漏洞属性的理解，现将各漏洞库中的所有属性进行一个比较全面的综合，它们分别为：攻击途径、攻击复杂度、认证、机密性、可用性、完整性、漏洞起源、漏洞来源、漏洞引入时间、漏洞时间影响力、漏洞标识、漏洞修复优先级、漏洞状态、漏洞类型、漏洞攻击所需权限等。总共归纳出 15 条相关属性。

2.2　属性的量化

由于所选取的属性大多是定性的属性，利用这些属性来评估软件漏洞的危害程度还比较困难，因此需要对各种属性所表现出来的不同状态进行具体的量化工作。

对相关属性的量化方法采取的原则是：对于在已知的能查阅到的漏洞库中有明确记载的属性量化值，这一部分属性的量化可以参考相关漏洞库直接加以引用或稍加修改，而对另一部分在相关漏洞数据库中并没有给出量化的属性，采用向软件领域内的专家发放专业制作的调查表的方法，通过收集到的专家调查表结果对具体属性进行量化。

下面以漏洞修复优先级这个属性为例，说明采用专家调查表方法的具体过程。

假设第 i 位专家对优先修复、正常修复和延迟修复这3种状态的量化向量为 $\boldsymbol{M}_i=(X_i,Y_i,Z_i)$，总共向 K 位专家发放了专家调查表。其中，X_i,Y_i,Z_i 区间为[0,1]，量化后的优先修复量化值为 $X=\frac{1}{k}\sum_{i=1}^{k}X_i$；同理，关于正常修复的量化值 $Y=\frac{1}{k}\sum_{i=1}^{k}Y_i$；延迟修复的量化值为 $Z=\frac{1}{k}\sum_{i=1}^{k}Z_i$[5]。

其他在相关漏洞数据库中没有量化过的属性参照此种方法发放专家调查表，将专家填写完成的调查表收集后按照上述算式得到相应的漏洞属性量化值，整理如表 3 所示。

表 3　具体漏洞属性量化值

Table 3　Specific vulnerability quantized value attribute

漏洞属性	可选值	量化值
攻击途径	远程/本地	0.7/1.0
攻击复杂度	高/中/低	0.6/0.8/1.0
认证	需要/不需要	0.6/1.0
机密性	不受影响/部分地/完全	0.5/0.7/1.0
完整性	不受影响/部分地/完全	0.5/0.7/1.0
可用性	不受影响/部分地/完全	0.5/0.7/1.0
漏洞起源	设计错误/操作错误	0.7/1.0
漏洞来源	内部触发/外部攻击	0.7/1.0
漏洞引入时间	小于 7 天/7 到 30 天/大于 30 天	0.5/0.7/1.0
漏洞时间影响力	短/中/长	0.5/0.7/1.0
漏洞标识	粗略/详细	0.6/1.0
漏洞修复优先级	优先修复/正常修复/延迟修复	0.5/0.7/1.0
漏洞状态	未被激活/已被激活	0.6/1.0
漏洞类型	语法/环境/接口	0.5/0.7/1.0
漏洞攻击所需权限	根/一般/普通	0.5/0.7/1.0

2.3　属性权值的确定

软件漏洞属性对应的权值采用专家环比法[6]，通过考虑软件属性的固有特点[7]，专家们通过多年从事软件相关行业的经验来评估软件缺陷漏洞的权值。

设 $F_1,F_2,\cdots,F_{15}$ 分别对应相应属性，其中，将 F_1 即攻击途径所对应的权重设为 1.00，然后利用相邻属性之间的比较来得出相应各属性的归一化权重，结果如表 4 所示。

表 4　软件漏洞属性权重

Table 4　Software vulnerabilities attribute weights

准则	F_k/F_{k-1}	权重	归一化权重
F_1	——	1.000	0.081
F_2	1.050	1.050	0.085
F_3	0.900	0.945	0.076
F_4	1.200	1.134	0.092
F_5	1.000	1.134	0.092
F_6	1.000	1.134	0.092
F_7	0.800	0.907	0.073
F_8	0.700	0.635	0.051
F_9	0.950	0.603	0.049
F_{10}	1.000	0.603	0.049
F_{11}	0.850	0.513	0.041
F_{12}	1.200	0.615	0.050
F_{13}	1.050	0.646	0.052
F_{14}	0.950	0.614	0.050
F_{15}	1.250	0.844	0.067

2.4 漏洞评估方法

对一个具体的软件漏洞的整体评估[8-9]，就是要用具体的数值来表示漏洞的危害程度，这是在综合考虑影响软件漏洞的属性及其属性的权重基础上而得到的。具体的评估方法如下：1）由 m 个属性构成属性集 $f=\{f_1,f_2,\cdots,f_m\}$，其对应属性的量化值向量为 $\boldsymbol{\alpha}=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$；2）属性权重向量为 $\boldsymbol{\beta}=(\beta_1,\beta_2,\cdots,\beta_m)^{\mathrm{T}}$，并满足约束条件 $\sum_{j=1}^{m}\beta_j=1$；3）漏洞危险程度系数 $K=\boldsymbol{\alpha}\cdot\boldsymbol{\beta}$。

