ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/TXXXXX—2022

信息安全技术 网络弹性评价准则

information security technology—Cyber-resilience evaluation criteria

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

2023-08-24

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：大连理工大学、中国软件评测中心、中国科学技术大学、国家工业信息安全发展研究中心、网络通信与安全紫金山实验室、联想（北京）有限公司、北京天融信网络安全技术有限公司、腾讯云计算（北京）有限责任公司、公安部第三研究所、中国信息通信研究院、国家计算机网络应急处理协调中心、中国检验认证（集团）有限公司、中国电信研究院、天翼云科技有限公司、中车大连机车车辆有限公司、国电南京自动化股份有限公司、中能融合智慧科技有限公司、华能信息技术有限公司、中国电子科技集团公司第十五研究所、国家信息技术安全研究中心、华为技术有限公司、中兴通讯股份有限公司、信华信技术股份有限公司、欧亚高科数字技术有限公司、湖北省烟草公司、解放军战略支援部队信息工程大学、东南大学、北京理工大学、北京路云天网络安全技术研究院有限公司、陕西省信息化工程研究院、长阳科技（北京）股份有限公司、深圳开源互联网安全技术有限公司、嵩山实验室、安芯网盾（北京）科技有限公司、郑州昂视信息科技有限公司、南京南瑞信息通信科技有限公司、深信服科技股份有限公司、南京汇荣信息技术有限公司、山石网科通信技术股份有限公司、北斗中认、广东网安联认证中心、中邦网络安全技术（深圳）有限公司、永信至诚、广东云百科技有限公司。

本文件主要起草人：宋明秋、左晓栋、杨春立、季新生、陈兴跃、张进、王冲华、李汝鑫、王龑、黎水林、卢春景、张哲宇、崔涛、汪慕峰、金伟、喻梁文、王宝雁、徐浩、呼博文、沈君、广小明、王大伟、辛晨、刘文彪、黄石海、林天翔、刘建、梁利、安宏杰、曹鲲鹏、赵赫、汤成俊、潘中英、孙宏伟、程军强、杨斯可、宋景民、马海龙、曹向辉、郭泽华、王少杰、赵晓荣、王柯懿、郑剑锋、顾希、余果、谢琴、张亚晶、王颉、张建辉、李天涯、李昂、魏兴慎、李鹏坤、叶润国、康杰、顾海群、阮懿宗、魏东、李伟、周柏魁。

信息安全技术 网络弹性评价准则

1 范围

本文件给出了网络弹性评价模型，提出了对象系统分析、网络弹性功能和网络弹性架构的评价指标和评价方法。

本文件适用于组织对系统网络弹性能力的自评价，网络安全服务机构对系统弹性能力的第三方评价，也适用于系统网络弹性能力的设计、建设和提升。

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 20988－2007 信息安全技术 信息系统灾难恢复规范

GB/T 25069－2022 信息安全技术 术语

GB/T 28827.3－2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 30146－2013/ISO 22301: 2012 业务连续性管理体系

GB/T 39204－2022 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 25069－2022 界定的以及下列术语和定义适用于本文件。

3.1

网络弹性 cyber resilience

网络面临不利条件、压力、攻击或妥协时，进行预测、承受、恢复和适应的能力。

注：本文件中术语“网络”指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.2

关键业务 critical business

一旦遭受网络安全事件（3.4）可能会严重影响组织或客户的安全和稳定，造成不可容忍的损害的重要业务。

注：不可容忍的损害指在程度上远大于常规意义上的损害或者不方便，在发生中断事件后，系统无法迅速恢复到正常运行的状态，或者存在无法有效补救的严重影响。

3.3

关键信息基础设施 critical information infrastructure; CII

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的信息设施。

［来源：GB/T 39204－2022, 3.1］

3.4

网络安全事件 cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，危害网络和信息系统或者其中的数据，导致业务中断，对国家、社会、经济造成负面影响的事件。

［来源：ISO 38645—2020, 3.1,有修改］

3.5

容错 fault tolerance

在出现故障或错误的情况下，功能单元持续执行所需功能的能力。

注：容错描述了系统对内部组件的随机失效和故障的容忍能力。

示例：通过结构上的冗余来吸收故障造成的影响，或者通过冗余资源来换取高可靠性。

［来源：ISO 22739—2020, 3.36,有修改］

3.6

鲁棒性 robust

系统结构能够承受网络安全事件，并保持其性能水平的能力。

［来源：ISO 19900—2019, 3.44,有修改］

注：鲁棒性描述了系统在环境干扰、输入异常等各类外部不利条件下，吸收外部干扰，具有持续、正确地执行其指定功能的系统内在能力。

示例：在软件/系统输入错误、磁盘故障、网络过载或有意攻击的情况下，通过系统内部反馈控制，保持系统不死机、不崩溃。

3.7

生存性 survivability

在攻击、失效或服务中断存在的条件下，产品或系统仍能提供基本服务，完成关键业务的能力。

［来源：ISO/IEC/IEEE 24765—2017, 3.4060，有修改］

4 缩略语

下列缩略语适用于本文件。

API：接口（application programming interface）

APT：高级持久性威胁（advanced persistent threat）

CRA：网络弹性架构（cyber resiliency architecture）

CRC：网络弹性能力（cyber resiliency capability）

CRF：网络弹性功能（cyber resiliency function）

MBCO：最低业务连续目标（minimum business continuity objective）

MTBF：平均失效间隔时间（mean time between failure）

MTPD：最长可容忍中断期（maximum tolerable period of disruption）

MTTR：平均修复时间（mean time torepair）

NAT：网关（network address translation）
OSA：对象系统分析（object system analysis）
RPO：恢复点目标（recovery point objective）
RTO：恢复时间目标（recovery time objective）

5 概述

5.1 网络弹性

弹性是系统吸收和适应内部和外部环境变化，保持其功能和结构稳定并在必要时适度降级的能力。其中，吸收是指通过有效地响应，使系统具有应对、解决或在适当条件下利用非预期事件的能力，吸收能力可以通过容错和鲁棒性等方法实现；适度降级是指当遭受重大网络安全事件时，系统能够采用比正常系统运行模式功能降低、级别降低的模式运行，保证系统持续提供基本业务功能的能力，保证关键业务的生存性。

网络弹性是指当网络面临不利条件、压力、攻击或妥协等网络安全事件时，其本身所应具有的“预测、承受、恢复和适应”能力，其主要目的为实现当系统遭受攻击或服务中断等网络安全事件时，保证关键业务的稳定运行。网络弹性 4 个能力要素的关系如图 1 所示，它们的含义为；

a） 预测能力。保持一种对网络安全事件有充分准备状态的能力；

b） 承受能力。在网络安全事件发生后快速应急响应、吸收网络安全事件，在事件中生存下来，并持续运行关键业务的能力；

c） 恢复能力。在网络安全事件发生后快速恢复关键业务功能的能力；

d） 适应能力。系统具有修改业务功能或操作，以适应环境变化，不断提升抵抗风险的能力。

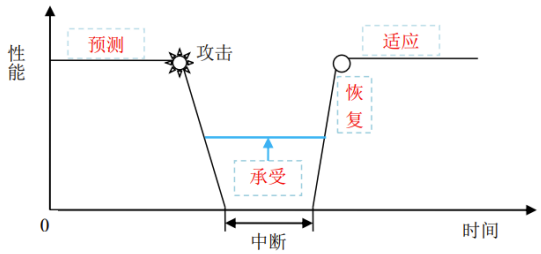

图 1 网络弹性能力要素关系改）

网络安全的三个基本属性为保密性、完整性、可用性，网络弹性为在网络安全三个基本属性基础上新增的系统属性，可以为系统的内在弹性能力建设提供指导。

5.2 网络弹性评价

网络弹性的评价对象为一个组织或部门的系统，也包括系统所处的环境、系统运营所涉及的组织、管理、人员及相关内容。评价原则包括：

a） 面向攻防。面对零日漏洞高发和层出不穷的网络攻击新模式，保证系统关键业务平稳运行，必要情况下使能系统战略威慑能力，是信息系统开发方和运营方必须要解决的问题。因此，系统中存在攻击是网络弹性能力的基本应用假设；

