ICS 03.220.30

Q/CR

中国国家铁路集团有限公司企业标准

Q/CR 853—2021

铁路网络安全等级保护定级指南

Railway classification guide for classified protection of cybersecurity

2021-12-09 发布　　2022-01-09 实施

中国国家铁路集团有限公司　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国铁道科学研究院集团有限公司电子计算技术研究所归口。

本文件起草单位：中国铁道科学研究院集团有限公司电子计算技术研究所、公安部第三研究所、中国铁路信息科技集团有限公司。

本文件主要起草人：朱广劼、周泽岩、姚洪磊、王文婷、王彤、王瑞民、朱涛、刘刚、罗峥、袁静、尹湘培、付晓丹、杨晓冬、卫婧、司群、吴晓南、李琪。

引　言

本文件在GB/T 22240—2020《信息安全技术　网络安全等级保护定级指南》基础上，依据中国国家铁路集团有限公司（以下简称国铁集团）等级保护对象的特征，从国铁集团实际情况出发，提出和规定了国铁集团等级保护定级对象的安全保护等级定级原理及各阶段的要求，适用于指导国铁集团等级保护对象按照等级保护要求进行安全保护定级。进一步满足铁路移动互联、云计算、大数据、物联网和工业控制等新技术、新应用开展网络安全等级保护工作的需要。

与本文件相关的国家标准包括：

——GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求；

——GB/T 22240—2020　信息安全技术　网络安全等级保护定级指南；

——GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇。

铁路网络安全等级保护定级指南

1　范围

本文件规定了国铁集团非涉及国家秘密等级保护对象的安全保护等级定级原理及各阶段的要求。

本文件适用于指导国铁集团(国铁集团及所属各单位、控股合资公司)开展非涉及国家秘密的等级保护对象的定级工作。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 22240—2020　信息安全技术　网络安全等级保护定级指南

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇

3　术语和定义

GB/T 22239—2019、GB/T 29246—2017 和 GB/T 22240—2020 界定的以及下列术语和定义适用于本文件。

3.1

网络安全　cybersecurity

通过采取必要措施,防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。

[来源:GB/T 22239—2019,3.1]

3.2

等级保护对象　target of classified protection

网络安全等级保护工作直接作用的对象。

注:主要包含信息系统、通信网络设施和数据资源等。

[来源:GB/T 22240—2020,3.2]

3.3

受侵害的客体　object of infringement

受法律保护的、等级保护对象受到破坏时所侵害的社会关系。

注:本标准中简称"客体"。

[来源:GB/T 22240—2020,3.6]

3.4

客观方面　objective

对客体造成侵害的客观外在表现,包括侵害方式和侵害结果等。

[来源:GB/T 22240—2020,3.7]

4 定级原理

4.1 安全保护等级

根据等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，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侵害程度等因素，等级保护对象的安全保护等级分为以下五级：

a） 第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益；

b） 第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

c） 第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；

d） 第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害；

e） 第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害。

[来源：GB/T 22240—2020，4.1]

