ICS 35.020
L 01

中华人民共和国国家标准

GB/T 19668.6—2007

信息化工程监理规范
第6部分:信息化工程安全监理规范

Information system project surveillance specification—
Part 6:Information system project security surveillance specification

2007-08-24 发布　　2008-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T 19668《信息化工程监理规范》分为六部分：

——第1部分：总则；

——第2部分：通用布缆系统工程监理规范；

——第3部分：电子设备机房系统工程监理规范；

——第4部分：计算机网络系统工程监理规范；

——第5部分：软件工程监理规范；

——第6部分：信息化工程安全监理规范。

本部分为GB/T 19668的第6部分。

本部分由国家电子政务标准化总体组提出并归口。

本部分项目召集单位：中国电子技术标准化研究所。

本部分项目副召集单位：北京市质量技术监督局、上海市信息化办公室、中国电子信息产业发展研究院。

本部分专家组：葛迺康、张保栋、马应章、包兵、窦传义。本部分工作组秘书：徐全平。

本部分主要起草单位：上海三零卫士信息安全有限公司、北京市信息安全测评中心、广州赛宝联睿信息工程监理有限公司、北京同方信息安全技术股份有限公司、山东正中计算机网络技术咨询有限公司、新疆天衡信息工程监理公司、北京知识安全工程中心。

本部分主要起草人：孔一童、张晓梅、闵京华、彭细正、周鸣乐、董火民、张斌、王新杰、姚世全。

目　　次

信息化工程监理规范
第6部分:信息化工程安全监理规范

1 范围

GB/T 19668的本部分规定了信息化工程新建、升级、改造过程中各监理阶段安全监理工作的主要目标、内容和要点。

本部分适用于GB/T 19668.1—2005中各监理对象中涉及信息安全的监理工作。

本部分不对信息化工程安全监理中涉及的产品、服务的技术规格和条件做出规定或要求,有关内容参见相应的产品或服务的技术标准。

2 规范性引用文件

下列文件中的条款通过GB/T 19668的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB 9361—1988 计算站场地安全要求

GB/T 19668.1—2005 信息化工程监理规范 第1部分:总则

3 术语和定义

GB/T 19668.1—2005确立的以及下列术语和定义适用于GB/T 19668的本部分。

3.1

信息安全 information security

保持信息的保密性、完整性、可用性;另外也可包括诸如真实性、可核查性、不可否认性和可靠性等。

注:见ISO/IEC 17799:2005,定义2.5。

3.2

信息化工程安全监理 information system project security surveillance

信息化工程新建、升级、改造过程中涉及信息安全的监理活动。

4 一般要求

本部分遵循GB/T 19668.1—2005的一般原则和要求,重点描述信息化工程安全监理各监理阶段的监理目标、监理内容和监理要点等。

在信息化工程的安全监理工作中,应同时使用GB/T 19668.1—2005和本部分。

信息化工程安全监理的监理对象为GB/T 19668.1—2005所包括的各类信息化工程中涉及信息安全的工程活动。信息化工程安全监理以保障信息系统安全作为监理活动的最终目标,对各监理对象实施监理。

5 工程招标阶段

5.1 监理目标

监理机构通过监理工作,应实现如下目标:

a) 协助业主单位明确工程的安全需求；
b) 如适用，协助业主单位确定系统安全保护等级；
c) 协助业主单位编制的招标文件与安全相关的内容在技术上合理有效；
d) 协助业主单位对投标文件中与安全相关的内容进行评审，对投标单位的安全资质进行审核，选出适合的承建单位；
e) 促使承建合同中与安全相关的条款在技术、经济上合理有效。

5.2 监理内容

工程招标阶段的主要监理内容如下：

a) 监理机构应根据监理合同编制监理规划，经业主单位签认后作为监理工作的依据；
b) 如适用，监理机构应协助业主单位依据国家等级保护相关标准，确定系统安全保护等级；
c) 监理机构应协助业主单位在深入调研的基础上，明确信息化工程的安全目标和安全需求；
d) 监理机构应检查业主单位提出的安全需求与安全目标是否一致，与国家和地方的信息安全政策法规、行业标准是否符合；
e) 监理机构应检查招标文件中工程的安全需求、安全范围、产品及服务等技术要求是否明确；
f) 监理机构可参与招标答疑工作，协助业主单位对工程所涉及的安全功能、安全技术指标向投标单位解释，并保存会议纪要(见 GB/T 19668.1—2005 表 C.6)和相关文件；
g) 监理机构宜参与投标文件评审，监督评审过程的合理性与公正性，对投标单位的安全相关资质进行审查，并提出监理意见，协助业主单位挑选出适合的承建单位；
h) 监理机构宜参与承建合同的签订过程，检查承建合同中安全功能、技术要求、测试标准、验收要求和质量责任等条款的合理性，在承建合同中应明确要求承建单位接受监理机构的监理；
i) 若工程建设中涉及到各方的内部敏感信息，监理机构应促使三方(业主单位、承建单位、监理单位)签署保密协议。