b） 关注应急响应与恢复。从系统破坏中迅速恢复的能力是弹性概念的基本特征，因此对网络安全事件采取应急响应措施，将损失降低到最低可接受水平，并采取适当的恢复或重构策略实现业务的迅速恢复，是网络弹性能力的主要特征；

c) 底线思维。以业务风险为核心，提高系统关键业务在面临重大灾难网络安全事件时的生存能力，是网络弹性能力与传统业务连续性的主要区别；

d) 功能与结构统一。通过对象系统与弹性功能和弹性架构要素映射关系的构建，为网络弹性功能和结构的设计和实现提供指导。

本文件从对象系统分析、网络弹性功能和网络弹性架构三个方面，提出一种多指标综合网络弹性能力评价方法，根据每一项评价指标对于网络弹性能力的重要性设定评价指标的类型（包括基本要求和推荐要求），依据具体评价情况划分网络弹性能力等级。

6 评价模型

6.1 评价指标体系模型

本文件提出的多指标综合网络弹性能力评价指标体系模型如图 2 所示。其中：

a) 基于网络弹性定义，将“预测、承受、恢复、适应”四个能力要素作为网络弹性能力评价的一级指标；

b) 二级指标包括三个模块，分别是对象系统分析OSA、网络弹性功能CRF和网络弹性架构CRA，共同支撑网络弹性能力4个一级指标的实现。其中：

1) 对象系统分析OSA包括5个二级指标，确定关键业务、重要资产与服务的优先级和恢复顺序，识别约束条件，确定关键业务所依赖的重要网络资源的网络弹性能力需求和业务连续性需求，明确网络弹性目的；

2) 网络弹性功能CRF是指为实现网络弹性能力，评价对象系统所依赖的所有网络资源的集合，包括硬件、软件和固件。CRF从预测、承受、恢复和适应4个网络弹性能力要素一级指标出发，通过4个能力要素的指标分解产生网络弹性功能12个二级指标，指导网络弹性功能设计。网络弹性功能CRF与网络弹性4个能力要素的映射关系见附录D；

3) 网络弹性架构CRA采用自顶向下的方法，从网络弹性能力需求和业务连续性需求出发，通过逻辑架构弹性、物理架构弹性、通信网络架构弹性逐层分解为12个二级指标，指导网络弹性结构设计。网络弹性架构CRA与网络弹性4个能力要素的映射关系见附录E；

c) 在二级指标之下，可再分解为三级指标，具体评价指标体系见附录A、附录B和附录C。

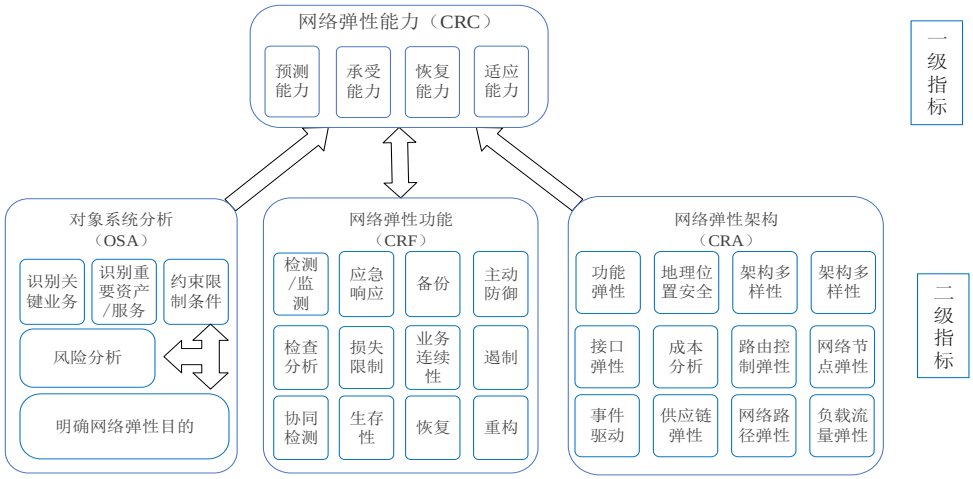

图2 网络弹性评价指标体系模型

6.2 网络弹性能力

6.2.1 预测能力

为实现对网络安全事件有充分准备状态的能力，网络应具有以下弹性功能和架构特征：

a) 对象系统分析（6.3），识别关键业务、重要资产和服务及其风险分析等,明确网络预测能力的需求；
b) 在功能方面，包括检测/监测组件（6.4.1），对特定网络安全事件进行详细分析（6.4.2），并加入行业或国家的威胁共享平台，实现协同检测（6.4.3）；
c) 在架构方面，根据具体应用场景，将检测/监测组件部署于不同物理位置（6.5.4）和网络架构层次（6.5.11）。

6.2.2 承受能力

为实现遭受重大网络安全事件时系统关键业务的生存能力，网络应具有以下弹性功能和架构特征：

a) 对象系统分析，明确网络承受能力需求；
b) 在功能方面，包括对重大网络安全事件应急响应（6.4.4）、采取措施限制损失（6.4.5），并通过安全失效模式、防故障模式等保证关键业务的生存性（6.4.6）等；
c) 在架构方面，包括功能弹性（6.5.1）、接口弹性（6.5.2）、供应链弹性（6.5.6）、架构多样性（6.5.7）、路由控制机制弹性（6.5.8）等特征。

6.2.3 恢复能力

为实现在网络安全事件发生后快速恢复关键业务功能的能力，网络应具有以下弹性功能和架构特征：

a) 对象系统分析，明确网络恢复能力需求；
b) 在功能方面，包括备份（6.4.7）、业务连续性（6.4.8）和恢复（6.4.9）功能；
c) 在架构方面，包括事件驱动（6.5.3）、供应链弹性（6.5.6）、架构多样性（6.5.7）、路由控制机制弹性（6.5.8）、网络路径弹性（6.5.9）等特征。

6.2.4 适应能力

为适应业务和环境变化，实现自适应地修改业务功能或操作的能力，网络应具有以下弹性功能和架构特征：

a) 对象系统分析，明确网络适应能力需求；
b) 在功能方面，包括主动防御（6.4.10）、遏制（6.4.11）和重构（6.4.12）功能；
c) 在架构方面，包括功能弹性（6.5.1）、接口弹性（6.5.2）、事件驱动（6.5.3）、物理位置（6.5.4）、架构多样性（6.5.7）等特征。

注1：网络弹性能力要素与网络弹性功能和网络弹性架构要素的映射关系可能是不是一对一的关系，而是多对多的关系，因此此处列出的网络弹性能力包含的功能要素和架构要素仅作为网络弹性功能和架构设计的参考，而不是唯一的依据。

注2：更多的网络弹性功能、网络弹性架构与网络弹性能力要素的映射关系见附录D和附录E。

6.3 对象系统分析

6.3.1 识别关键业务

依据GB/T 39204－2022标准，识别关键业务，包括：

a） 识别系统中包含的关键业务，以及非关键业务和相关联外部业务；

b） 关键业务对非关键业务和外部业务的依赖性和重要性；

c） 对系统关键业务进行优先级排序。

6.3.2 识别重要资产和服务

识别关键业务流程中重要的资产和服务，包括：

a） 资产和服务重要性分析。依据GB/T 39204－2022标准，明确支撑关键业务的重要信息资产、服务、业务数据，并输出重要资产、服务分布和运营情况；

b） 资产和服务优先级排序。

注：资产指对象系统中包含的所有有价值的东西，包括有形资产如硬件设备、固件，和无形资产如软件、数据、专利、知识产权、企业声誉等。服务包括对象系统提供给客户的服务（产品），也包括为了实现用户的业务需求，而由第三方服务机构提供给对象系统的服务。

