信息系统热点实践系列丛书

信息系统安全等级保护测评实践

李　嘉　蔡立志　张春柳　吴建华　编著

HEUP 哈尔滨工程大学出版社

信息系统安全等级保护测评实践

李　嘉　蔡立志　张春柳　吴建华　编著

哈爾濱工程大學出版社

内容简介

本书由信息安全等级测评资深人员在深入理解与信息安全等级保护有关的法律法规、政策和标准的基础上，结合自身的工作实践编写。本书针对信息安全等级测评的全部内容都采用丰富实例描述各测评项的理解、检查步骤和判别标准，对信息安全等级保护测评师工作开展有很好的指导作用。本书内容包括：信息安全等级保护概述、信息安全等级保护的过程与要求、等级测评过程解读、测评工具、风险分析、物理安全、网络安全、主机安全、应用与数据安全、信息安全管理基础、系统建设管理和系统运维管理。

本书可作为信息安全测评人员开展等级保护测评工作的参考书，也可以为信息系统运营、使用单位及其主管部门实施安全保护提供支持，或作为信息系统建设人员、运维人员、大专院校信息安全相关专业人员的参考用书。

图书在版编目(CIP)数据

信息系统安全等级保护测评实践/李嘉等编著.
—哈尔滨：哈尔滨工程大学出版社，2016.1

ISBN 978-7-5661-1184-5

Ⅰ.①信… Ⅱ.①李… Ⅲ.①信息系统-安全技术-研究 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2016)第 000632 号

选题策划 沈红宇
责任编辑 张忠远 付梦婷
封面设计 恒润设计

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 哈尔滨市石桥印务有限公司
开　　本 787mm×1 092mm 1/16
印　　张 20.25
字　　数 500 千字
版　　次 2016 年 1 月第 1 版
印　　次 2016 年 1 月第 1 次印刷
定　　价 55.00 元

http://www.hrbeupress.com
E-mail:heupress@hrbeu.edu.cn

编　写　组

编　　著	李　嘉	蔡立志	张春柳	吴建华
编著成员	李　嘉	蔡立志	张春柳	吴建华
	刘　刚	沈与辛	王　静	杨亚萍
	张延国	荣志文	严　超	闫　莅
	熊　琭	陈佩璇		

前言

近年来，“信息安全”与“大数据”“云计算”“移动互联网”一样，是IT领域出现频度最高的几个名词之一。在进入互联网时代之后，随着信息技术的飞速发展，基于网络的应用越来越广泛，针对信息系统的恶意攻击与窃取个人敏感信息的黑客行为也越来越频繁，信息安全也越来越深入地影响到了我们每一个人的日常生活。

在信息安全的经典定义中，是这样描述信息安全的：“信息安全为数据处理系统建立和采取的技术和管理的安全保护。保护计算机硬件、软件、数据不因偶然或恶意的原因而受到破坏、更改、泄露。”其基本思路是通过采取必要的技术措施和管理制度，使得信息系统具备与其自身价值相符合的抵御黑客入侵的安全防护能力。它的核心关键点就是安全防护能力和系统实现价值之间的匹配性。众所周知，信息系统安全性的提升往往意味着建设成本的上升和使用便利性的下降，如何在这三者之间找到平衡点，建立符合企业自身需求的安全目标才是信息安全工作成功与否的关键。过低的安全目标，会导致系统门户大开，数据遭到泄露。而过高的安全目标，会导致系统的运营成本实现上升，并严重影响用户的使用体验和系统运行效率。

同时，随着信息技术的发展和信息化程度的提高，国家政治、经济、国防、文化、教育等社会的各个领域对于信息基础设施和信息资源的依赖程度也越来越高。国家的安全、社会的稳定已经不再仅仅局限于现实物理空间的安全，网络与信息安全也已经成为国家安全保障体系的重要组成部分。如何建立一套适合中国国情的信息安全标准体系，如何从全国范围内对影响社会运行和国家安全的重要信息系统进行梳理、建设与管理，如何从国家层面指导各级主管部门和各个信息系统的使用单位开展标准化的信息安全工作，这些问题成为了当前国家安全保障工作的重中之重。

正是在这样的背景下，信息安全等级保护制度应运而生，并且作为我国信息安全保障工作中的一项基本制度在全国范围内开始实施。信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查这五个阶段。其中，等级测评是验证信息系统是否满足相应安全保护等级的评估过程，更是整个等级保护工作中的重要环节。通过等级测评可以全面掌握系统的安全状况，为安全建设整改工作和信息安全职能部门的日常监督检查提供参照。