4.2 定级要素

4.2.1 定级要素概述

等级保护对象的定级要素包括：

a） 铁路业务重要性级别；

b） 业务信息类别；

c） 系统服务范围；

d） 受侵害的客体；

e） 对客体的侵害程度。

4.2.2 铁路业务重要性级别

4.2.2.1 非常重要业务包括：

a） 运输生产调度、控制和涉及行车安全的监控业务；

b） 直接影响国铁集团客货运生产和客户服务业务；

c） 存储和处理国铁集团重要数据的网络和系统；

d） 国铁集团非常重要的经营开发业务；

e） 服务于国铁集团的重要业务的基础设施，包括骨干通信网络、云平台、网络安全平台、数据中心等；

f） 服务于工程建设中重大工程的关键系统和基础设施；

g） 其他经国铁集团确定为非常重要业务的。

4.2.2.2 重要业务包括：

a） 行车监测、检测、维护等辅助业务；

b） 客货运服务辅助管理系统；

c） 国铁集团及所属各单位、控股合资公司公文流转、日常办公、邮件处理等管理业务；

d） 国铁集团经营开发相关业务；

e） 服务于铁路局（单位）范围内的重要业务的基础设施，包括骨干通信网络、云平台、网络安全平台、数据中心等；

f） 服务于工程建设的重要系统和基础设施；

g） 其他经国铁集团确定为重要业务的。

4.2.2.3 一般业务包括：

a） 不属于非常重要、重要的业务；

b） 经国铁集团确定为一般业务的。

4.2.3 业务信息类别

商业信息：关系国铁集团及所属各单位、控股合资公司的经济利益和竞争优势，涉及与科研、生产、经营相关的技术信息和经营信息。

工作信息：关系国铁集团及所属各单位、控股合资公司的公务活动和内部管理的事项，如文件类、信息类、政务类、专项业务类、内部管理类等与工作相关信息。

个人信息：以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

4.2.4 系统服务范围

系统服务范围包括全路性、区域性、局部性。

全路性指服务范围为国铁集团统建系统。

区域性指服务范围为国铁集团本级，或两个及以上路局级单位，路局级自建系统。

局部性指服务范围为路局级本级，或站段级自建系统。

4.2.5 受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a） 公民、法人和其他组织的合法权益；

b） 社会秩序、公共利益；

c） 国家安全。

[来源：GB/T 22240—2020，4.2.2]

4.2.6 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此对客体的侵害外在表现为对等级保护对象的破坏，通过侵害方式、侵害后果和侵害程度加以描述。

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

a） 造成一般损害；

b） 造成严重损害；

c） 造成特别严重损害。

[来源：GB/T 22240—2020，4.2.3]

5 确定定级对象

5.1 系统定级对象

定级对象应具有如下基本特征：

a） 具有确定的主要安全责任主体；

b） 承载相对独立的业务应用，不应将不同功能业务数据类型的应用合并定级；

c） 包含相互关联的多个资源，不应将某个单一的系统组件，如服务器、终端或网络设备作为定级对象。

在确定定级对象时，云计算平台/系统、物联网、工业控制系统以及采用移动互联技术的系统在满足以上基本特征的基础上，还应符合 GB/T 22240—2020 中 5.1.2～5.1.5 的相关规定。

5.2 网络设施定级对象

对铁路通信网络和铁路信息网络，宜根据安全责任主体、服务类型或服务地域等因素将其划分为不同的定级对象。

对铁路通信网络可作为一个整体对象定级，或按照国铁集团所属单位管辖区域进行划分，分别作为定级对象。

对铁路综合信息网等铁路信息网络可作为一个整体对象定级，或按照国铁集团所属单位管辖区域进行划分，分别作为定级对象。

6 确定安全保护等级

6.1 定级方法概述

定级对象的安全主要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，安全保护等级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定级对象安全保护等级称为业务信息安全保护等级；从系统服务安全角度反映的定级对象安全保护等级称为系统服务安全保护等级。