6.3.3 风险分析

依据GB/T 20984等风险评估标准，开展风险分析，对评估对象系统关键业务的网络安全状况进行评估，识别资产脆弱性，为资产的风险进行排序。

6.3.4 约束与限制条件

约束与限制条件包括：

a） 明确组织风险管理策略。包括：风险偏好、风险分析、风险决策、风险应对以及法律法规的符合性约束等；

b） 识别限制要素。识别组织风险管理策略中安全事件的限制要素(例如，对特定技术的承诺，与其它系统的交互需求，或依赖于其它系统的需求)，评估哪些要素可以（或不能）用于网络弹性解决方案；

c） 识别依赖关系。厘清系统资产内外部依赖关系，更好地理解安全事件的影响因素和作用机制，以利于风险决策，包括：

1） 识别网络系统业务流程中资产或服务的内部依赖关系，例如紧前关系、时序关系、并行关系、顺序关系等；

2） 识别网络系统业务流程中资产或服务的外部依赖关系,例如业务活动所涉及的硬件是否到位，或者软件供应商是否开发了系统补丁程序等，这些可能涉及供应链弹性问题。

6.3.5 明确网络弹性目的

网络弹性目的包括：

a） 系统中关键业务及其业务流程中重要资产和服务的优先级排序；

b） 关键资产和服务的网络弹性能力需求；

c） 关键业务的业务连续性需求及其优先级排序，包括服务可用性需求SLA,最长可接受中断时间MAO、最大可容忍中断时间MTPD、最小业务连续目标MBCO等。

6.4 网络弹性功能

6.4.1 检测/监测

系统能够基于指示器、报警信息和预测活动，发现或识别已经发生、正在发生或将要发生的事实，

识别网络安全事件（包括已知威胁和未知威胁）及其影响，降低网络安全事件的影响范围和发生的可能性。其评价指标可以包括对网络安全事件检测/监测的准确率和召回率。

注：此种检测/监测模式比较适合于传统的威胁，对于新型复杂攻击威胁，例如：APT 攻击，攻击活动可能会基于防御反应的影响而做出动态调整，在此情景下此种检测/监测模式存在不足。

6.4.2 检查分析

针对特定网络安全事件（如某类 APT 攻击）及相关系统组件进行仔细检查分析，特别要分析漏洞利用、触发条件和脆弱点模式，以提高检测的准确率，降低网络安全事件的影响范围和发生的可能性。基于特定威胁活动的分析，可以更好地理解攻击方。分析应包括与其他活动的相关性、对相关活动的影响以及特定活动的可观测性，从而识别攻击方的攻击策略-技术-过程。

6.4.3 协同检测

应支持利益相关方群体共同、联合或协同的风险应对方案，提高风险因素识别和补救措施的有效性，减少网络安全事件影响的时间和空间范围，降低网络安全事件由一个组织系统传递到另一个组织系统的感染和破坏能力。具体包括：

a） 关键信息基础设施应与国家\行业威胁信息共享平台建立信息共享渠道或者机制；
b） 依据权威机构的标准建立适合自身规模和质量的威胁情报库，并及时向利益相关方群体分享和披露威胁信息，以增强利益相关方群体对网络安全事件特征和行为的了解；
c） 建设自然灾难历史数据库或对接国家自然灾难预警系统，降低灾难事件造成的潜在损失。

6.4.4 应急响应

依据 GB/T 28827.3－2012 标准，对应急事件采取相应的措施和活动。具体包括：

a） 应急预案及执行度。基于关键业务、资产和服务的优先级排序，依据国家标准和规范制定应急响应预案，并通过定期应急演练保证在网络安全事件发生时应急响应预案的有效执行；
b） 监测预警。根据日常监测结果，及时发现应急事件并有效预警，对事件进行核实和评估，启动应急预案并持续跟踪；
c） 应急处置。采取必要应急调度手段，开展故障排查与诊断，根据业务、资产与服务的优先级排序，对故障进行快速有序地处理和恢复，及时通报应急事件，提供持续性服务保障，对应急结果进行评价并关闭事件。

6.4.5 损失限制

通过限制网络安全事件在时间、系统资源或业务方面造成的损害或影响来限制网络安全事件的后果。降低相同网络安全事件情景下次生安全事件发生的可能性和影响的范围，限制网络安全事件的效力。具体包括：

a） 减小攻击面/收敛暴露面。减少系统输入/输出节点的数量，减少系统遭受攻击的可能性和影响；
b） 分离关键业务和非关键业务。尽量减少关键业务和非关键业务之间的连接，降低非关键业务故障影响关键业务的可能性，最小化非关键业务功能被利用作为攻击向量的可能性；
c） 缩短时间窗。限制网络安全事件持续时间或触发的条件，使攻击方活动产生预期效果的时间窗口有限，降低网络安全事件的潜在影响。例如：对于时间要求高的组件，防御方可以采用不同的供应商（供应链多样性），当攻击方攻击一个供应商并导致其关闭的时候，防御方可以增加使用其他供应商的产品，从而缩短没有关键组件的时间；
d） 分段与隔离。
- 分段。根据组织使命、系统或业务的不同属性对网络进行分段，以实现对不同业务及其不

同属性的访问控制；

- 隔离。当网络安全事件发生后，将危险区域迅速关闭或与其它区域相隔离，避免网络安全事件带来的风险传播，降低次生安全事件造成的影响。例如，攻击事件发生后，系统能够迅速检测出攻击，并将感染节点从网络中分离。

6.4.6 生存性

基于 3.7 的定义，生存性是指当系统遭受攻击或服务中断的情况下，持续提供基本业务功能、保证关键业务的生存底线。具体包括：

a) 安全失效模式。采用适当方法和技术保证系统以可控的方式失效，保证失效事件不会对系统造成损失或者尽量减小损失；

注：其中，失效模式指一个系统或组件没有满足其设计目的或功能，包含了从致使失效的因素、失效机理、失效发展过程到临界状态等整个失效过程。

b) 防故障模式。防止由于机理性原因引发的系统故障，例如防止网络设备故障、防止网络负载均衡故障等；

c) 降级模式。当遭受重大网络安全事件时，系统能够采用比正常模式功能降低、级别降低的模式运行，保证系统持续提供基本业务功能的能力，保证关键业务的生存性；

d) 吸收模式。采用鲁棒性和容错等技术，吸收网络安全事件或故障，保证系统提供持续服务。

6.4.7 备份

对重要数据或文件进行备份，提高系统恢复能力，包括：

a) 备份策略。明确备份的策略、需要备份的数据和文件内容、以及备份时间和备份方式。常见的备份策略有完全备份、增量备份、差异备份三种；

b) 受保护的备份。对备份数据或文件提供必要的安全保护，确保备份文件是干净的、可用的、没有被篡改或者破坏的。

6.4.8 业务连续性

关键业务应具有平稳连续运行的能力，包括：

a) 高可用性。可依据相关标准规范定义系统关键业务的可用性水平，例如在供应商服务协议 SLA 中约定。可用性的计算方法如下：

- 系统的可用性=可用时间/（可用时间+不可用时间）；
- 组件的可用性=MTBF/(MTBF+MTTR)。

b) 连续操作。在出现系统运行故障和服务中断的情况下，应具有通过手动操作、组件替换或切换等功能保证关键业务运行不中断；

c) 回滚。对于网络安全事件产生的不期望后果或发生网络安全事件时尚未完成的业务，系统应具有还原或回滚的功能，特别是与关键业务相关的后果，以降低事件的影响；

d) 重续运行。网络安全事件发生时，运行系统从主中心转移到灾难备份中心，再回到主中心运行的过程。

6.4.9 恢复

采用适当的恢复策略，实现系统恢复目标，包括：

a) 恢复数据源。对于已经损坏或可疑的资源(通过完整性检查、行为确认)，应从干净的受保护的备份中恢复；

b) 恢复策略。系统在遭受攻击后，可以通过节点修复和连边重构的方式快速恢复业务功能，包括

两种恢复策略：

- 节点备份恢复策略。在网络中某功能节点失效后，可以采用备份节点替代失效节点，实现相应的功能；
- 节点接替恢复策略。在网络中某功能节点失效后，可以采用其它具备相似功能的节点接替原失效节点的功能，实现节点接替；

