ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44862—2024

网络安全技术　网络弹性评价准则

Cybersecurity technology—Cyber-resilience evaluation criteria

2024-10-26 发布　　2025-05-01 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。

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。

本文件由全国网络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(工业和信息化部软件与集成电路促进中心)、国家工业信息安全发展研究中心、公安部第三研究所、中国科学技术大学、紫金山实验室、中国电子技术标准化研究院、联想(北京)有限公司、北京天融信网络安全技术有限公司、中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国检验认证(集团)有限公司、国家信息技术安全研究中心、中国电信集团有限公司、中车大连机车车辆有限公司、天翼云科技有限公司、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、公安部第一研究所、华能信息技术有限公司、武汉金银湖实验室、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、中国烟草总公司湖北省公司、战略支援部队信息工程大学、东南大学、北京理工大学、深信服科技股份有限公司、陕西省信息化工程研究院、长扬科技(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、网安联信息技术有限公司、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、黎水林、朱雪峰、张进、陈兴跃、上官晓丽、王惠莅、王冲华、李汝鑫、王少杰、于盟、卢春景、崔涛、喻梁文、王宝雁、刘亚天、呼博文、沈军、广小明、王大伟、朱良海、辛晨、刘文彪、黄石海、赵赫、汤成俊、赵硕、余果、汪慕峰、梁利、安宏杰、曹鲲鹏、潘中英、孙伟宏、杨斯可、宋景民、马海龙、曹向辉、郭泽华、赵晓荣、金伟、王语涵、谢琴、张亚京、王颉、张建辉、李天涯、李昂、伊玮珑、江文、阮懿宗、周柏魁。

网络安全技术　网络弹性评价准则

1　范围

本文件规定了网络弹性评价准则，给出了网络弹性评价指标体系和评价方法。

本文件适用于组织对网络弹性的自评价，网络安全服务机构对网络弹性的第三方评价，也适用于组织的网络弹性设计、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　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 30146—2023　安全与韧性　业务连续性管理体系　要求

GB/T 43269—2023　信息安全技术　网络安全应急能力评估准则

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

网络存在不利条件、压力、攻击或失陷组件时，自身所应具有的预防、承受、恢复和适应的能力，以保持系统功能和结构稳定，实现对重大网络安全事件的有序、有效应对，保证关键业务稳定运行。

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可能严重影响组织或客户网络安全和稳定，造成重大损失的业务。

3.3

生存性　survivability

在攻击、失效、故障或中断发生的情况下，系统仍能运行基本业务功能，完成关键业务的能力。

注：失效是指一个系统或组件失去其设计所规定的目的或功能，尽管可以运行，但不能输出正确的结果。故障是指系统或设备不能执行规定功能的状态。基本业务功能是指组成业务功能的基本功能单元，如进程、线程或算法模块等。

[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）
ARP：地址解析协议（Address resolution protocol）
BGP：边界网关协议（Border gateway protocol）
DDOS：分布式拒绝服务（Distributed denial of service）
DHCP：动态主机配置协议（Dynamic host configuration protocol）
I/O：输入/输出（Input/output）
IP：网际互联协议（Internet protocol）
ISIS：中间系统到中间系统（Intermediate system-to-intermediate system）
MAC：媒体访问控制（Media access control）
MBCO：最低业务持续目标（Minimum business continuity objective）
MTPD：最大可容忍中断期（Maximum tolerable period of disruption）
OSPF：开放式最短路径优先（Open shortest path first）
RIP：路由通信协议（Routing information protocol）
RPO：恢复点目标（Recovery point objective）
RTO：恢复时间目标（Recovery time objective）
SLA：服务水平协议（Service-level agreement）
UPS：不间断电源（Uninterruptible power supply）
VIP：虚拟 IP（Virtual internet protocol）

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收缩、性能降低或服务降级的模式运行，保证系统基本业务功能的生存性，保证关键业务的连续性。