定级方法流程应符合图 1 的规定。

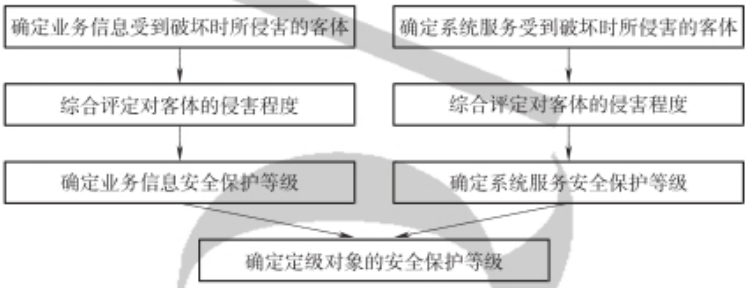

图 1 定级方法流程示意图

具体流程如下：

a） 确定受到破坏时所侵害的客体：

1） 确定业务信息受到破坏时所侵害的客体；

2） 确定系统服务受到侵害时所侵害的客体。

b） 确定对客体的侵害程度：

1） 根据不同的受侵害客体，分别评定业务信息安全被破坏对客体的侵害程度；

2） 根据不同的受侵害客体，分别评定系统服务安全被破坏对客体的侵害程度。

c） 确定安全保护等级：

1） 确定业务信息安全保护等级；

2） 确定系统服务安全保护等级；

3） 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。

6.2 确定受侵害的客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益。

侵害国家安全的事项包括以下方面：

a） 影响国家政权稳固和领土主权、海洋权益完整；

b） 影响国家统一、民族团结和社会稳定；

c） 影响国家社会主义市场经济秩序和文化实力；

d） 其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：

e） 影响国铁集团的运输秩序、经营秩序、生产建设秩序、科研秩序、公共卫生秩序；

f） 影响客货运组织、旅客出行秩序；

g） 其他影响社会秩序的事项。

侵害公共利益的事项包括以下方面：

h） 影响社会成员使用客货运公共设施；

i） 影响社会成员获取国铁集团提供的公开数据；

j） 影响社会成员接受铁路公共服务等方面；

k） 其他影响公共利益的事项。

侵害公民、法人和其他组织的合法权益是指受法律保护的公民、法人和其他组织所享有的社会权利和利益等受到损害。

确定受侵害的客体时，首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公共利益，最后判断是否侵害公民、法人和其他组织的合法权益。

6.3 确定对客体的侵害程度

6.3.1 侵害的客观方面

在客观方面，对客体的侵害外在表现为对定级对象的破坏，其侵害方式表现为对业务信息安全的破坏和对系统服务安全的破坏。其中，业务信息安全是指确保定级对象中信息的保密性、完整性和可用性等，系统服务安全是指确保定级对象可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种侵害方式。

业务信息安全和系统服务安全受到破坏后，可能产生以下侵害后果：

——影响行使工作职能；

——导致业务能力下降；

——引起法律纠纷；

——导致财产损失；

——造成社会不良影响；

——对其他组织和个人造成损失；

——其他影响。

[来源：GB/T 22240—2020，6.3.1]

6.3.2 综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现，因此，首先根据不同的受侵害客体、不同侵害后果分别确定其侵害程度。对不同侵害后果确定其侵害程度所采取的方法和所考虑的角度可能不同，例如，系统服务安全被破坏导致业务能力下降的程度可以从定级对象服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，参照以下不同的判别基准：

a） 如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；

b） 如果受侵害客体是社会秩序、公共利益或国家安全，则以整个行业或国家的总体利益作为判断侵害程度的基准。

不同侵害后果的三种侵害程度描述如下：

c） 一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害；

d） 严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较高损害；

e） 特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常高损害。

通过对不同侵害后果的侵害程度进行综合评定得出对客体的侵害程度。

6.4 综合判定等级

分析定级对象的铁路业务重要性级别和业务信息类别，判断受侵害的客体，参考表 A.1，确定对客体的侵害程度，依据表 1 得到业务信息安全保护等级。

表 1 业务信息安全保护等级矩阵表

业务信息安全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

根据定级对象的铁路业务重要性级别，分析系统服务范围，判断受侵害的客体，参考表 A.2，确定对客体的侵害程度，依据表 2 得到系统服务安全保护等级。

表 2 系统服务安全保护等级矩阵表

系统服务安全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

定级对象的初步安全保护等级由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决定。安全保护等级的确定按 GB/T 22240—2020 第 7 章要求执行，定级报告参考附录 B。

7　等级变更

当等级保护对象的网络安全责任主体所处理的信息和系统服务范围发生变化，可能导致业务信息安全或系统服务安全受到破坏后的受侵害客体和对客体的侵害程度发生变化，应根据本文件重新确定定级对象和安全保护等级。

附 录 A
（资料性）
确定受侵害的客体及对客体的侵害程度

涉及侵害客体为国家安全的参考 GB/T 22240—2020 的相关内容；涉及侵害客体为社会秩序、公共利益，公民、法人和其他组织的合法权益的参考本文件。

确定业务信息安全受侵害的客体和对客体的侵害程度的过程如下：

a） 分析定级对象业务特点确定“铁路业务重要性级别”；

b） 分析其承载的信息类别确定“业务信息类别”；

c） 分析业务信息受到破坏后受侵害的客体；

d） 参考表 A.1 分析确定对客体的侵害程度。

表 A.1 业务信息安全定级要素对应表

铁路业务重要性级别	业务信息类别	受侵害客体	对客体的侵害程度
非常重要业务	商业信息	社会秩序、公共利益	严重损害或特别严重损害
	工作信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	个人信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
重要业务	商业信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	工作信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
	个人信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
一般业务	商业信息	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	工作信息	社会秩序、公共利益	一般损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
	个人信息	社会秩序、公共利益	一般损害
		公民、法人和其他组织的合法权益	一般损害或严重损害