c） 恢复目标，包括：

- 恢复点目标 RPO。网络安全事件发生后，业务系统从停顿到必须恢复的时间要求；
- 恢复时间目标 RTO。网络安全事件发生后，业务系统必须恢复到的时间点要求。

注：RTO 值越小数据恢复能力越强，RPO 值越小系统对数据完整性的保证能力越强。

6.4.10 主动防御

为适应环境变化，系统采用主动防御策略，降低网络安全事件发生概率，控制危害程度，主要功能包括：

a） 清除受损数据。删除不安全的、不正确的或已经损坏的、可能造成损害的网络资源或数据，及时更新或修复失陷组件，降低网络安全事件发生的可能性。例如:使用虚拟化技术以随机间隔刷新关键软件，使攻击方植入该软件的恶意代码被清除；

b） 按需激活。创造网络安全事件不能产生效果的条件，减少潜在的影响。例如：关键软件在需要时才组装或激活，缩短攻击方侦察和探测关键软件的时间窗口，因而无法定制目标恶意软件；

c） 先发制人。在适当的情况下（例如发现即将发生的攻击或中断威胁），可以采取先发制人的行动策略，避免网络安全事件的发生或产生影响，或者降低网络安全事件发生的可能性和潜在的损失。

6.4.11 遏制

采取措施增加网络安全事件造成不利影响或后果的难度，以遏制攻击活动的进展，或者延缓网络安全事件产生后果的时间。具体包括：

a） 重定向。将攻击活动重定向，使其远离防御方选定的目标。例如防御方选择性植入错误信息(虚假信息)或部署蜜网，误导攻击方将恶意软件部署在沙箱中；或使用混淆手段隐藏实际资源，使攻击偏离受保护的重要资源；

b） 动态隔离。采用内部防火墙或网络边界隔离组件进行动态隔离，将网络安全事件的影响限制在一组受限的资源，降低影响的水平；

c） 延迟。增加网络安全事件产生不利影响所需要的时间，导致攻击方可能无法在预定的时间内达到预期的效果，增加攻击方活动被发现的可能性，降低风险。例如：根据资产的重要性增加保护措施的数量和强度、身份验证发出的挑战信息频率是随机变化的。

6.4.12 重构

当系统组件发生损坏或失陷时，能够利用可用资源，快速实现系统重构，保持系统功能或性能水平。包括：

a） 冗余。从安全角度考虑系统单元的额外数量，保证组件发生损坏或失陷时，存在可利用的资源实现系统重构。冗余可以通过设置多重单元、系统或其他实现同一功能的装置来实现，例如：设备冗余、组件冗余、网络冗余、信道冗余；

b） 替换。由于发生网络安全事件而导致系统功能异常或部分组件损坏时，系统能够快速切换到未损坏的组件，替换已经损坏的组件，保证关键业务的连续运行；

c） 重排。在不同结构层面、不同位置或者为了实现可信性的不同方面，对系统的关键业务流程进

行重新编排或协调处理，避免引发级联故障或系统整体服务中断，保证关键业务的连续运行；

d) 重组。通过软件功能的多样性集成和动态调度，支持关键业务或重要服务不中断，提高网络弹性能力。

6.5 网络弹性架构

6.5.1 功能弹性

功能弹性包括：

a) 软件定义弹性。可基于软件定义的思想，将应用软件功能和业务连续性需求相分离，从功能需求中分离出非功能需求（如质量属性、安全性、可靠性、弹性等），根据需求的变化对软件功能进行重组，实现业务连续性目标；

b) 业务流程弹性。系统应具有根据业务需求变化调整其业务流程的能力，确保业务流程和应用程序紧密相连。包括：关键流程的冗余，调整资源配置、数据保护和可用性策略，调整业务流程的弹性等。

6.5.2 接口弹性

接口弹性包括：

a) 弹性网络接口。一个逻辑网络组件，以虚拟网卡为代表；

b) 弹性 API 接口。API 弹性伸缩提供了丰富的 API 接口，可用于创建伸缩组、增加实例或负载均衡；

c) 匿名系统接入的验证机制，可提供多种动态验证机制等。

6.5.3 事件驱动

系统能够根据当前时间节点的事务处理状况进行决策，调动可用资源执行相关任务，提高事务处理速度，防止事务堆积。例如：采用多线程、异步操作等技术。

6.5.4 物理位置

可基于位置的系统实际物理拓扑结构来评价物理位置的弹性，具体包括：

a) 节点地理分布、物理环境、位置约束；

b) 硬件、软件、网络环境的安全性和弹性；

c) 数据与网络物理或逻辑分离与冗余；

d) 对关键服务部署控制和传感器监控的比例；

e) 网络中物理设备被干扰或中断但没有导致崩溃或功能丧失的比例。

6.5.5 成本分析

在物理拓扑结构下分析节点的成本，帮助确定网络中关键设备或组件的备份或供应链策略。包括：

a) 网络安全事件的直接损失成本；

b) 与环境的依赖关系造成级联安全事件而产生的间接损失成本；

c) 数据备份与恢复、节点设备与组件替换所需要的成本。

6.5.6 供应链弹性

系统应具备抵御供应链威胁，并实现快速恢复的能力。具体包括：

a) 关键设备采购清单。采购网络关键设备和网络安全专用产品目录中的设备或产品时，应考虑关

键设备采购目录清单。采购、使用的网络产品和服务应符合相关国家标准的要求，可能影响国家安全的，应通过国家网络安全审查；

b） 多供应商服务。可以合同的形式与多家有保障的供应商签订服务协议，保证在供应链发生部分失效时，仍能持续供应且快速恢复到正常供应状态的能力；

c） 安全库存与备份。对于重要的硬件设备或软件、数据，应实行备份制度，保证安全库存与备份；

d） 关键软硬件产品、设备与服务提供商证书和资质的备案制度。

6.5.7 架构多样性

对于复杂连接的通信网络，可根据业务类型的不同特征，采用多种操作系统、通信协议或网络模态。

6.5.8 路由控制机制弹性

可根据系统实际需求，制定路由策略或选择路由，提高路由选择的灵活性和可控性。具体包括：

a） 分布式路由算法。可以采用分布式路由算法或软件定义路由等方法实现路由的弹性调度；

b） 路由协议多样性。可以采用多种路由协议，提高路由协议的安全性；

c） 浮动路由。可以配置两条静态路由，其中一条作为主路径。当主路径路由出现故障时，由另一条路径代替主路径，转发数据；

d） 网络负载均衡性。数据能够均匀分布到所有节点；

e） 隔离性。当网络中有新节点加入，系统能够自动重新分配数据，原有节点数据不变；

f） 适应性。路由算法可以自动调整。

6.5.9 网络路径弹性

可根据系统实际需求，采用多样性技术实现网络路径的弹性，提高传输效率。具体包括：

a） 路径多样性。提供多个独立的调度命令、控制协议和通信路径。例如建立备用电信服务(如地面电路、卫星通信)，使用备用通信协议或带外通道；

b） 路径综合可用性。采用网络容错技术，保证网络路径整体可用性；

c） 网络拓扑结构鲁棒性。删除少量网络节点后，网络拓扑结构的整体联通度仍能够实现预期业务连续性目标；

d） 节点失效率。对连接节点失败的次数进行评估，将节点成功连接次数作为节点可靠性的指标；

e） 链路失效率。对链路失败次数进行评估，保证关键传输路径是有效的，传输不会失败。

6.5.10 网络地址弹性

考虑用户账户关联的 IP 地址与服务器、虚拟 IP、负载均衡、NAT 网关等资源的灵活绑定或解绑。具体包括：

a） 随机 IP 地址生成技术；

b） IP 地址受控访问；

c） 虚拟 IP 地址；

d） 地址绑定与解绑的便利性。

6.5.11 网络节点弹性

新型复杂连接的网络环境下，网络节点具有多种技术特点，承担着如传感器、存储器、路由器、通信节点、甚至控制器（如边缘节点）的功能，因此节点架构的弹性特别是关键业务节点的弹性能力对于整体网络弹性能力至关重要。具体包括：

a） 采用彼此隔离的异构组件；

b） 自动识别并替换受损组件；
c） 感知并抵御已知威胁；
d） 感知并抵御未知威胁。

6.5.12 负载流量弹性

可通过流量控制策略，提高网络负载均衡和适应性。具体包括：
a） 吞吐量波动程度；
b） 带宽波动范围；
c） 传输速率波动程度；
d） 时延(波动程度)；
e） 丢包率(波动程度)。