近年来，全国的等级保护测评机构在公安部的领导下得到了快速发展，机构数量达到了一百四十余家，在推进等级测评工作中发挥了重要的技术支撑作用。等级测评工作涉及的信息系统范围广、技术架构复杂、涉及各行各业的业务应用，测评人员对测评指标的理解、测评技能的掌握将直接影响到测评工作的质量，往往需要有很强的理论和技术能力。

如何将多年来的工作经验和成果汇总起来，为测评人员针对不同系统的具体测评实施工作提供指导与参考，这个想法一直萦绕在编著者脑中。直到2014年底，借着全国信息安全测试机构联盟成立的东风，编者才决定把这些想法编著成书，以便和同行们分享交流。

本书对《信息系统安全等级保护基本要求》GB/T 22239—2008中物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全、系统建设管理、系统运维管理等十个方面的测评项进行逐一解读，并给出丰富的实例、检查步骤和判别标准，供读者参考、借鉴；并对测评过程中可能涉及的等级保护政策和标准、测评过程、测评工具、风险分析等进行了概要介绍。让信息安全测评人员能够迅速掌握各测评项的测评要点，顺利开展测评工作。

本书由上海计算机软件技术开发中心（上海市计算机软件评测重点实验室）组织编写，参加编写的有李嘉、蔡立志、张春柳、吴建华、沈与辛、刘刚、杨亚萍、王静、张延国、荣志文、严超、闫莅、熊琭、陈佩璇等。在编写过程中，编著者收集和参考了大量的文献资料和最新的网页信息，本书的编著离不开这些宝贵的资料，在此表示感谢。限于编著者的水平，书中难免有遗漏和不足之处，欢迎信息安全职能部门、有关信息系统使用单位、测评机构和信息安全专业人员对本书提出意见和建议，使其更加完善。

编著者

2015年11月

目录

第1篇 理 论 篇

第2篇 测评综述篇

第3篇 测评技术篇

第4篇 测评管理篇

第1篇 理 论 篇

第1章　信息安全等级保护概述

随着互联网、移动应用逐步渗透到人们生活的各个方面，信息安全形势也日渐严峻，重大信息安全问题可能会直接威胁国家安全、社会稳定和经济发展。按照“适度安全、保护重点”的目的，以“自主保护、重点保护、同步建设、动态调整”为原则确定信息系统安全保护等级、推进信息安全保护工作，在国家层面建立了国家网络与信息安全协调小组办公室，并由公安部牵头制定了一系列与信息安全和等级保护有关的政策文件和标准体系。重点行业在国家标准基础上制定了符合行业特点的标准和规范。

1.1　国内外信息安全形势

2013年6月，由美国中情局前特工爱德华·斯诺登曝光的“棱镜计划”，引发了人们对目前所处的互联网高度发达时代信息泄露的担忧和对网络安全事件的惊慌。

2014年是多个网络严重级别安全漏洞集中爆发的一年，如OpenSSL的心脏出血（Heartbleed）漏洞、IE的0Day漏洞、Struts漏洞、Flash漏洞、Linux内核漏洞、Synaptics触摸板驱动漏洞、贵宾犬、USBbad、破壳等重大安全漏洞被先后曝光，受影响的操作系统、硬件设备、应用软件、涉及人员的范围之广、之深，闻所未闻。

2014年4月的心脏出血漏洞是一个出现在开源加密库OpenSSL的程序漏洞，在整个IT及更广的周边行业内引起了普遍的恐慌。黑客利用该漏洞可以读取到包括用户名、密码和信用卡号等隐私信息在内的敏感数据。这波及了大量的互联网公司，受影响的服务器数量可能多达几十万，其中已确认受到影响的网站包括Imgur、OKCupid、Eventbrite以及FBI等。

在国内，信息安全事件也层出不穷。如2014年1月21日，国内通用顶级域的根服务器突然出现异常，导致中国众多知名网站出现大面积DNS解析故障。这一次事故影响了国内绝大多数DNS服务器，造成近2/3的DNS服务器瘫痪，时间持续数小时之久。事故发生期间，超过85%的用户遭遇了DNS故障，因此出现网速变慢和打不开网站的情况，部分地区用户甚至出现断网现象。

