**1、前言**

**1.1 轨道交通行业IT现状**

随着城市轨道交通事业的蓬勃发展，轨道交通的建设、运营和资源开发通过信息化手段辅助管理，能有效提高工作效率与管理水平，控制成本费用，促进资源的科学、高效利用。但在信息化建设过程中，信息系统作为信息的载体，同样面临着来自各方面的威胁。随着信息化在轨道交通行业中越来越多的应用起来，信息系统在安全方面存在的问题以及面临的威胁，贯穿于信息系统中信息生命周期的整个过程。因此只有加强信息系统安全管理，建设好一套成熟的信息安全管理体系，并对信息系统运维作出明确的安全规划，成为一项保障信息系统更好地为轨道交通服务的迫切需求。

目前，宁波轨道交通运营分公司已建成的信息系统包括信号系统、自动售检票系统(AFC)、乘客信息系统（PIS）、综合监控系统（ISCS）等。对于一个现代化信息程度非常高的企业来说，这些信息系统的正常运行与宁波轨道交通运营分公司的核心业务息息相关。不仅如此，一旦这些信息系统受到安全威胁，造成的影响绝不局限于宁波轨道交通运营分公司，更会造成一定程度上的社会秩序与公民利益的损害。在依靠众多信息系统支撑运行的轨道交通行业来说，信息系统不仅让你别轨道交通运营分公司在公共交通方面取得了显著的成绩，同时也带来了一系列问题：多系统引发的应用复杂性问题、授权不当引发的信息安全问题、员工工作变动引发的管理效率问题等等。

**1.2 轨道交通信息系统面临的风险**

近年来，轨道交通行业发展迅速，工业控制系统在轨道交通方面的应用迅速增加，越来越多地采用通用协议，通用硬件和通用软件，以各种方式与公共网络连接，病毒、木马等威胁工业控制信息系统的安全问题日益突出。同时，主流系统仍然是以国外技术为主导，信息系统安全隐患突出，对信息系统安全的研究比较匮乏，对安全事件风险缺乏有效的应对措施。近年发生的多起重大事故，如2009年深圳地铁龙华线停运事故、2010年上海地铁10号线的追尾事故、2011年“7·23”甬温线动车追尾事故等。这些安全运营事件都与轨道交通信息系统安全问题相关，只有重视了轨道交通信息系统的信息安全管理，明确了信息安全管理规划，完善了信息安全管理体系，才能避免安全事故的发生。

以轨道交通最为重要的信号系统为例，其担负着列车运行、保障行车安全、提高运输效率等重要任务。轨道交通信息系统当前主流供应商进行数据传输的频段与城市无限网络共用2.4G频段。随着信息量的快速提升，信息系统面临更加复杂的外部干扰。导致列车发生故障。更为严重的是，攻击者可以向信号控制系统注入恶意代码，对可编程控制器进行非法操作，进行错误的安全策略配置，从而导致更为严重的列车运行事故。

**1.3 轨道交通信息系统的安全需求**

当今的轨道交通行业在工业控制信息系统安全领域面临比以往更为复杂的局面。这既有来自于轨道交通企业外部的层出不穷的入侵和攻击，也有来自于轨道交通企业内部的违规操作和信息泄漏。

对于大多数城市的轨道交通行业来说，技术上的安全防范基本都会布置到位，单纯技术上的安全需求都会考虑周全。但是对于信息安全中更重要的信息安全管理来说，往往容易被忽视。

通过对之前资料汇总与分析，轨道交通行业进行的安全风险评估结果表明，绝对大多数城市的轨道交通信息安全管理上都存在着以下几个问题：

1. 在系统运行后仍缺乏一体化的应急机制；
2. 没有明确的信息安全防范应急处置机制；
3. 没有明确的信息安全管理制度，人员信息安全意识缺乏；
4. 工业控制信息系统缺乏足够的安全性考虑，易被攻击者利用；
5. 严重的威胁和安全隐患难以及时处置，没有明确的处置流程，容易放大系统安全风险；
6. 安全防范法规和标准出台滞后，安全管理防范措施存在不足；
7. 没有相关的信息安全法律法规来保障；
8. 缺乏高效的信息安全管理平台。

**1.4 轨道交通行业相关规范与要求**

（1）工信部协【2011】451号文件《关于加强工业控制系统信息安全管理的通知》，明确规定加强重点领域工控信息系统安全管理措施，特别提到了与国计民生紧密相关领域的控制系统，如核设施、电力、天然气、铁路、城市轨道交通、民航、城市供水等。

（2）国务院国发（2012）23号文《关于大力推进信息化发展和切实保障信息安全的若干意见》，明确要求保障工业控制系统安全。加强核设施、航空航天、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统，定期开展安全检查和风险评估。

（3）最新颁布实施的《中华人民共和国网络安全法》中明确要求“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务”。