7 综合评价

7.1 评价过程

本文件网络弹性能力评价过程模型如图3，具体评价过程如下：
a） 分析评价对象系统OSA，确定关键业务、重要资产与服务的优先级和恢复顺序，确定关键业务所依赖的重要网络资源的网络弹性能力和业务连续性需求，明确网络弹性目的；
b） 评价网络弹性功能的符合性，得到网络弹性功能CRF评价的中间结果；
c） 评价网络弹性架构的符合性，得到网络弹性架构CRA评价的中间结果；
d） 对评价结果进行汇总，得到总体网络弹性能力CRC评价结果，依据7.6.节中表1对网络弹性能力进行分级；
e） 依据7.6.2结果接受准则，对系统弹性能力评价结果进行处理，不断改进优化功能和结构以提高网络弹性能力。

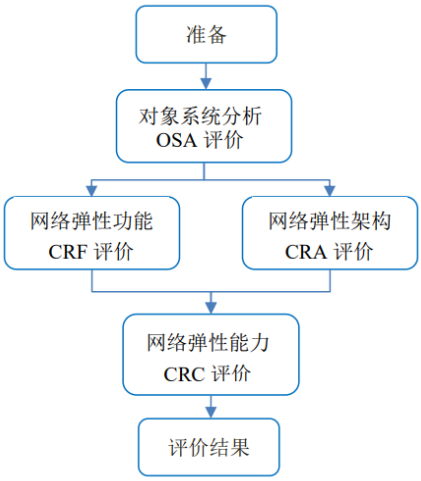

图3 网络弹性能力评价过程模型

7.2 网络弹性能力评价

7.2.1 评价指标

基于 6.2，网络弹性能力 CRC 评价包含预测能力、承受能力、恢复能力、适应能力 4 个一级指标。

7.2.2 评价方式

采用简单的统计法，通过对象系统分析 OSA 评价（7.2）、网络弹性功能 CRF 评价（7.3）和网络弹性架构 CRA 评价（7.4）三个中间评价结果汇总得到网络弹性能力 CRC 评价结果，并实现以下目标：

a) 判断网络弹性目的是否实现；
b) 判断网络弹性功能是否满足网络弹性能力需求；
c) 判断网络弹性架构是否满足网络弹性能力和业务连续性需求。

注：考虑当前网络弹性应用发展状况，此部分内容未分别计算每一项网络弹性能力要素一级指标的评价结果，而是基于 OSA、CRF 和 CRA 三个模块评价的中间结果对系统的整体网络弹性能力进行评价，避免了网络弹性能力要素与网络弹性功能要素和网络弹性架构要素之间复杂的多对多交叉映射关系而带来的不确定性和重复度量。

7.2.3 评价方法

评价方法包括：

a） 三级指标按照其对网络弹性能力的重要性分为基本要求和推荐要求；
b） 对基本要求性指标和推荐要求性指标的符合性分别进行汇总统计；
c） 基本要求指标的集合成为网络弹性能力CRC的基线要求；
d） 推荐要求指标的集合成为网络弹性能力CRC的增强要求；
e） 依据网络弹性能力等级划分原则(7.6.1)，对CRC评价结果进行等级划分。

7.3 对象系统分析评价

7.3.1 评价指标

基于6.3对象系统分析的基本内容，设计对象系统分析评价指标体系，包括5项二级指标，10项三级指标，见附录A。为保证准则的可操作性，三级指标被设计为可明确提供的文件。

7.3.2 评价方式

采用文件审查的方式，对每一项三级指标所述文件的完整性进行评价。

7.3.3 评价方法

评价方法包括：

a） 相关文件可由组织或第三方服务机构提供的对象系统分析结果报告或清单，包括中间结果；
b） 国家法律法规有要求的，需提供权威部门出具的测试或评估报告；
a） 根据相关标准规范要求以及系统实际运营经验，设置每一项三级指标的预期值和类型；
a） 确认评价对象系统的信息是否满足评价指标内容、形式的要求，根据每一项的符合度（完全不符合、部分符合、符合、不适用），评价每一项指标的符合性。

7.4 网络弹性功能评价

7.4.1 评价指标

基于网络弹性能力4个基本要素，设计网络弹性功能CRF的评价指标体系，包括12项二级指标，37项三级指标，见附录B。

7.4.2 评价方式

针对每一项网络弹性功能CRF的三级评价指标，提出相应的评价方式，见附录B。

7.4.3 评价方法

评价方法包括：

b) 根据相关标准规范要求以及系统实际运营经验，设定网络弹性功能三级指标的预期值；
c) 设置每一项三级指标的类型，其中，评价指标类型按照对网络弹性能力的重要性分为基本要求和推荐要求两种，基本要求指标的集合成为网络弹性功能的基线要求，推荐要求指标的集合则为网络弹性功能的增强要求；
d) 确认评价对象系统的信息是否满足评价指标内容、形式的要求，
e) 根据每一项的符合度（完全不符合、部分符合、符合、不适用），评价每一项指标的符合性。

7.5 网络弹性架构评价

7.5.1 评价指标

基于 6.5 网络弹性架构（CRA）的基本内容，设计网络弹性架构评价指标体系，包括 12 项二级指标，46 项三级指标，见附录 C。

7.5.2 评价方式

针对网络弹性架构（CRA）评价指标体系的每项三级指标，提出相应的评价方式，见附录 C。

7.5.3 评价方法

评价方法包括：

a) 根据相关标准规范要求以及系统实际运营经验，设定网络弹性架构三级评价指标的预期值；
b) 设置每一项三级指标的类型，对于每一项指标，按照其对网络弹性能力的重要性分为基本要求和推荐要求两种类型，基本要求指标的集合成为网络弹性架构的基线要求，推荐要求指标的集合则为网络弹性架构的增强要求；
c) 确认评价对象系统的信息是否满足评价指标内容、形式的要求，评价每一项指标的符合性。

7.6 评价结果

7.6.1 结果分级

根据网络弹性能力 CRC 评价结果，可进行网络弹性能力等级评价。网络弹性能力等级的划分原则及其物理意义见表 1。

表 1 网络弹性能力 CRC 等级划分及物理意义

评价结论	等级的意义
AAA 级	基本要求性指标的符合率达到 100%，推荐要求性指标的符合率大于 75%，包括 75%
AA 级	基本要求性指标的符合率达到 100%，推荐要求性指标的符合率在 50%~75%，包括 50%
A 级 （三级）	基本要求性指标的符合率达到 100%，推荐要求性指标的符合率在 0%~50%
B 级 （相对全面级）	基本要求性指标的符合率达到 75%以上（包括 75%）
C 级 （基本级）	基本要求性指标的符合率达到 60%以上（包括 60%）