当相应漏洞属性值和权重都已知时，其漏洞危险程度系数 K 也就能够得到，而难度系数 K 的范围为 0.5～1.0。可进一步将 K 细化，当 $K\in[0.5,0.65]$ 时，该漏洞危险程度为低；当 $K\in(0.65,0.85)$ 时，该漏洞危险程度为中等；当 $K\in[0.85,1.00]$ 时，该漏洞危险程度为高。

3 实例分析

通过国家信息安全漏洞共享平台上提供的 Oracle MySQL Server Optimizer 子件远程拒绝服务漏洞，其在 CNVD 中的编号为 CNVD-2014-00285，对应的 BUGTRAQ ID 为 64904，CVE ID 为 CVE-2014-0386。该漏洞的具体表现特性为 Oracle MySQL Server Optimizer 子件存在未明安全漏洞，允许远程攻击者利用漏洞使服务程序崩溃，漏洞所表现出来的危险级别为中等。漏洞库中漏洞表现的属性有：攻击途径为远程网络；攻击复杂度为低；认证为一次；机密性为不受影响；完整性为不受影响；可用性为部分的。其他的属性对应状态通过查阅该漏洞的详细信息而得到具体的量化值，如表5所示。

表5 具体软件漏洞属性量化

Table 5 Quantification of specific software vulnerabilities property

漏洞属性	属性对应状态	量化值
攻击途径	远程	0.7
攻击复杂度	低	1.0
认证	需要	0.6
机密性	不受影响	0.5
完整性	不受影响	0.5
可用性	部分的	0.7
漏洞起源	设计操作	0.7
漏洞来源	外部攻击	1.0
漏洞引入时间	7到30天	0.7
漏洞时间影响力	短	0.5
漏洞标识	详细	1.0
漏洞修复优先级	正常修复	0.7
漏洞状态	已被激活	1.0
漏洞类型	接口	1.0
漏洞攻击所需权限	一般	0.7

由表5可以得到 Oracle MySQL Server Optimizer 子件远程拒绝服务漏洞相对应属性的量化值向量 $\boldsymbol{\alpha}$，由表4可以得到该软件漏洞属性权值向量 $\boldsymbol{\beta}$，而由软件漏洞危险程度的算式 $K=\boldsymbol{\alpha}\cdot\boldsymbol{\beta}$，可以计算出该软件漏洞危险程度系数值为 0.730。利用此评估计算方法所计算出的结果与该漏洞所表现出来的中等危险级别相一致。

4 小结

本文通过相关漏洞数据库整理出对软件缺陷影响较大的属性并进行属性的量化工作，提出了一种基于专家经验的软件漏洞评估方法，最后通过具体的实例验证了该方法的准确性。该评估方法能将对软件漏洞的评估量化到一个具体的值，能将软件漏洞的危险程度量化到一个具体的值，这对于以后的软件漏洞修复工作是大有好处的。但是本文对于评估值的进一步精确有待继续研究和探讨。

参考文献

[1] YUE C. Software security economics and threat modeling based on attack path analysis: a stakeholder value driven approach[DB/OL]. [2007-10-01]. http://sunset.usc.edu/case/TECHRPTS/phD_Dissertation.pdf.

[2] 鲁伊莎，曾庆凯. 软件脆弱性分类方法研究[J]. 计算机应用，2008，28(9)：2245-2248.（LU Y S, ZENG Q K. Survey of software vulnerability taxonomies[J]. Computer Application, 2008, 28(9): 2245-2248.）

[3] 张永铮，云晓春，胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报，2004，25(7)：107-114.（ZHANG Y Z, YUN X C, HU M Z. Communications privilege escalation study multi-dimensional quantitative attributes weakness taxonomy[J]. Journal of Institute of Communications, 2004, 25(7): 107-114.）

[4] 李新明，李艺，徐晓梅，等. 软件脆弱性分类法研究[J]. 计算机工程与设计，2004，25(2)：209-212.（LI X M, LI Y, XU X M, et al. Research software vulnerability taxonomy[J]. Computer Engineering and Design, 2004, 25(2): 209-212.）

[5] 胡冠林，汪厚祥. 软件缺陷分类及其度量技术研究[J]. 舰船电子工程，2005(3)：55-58.（HU G L, WANG H X. Software defect classification and measurement technique[J]. Ship Electronic Engineering, 2005(3): 55-58.）

[6] 王小艺，刘载，唐立军. 一种基于专家知识的软件质量多属性评价方法[J]. 计算机技术与应用发展，2008，

（下转第86页）

[8] 刘超. 基于DM368的嵌入式数字高清网络摄像机采集处理模块设计[D]. 南京:南京航空航天大学,2012. (LIU C. DM368-based embedded digital HD IP network camera acquisition and processing module design[D]. Nanjing:Nanjing University of Aeronautics and Astronautics, 2012.)