5.3 监理要点

5.3.1 安全需求

监理机构应从如下方面了解业主单位的安全需求：

a) 监理机构应协助业主单位通过调查研究，明确信息化工程建设的安全目标，从安全目标导出安全需求；
b) 监理机构应检查业主单位提出的安全需求与安全目标的一致性，与国家和地方信息安全法律、法规和标准的符合性；
c) 如适用，在确定安全等级后，监理机构宜协助业主单位将确定的安全保护等级结果报相应主管部门审查或备案。

5.3.2 招标文件

监理机构宜参与招标文件的编制，从如下方面对招标文件提出监理意见：

a) 工程安全体系建设，应能达到预定的安全目标与安全需求；
b) 投标单位的资质要求，如信息系统安全集成或服务资质、类似成功案例等；
c) 投标单位项目组人员的资格要求，如信息安全领域的相关资质，安全领域的工作年限和项目经验等；
d) 新建工程项目对原有信息系统安全性的可能影响及处理；
e) 所参照的相关法规、标准，投标文件应符合国家信息安全相关法律、法规和标准。

5.3.3 承建合同

监理机构应参与承建合同的签订，协助业主单位对承建合同的如下内容进行检查，并提出监理意见：

a) 信息安全相关建设内容，包括名称、范围和要求等；

b) 潜在安全风险的处理办法；
c) 保密条款和安全责任条款；
d) 项目验收标准、方法及文档交付；
e) 监理机构在工程款支付中的作用；
f) 工程变更和扩展引发安全问题的处理方法。

6 工程设计阶段

6.1 监理目标

监理机构通过监理工作，应实现如下目标：
a) 促使业主单位与承建单位进行充分的沟通，形成深化的设计需求；
b) 推动承建单位对工程的安全设计进行规范化的技术描述，形成优化的安全设计方案；
c) 促使业主单位、承建单位消除设计文档在进入工程实施前可预见的信息安全缺陷。

6.2 监理内容

工程设计阶段的主要监理内容如下：
a) 监理机构应根据监理规划、承建合同、安全设计方案等文档编制监理细则；
b) 监理机构应促使业主单位和承建单位就工程安全需求进行专门的讨论，对系统的安全需求形成一致的理解；
c) 监理机构应建议承建单位在信息安全需求调研和信息安全风险评估的基础上进行安全设计；
d) 如适用，已确定的信息安全保护等级也应作为安全设计的基础；
e) 监理机构应建议承建单位在进行系统安全性设计时，充分考虑新建项目对现有系统和目标系统安全性可能造成的影响，并在设计方案中有所体现；
f) 要求承建单位提交工程设计方案和工程实施组织设计方案（设计方案报审表见GB/T 19668.1—2005 表B.1），监理机构对其中的安全设计内容进行审核后提出监理意见；
g) 监理机构应协助业主单位调动适当的资源，配合承建单位完成工程设计前期的安全需求调查和分析工作；
h) 监理机构应协助业主单位和承建单位与信息安全相关主管部门进行充分的沟通和协调，确保安全设计方案符合政策要求；
i) 监理机构应就设计阶段的各种变更对工程安全性的可能影响提出监理意见。

6.3 监理要点

6.3.1 安全需求分析

监理机构应从如下方面审核承建单位提交的工程安全需求文档，并提出监理意见：
a) 信息安全相关法规、标准、其他因素；
b) 系统的用途及其与业主单位业务安全的关联性；
c) 系统的安全功能、性能、互操作性、接口要求的描述是否明晰；
d) 安全性检验手段。

6.3.2 工程设计方案

监理机构应从如下方面对设计方案进行审核，并提出监理意见：
a) 与安全目标和安全需求的一致性；
b) 技术设计和施工组织的安全性；
c) 残余风险的考虑；
d) 对项目实施过程中可能存在的安全风险和处理办法的考虑；
e) 技术方案的开放性、兼容性、可扩展性；
f) 设计方案中安全设计与承建合同的符合性；