7.6.2 结果接受

组织应根据本文件所述方法的评价结果，制定与自身业务连续性需求相适配的网络弹性能力接受准则，以帮助组织更好地运用本文件，提高系统网络弹性能力。

附 录 A
（资料性）
对象系统分析评价指标与评价方法

对象系统分析OSA评价指标与评价方法如表A-1所示。

附表A-1 对象系统分析OSA评价表

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
1	识别关键业务	识别关键业务和相关业务清单	文件审查	是/否	基本要求	
		关键业务优先级排序清单	文件审查	是/否	基本要求	
2	识别重要资产和服务	支撑关键业务的资产/服务清单	文件审查	是/否	基本要求	
3	风险分析	风险分析报告	文件审查	是/否	基本要求	
4	约束与限制条件	组织风险管理策略	文件审查	是/否	基本要求	
		识别限制要素	文件审查	是/否	基本要求	
		内外部依赖关系	文件审查	是/否	基本要求	
5	明确网络弹性目的	关键业务和重要资产/服务优先级排序表	文件审查	是/否	基本要求	
		关键资产/服务与网络弹性能力需求	文件审查	是/否	基本要求	
		关键业务的业务连续性需求	文件审查	是/否	基本要求	

附 录 B
（资料性）
网络弹性功能评价指标与评价方法

网络弹性功能CRF评价指标与评价方法如表B-1所示。

附表B-1 网络弹性功能CRF评价表

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
1	检测/监测	准确率	对威胁或中断测试正确的次数占测试总次数的比例	≥90%	基本要求	
		召回率	对威胁或中断正样本测试成功的次数占正样本总数的比例	≥90%	基本要求	
		态势感知	是否建立本单位网络安全全景图并保持为最新	是/否	基本要求	
2	检查分析	特定威胁事件分析	提供包括具体网络安全事件的漏洞利用、触发条件和脆弱点模式的威胁分析报告，例如紧急发布漏洞的威胁分析报告	是/否	基本要求	
3	协同检测	情报共享	是否对接国家威胁情报共享平台	是/否	基本要求	
		建设内部威胁情报库	是否建设内部威胁情报库	是/否	推荐要求	
		自然灾害预警	是否建设自然灾难历史数据库或对接国家自然灾难预警系统	是/否	推荐要求	
4	应急响应	应急预案与执行度	是否制定了完备的应急预案，并定期开展应急预案演练，能提供系统演练记录	是/否	基本要求	
		监测预警	是否具备技术手段能及时发现应急事件并有效预警	是/否	基本要求	
		应急处置	是否具备必要的应急调度手段支撑开展故障排查、诊断、处理和恢复	是/否	基本要求	
5	损失限制	减小攻击面(收敛暴露面)	a）是否具备暴露面资产清单，包括信息资产、关键业务数据、内部信息、技术文档等 b）是否具备识别和减少互联网资产、内网资产、关键业务数据、内部信息、技术文档等暴露面的机制	是/否	基本要求	
		分离关键业务和非关键业务	是否具有有效隔离关键业务资产与非关键业务资产的机制	是/否	基本要求	
		缩短时间窗	a）应急事件被识别至故障排除时间是否能够被接受 b）是否具备缩短网络安全事件持续时间并使业务保持正常运行，或能够快速从异常状态恢复到正常状态的能力 c)是否具备相应的故障切换预案等	是/否	基本要求	
		分段与隔离	a）是否根据关键业务的不同属性对网络进行分段或分区管理 b）是否具备发现受损坏资产（例如被病毒感染，被植入木马等）并将其从网络中迅速隔离的机制	是/否	基本要求	
6	生存性	安全失效模式	a）是否采用适当方法和技术保证系统在网络安全事件发生时，以可控的方式失效；是否有能力控制和减少对系统自身及其用户造成的伤害 b）是否对已检测和未检测到的安全失效进行了有效分析，识别了导致系统失去安全功能的执行能力的潜在风险	是/否	关基基本要求，其他推荐要求	
		防故障模式	a） 是否具备常见故障类型清单及防故障处置方案 b） 在故障发生时，系统是否能够自动进行故障处置，实现防故障模式的预期目标	是/否	关基基本要求，其他推荐要求	

附表B-1 网络弹性功能评价表（续）

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
6	生存性	降级模式	a）是否清晰识别系统使命任务或核心服务,确定哪些任务或核心服务在降级模式下必须得到保证,例如：参考日志级别设置预案的能力 b）是否具备系统切换并以更低级别模式运行系统的能力	是/否	关基基本要求，其他推荐要求	
		吸收模式（鲁棒性、容错）	a）当系统内部运行出现偶然故障，是否仍然能够输出正确的结果。可依据系统运行记录或系统设计文档判断 b）当系统偶然输入了错误信息，是否具备反馈控制机制输出正确结果的能力。可依据系统运行记录或设计文档判断。	是/否	推荐要求	
7	备份	备份策略	a)对重要数据资产是否具备确定的备份策略（包括备份内容、备份时间和备份方式）并正确执行 b)备份结果是否与备份预期目标一致	是/否	基本要求	
		受保护的备份	a)是否使用适当访问控制策略或符合国家密码管理部门要求的密码技术保护备份数据的保密性、完整性和可用性 b)是否基于系统或业务数据的重要性，提供异地备份功能，利用通信网络将重要业务数据实时备份至备份场地	是/否	基本要求	
8	业务连续性	高可用性	按国家、行业、企业等多维度规定，基于业务重要程度，提供高可用性验证文档（测试文档等），验证系统的可用性、设备组件的可用性指标是否满足规范或用户要求	是/否	基本要求	
		连续操作	是否具有手动操作、组件替换或切换等方式,保持关键业务或重要服务不中断的能力	是/否	基本要求	
		回滚	对关键业务，是否具备回滚机制及回滚测试记录	是/否	基本要求	
		重续运行	网络安全事件发生时，运行系统从主中心转移到灾难备份中心，再回到主中心运行的过程，是否达到了预期	是/否	基本要求	
9	恢复	恢复数据源	a）通过完整性检查、行为确认等判断数据源是否完整 b）备份结果是否与备份策略预期保持一致	是/否	基本要求	
		恢复策略	a）是否具备系统遭受攻击后的节点备份恢复策略或节点接替恢复策略等恢复策略 b）恢复测试记录是否能够进行正常的数据恢复	是/否	基本要求	
		恢复目标 RPO、RTO	a） 从业务需求角度评估 RPO、RTO 是否在可接受范围 b）系统测试中，是否达到了 RPO\RTO 的要求	是/否	基本要求	
10	主动防御	清除受损数据	是否采取了必要的技术手段定时检查和消除威胁,包括但不限于定时任务、静态数据、暂态数据	是/否	推荐要求	
		按需激活	关键软件是否在使用时才组装或激活,创造条件防止攻击事件的发生	是/否	推荐要求	
		先发制人	发现攻击或中断威胁时，是否能够采取主动策略，主动出击，防止网络安全事件的发生	是/否	推荐要求	
11	遏制	重定向	是否具备重定向机制及重定向记录，并验证重定向有效	是/否	推荐要求	
		动态隔离	是否具备动态隔离策略设置机制及隔离记录	是/否	基本要求	
		延迟	按照资产重要度，能够提供不同防御措施，增加攻击复杂度，增加攻击成功的时间	是/否	推荐要求	
12	重构	冗余	a）对于关键资源，是否具备冗余策略设置机制及冗余记录，并验证单元或系统冗余功能的能力 b）是否存在适用的设备备用站点	是/否	基本要求	
		替代	是否具备组件替换记录	是/否	基本要求	
		重排	是否具备不同层次或不同位置的业务重排记录	是/否	推荐要求	
		重组	是否具备软件多样性集成和调度策略	是/否	推荐要求	