**2、项目概述**

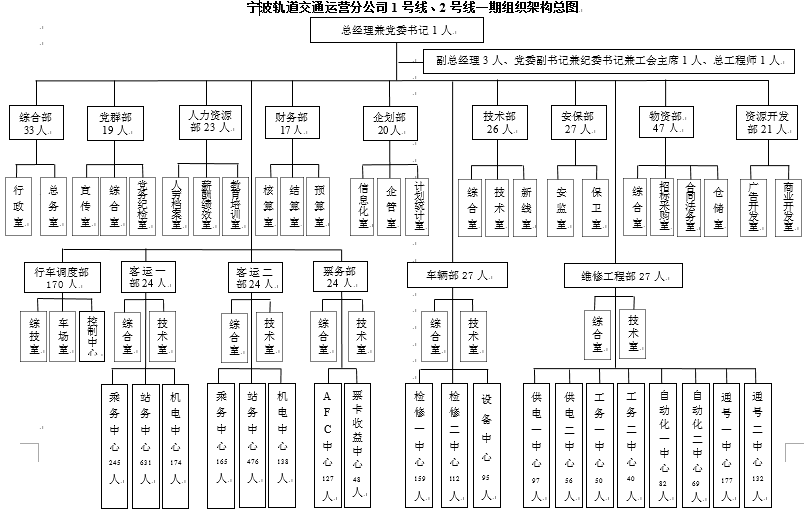
**2.1 项目建设背景**

为进一步贯彻宁波轨道交通运营分公司对各核心信息系统系统安全防护的规范要求，有效防范核心信息系统和重要企业信息数据遭到非法访问、违规操作以及信息泄露，确保系统和数据安全。我们将针对现有信息安全管理上存在的问题制定解决方案。

**2.2 项目建设范围**

2017年度宁波轨道交通运营分公司信息系统安全管理规划主要面向的对象分为人员和信息系统两大块。人员方面从宁波轨道交通运营分公司信息系统的分管领导至最具体的信息系统操作人员，都将学习了解并有效落实信息安全管理规划中设定的个人职责；信息系统方面则为宁波轨道交通运营分公司支撑维系日常业务正常运行的各个信息系统。

人员组织结构：



**图2.1宁波轨道交通运营分公司人员组织结构**

主要信息系统组织结构：运营分公司管理范围内的信息系统主要包括非生产管理类信息系统和生产类信息系统（生产类信息系统见下表）：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 中心名称 | 运维情况 |
| 1 | 宁波市轨道交通1号线一期PIS系统 | 维修工程部通号一中心 | 国内厂商提供运维服务 |
| 2 | 轮对踏面故障动态监测系统 | 车辆部设备中心 | 中心自己运行维护 |
| 3 | 列车驾驶仿真培训系统 | 车辆部设备中心 | 中心自己运行维护 |
| 4 | 宁波市轨道交通1号线一期开利冷水机组群控系统 | 客运一部机电中心 | 国内厂商提供运维服务 |
| 5 | 宁波市轨道交通1号线一期AFC系统 | 票务部AFC中心 | 国内厂商提供运维服务 |
| 6 | 综合监控系统 | 维修工程部自动化一中心 | 中心自己运行维护 |
| 7 | 宁波市轨道交通1号线一期DTS系统 | 维修工程部自动化一中心 | 中心自己运行维护 |
| 8 | 宁波市轨道交通1号线一期FAS系统 | 维修工程部自动化一中心 | 中心自己运行维护 |
| 9 | 宁波市轨道交通1号线一期ACS系统 | 维修工程部自动化一中心 | 中心自己运行维护 |
| 10 | 宁波市轨道交通1号线一期车载PIS系统 | 车辆部检修一中心 | 国内厂商提供运维服务 |
| 11 | 宁波市轨道交通1号线一期PA系统 | 维修工程部通号一中心 | 国内厂商提供运维服务 |
| 12 | 宁波市轨道交通1号线一期CCTV系统 | 维修工程部通号一中心 | 国内厂商提供运维服务 |
| 13 | 宁波市轨道交通1号线一期信号系统 | 维修工程部通号一中心 | 国内厂商提供运维服务、中心自己运行维护 |
| 14 | 宁波市轨道交通1号线一期客服热线系统 | 维修工程部通号一中心 | 国内厂商提供运维服务 |
| 15 | 宁波市轨道交通2号线一期车辆PIS系统 | 维修工程部检修二中心： | 国内厂商提供运维服务、  中心自己运行维护 |
| 16 | 宁波市轨道交通2号线一期视频监视系统 | 维修工程部通号二中心： | 国内厂商提供运维服务、  中心自己运行维护 |
| 17 | 宁波市轨道交通2号线一期PIS系统 | 维修工程部通号二中心： | 国内厂商提供运维服务、  中心自己运行维护 |
| 18 | urbalis 888 信号系统 | 维修工程部通号二中心 | 国内厂商提供运维服务、  中心自己运行维护 |
| 19 | 宁波市轨道交通2号线一期门禁系统 | 维修工程部自动化二中心 | 国内厂商提供运维服务、  中心自己运行维护 |
| 20 | 宁波市轨道交通2号线一期FAS系统 | 维修工程部自动化二中心 | 国内厂商提供运维服务、  中心自己运行维护 |
| 21 | 宁波市轨道交通2号线一期DTS系统 | 维修工程部自动化二中心 | 国内厂商提供运维服务、  中心自己运行维护 |
| 22 | 宁波市轨道交通2号线一期ISCS&SCADA系统 | 维修工程部自动化二中心 | 国内厂商提供运维服务、  中心自己运行维护 |