g) 与国家相关法律、法规、标准的符合性。

7 工程实施阶段

7.1 监理目标

监理机构通过监理工作，应实现如下目标：

a) 促使工程实施方案安全、合理，与设计方案符合；

b) 促使工程中所使用的产品和服务符合国家相关法律、法规和标准；

c) 促使工程实施计划合理、受控；

d) 确认工程实施过程满足承建合同提出的安全要求，并与安全设计方案、实施方案、实施计划相符。

7.2 监理内容

工程实施阶段的主要监理内容如下：

a) 在工程实施前，监理机构应督促承建单位提供工程实施方案、工程实施计划、工程进度安排等文档，确定实施人员组成；

b) 监理机构应对工程实施方案进行审核，检查实施方案与承建合同、安全设计方案的一致性，并提出监理意见；

c) 监理机构应对承建单位提交的工程进度安排进行审核，保证信息化工程中的各项安全措施实施符合信息化工程的总体时间安排，在时间进度上合理、有效；

d) 在工程实施中，监理机构应检查工程实施过程与实施方案的一致性，对工程实际建设中的变更进行记录并给出监理意见；

e) 监督对到货安全设备的验收；

f) 督促承建单位按照规范进行系统和设备的安装与调试；

g) 监理单位应促使业主单位和承建单位做好工程实施中的安全管理工作；

h) 如工程实施中存在重大变更，监理单位应督促承建单位对系统安全性进行再评估。

7.3 监理要点

7.3.1 工程实施方案和工程实施组织方案

监理机构应从如下方面对承建单位提交的工程实施方案和工程实施组织方案提出监理意见：

a) 实施方案与安全设计方案的符合性；

b) 安全设备安装调试规划，包括各类安全设备的采购、进场、配置、调试和管理的规划等；

c) 工程实施组织中的安全，如工程实施人员安全管理措施等；

d) 如适用，项目分包工程实施的安全控制措施。

7.3.2 安全设备验收

监理机构应从如下方面对主要设备进行到货验收，并提出监理意见：

a) 具有合法销售许可证；

b) 由合法供应商供应；

c) 符合设计规定的功能、性能；

d) 安全设备及型号与安全产品认证证书一致；

e) 如适用，由第三方测试机构出具的测试报告；

f) 设备运转正常，功能、性能达到合同要求。

7.3.3 工程实施管理

监理机构应从如下方面对工程实施中的安全管理进行监督：

a) 督促承建单位严格按照审批通过的实施方案进行施工；

b) 对承建单位施工人员的身份与资格进行审查；

c) 督促承建单位在施工中严格遵守业主单位的相关安全管理规定。

8 工程验收阶段

8.1 监理目标

监理机构通过监理工作，应实现如下目标：

a) 明确工程安全测试验收方案的符合性及可行性；

b) 促使工程的最终安全性能和功能符合承建合同、法律、法规和标准的要求；

c) 促使承建单位所提供的工程技术、管理文档的内容符合相关标准。

8.2 监理内容

验收阶段的主要监理内容如下：

a) 依据承建合同、安全设计方案、实施方案、实施记录、国家或地方相关标准和技术指导文件，对信息化工程进行安全符合性检查，以验证项目是否实现了项目设计目标和安全等级要求；