[9] 颜学究. 基于TMS320DM6467的视频编码系统研究与实现[D]. 重庆:重庆大学,2012. (YAN X J. The research and implementation on video coding system based on TMS320DM6467[D]. Chongqing:Chongqing University, 2012.)

[10] 李宏,吴衡. 机载LVDS数字视频信号采集记录技术研究[J]. 电光与控制,2011,18(5):72-75. (LI H, WU H. Acquisition and recording of onboard LVDS digital video signal[J]. Electronics Optics & Control, 2011, 18(5):72-75.)

[11] 陈智,邱跃洪,董佳. LVDS接口原理及其在电路设计中的应用[J]. 科学技术与工程,2005,5(21):1656-1657. (CHEN Z, QIU Y H, DONG J. LVDS interface principle and its application in the circuit design[J]. Science Technology and Engneering, 2005,5(21):1656-1657.)

[12] 高非非,刘辛国. ARM-Linux中I2C总线驱动开发[J]. 微型机与应用,2012,31(5):57-58. (GAO F F, LIU X G. Design of I2C bus driver based on ARM-Linux[J]. Microcomputer & Its Applications, 2012, 31(5):57-58.)

(上接第65页)

[22] GU J, PECHT M. Prognostics and health management using physics-of-failure[C]//54th Annual Reliability & Maintainability Symposium, RAMS 2008:481-487.

[23] AVIZIENIS A, LAPRIE J C, RANDELL B. Fundamental concepts of dependability[C]//Proceedings of the 3rd Information Survivability, 2000:7-12.

[24] 章新瑞,任占勇. 可靠性试验中环境应力与产品故障机理间关系研究[J]. 环境技术,2000(5):7-11. (ZHANG X R, REN Z Y. Research on relationship between stress and product reliability failure mechanisms environment experiment[J]. Environment Technology, 2000(5):7-11.)

[25] 丛伟,景博,樊晓光. 综合航电系统健康管理体系结构设计[J]. 测控技术,2013,32(8):126-130. (CONG W, JING B, FAN X G. Design of health management architecture of integrated avionics system[J]. Measurement & Control Technology, 2013, 32(8):126-130.)

[26] SAHA B, GOEBEL K, POLL S, et al. Prognostics methods for battery health monitoring using a Bayesian framework[J]. IEEE Transactions on Instrumentation and Measurement, 2009, 58(2):291-296.

(上接第70页)

34(3):227-229. (WANG X Y, LIU Z, TANG L J. A multi-attribute evaluation based on expert knowledge of software quality methods[J]. Computer Technology and Application Development, 2008, 34(3):227-229.)

[7] 李文静. 软件缺陷与软件测试[J]. 计算机与网络,2001(21):31-32. (LI W J. Software defects and software testing[J]. Computer and Network, 2001(21):31-32.)

[8] FENTON N, NEIL M. A critique of software defect prediction models[J]. IEEE Transactions on Software Engineering, 1999, 25(5):675-689.

[9] 郭飞,侯朝桢,戴忠建,等. 基于模糊-证据理论的软件缺陷评估新方法[J]. 计算机应用,2006(s1):275-276. (GUO F, HOU C Z, DAI Z J, et al. Fuzzy-software defects evidence theory methods to evaluate new computer application[J]. Computer Applications, 2006(s1):275-276.)

(上接第75页)

45. (WANG W W, YANG G P, LYU C, et al. New image segmentation model based on the level set method[J]. Journal of Xidian University, 2013, 40(6):39-45.)

[11] DIRAMI A, HAMMOUCHE K, DIAF M, et al. Fast multilevel thresholding for image segmentation through a multiphase level set method[J]. Signal Processing, 2013, 93(1):139-153.

[12] BALLA-ARABÉ S, GAO X, WANG B. A fast and robust level set method for image segmentation using fuzzy clustering and lattice Boltzmann method[J]. IEEE Transactions on Cybernetics, 2013, 43(3):910-920.

[13] WANG L F, PAN C H. Image-guided regularization level set evolution for MR image segmentation and bias field correction[J]. Magnetic Resonance Imaging, 2014, 32(1):71-83.

[14] DONG F F, CHEN Z S, WANG J W. A new level set method for inhomogeneous image segmentation[J]. Image and Vision Computing, 2013, 31(10):809-822.

[15] 崔玉玲. 基于改进符号距离函数的变分水平集图像分割算法[J]. 模式识别与人工智能,2013,26(11):1033-1040. (CUI Y L. A variational level set method for image segmentation based on improved signed distance function[J]. Pattern Recognition and Artificial Intelligence, 2013, 26(11):1033-1040.)

[16] DIRAMIA A, HAMMOUCHEA K, DIAFA M. Fast multilevel thresholding for image segmentation through a multiphase level set method[J]. Signal Processing, 2013, 93(1):139-153.