表（1）

**2.3 项目建设目标**

按照信息安全管理体系ISMS的安全管理规范的要求，本次项目启动了宁波轨道交通运营分公司的信息安全管理体系的建设，通过确定信息安全管理体系范围，制定信息安全方针，明确管理职责，选择控制目标与控制措施等来建立信息安全管理体系，以达成以下四点基本要求。

1. 成为分公司全体员工通过此标准，日常信息系统安全工作基线；

2.各专业信息系统等级保护定级标准（是否定级、定几级）；

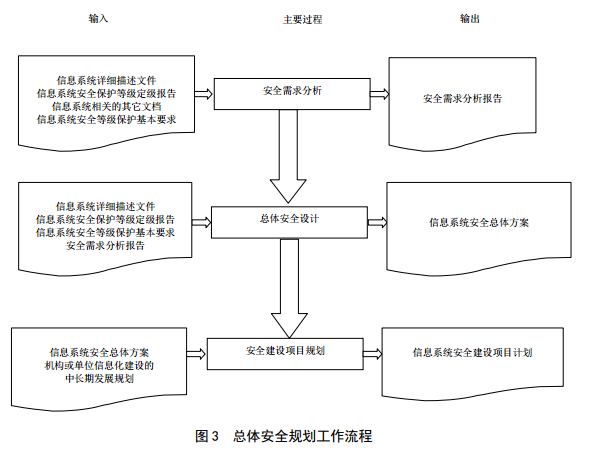
3.配合信息系统安全上级主管部门对运营完成检查及相关工作；

4.此标准体系通过专家评审，达到宁波轨道交通信息安全工作标准体系示范。

**3.总体安全规划**

**3.1 总体安全规划阶段的工作流程**

总体安全规划阶段的目标是根据信息系统的划分情况、信息系统的定级情况、信息系统承载业务情况，通过分析明确信息系统安全需求，设计合理的、满足等级保护要求的总体安全方案，并制定出安全 实施计划，以指导后续的信息系统安全建设工程实施。对于已运营（运行）的信息系统，需求分析应当首先分析判断信息系统的安全保护现状与等级保护要求之间的差距。总体安全规划阶段的工作流程(见图3)。



**3.2 安全需求分析**

明确运营分公司管理范围内的所有信息系统及人员纳入此标准体系，且需要明确活动组织及活动所需的输入文挡由磋商申请人负责。

**3.2.1 基本安全需求的确定**

活动目标：

本活动的目标是根据《信息安全等级保护管理办法》《信息安全等级保护定级指南》等国标类文件确定宁波轨道交通运营分公司相关信息系统的信息安全保护等级，判断信息系统现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出信息系统的基本安全保护需求。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：《信息系统详细描述文件》，《信息系统安全保护等级定级报告，信息系统备案表》及信息系统相关的其它文档

活动描述：本活动主要包括以下子活动内容：

a) 确定系统范围和分析对象 明确不同等级信息系统的范围和边界，通过调查或查阅资料的方式，了解信息系统的构成，包括网 络拓扑、业务应用、业务流程、设备信息、安全措施状况等。初步确定每个等级信息系统的分析对象， 包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。

b) 形成评价指标和评估方案 根据各个信息系统的安全保护等级从信息系统安全等级保护基本要求中选择相应等级的指标，形成评价指标。根据评价指标，结合确定的具体对象制定可以操作的评估方案，评估方案可以包含以下内容：

1) 管理状况评估表格；

2) 网络状况评估表格；

3) 网络设备（含安全设备）评估表格；

4) 主机设备评估表格；

5) 主要设备安全测试方案；

6) 重要操作的作业指导书。

c) 现状与评价指标对比：通过观察现场、询问人员、查询资料、检查记录、检查配置、技术测试、渗透攻击等方式进行安全 技术和安全管理方面的评估，判断安全技术和安全管理的各个方面与评价指标的符合程度，给出判断结论。整理和分析不符合的评价指标，确定信息系统安全保护的基本需求。

活动输出： 《信息系统基本安全需求》。

**3.2.2 额外/特殊安全需求的确定**

活动目标：本活动的目标是通过对信息系统重要资产特殊保护要求的分析，确定超出相应等级保护基本要求的部分或具有特殊安全保护要求的部分，采用需求分析/风险分析的方法，确定可能的安全风险，判断对 超出等级保护基本要求部分实施特殊安全措施的必要性，提出信息系统的特殊安全保护需求。参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，信息系统相关的其它文档。

活动描述：确定特殊安全需求可以采用目前成熟或流行的需求分析/风险分析方法，或者采用下面介绍的活动：

a) 重要资产的分析：明确信息系统中的重要部件，如边界设备、网关设备、核心网络设备、重要服务器设备、重要应用系统等。

b) 重要资产安全弱点评估：检查或判断上述重要部件可能存在的弱点，包括技术上和管理上的；分析安全弱点被利用的可能性。

c) 重要资产面临威胁评估：分析和判断上述重要部件可能面临的威胁，包括外部的威胁和内部的威胁，威胁发生的可能性或概率。

d) 综合风险分析：分析威胁利用弱点可能产生的结果，结果产生的可能性或概率，结果造成的损害或影响的大小，以及避免上述结果产生的可能性、必要性和经济性。按照重要资产的排序和风险的排序确定安全保护的要求。