随着我国国民经济的不断发展和社会发展信息化进程的全面加快，我国各行业信息化的程度越来越高，关系国计民生的重要领域信息系统也已经成为国家的关键基础设施。这些基础信息网络和重要信息系统的安全问题，已经严重关系到国家安全、社会稳定和广大人民群众切身利益。

我国基础信息网络和重要信息系统安全面临的形势十分严峻，既有外部威胁的因素，又有系统自身的脆弱性和薄弱环节，维护国家信息安全的任务十分艰巨、繁重。主要表现在以下几方面：

1. 针对基础信息网络和重要信息系统的违法犯罪持续上升

不法分子利用一些系统存在的安全漏洞，使用病毒、木马、网络钓鱼等技术进行网络盗窃、网络诈骗、网络赌博等违法犯罪，对我国的经济秩序、社会管理秩序和公民的合法权益造成严重侵害。

2. 基础信息网络和重要信息系统安全隐患严重

由于我国各基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口，在操作系统、专用芯片和大型应用软件等方面不能自主可控，使我国的信息安全存在深层的技术隐患。

3. 我国的信息安全保障工作基础还很薄弱

国内人员的信息安全意识和安全防范能力比较薄弱，信息系统安全建设、监管缺乏详细的依据和标准，安全保护措施和安全制度不落实，监管措施不到位。

面对当前信息安全面临的复杂、严峻形势，基础信息网络和重要信息系统一旦出现大的信息安全问题，不仅仅影响本单位、本行业，而且直接威胁国家安全、社会稳定和经济发展。

面对严峻的网络信息安全形势，中央网络安全和信息化领导小组于2014年2月27日宣告成立，习近平亲自担任组长，李克强、刘云山任副组长，并在北京召开了第一次会议。中央网信小组将着眼于国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强网络及信息安全保障能力。

1.2 信息安全等级保护的目的和意义

1.2.1 什么是信息安全等级保护

信息安全等级保护是国家信息安全保障工作的基本制度、基本策略、基本方法。开展信息安全等级保护工作不仅是实现国家对重要信息系统重点保护的重大措施，也是一项事关国家安全、社会稳定的政治任务。通过开展信息安全等级保护工作，可以有效解决我国信息安全面临的威胁和存在的主要问题，充分体现“适度安全、保护重点”的目的，将有限的财力、物力、人力投入到重要信息系统安全保护中，按标准建设安全保护措施，建立安全保护制度，落实安全责任，有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统的安全，有效提高我国信息安全保障工作的整体水平。

信息安全等级保护是当今发达国家保护关键信息基础设施，保障信息安全的通行做法，也是我国多年来信息安全工作经验的总结。实施信息安全等级保护，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于为信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务；有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。

1.2.2 信息安全等级保护的目的与原则

1. 信息安全等级保护的目的

信息安全等级保护是国家信息安全保障工作的基本制度、基本策略、基本方法。通过开展信息安全等级保护工作，可以有效解决我国信息安全面临的威胁和存在的主要问题，

充分体现“适度安全、保护重点”的目的。

2. 信息安全等级保护的原则

信息系统安全等级保护的核心是对信息系统分划等级，按标准进行建设、管理和监督。信息系统安全等级保护实施过程中应遵循以下基本原则：

(1)自主保护原则

信息系统运营、使用单位及其主管部门应按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

(2)重点保护原则

根据信息系统的重要程度、业务特点划分不同安全保护等级的信息系统，以实现不同强度的安全保护，并集中资源优先保护涉及核心业务或关键信息资产的信息系统。

(3)同步建设原则

信息系统在新建、改建、扩建时，应当同步规划、设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

(4)动态调整原则

要跟踪信息系统的变化情况，并根据变化来调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因使安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

1.2.3　信息系统安全保护等级的划分和监管要求

《信息安全等级保护管理办法》(公通字[2007]43 号) 指出信息安全等级保护应坚持自主定级、自主保护的原则。应根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统的数据和服务遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素进行综合考虑，以此来确定信息系统的安全保护等级。

信息系统的安全保护等级分为五级：

第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

针对不同等级的信息系统，信息系统运营、使用单位需采取不同的保护措施，国家信息安全监管部门也会采取不同的监管措施，如表 1 - 1 所示。

表1-1 各等级信息系统的保护和监管措施

信息系统安全保护等级	信息系统运营、使用单位	国家监管措施
第一级	依据国家有关管理规范和技术标准进行保护	
第二级	依据国家有关管理规范和技术标准进行保护	国家信息安全监管部门进行指导
第三级	依据国家有关管理规范和技术标准进行保护	国家信息安全监管部门进行监督、检查
第四级	应当依据国家有关管理规范、技术标准和业务专门需求进行保护	国家信息安全监管部门进行强制监督、检查
第五级	依据国家管理规范、技术标准和业务特殊安全需求进行保护	国家指定专门部门进行专门监督、检查