附 录 C
（资料性）
网络弹性架构评价指标与评价方法

网络弹性架构评价指标与评价方法如表C-1所示。

附表C-1 网络弹性架构CRA评价表

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
1	功能弹性	功能与需求解耦	是否能够将应用软件的功能和需求相分离，从功能需求中分离出非功能需求	是/否	推荐要求	
		功能重组	是否能够根据业务功能需求变化对软件功能进行重组	是/否	推荐要求	
		业务流程冗余	关键业务流程是否存在冗余	是/否	推荐要求	
2	接口弹性	弹性网络接口	当网卡出现故障时，是否有其他网卡接口可以接替其工作	是/否	推荐要求	
		弹性 API 接口	是否存在 API 弹性伸缩、易扩展资源组或增加负载均衡实例	是/否	推荐要求	
		匿名系统接入动态验证机制	对匿名接入系统，至少提供 2 种不同类型的认证机制，如基于密码、生物特征以及令牌、短信等认证机制	是/否	基本要求	
3	事件驱动	基于事件的决策	是否提供基于事件优先级的处理方式	是/否	推荐要求	
		资源的调度	a）是否能够针对关键业务的优先级采用不同的调度策略或调度算法，提高服务质量 b）是否能够根据事件的处理数量、处理优先级、计算与存储资源需求和 I/O 消耗量动态调度对应的资源	是/否	推荐要求	
		事件处理效率	是否能够使用硬件、软件测量工具或模拟模型，触发事件并收集数据，通过工作负载、响应特性等数据计算分析事件处理效率	是/否	推荐要求	
4	物理位置	节点地理分布、物理环境、位置约束	a)是否具备全面的物理安全设计 b)系统选址、物理环境和位置约束是否符合相关标准（如等保 2.0）	是/否	基本要求	
		硬件、软件环境、网络环境的安全与弹性	a）硬件：不应存在单点故障，至少有一个冗余备份可以接替故障设备继续工作 b)软件：无论是组件、节点、进程还是模块，均应该有接替其工作的对应设施 c)网络：对于关键网络，至少实现双网双平面的组网方式，保证在任何网络节点出现故障时可以由另一网络平面来承接其工作	是/否	基本要求	
		数据与网络物理或逻辑分离与冗余	a）存储单元与控制单元需要隔离在不同的网络平面 b）是否具备数据的安全与弹性设计，如数据备份和恢复，加密和去标识化处理等	是/否	基本要求	
		对关键服务部署控制和传感器监控的比例	监控服务数量：总服务数量 监控传感器节点数量：部署总节点数量	≥90% ≥0.1%	推荐要求	
		网络中物理设备被干扰或中断但没有导致崩溃或功能丧失的比例	被干扰/中断设备数：部署总设备数	≥10%	推荐要求	

附表C-1 网络弹性架构CRA评价表（续1）

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
5	成本分析	网络安全事件的直接损失	网络安全事件导致的物理资产、数字资产与业务中断损失评估	损失可接受或可恢复	基本要求	
		级联效应导致的间接损失	a）第一方人身伤害、以及第三方物理、软件、数据等信息资产损失和人身伤害损失评估 b）对组织品牌、声誉等无形资产造成的损失，以及其它无形资产损失	损失可接受或可恢复	基本要求	
		节点设备、组件替换成本	节点设备、组件替换的硬件成本+软件成本+替换操作(包括硬件、软件安装及数据重新加载配置)人工成本	<网络安全事件的直接损失	基本要求	
6	供应链弹性	关键设备采购清单	a）采购网络关键设备和网络安全专用产品目录中的设备或产品时，应考虑关键设备采购目录清单 b）弹性系统应具备网络关键设备组件清单，并考虑全生命周期的安全管理和技术实现	是/否	基本要求	
		多供应商服务	对于关键设备或服务，至少有两个不同源的供应商提供产品或服务，并可以在这两个供应商服务间做切换	是/否	基本要求	
		安全库存与备份	a）是否有足够的库存和备用设备来面对突发的重大安全事件，例如备件数至少准备可以平稳度过两个最大可容忍中断期 MTPD 的数量 b)库存和备用设备应保存在设计安全距离内	a)≥2MTPD b）是/否	基本要求	
		关键软硬件产品、设备服务提供商的证书和资质备案	a）关键软硬件产品、设备服务提供商具备符合国家相关法律法规和标准要求的资质证书并进行备案 b）有长时间不录用机制	是/否	基本要求	
7	架构多样性	架构多样性	是否部署 2 种或 2 种以上操作系统、通信协议或网络模态	是/否	推荐要求	
8	路由控制机制弹性	路由调度算法	是否采用分布式路由算法、软件定义路由算法等，实现弹性路由调度，以降低网络拥塞	是/否	推荐要求	
		路由协议多样性	至少采用 3 种以上路由协议（如 RIP/OSPF/ISIS/BGP）	是/否	基本要求	
		浮动路由	网络中关键路由器（如网络的出入口路由器）是否配置浮动路由	是/否	基本要求	
		均衡性	是否支持配置负载均衡策略，具备基于内容分布或节点状态等均衡方法	是/否	基本要求	
		隔离性	不同虚拟网络之间的路由表是否具备相互隔离能力	是/否	基本要求	
		适应性	a）路由控制机制是否能够根据网络拓扑和业务负载的变化情况，动态调整路由决策，具备路由适应能力 b）支持节点失效后路由重构策略，具备在网络调整后路由条目数基本不变、新路由与原路由尽可能重合	是/否	推荐要求	
9	网络路径弹性	路径多样性	a）同一源/目的对节点的多条路径中，每两条路径中链路重合的比例 b）具备多个运营商提供的广域网通信链路，或为业务通信提供多条冗余的路径 c）关键设备/系统至少具备一个带外通道，并提供多个独立的命令、控制和通信路径可供选择	是/否	关基基本要求，其他推荐	
		路径综合可用性	应用了冗余或者容错技术后，端到端路径整体可用性	≥99.999%	基本要求	

附表 C-1 网络弹性架构 CRA 评价表（续 2）

序号	二级指标	三级指标	评价方式	预期值	指标类型	符合性
9	网络路径弹性	网络拓扑结构鲁棒性	删除少量（低于 10%）网络节点后，网络整体连通度的下降程度	≤50%	推荐要求	
		节点失效率	单位时间内失效的节点数占总节点数的比例，也称平均失效率	≤20%	推荐要求	
		链路失效率	单位时间内失效的链路数占总链路数的比例	≤20%	推荐要求	
10	网络地址弹性	随机 IP 地址生成技术	a）网络环境具备弹性 IP 地址分配池及管理算法 b）检查地址是否通过随机方式生成，包括但不限于 DHCP 分配、代理分配、虚拟专网分配等	是/否	推荐要求	
		IP 地址受控访问	关键服务节点是否采用地址隐藏、跳变等受控访问机制	是/否	基本要求	
		虚拟 IP 地址	a）是否采用虚拟 IP 地址（VIP）支持多个网卡与服务器的绑定，实现服务器的高可用性 b）关键路由节点是否采用虚拟浮动地址	是/否	基本要求	
		地址绑定与解绑的便利性	基于简单配置绑定 IP 到服务器，并易于设置解绑操作	是/否	基本要求	
11	网络节点弹性	采用彼此隔离的异构组件	基于具体业务场景，网络节点可采用彼此隔离的异构组件。可结合节点设备或系统架构设计说明书、安全测试报告进行评估	是/否	推荐要求	
		自动识别并替换受损组件	网络节点是否能够自动识别并替换受损组件。可结合节点设备或系统架构设计说明书、安全测试报告进行评估	是/否	基本要求	
		感知并抵御已知威胁	针对特征已知的网络攻击的感知及抵御成功率。可结合节点设备或系统安全测试报告进行评估	≥95%	基本要求	
		感知并抵御未知威胁	针对特征未知的网络攻击（如 0-day 漏洞）的感知及抵御成功率。可结合节点设备或系统安全测试报告进行评估	≥90%	推荐要求	
12	负载流量弹性	吞吐量波动程度	设备吞吐量超过标称值 10%时，设备可以发生服务降级，但不能出现宕机	是/否	基本要求	
		带宽波动范围	a)协商的物理连接最大传输速率，受交换机接口处理器、接口卡和数据总线吞吐量限制 b)根据 SLA 协议文件评估，满足业务高峰期服务需求	是/否	推荐要求	
		传输速率波动程度	设备传输速率超过标称值 10%时，设备可以发生服务降级，但不能出现宕机	是/否	推荐要求	
		时延波动程度	在网络轻、重负载时，关键业务时延的上升幅度	≤100%	基本要求	
		丢包率波动程度	a）在网络重负载时，网络通信丢包率应控制在≤5% b）设备正常负载的丢包率应≤10^-6（可根据文件记录或者设计文档进行评估）	是/否	基本要求	