活动输出：《重要资产的特殊保护要求》。

**3.2.3 形成安全需求分析报告**

活动目标：本活动的目标是总结基本安全需求和特殊安全需求，形成安全需求分析报告。

角色：信息系统运营，使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，基本安全需求，重要资产的特殊保护要求。

活动描述：本活动主要包括以下子活动内容：

a) 完成安全需求分析报告：根据基本安全需求和特殊的安全保护需求等形成安全需求分析报告。安全需求分析报告可以包含以下内容：

1) 信息系统描述；

2) 安全管理状况；

3) 安全技术状况；

4) 存在的不足和可能的风险；

5) 安全需求描述。

活动输出：《安全需求分析报告》。

**3.3 总体安全设计**

**3.3.1 总体安全策略设计**

活动目标：本活动的目标是形成机构纲领性的安全策略文件，包括确定安全方针，制定安全策略，以便结合等级保护基本要求和安全保护特殊要求，构建机构信息系统的安全技术体系结构和安全管理体系结构。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，安全需求分析报告。

活动描述：本活动主要包括以下子活动内容：

a) 确定安全方针：形成机构最高层次的安全方针文件，阐明安全工作的使命和意愿，定义信息安全的总体目标。

b) 制定安全策略：形成机构高层次的安全策略文件，说明安全工作的主要策略，包括安全组织机构划分策略、业务系 统分级策略、数据信息分级策略、子系统互连策略、信息流控制策略等。

活动输出：《总体安全策略文件》。

**3.3.2 安全技术体系结构设计**

活动目标： 本活动的目标是根据信息系统安全等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，提出系统需要实现的安全技术措施，形成机构特定的系统安全技术体系结构，用以指导信息系统分等级保护的具体实现。

参与角色： 信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，安全需求分析报告，信息系统安全等级保护基本要求。

活动描述：本活动主要包括以下子活动内容：

a) 规定骨干网/城域网的安全保护技术措施根据机构总体安全策略文件、等级保护基本要求和安全需求，提出骨干网/城域网的安全保护策略和安全技术措施。骨干网/城域网的安全保护策略和安全技术措施提出时应考虑网络线路和网络设备共享的情况，如果不同级别的子系统通过骨干网/城域网的同一线路和设备传输数据，线路和设备的安全保护策略和安全技术措施应满足最高级别子系统的等级保护基本要求。

b) 规定子系统之间互联的安全技术措施 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出跨局域网互联的子系统之间的信 息传输保护策略要求和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等；提出局域网内部互联的子系统之间的信息传输保护策略要求和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等。

c) 规定不同级别子系统的边界保护技术措施，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别子系统边界的安全保护 策略和安全技术措施。子系统边界安全保护策略和安全技术措施提出时应考虑边界设备共享的情况，如果不同级别的子系统通过同一设备进行边界保护，这个边界设备的安全保护策略和安全技术措施应满足 最高级别子系统的等级保护基本要求。

d) 规定不同级别子系统内部系统平台和业务应用的安全保护技术措施 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别子系统内部网络平台、系统平台和业务应用的安全保护策略和安全技术措施。

e) 规定不同级别信息系统机房的安全保护技术措施，根据机构总体安全策略文件、等级保护基本要求和安全需求，提出不同级别信息系统机房的安全保 护策略和安全技术措施。信息系统机房安全保护策略和安全技术措施提出时应考虑不同级别的信息系统 共享机房的情况，如果不同级别的信息系统共享同一机房，机房的安全保护策略和安全技术措施应满足最高级别信息系统的等级保护基本要求。

f) 形成信息系统安全技术体系结构，将骨干网/城域网、通过骨干网/城域网的子系统互联、局域网内部的子系统互联、子系统的边界、子系统内部各类平台、机房以及其他方面的安全保护策略和安全技术措施进行整理、汇总，形成信息系 统的安全技术体系结构。

活动输出：《信息系统安全技术体系结构》。

**3.3.3 整体安全管理体系结构设计**

活动目标：本活动的目标是根据等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，调整原有管理模式和管理策略，既从全局高度考虑为每个等级信息系统制定统一的安全管理策略，又从每个信息系统的实际需求出发，选择和调整具体的安全管理措施，最后形成统一的整体安全管理体系结构。 参与角色： 信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统详细描述文件，信息系统安全保护等级定级报告，安全需求分析报告，信息系统安全等级保护基本要求。