1.3 发展历程

1994年发布的国务院第147号令《中华人民共和国计算机信息系统安全保护条例》第九条中，明确了“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法由公安部会同有关部门制定”的具体制度、任务和职责分工，首次以国家行政法规形式确立了信息安全等级保护制度的法律地位。

在2003年，中办、国办转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）中明确提出“实行信息安全等级保护”“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”等意见。这标志着等级保护从计算机信息系统安全保护的一项制度提升到国家信息安全保障一项基本制度。

2003年8月，国家网络与信息安全协调小组办公室明确将实行信息安全等级保护工作交由公安部牵头，并要求公安部会同有关部门研究提出实行信息安全等级保护的意见。国家网络与信息安全协调小组在2004年7月召开的第三次会议上通过了公安部提出的《关于信息安全等级保护工作的实施意见》。

按照《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）的相关规定和《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）文件精神，公安部会同国家保密局、国家密码管理局和国务院信息办于2004年9月联合出台了《关于信息安全等级保护工作的实施意见》（公通字[2004]66号），于2007年6月联合出台了《信息安全等级保护管理办法》（公通字[2007]43号，以下简称《管理办法》），明确了信息安全等级保护制度的基本内容、流程及工作要求以及信息系统运营使用单位和主管部门、监管部门在信息安全等级保护工作中的职责、任务，为开展信息安全等级保护工作提供了规范保障，制定了包括《计算机信息系统安全保护等级划分准则》（GB 17859—1999）及《信息系统安全等级保护定级指南》《信息系统安全等级保护基本要求》《信息系统安全等级保护

实施指南》《信息系统安全等级保护测评要求》等五十多个国标和行标，初步形成了信息安全等级保护标准体系。

2005 年底，公安部和国务院信息化工作办公室联合印发了《关于开展信息系统安全等级保护基础调查工作的通知》（公信安[2005]1431 号）。2006 年上半年，公安部会同国信办在全国范围内开展了信息系统安全等级保护基础调查，调查对象共计 65 117 家单位，涉及 115 319 个信息系统。通过基础调查，基本摸清和掌握了全国信息系统特别是重要信息系统的基本情况，为制定信息安全等级保护政策奠定了坚实的基础。

2006 年 6 月，公安部、国家保密局、国家密码管理局、国务院信息办联合下发了《关于开展信息安全等级保护试点工作的通知》（公信安[2006]573 号），在 13 个省区市和 3 个部委联合开展了信息安全等级保护试点工作。通过试点，完善了开展等级保护工作的模式和思路，检验和完善了开展等级保护工作的方法、思路、规范标准，探索了开展等级保护工作领导、组织、协调的模式和办法，为全面开展等级保护工作奠定了坚实的基础。

2014 年 12 月，公安部发布“关于传发《信息安全等级保护测评报告模版（2015 年版）》的通知”（公信安[2014]2866 号）。相比 2009 版报告模板，2015 版报告模板具有以下特点：

（1）确定了测评指标权重，测评结果量化，为 GB/T 22239—2008 标准中二级、三级、四级等级保护等级中每一个测评项给予 1、0.5、0.2 三个等级的权重赋值，测评项的符合程度从“符合”“部分符合”“不符合”的定性结论改为采用 5 分制定量打分的方式（符合 5 分；不符合 0 分；部分符合 1～4 分，根据对测评项的满足程度给出）。测评项最终得分为采用该测评项的所有测评对象得分的算术平均值。控制点得分、层面得分、系统总体得分均从其包含的测评项符合程度得分加权平均后得出。

（2）建立风险分析模型，引入量化风险分析。针对等级测评结果中存在的所有安全问题，结合关联资产和威胁分别分析安全危害，采用风险分析的方法，对安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等进行危害分析和风险等级判定。

（3）增加现场测评深度、注重测评工具的使用。要求明确使用的测评工具、接入点等信息，并加强对测评结果的验证，将验证测试发现的安全问题对应到相应的测评项的结果记录中，作为报告附件一起提交。

（4）增加评估的广度和多样性，加强对运维、管理和业务客户端的测评；强调对系统集成、安全集成、安全运维、安全测评、应急响应、安全监测等安全服务风险的评估，强化风险责任意识。