附 录 D
（资料性）
网络弹性功能与网络弹性能力要素的映射关系

网络弹性功能CRF与网络弹性能力要素的映射关系如表D-1所示。

附表 D-1 网络弹性功能 CRF 与网络弹性能力要素的映射关系

序号	网络弹性能力要素 网络弹性功能	预测能力	承受能力	恢复能力	适应能力
1	检测/监测	×			
2	检查分析	×			
3	协同检测	×			
4	应急响应		×		
5	损失限制		×		
6	生存性		×		
7	备份			×	
8	业务连续性			×	
9	恢复			×	
10	主动防御				×
11	遏制				×
12	重构				×

附 录 E
（资料性）
网络弹性架构与网络弹性能力要素的映射关系

网络弹性架构CRA与网络弹性能力要素的映射关系如表E-1所示。

附表 E-1 网络弹性架构 CRA 与网络弹性能力要素的映射关系

序号	网络弹性能力要素 网络弹性架构	所处架构的层次	预测能力	承受能力	恢复能力	适应能力
1	功能弹性	逻辑架构		×		×
2	接口弹性	逻辑架构		×		×
3	事件驱动	逻辑架构			×	×
4	物理位置	物理架构	×	×	×	×
5	成本分析	物理架构		×	×	
6	供应链弹性	物理架构		×	×	×
7	架构多样性	通信网络架构		×	×	×
8	路由控制机制弹性	通信网络架构		×	×	×
9	网络路径弹性	通信网络架构			×	×
10	网络地址弹性	通信网络架构			×	×
11	网络节点弹性	通信网络架构	×	×		×
12	负载流量弹性	通信网络架构		×	×	×

参 考 文 献

［1］面向行业的5G网络SLA定义及需求规范。中国互联网产业联盟标准规范。

［2］T/SIA 031.1-2021，系统安全工程网络弹性构建指南第一部分概述.

［3］T/SIA 031.2-2021，系统安全工程网络弹性构建指南第二部分网络弹性工程框架

［4］T/SIA 031.3-2021，系统安全工程网络弹性构建指南第三部分网络弹性构建过程

［5］T/SIA 031.4-2022，系统安全工程网络弹性构建指南第四部分网络弹性技术

［6］T/SIA 031.5-2022，系统安全工程网络弹性构建指南第五部分网络弹性设计原则

［7］CISA. Infrastructure Resilience Planning Framework (IRPF).2021.10,Vol.1.

［8］NIST SP 800-160 Vol.1. Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

［9］NIST SP800-160 Vol.2. Developing Cyber Resilient Systems: A Systems Security Engineering Approach.

［10］NIST’s draft cyber resiliency framework rests on system engineering. Inside Cybersecurity, 2021.8.10.

［11］Sara Friedman. MITRE report proposes use of 'chaos engineering' to boost cyber resiliency in government. Inside Cybersecurity, 2021.8.24.

［12］eRikHollnagel, Jean PaRiès, DaviDWooDs, John Wreathall. Resilience Engineering in Practice. A Guide Book.CRC Press，2017.

［13］Helm, Patrick. Risk and Resilience: Strategies for security. Civil engineering and environmental systems, 2015.04.03, Vol.32 (1-2), p.100-118.

［14］Höller, T. Rauter, J. Iber and C. Kreiner. Towards Dynamic Software Diversity for Resilient Redundant Embedded Systems (Lecture Notes in Computer Science 9274), in Proceedings of Software Engineering for Resilient Systems: 7th International Workshop, SERENE 2015, Switzerland, Springer, p. 16-30.

［15］Igor Linkov, Daniel A. Eisenberg ,Kenton Plourde,Thomas P. Seager, Julia Allen, Alex Kott. Resilience metrics for cyber systems. Environ SystDecis (2013) 33:471–476

［16］Jean Christophe Le Coze. Towards a constructivist program in safety,Safety Science,2012,Vol 50, Issue 9, p.1873-1887,ISSN 0925-7535,https://doi.org/10.1016/j.ssci.2012.03.019.

［17］K. E. Heckman, F. J. Stech, R. K. Thomas, B. Schmoder and A. W. Tsow. Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense (Advances in Information Security 63), Switzerland: Springer, 2015.

［18］Manikam Pillay. Resilience Engineering: An Integrative Review of Fundamental Concepts and Directions for Future Research in Safety Management. Open Journal of Safety Science and Technology, 2017, 7, p.129-160.

［19］M. Vaez-Alaei, A. Baboli and R. Tavakkoli-Moghaddam. A New Approach to Integrate Resilience Engineering and Business Process Reengineering Design. 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2018, p. 778-782, doi: 10.1109/IEEM.2018.8607662.

［20］Nii O. Attoh-Okine. Resilience Engineering. ModelsandFramework. Cambridge University Press. 2016.

［21］Royce Francis, BehailuBekera. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering and System Safety. 2014,121, p.90-123.

［22］ Sansavini, Giovanni. EngineeringResiliencein Critical Infrastructures. Resilienceand Risk, 2017. 8.3, p.189-203.

［23］ S. Jackson. A Multidisciplinary Framework for Resilience to Disasters and Disruptions. Journal of Integrated Design and Process Science, 2007,Vol. 11, No. 2, p.91-108.

［24］ Sobol, Amir; Pass, Yaron. OT AUTOMATION: CYBERSECURITY: Six ways to improve cybersecurity: Barriers vs. resiliency: Overcome three OT/IT cybersecurity barriers and move towards cyber-resiliency in three cybersecurity steps. Control engineering, 2020.11.01, Vol.67, No.11, p.35.

［25］ Thoma, Klaus ;Scharte, Benjamin ; Hiller, Daniel ; Leismann, Tobias. Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches. European journal for security research, 2016.3.15, Vol.1 No.1, p.3-19.

［26］ Thompson, Marcus A ; Ryan, Michael J. A Useful Framework for Security, Resilience and Governance.Insight (International Council on Systems Engineering), 2016.07, Vol.19 No.2, p.29-31.

［27］ Toonen, Theo ;Paté - Cornell, Elisabeth ; Vest, Charles M ; Rouse, William B. Engineering for Resilience. Perspectives on Complex Global Challenges: Education, Energy, Healthcare, Security and Resilience, 2016.7.25, p.183-194.

［28］ UdaraRanasinghe, Marcus Jefferies, Peter Davis, Manikam Pillay. Resilience Engineering Indicators and Safety Management: A Systematic Review,Safety and Health at Work,2020,Vol. 11, Issue 2, p. 127-135,ISSN 2093-7911,https://doi.org/10.1016/j.shaw.2020.03.009.

［29］ 李稳国. 电力网络拓扑优化与弹性提升方法研究. 吉林大学出版社, 2021年.

［30］ 崔琼,李建华,冉溟丹,南明莉. 基于任务能力的指挥系统超网络弹性度量. 指挥与控制学报，2017.6，Vol.3 No.2,p.137-143.

［31］ 高先明,王宝生,邓文平.SDRS：集中与分布控制相结合的弹性多路径路由机制. 计算机学报，Vol.41 No.9, 2018.9, p1976-1989.