活动描述：本活动主要包括以下子活动内容：

a) 规定信息安全的组织管理体系和对各信息系统的安全管理职责 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出机构的安全组织管理机构框架，分配各个级别信息系统的安全管理职责，规定各个级别信息系统的安全管理策略等。

b) 规定各等级信息系统的人员安全管理策略 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的管理人 员框架，分配各个级别信息系统的管理人员职责，规定各个级别信息系统的人员安全管理策略等。

c) 规定各等级信息系统机房及办公区等物理环境的安全管理策略 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的机房和 办公环境的安全策略。

d) 规定各等级信息系统介质、设备等的安全管理策略 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的介质、 设备等的安全策略。

e) 规定各等级信息系统运行安全管理策略 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的安全运行与维护框架和运维安全策略等。

f) 规定各等级信息系统安全事件处置和应急管理策略 根据机构总体安全策略文件、等级保护基本要求和安全需求，提出各个不同级别信息系统的安全事 件处置和应急管理策略等。

g) 形成信息系统安全管理策略框架 将上述各个方面的安全管理策略进行整理、汇总，形成信息系统的整体安全管理体系结构。

活动输出：《信息系统安全管理体系结构》。

**3.3.4 设计结果文档化**

活动目标： 本活动的目标是将总体安全设计工作的结果文档化，最后形成一套指导机构信息安全工作的指导性文件。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：安全需求分析报告，信息系统安全技术体系结构，信息系统安全管理体系结构。

活动描述：对安全需求分析报告、信息系统安全技术体系结构和安全管理体系结构等文档进行整理，形成信息 系统总体安全方案。 信息系统总体安全方案包含以下内容：

a) 信息系统概述；

b) 总体安全策略；

c) 信息系统安全技术体系结构；

d) 信息系统安全管理体系结构。

活动输出：《信息系统安全总体方案》。

**3.4 安全建设项目规划**

**3.4.1 安全建设目标确定**

活动目标：本活动的目标是依据信息系统安全总体方案（一个或多个文件构成）、机构或单位信息化建设的中 长期发展规划和机构的安全建设资金状况确定各个时期的安全建设目标。

参与角色：信息系统运营、使用单位，信息安全服务机构。活动输入：信息系统安全总体方案、机构或单位信息化建设的中长期发展规划。

活动描述：本活动主要包括以下子活动内容：

a) 信息化建设中长期发展规划和安全需求调查 了解和调查单位信息化建设的现况、中长期信息化建设的目标、主管部门对信息化的投入，对比信 息化建设过程中阶段状态与安全策略规划之间的差距，分析急迫和关键的安全问题，考虑可以同步进行的安全建设内容等。

b) 提出信息系统安全建设分阶段目标 制定系统在规划期内（一般安全规划期为3年）所要实现的总体安全目标；制定系统短期（1年以内）要实现的安全目标，主要解决目前急迫和关键的问题，争取在短期内安全状况有大幅度提高。

活动输出：《信息系统分阶段安全建设目标》。

**3.4.2 安全建设内容规划**

活动目标：本活动的目标是根据安全建设目标和信息系统安全总体方案的要求，设计分期分批的主要建设内容，并将建设内容组合成不同的项目，阐明项目之间的依赖或促进关系等。

参与角色：信息系统运营、使用单位，信息安全服务机构。 活动输入：信息系统安全总体方案，信息系统分阶段安全建设目标。

活动描述：本活动主要包括以下子活动内容：

a）确定主要安全建设内容，根据信息系统安全总体方案明确主要的安全建设内容，并将其适当的分解。主要建设内容包括不限于以下内容：

1) 安全基础设施建设；

2) 网络安全建设；

3) 系统平台和应用平台安全建设；

4) 数据系统安全建设；

5) 安全标准体系建设；

6) 人才培养体系建设；

7) 安全管理体系建设。

b）确定主要安全建设项目

组合安全建设内容为不同的安全建设项目，描述项目所解决的主要安全问题及所要达到的安全目标，对项目进行支持或依赖等相关性分析，对项目进行紧迫性分析，对项目进行实施难易程度分析，对项目进行预期效果分析，描述项目的具体工作内容、建设方案，形成安全建设项目列表。

**3.4.3 形成安全建设项目计划**

活动目标：本活动的目标是根据建设目标和建设内容，在时间和经费上对安全建设项目列表进行总体考虑，分到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设项目计划。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案，信息系统分阶段安全建设目标，安全建设内容等。

活动描述：对信息系统分阶段安全建设目标、安全总体方案和安全建设内容等文档进行整理，形成信息系统安全建设项目计划。

安全建设项目计划包含不限于以下内容：

a) 规划建设的依据和原则；

b) 规划建设的目标和范围；

c) 信息系统安全现状；

d) 信息化的中长期发展规划；

e) 信息系统安全建设的总体框架；

f) 安全技术体系建设规划；

g) 安全管理与安全保障体系建设规划；

h) 安全建设投资估算；

i) 信息系统安全建设的实施保障等内容。

活动输出：《信息系统安全建设项目计划》。

1. **安全设计与实施**

项目实施阶段及所需时间须经过需求调研之后由甲方最终确认。

**4.1项目实施计划**

**4.1.1项目实施计划**

项目实施过程共分为三项活动，即现场调研，文档规划，根据等级保护管理体系制定相应运维手册。

**第一阶段：现场调研阶段**

在此阶段中，我们工作的重点包括：

1.组织相关技术人员对宁波轨道交通运营分公司进行3-5次现场调研，盘查信息系统的范围、网络拓扑、业务情况、保护情况、信息系统的管理模式和相关部门及角色等内容。

2.由甲乙双方组成的项目工作小组成员对2至3家国内信息系统安全基础优秀的兄弟地铁单位进行现场调研，了解信息安全管理体系在实际运用中的客观存在的问题，以及相关业务情况，保护情况等。