网络弹性包括“预防、承受、恢复和适应”能力，其含义如下：

a) 预防能力，保持一种对网络安全事件充分预测和协同防御的能力；
b) 承受能力，系统能够应对网络安全事件带来的影响，保证关键业务功能生存的能力；
c) 恢复能力，在网络安全事件发生后，系统能够依据优先级排序，在预期时间内有序地恢复业务功能的能力；
d) 适应能力，系统自我修复和完善，加固和优化其功能和结构，以适应内、外部环境变化并不断提升抵抗风险的能力。

网络弹性的目的是通过“预防、承受、恢复、适应”能力的实现，有效化解重大网络安全风险，避免风险级联效应导致重大或极端网络安全事件，保证关键业务稳定运行。

5.2 评价指标体系

网络弹性的评价对象为一个组织或部门的网络（3.1 注）或系统，及其运营、管理等相关内容。

网络弹性包括“预防、承受、恢复、适应”4 种能力，将其作为网络弹性评价的一级指标。其中，预防能力包括了态势感知、检查分析、协同防御、供应链管理 4 项二级指标，承受能力包括应急响应、损失限制、遏制、生存性 4 项二级指标，恢复能力包括灾难备份、业务连续性、数据与业务恢复 3 项二级指标，适应能力包括自主管理、重构、节点适应性、网络适应性 4 项二级指标。每个二级指标又包括多项三级指标。二级指标共 15 项，三级指标共 63 项。评价指标体系见图 1。