b) 根据信息系统的安全等级，协助业主单位委托外部测评机构对安全建设项目进行测评；

c) 协助业主单位建立验收工作机构，组织最终的项目验收会议；

d) 协助验收工作机构审核承建单位提供的验收工作方案，并提出监理意见；

e) 协助业主单位对承建单位提供的项目验收报告进行评审，并提出监理意见；

f) 协助业主单位收集工程实施中的各种关键文档。

8.3 监理要点

8.3.1 测试

监理机构应从如下方面开展测试中的监理工作：

a) 监理单位应督促承建单位按照网络、操作系统、应用系统、各类产品等安全功能及性能的不同，采用不同的技术检测方法，设计详细的测试技术方案和控制流程。

b) 监理机构应督促承建单位对工程进展中安装的设备或产品进行测试，以评估产品是否能符合业主单位或工程的安全要求。

c) 监理机构应督促承建单位在系统建设完成之后，在开通和交付业主单位验收、使用之前，进行总体安全性测试。

d) 监理机构应督促承建单位对安全测试的内容做详细的工作文档记录，包括安全工程测试方法、测试结果、测试指标结果等。

e) 如适用，监理机构应督促承建单位及时纠正测试中发现的安全问题。

f) 监理机构应从以下方面对测试结果进行审查，并提交监理意见：

1) 系统安全功能，如用户授权管理、访问控制、传输加密等；

2) 系统安全性能，如密码算法强度等。

8.3.2 信息系统安全测评

监理机构应从如下方面开展信息系统安全测评中的监理工作：

a) 协助业主单位做好与安全测评机构的沟通，协调项目各方与测评机构做好配合工作；

b) 协助业主单位审核测评机构编写的安全验收测评方案；

c) 对业主单位和承建单位进行的安全验收测评的技术准备、文档准备和人员准备情况进行检查；

d) 如适用，监理机构应协助业主单位，并督促承建单位整改安全测评中发现的问题。

8.3.3 工程验收

监理机构应从如下方面开展工程验收中的监理工作：

a) 监理机构应督促承建单位在系统验收前先进行系统的测试和试运行，并进行详细的文档记录；

b) 监理机构应建议业主单位和承建单位根据详细设计书及相关部门颁发的有关文件、各专业的设计规范、建设规范和验收规范进行项目验收；

c) 如适用，承建单位应提供由国家授权信息安全测评机构提供的系统安全测评报告，作为工程验收的材料。

9 各类信息化工程的安全监理要点

9.1 通用布缆系统工程的安全监理要点

监理机构可从如下方面对通用布缆系统工程进行安全监理：

a) 电源和运载数据或支持信息服务的电信布缆应免受窃听或损坏。

b) 线缆的选择除满足数据传输的技术要求外，还应注意电缆敷设的环境要求，如在强电磁干扰区域应采用屏蔽线或光缆。

c) 进入信息处理设施的电源和通信线路宜在地下，若可能，或提供足够的可替换的保护。

d) 线缆应免受未授权窃听或损坏，如利用电缆管道或使路由避开公众区域。

e) 为了防止干扰，电源电缆要与通信电缆分开。

f) 对于敏感或关键的系统，还应考虑以下的措施：

1) 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子；

2) 使用可替换的路由选择和/或传输介质；

3) 使用光纤或屏蔽线布缆；

4) 使用电磁防辐射装置保护电缆。

9.2 电子设备机房系统工程的安全监理要点

监理机构可从如下方面对电子设备机房系统工程进行安全监理：

a) 电子设备机房的安全设计应符合 GB 9361—1988 的规定。

b) 电子设备机房应保证供配电系统的安全，包括安装防雷和接地装置，部署不间断电源设备等。

c) 电子设备机房应安装消防设施，包括安装火灾报警装置，放置手提式灭火器等。凡设有气体灭火装置的电子设备机房，应安装排气装置。

d) 电子设备机房应根据其重要性，安装门禁系统、视频监视系统、入侵报警系统等安防系统。

e) 电子设备机房应保证电子设备运行的温度、湿度要求，部署空调系统；重要的电子设备机房应安装精密空调等装置以保证对温湿度的精确控制。

f) 电子设备机房应保证对静电的防护或处理，采取防静电地板、接地等措施，防止静电对机房内电子设备的损害。

9.3 计算机网络系统工程的安全监理要点

监理机构可从如下方面对计算机网络系统工程进行安全监理：

a) 网络系统工程中的中心机房应满足 9.2 的要求，各种服务器及网络核心设备宜放置在专门的电子设备机房；

b) 信息网络平台中涉及的防火墙、防病毒系统等网络安全软硬件设备应通过国家相关安全测评认证机构的认证；

c) 交换机、路由器和防火墙等网络设备初始安装后应重新配置，以符合系统安全策略或系统对应的安全等级保护要求；

d) 合理划分网络安全域，对外提供服务的区域应和内部网络隔离；内部服务器及办公主机应放置在内网，对外提供服务的服务器应放置在对外服务区；

e) 在网络系统与外部网络接口处应设置防火墙、隔离网闸等边界保护设备；

f) 应分别从网络防病毒、主机防病毒等各个层次加强网络对病毒的防范能力；

g) 网络应用的安全应满足 9.4 的要求。

9.4 软件工程的安全监理要点

监理机构可从如下方面对软件工程进行安全监理：

a) 应用软件在设计上应考虑合适的控制和审核跟踪或活动日志，以防止丢失、修改或滥用应用系统中的用户数据，包括输入数据确认、内部处理控制、输出数据确认等；
b) 软件系统应采用适当的密码系统和技术来保护信息的保密性、真实性和完整性；
c) 对于重要的信息系统，应分离开发、测试和运行设施，规定从开发状态到运行状态的安全控制措施并形成文件，以防止开发和测试活动可能引起的问题；
d) 软件的测试过程应注意保护和控制测试数据，避免使用包含个人信息的运行数据库；
e) 软件的开发过程中，对源程序库的访问应维护严格的控制，以减少计算机程序被损坏的可能；
f) 如存在外包的软件开发，应注意对外包过程的信息管理。

中 华 人 民 共 和 国
国 家 标 准
信息化工程监理规范
第6部分:信息化工程安全监理规范
GB/T 19668.6—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 16千字
2007年11月第一版 2007年11月第一次印刷
*
书号:155066·1-30203 定价 14.00 元

GB/T 19668.6-2007