**工作目标：摸清信息系统与网络环境等基本情况，为下一步编写系统定级指引及员工日常信息安全指导手册做准备**

**所需时间：45天（自然日）**

**第二阶段：定级规划阶段**

出台单位内部红头文件，成立信息安全等级保护工作领导小组，明确工作职责。

根据现场调研阶段所收集的信息，对相关信息进行整合，确定信息系统情况及数量。

根据《信息安全等级保护定级指南》对信息系统进行自定级，并填写相关《备案表》。

**工作目标：梳理信息系统数量，确定信息系统自定级报告、备案表等文件后报送本地公安网警。**

**输出文档**：《信息安全等级保护工作领导小组红头文件》，《信息系统等级报告》，《信息系统备案表》。

**所需时间：45天（自然日）**

**第三阶段:根据等级保护管理体系制定相应运维手册**

随着信息安全管理体系的逐步建立，在最终建设成一套成熟的信息安全管理体系的过程中，时刻要把握住PDCA、文件化、领导重视、全员参与这四大原则，制定相应规章制度。

**工作目标：建立完整的信息安全管理体系，使之成为日常单位内部信息安全工作的准则，为单位内部信息的正常运行保驾护航，并随时接受上级领导检查。**

**输出文档**：《信息安全管理汇编》（制度类25个，记录表单类28张，详见4.1.1.3章节表格）

**所需时间：80天（自然日）**

**4.1.1.1信息安全等级保护现场调研阶段**

1. 信息安全等级保护现场调研阶段

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 项目启动 | 项目计划书 | 项目概述、工作依据、技术思路、工作内容和项目组织等 |
| 信息收集和分析 | 信息系统基本情况分析报告 | 说明信息系统的范围、网络拓扑、业务情况、保护情况、信息系统的管理模式和相关部门及角色等 |

表（2）

**4.1.1.2信息安全等级保护定级规划阶段**

1. 依据标准

依据《信息安全技术 信息系统安全等级保护定级指南GB/T 22240—2008》，对轨道交通相关信息系统进行定级，该是信息安全等级保护相关系列标准之一。

与该相关的系列标准包括：

——GB/T 22239—2008《信息系统安全等级保护基本要求》；

——国家标准《信息系统安全等级保护实施指南》。

该依据等级保护相关管理文件，从信息系统所承载的业务在国家安全、经济建设、社会生活中 的重要作用和业务对信息系统的依赖程度这两方面，提出确定信息系统安全保护等级的方法。

1. 信息系统等级划分

根据等级保护相关管理文件，信息系统的安全保护等级分为以下五级：

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。

1. 信息系统定级要素

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

客体包括三个方面：即公民、法人和其他组织的合法权益，社会秩序、公共利益，国家安全。

侵害的程度归结为三种：即造成一般损害，造成严重损害，造成特别严重损害。

1. 信息系统定级要素与等级的关系

定级要素与安全保护等级的关系

|  |  |  |  |
| --- | --- | --- | --- |
| 所侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

图（1）

|  |  |  |  |
| --- | --- | --- | --- |
| 业务信息被破坏时所侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

图（2）

|  |  |  |  |
| --- | --- | --- | --- |
| 系统服务被破坏时所侵害的客体 | 对相应客体的侵害程度 | | |
| 一般损害 | 严重损害 | 特别严重损害 |
| 公民、法人和其他组织的合法权益 | 第一级 | 第二级 | 第二级 |
| 社会秩序、公共利益 | 第二级 | 第三级 | 第四级 |
| 国家安全 | 第三级 | 第四级 | 第五级 |

图（3）

1. 定级方法

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能 不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。 从业务信息安全角度反映的信息系统安全保护等级称业务信息安全保护等级。 从系统服务安全角度反映的信息系统安全保护等级称系统服务安全保护等级。 确定信息系统安全保护等级的一般流程如下：