确定系统服务安全受侵害的客体和对客体的侵害程度过程如下：

e） 分析定级对象业务特点确定“铁路业务重要性级别”；

f） 分析确定“系统服务范围”；

g） 分析系统服务受到破坏后受侵害的客体；

h） 参考表 A.2 分析确定对客体的侵害程度。

表 A.2　系统服务安全定级要素对应表

铁路业务重要性级别	系统服务范围	受侵害客体	对客体的侵害程度
非常重要业务	全路性	社会秩序、公共利益	严重损害或特别严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	区域性	社会秩序、公共利益	严重损害或特别严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	局部性	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
重要业务	全路性	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	区域性	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	严重损害或特别严重损害
	局部性	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
一般业务	全路性	社会秩序、公共利益	一般损害或严重损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
	区域性	社会秩序、公共利益	一般损害
		公民、法人和其他组织的合法权益	一般损害或严重损害
	局部性	社会秩序、公共利益	一般损害
		公民、法人和其他组织的合法权益	一般损害或严重损害

附 录 B
（资料性）
定级报告模板

定级报告模板见图 B.1。

××××（定级对象名称）
网络安全等级保护定级报告

一、××××（定级对象名称）描述

简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担网络安全责任的相关单位或部门，说明本单位或部门对定级对象具有网络安全保护责任，该系统为本单位或部门的定级对象；二是该定级对象是否承载着单一或相对独立的业务，业务情况描述；三是该定级对象是否具有系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备。（下附网络结构图）

二、××××（定级对象名称）安全保护等级确定

（一）业务信息安全保护等级的确定

1. 业务信息描述

描述定级对象处理的主要业务信息、业务信息规模等。

2. 业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时侵害的客体是什么，即对国家安全；社会秩序和公共利益；公民、法人和其他组织的合法权益中的哪些客体造成侵害。

3. 业务信息受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4. 业务信息安全等级的确定

依据业务信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级为第 X 级（相应等级）。

业务信息安全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

（二）系统服务安全保护等级的确定

1. 系统服务描述

描述定级对象的服务范围、服务对象、系统服务连续性等。

2. 系统服务受到破坏时所侵害客体的确定

说明系统服务受到破坏时侵害的客体是什么，即国家安全；社会秩序和公共利益；公民、法人和其他组织的合法权益中的哪些客体造成侵害。

3. 系统服务受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4. 系统服务安全等级的确定

依据系统服务受到破坏时所侵害的客体以及侵害程度，确定系统服务安全等级为第 X 级（相应等级）。

图 B.1 定级报告模板

系统服务安全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

（三）安全保护等级的确定

依据 GB/T 22240—2020，××××（定级对象名称）的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定××××（定级对象名称）安全保护等级为第×级（相应等级）。

系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
（定级对象名称）	第×级	第×级	第×级

（网络安全主体责任单位名称）

图 B.1　定级报告模板（续）

参 考 文 献

[1] GB 17859—1999 计算机信息系统 安全保护等级划分准则
[2] GB/T 25069—2010 信息安全技术 术语
[3] GB/T 29246—2017 信息安全 安全技术 信息安全管理体系 概述和词汇
[4] GB/T 31167—2014 信息安全技术 云计算服务安全指南
[5] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求
[6] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南
[7] GB/T 35273—2020 信息安全技术 个人信息安全规范

中国国家铁路集团有限公司
企 业 标 准
铁路网络安全等级保护定级指南
Railway classification guide for classified protection of cybersecurity
Q/CR 853—2021
*
中国铁道出版社有限公司出版
(100054,北京市西城区右安门西街 8 号)
北京建宏印刷有限公司印刷

*
开本:880 mm × 1 230 mm　1/16　印张:1.25　字数:25 千字
2021 年 12 月第 1 版　2021 年 12 月第 1 次印刷
*
统一书号:15113 · 6405(内部用书)