（5）扩充测评报告内容，对结构进行调整，增加可读性。

2015 年 1 月，为进一步加强测评行业自律管理，规范测评行为，提升测评能力，公安部信息安全等级保护评估中心、电力行业信息安全等级保护测评中心、国家信息技术安全研究中心等 9 家测评机构联合发起成立了“中关村信息安全测评联盟”。

1.4 政策体系和标准体系

1.4.1 总体政策文件

为保证信息安全等级保护工作顺利开展，公安部会同国家保密局、国家密码管理局、原国务院信息办和发改委等部门出台了一系列信息安全等级保护工作配套政策，公安部十一局还就具体工作出台了相关指导意见和规范。这些文件涵盖了等级保护制度、定级、备案、等级测评、安全建设、监督检查等工作的各个环节，构成了比较完备的政策体系，如图 1－1 所示。

图 1－1 信息安全等级保护法律政策体系

（1）公安部、国家保密局、国家密码管理局、原国务院信息办等四部门联合印发的《关于信息安全等级保护工作的实施意见》（公通字［2004］66 号）、《信息安全等级保护管理办法》（公通字［2007］43 号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字［2007］861 号）中，明确了等级保护制度的主要内容、职责分工、实施计划、工作要求，以及信息系统定级这一关键基础工作的主要内容和要求。

(2)国家发改委、公安部、国家保密局联合印发的《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》(发改高技[2008]2071 号)中明确了非涉密国家电子政务项目开展等级测评和信息安全风险评估的相关要求。

(3)公安部根据职责制定并印发的《关于开展信息系统等级保护安全建设整改工作的指导意见》(公信安[2009]1429 号)中明确了非涉及国家秘密信息系统开展安全建设整改工作的目标、内容、流程和要求等。

(4)公安部十一局根据职责制定并印发的《信息安全等级保护备案实施细则》(公信安[2007]1360 号)、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》(公信安[2010]303 号)、《关于印发〈信息系统安全等级测评报告模版(试行)〉的通知》(公信安[2009]1487 号)、《公安机关信息安全等级保护检查工作规范(试行)》(公信安[2008]736 号)等,分别就信息系统备案、测评机构及其测评活动管理、公安机关监督检查等工作明确了具体内容和要求。

1.4.2 标准体系介绍

十多年来,公安部会同相关的部委组织国内有关专家、研究机构、企业先后制定了信息安全等级保护工作需要的一整套国家标准和公安行业标准,形成了比较完备的信息安全等级保护标准体系,为开展信息安全等级保护工作提供了标准保障。该标准体系大致可以分为核心标准类、等保工作指导类、产品类、行业标准和支持类标准等几类。整个标准体系框架如图 1-2 所示。

1. 核心标准

此类标准是等级保护工作的核心,起基础支撑作用和全局性作用,包括以下标准:

(1)《计算机信息系统安全保护等级划分准则》(GB 17859—1999,以下简称《划分准则》);

(2)《信息系统安全等级保护基本要求》(GB/T 22239—2008,以下简称《基本要求》)。

《划分准则》及在其基础上制定的《信息系统通用安全技术要求》等技术类标准、《信息系统安全管理要求》等管理类标准和《操作系统安全技术要求》等产品类标准等是等级保护配套标准,是《基本要求》的基础。《基本要求》在上述标准的基础上,从技术和管理两方面提出并确定了不同安全保护等级信息系统的最低保护要求,即基线要求,是信息系统安全建设整改的具体依据。

2. 等级保护指导类标准

在等级保护整个生命周期中使用,以指导定级备案、安全建设整改、等级测评等活动。

(1)定级工作依据的标准,为信息系统定级工作提供了技术支持,包括以下标准:

《信息系统安全保护等级定级指南》(GB/T 22240—2008)。

(2)信息系统安全建设整改依据的标准,对信息系统安全建设的技术设计、管理设计等活动提供指导,是实现《基本要求》的必要途径,包括以下标准:

《信息系统安全等级保护实施指南》(GB/T 25058—2010);

《信息系统等级保护安全设计技术要求》(GB/T 25070—2010);

《信息系统安全管理要求》(GB/T 20269—2006);

《信息系统安全工程管理要求》(GB/T 20282—2006);

《信息系统通用安全技术要求》(GB/T 20271—2006);

《信息系统物理安全技术要求》(GB/T 21052—2007);