a) 确定作为定级对象的信息系统；

b) 确定业务信息安全受到破坏时所侵害的客体；

c) 根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度；

d) 依据表2，得到业务信息安全保护等级；

e) 确定系统服务安全受到破坏时所侵害的客体；

f) 根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度；

g) 依据表3，得到系统服务安全保护等级；

h) 将业务信息安全保护等级和系统服务安全保护等级的较高者确定为定级对象的安全保护等级。

**4.1.1.3信息安全等级保护管理类文档制定阶段**

根据等级保护管理体系制定相应运维手册，所制定的运维手册包括管理制度类与记录台帐两大类。

| **类别** | **输出文档** | **文档内容** |
| --- | --- | --- |
| 制度类文档 | 《总体安全管理制度》 | 单位内部关于信息系统安全工作的总体方针、政策性文件和安全策略文件 |
| 《系统安全管理制度》 | 包括系统建设、系统运维，物理、网络主机、应用等层面的安全管理制度 |
| 《设备管理制度》 | 设备的进出入，使用人等信息 |
| 《审批管理制度》 | 系统及设备接入内部网络及重要资源的访问动作进行检查与审核 |
| 《系统投入运行测试管理制度》 | 对准备投入的信息系统进行系统测试，并记录 |
| 《机房管理制度》 | 对机房进出入、环境管理、人员操作、消防安全等内容做出相关规定 |
| 《网络安全管理制度》 | 网络拓扑结构，FW访问控制，IP地址管理等内容 |
| 《数据恢复与备份管理制度》 | 确定备份方式，操作规程，数据管理等 |
| 《系统变更管理制度》 | 对已上线的系统明确变更流程 |
| 《资产安全管理制度》 | 明确资产管理相关信息 |
| 《信息系统补丁及版本管理制度》 | 系统补丁版本的管理，规范补丁及版本的部署流程 |
| 《安全事件报告和处置管理制度》 | 提高处置网络与信息安全突发公共事件的能力，保障系统安全运行 |
| 《恶意代码防范制度》 | 关于恶意代码防范意识与防治管理工作 |
| 《存储介质管理制度》 | 关于介质的管理及操作规程 |
| 《系统建设管理制度》 | 关于系统建设时的安全方案设计，产品采购与使用工程测试验收等 |
| 《网络漏洞扫描制度》 | 关于系统内部应用、服务器漏洞扫描周期，扫描程度等 |
| 《信息系统权限划分实施细则》 | 关于单位内部不同系统之间的互联互通进行访问控制策略制定 |
| 《安全事件定级》 | 对网络与信息安全事件进行定级 |
| 《年度安全培训计划》 | 制定年度培训计划 |
| 《办公环境管理办法》 | 关于办公区域环境管理办法 |
| 《关键设备操作规程》 | 对关键设备的操作进行规定，避免误操作的发生 |
| 《保密协议书》 | 各岗位人员对信息系统相关信息的保密条款 |
| 《岗位职责文件》 | 明确岗位人员，并注明相关岗位职责 |
| 台帐（记录表单） | 设备领用登记表 |  |
| 设备更新及更换申请表 |  |
| 设备报废鉴定表 |  |
| 外联授权审批表 |  |
| 网络外联及准入申请表 |  |
| 外部人员运维申请表 |  |
| 系统投入运行申请表 |  |
| 中心机房进出人员登记表( )月 |  |
| 外部人员访问审批单 |  |
| 机房安全检查记录表 |  |
| 网络设备及服务器更新记录表 |  |
| 系统运维记录 |  |
| 系统变更申请表 |  |
| 补丁安装操作记录 |  |
| 系统补丁更新记录 |  |
| 介质使用管理记录表 |  |
| 培训记录单 |  |
| 应急预案培训记录表 |  |
| 安全事件处理记录 |  |
| 设备带离机房审批记录 |  |
| 恶意代码培训记录 |  |
| 介质归档登记表 |  |
| 安全教育培训记录 |  |
| 管理制度评审记录 |  |
| 信息系统会议纪要 |  |
| 安全管理制度修订记录 |  |
| 安全技能考核记录 |  |
| 操作运维记录 |  |

表（3）

**4.1.1.4信息安全等级保护安全基线文档编写**

通过前期对信息安全等级保护相关规定的制订及完善，根据各专业实际业务开展的需要以及信息安全相关方面的内容达标，指导日常信息安全工作开展制订《信息安全日常运维操作手册》，通过该手册能够为各专业日常信息安全管理工作提供依据并按照手册指引开展工作。

**4.2.2保密控制管理**

**4.2.2.1人员保密管理**

1. 未经授权方书面许可，被授权方人员不得将所知的授权方秘密信息以任何方式提供给任何第三方；
2. 未经授权方书面许可，被授权方人员不得擅自披露授权方的秘密信息；
3. 除了双方约定的工作目的之外，未经授权方书面许可，被授权方人员不得擅自使用授权方的秘密信息；
4. 对于项目实施过程中采集到的数据、信息和服务结果的保管、访问，被授权方无关人员不能访问；因工作需要必须访问的人员，被授权方应进行严格的访问控制；被授权方应对管理以上秘密信息的人员进行严格筛选；
5. 被授权方人员在项目实施过程中负有风险预估、及时预报的责任，在具有风险性的工作进行之前应向授权方说明该项工作将带来的影响；
6. 被授权方保证，不会利用与本次项目相关的秘密信息为自己或第三方开发信息、技术和产品，或与另一方进行商业竞争。

**4.2.2.2设备保密管理**

1. 未经授权方书面许可，被授权方的移动设备、个人信息处理设备等不得擅自接入授权方的生产及办公网络；
2. 授权方以书面形式同意被授权方使用一定的资源，如网络、NOTES等，被授权方只能将其用于本次项目工作目的，不得从事任何侵害授权方利益的活动；
3. 授权方以书面形式同意被授权方使用的工具、技术和方法，如扫描、测试等，被授权方只能将其用于本次项目工作目的，不得用来从事任何侵害授权方利益的活动。

**4.2.2.3文档保密管理**

1. 未经授权方书面许可，被授权方不得带走从授权方得到的任何文档、图纸、资料、磁盘、胶片等载有授权方秘密信息的介质；
2. 被授权方因工作需要必须携带的数据资料，须经授权方书面许可后加密或封条存储；
3. 工作期满离开时，被授权方应将包含授权方秘密信息的一切资料及其复印件如数交还授权方，未经授权方书面许可，被授权方不得擅自保留。
4. **项目组成员要求**

在实施阶段磋商申请人应指定一名具有注册信息安全专业人员资质的的工程师为项目负责人并成立由2-4名具有CISSP,CISP认证的技术工程师组成的项目小组负责本项目，如在项目实施阶段需要更换项目组小组成员包括项目负责人需向磋商申请人提出申请，由磋商申请人审批同意后方可更换。

1. **售后服务表**

**6.1建立完善的服务方式**

在项目质保期内，根据磋商发起人要求进行服务如下：

* 根据磋商发起人实际工作需要开展现场服务与使用指导；
* 每季度至少组织2次与相关管理人员沟通协商并发现问题，解决问题；
* 每季度制定相应的预防计划，安排周全的预防计划；
* 每季度2次实施回访工作、进行检查等；
* 每年不少于4次对相关信息系统漏洞扫描与修复；
* 每年不少于4次检查服务器、网络层安全基线配置；
* 设立信息安全事件处置预案与方法；
* 根据实际情况，每年不少于2次围绕处置预案展开的应急演练；
* 根据实际情况，提供重大活动临时驻场技术保障需求；
* 每年2次举行安全讲座、针对人员安全意识及安全管理员的专题培训；
* 每年对新增补信息系统、关键设备按照上述评估方式进行综合评估安全性；
* 每年对信息系统安全管理体系进行1次评估、并持续改进。

**6.2服务响应承诺**

接到磋商发起人通知后2小时内派人到现场维护，协助最终用户处理有关维护和技术问题，直至问题解决完毕恢复正常服务。乙方将问题内容及原因、处理过程和方法、完成处理及恢复正常的时间和日期等以书面形式报告甲方。服务方式包括但不限于现场维护、电子邮件、即时通讯软件、电话支持等。

**6.3技术支持**

磋商申请人在售后阶段也应成立服务小组，由2-4名具有CISSP,CISP认证的技术工程师组成，及时响应维护、调整工作。并同时指派一支经验丰富，技术精湛的技术顾问队伍作为重要项目的技术支持，这些顾问将帮助一线的维护人员分析处理疑难问题。

建立并保存完整的系统文档，磋商申请人在系统调试交接时，将提供完整的完工文件，软、硬件文档，操作等，并帮助用户建立系统的运行、管理和维护文档，以便在项目发生风险时能及时提供资料，迅速找到并排除风险。

**6.4售后服务体系**

* 为了保证维护服务过程得到最可靠最有效的实施，磋商申请人指派相关专业经验丰富的系统工程师来负责相关售后维护服务事宜。并将人员名单报至磋商发起人，保证双方沟通联系。可以更快捷更准确地保证故障在规定时间内得到解决；
* 为使项目达到预期目标，系统的售后服务工作至关重要，磋商申请人应建立了一套完善的客户服务体系和严格的管理制度，以使磋商发起人的售后服务工作得到有力保障；
* 针对本项目，磋商申请人设立项目负责人一名，保证磋商发起人的每一个请求均有及时、唯一和有效的响应，并对内负责协调磋商申请人资源，杜绝推诿和延误；
* 其服务内容包括以几个方面：售后服务：响应服务、维修服务、维护服务、提供备品、备件；技术服务：提供技术资料和技术咨询及产品使用和改进的信息、用户必要培训、软件版本升级和修改；
* 在质保期结束时，须由专业工程师对系统进行另一次测试验证，任何问题须由磋商申请人自行解决并取得磋商发起人同意。问题修复后，磋商申请人需提供一式三份报告给磋商发起人，包括问题原因，解决措施，完成修复所费时间及恢复正常运行日期。 响应服务的主要内容：远程协助诊断；了解问题所在；提出解决方案；产品使用及操作特性说明；技术文件说明

**6.5 项目验收计划**

对于项目的验收，由磋商申请人负责邀请信息安全主管部门组成的专家组对本次项目进行验收，采用的验收方式参照了SSE-CMM中保证过程的过程域中的相应要求，这些过程域也是验收的理论依据。DIEM安全模型的安全保证(Ensure)过程部分是专门的验收过程，采用这种规范的安全咨询验收方法，严格按照这一过程中定义的实施过程和文档进行。

参照DIEM安全咨询模型，在验收阶段主要应做以下几方面的工作：

* 确定验收目标及指标
  + 满足各专业日常信息系统安全工作基线的实施准绳；
  + 满足各专业对信息安全等级保护相关方面规定的修订和补充；
  + 现场实施工作完成；
  + 服务结果分析并提交相关报告。

**7信息安全管理体系建设总结报告**

# 在信息安全管理体系文件编制完成后，由运营分公司信息系统安全领导小组办公室组织按照文件的控制要求进行审核。结合实际情况，在体系文件编制阶段，将该标准与分公司的现有其他体系，如质量、环境保护等体系文件做归并与修订直至正式批准发布实施《信息安全管理体系》有关文档的发布。文件编制完成后出一份针对现阶段信息系统整体报告。