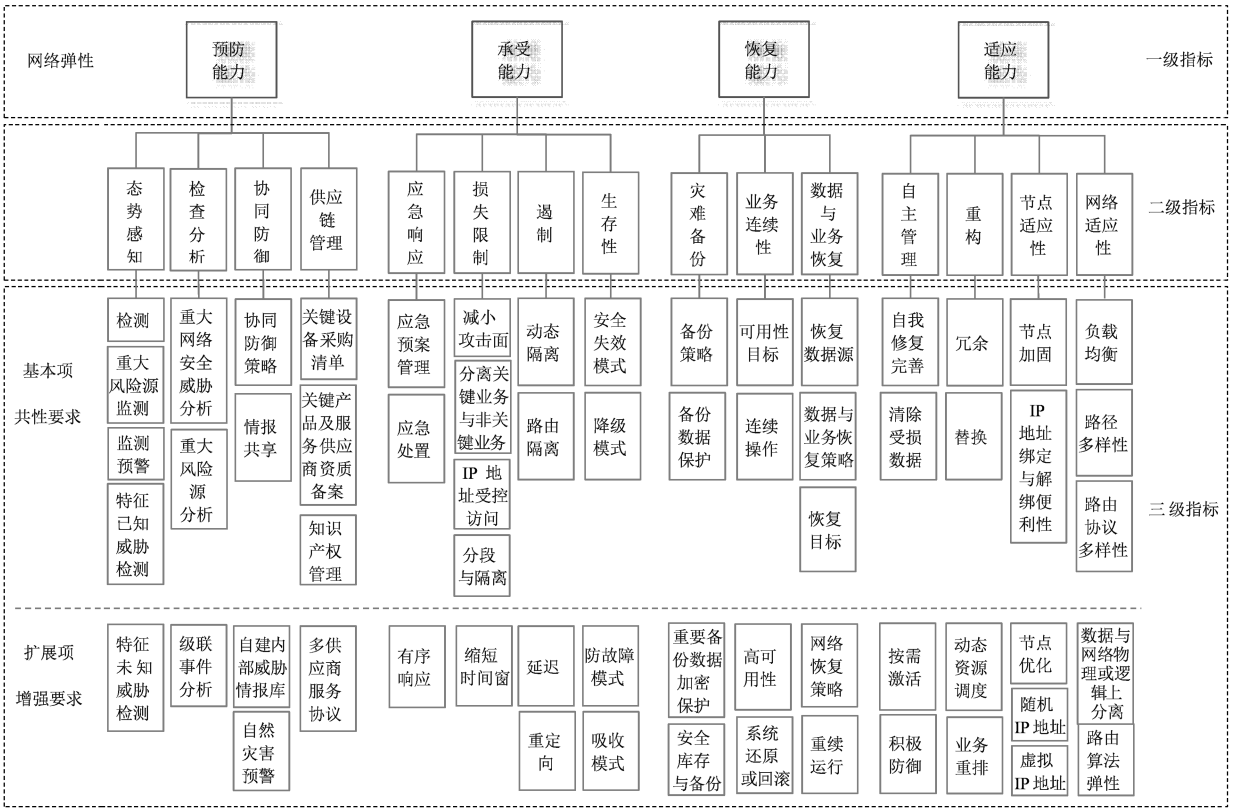

图 1　网络弹性指标体系

5.3　标准结构

第 6 章给出了网络弹性指标体系和每项指标的具体内容，第 7 章给出了网络弹性的评价方法和打分方法。附录 A 规定了网络弹性各项指标的评价方法；附录 B 描述了极限场景、极端网络安全事件及相关网络弹性指标示例，提出了网络弹性需要解决的重点问题；附录 C 给出了多业务协同的复杂连接系统的网络弹性需求分析方法；附录 D 给出了一种网络弹性架构设计方法，支持“态势感知、检查分析、协同防御”等指标的实现。

6　网络弹性指标

6.1　预防能力

6.1.1　态势感知

态势感知是指通过采集网络流量、资产信息、日志、漏洞、告警信息、威胁信息等数据，分析和处理网络及用户行为等因素，掌握网络安全状态，预测网络安全发展趋势，并进行展示和检测预警的活动。

该指标包括以下内容。

a）　基本项。

1）　检测。系统能够基于指示器信息和预测活动，对网络安全状态数据进行动态、整体的分析，检测网络安全状态。

2）　重大风险源监测。在关键业务所依赖的重要资产、服务和主要设备设施上部署传感器，对重大网络安全事件风险源进行监测。

3）　监测预警。根据日常监测结果，及时发现网络安全事件并有效预警，对事件进行核实和评估，并持续跟踪。

4） 特征已知威胁的检测。针对特征已知威胁的检测成功率应达到100%。

b） 扩展项。

特征未知威胁的检测。针对特征未知的威胁应具有检测、发现的能力。

6.1.2 检查分析

检查分析是指对重大网络安全事件进行研判，分析漏洞利用、触发条件和网络攻击模式，分析系统重要功能失效、主要设备设施故障等隐患，实现对重大网络安全事件的早期发现。

该指标包括以下内容。

a） 基本项。

1） 重大网络安全威胁分析。对重大网络安全威胁（如某类APT攻击）进行研判，分析其漏洞利用、触发条件、脆弱点模式及可能产生的后果，及时发现并采取措施防止重大网络安全事件的发生。

2） 重大风险源分析。针对可能导致重大网络安全事件的风险因素进行研判，综合分析关键业务所依赖的重要资产和服务或主要设备的网络安全状态，分析其功能失效模式、故障模式以及可能造成的影响，及时发现重大网络安全风险隐患。

注1：失效模式是指从致使系统或组件失效的因素、失效机理、失效发展过程到临界状态等整个失效过程。故障模式是指系统、重要设备或关键部位可能产生的潜在故障、后果及原因。

b） 扩展项。

级联事件分析。对可能存在级联效应的网络安全事件，应在物理拓扑结构下计算网络安全事件潜在损失（D.3.2），采取措施避免极端事件的发生并减少损失。

注2：级联事件是指一系列事件，其中每一个事件都为下一个事件的发生提供条件。在网络安全领域，级联事件指一个事件影响下游数据处理程序或相关业务系统而引发一系列的意外事件。

6.1.3 协同防御

协同防御是指支持利益相关方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，降低网络安全事件传播范围和破坏能力。

该指标包括以下内容。

a） 基本项。

1） 协同防御策略。明确协同防御相关方及策略，提高对网络攻击的整体感知和抵御成功率。

2） 威胁信息共享。支持利益相关方群体共同、联合或协同的风险应对方案，降低网络安全事件由一个组织系统传播到另一个组织系统的可能性，包括：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） 扩展项。

1） 自建威胁情报库。建立适合自身规模的威胁情报库，并及时向利益相关方分享和披露威胁信息，以增强利益相关方对网络安全事件特征和行为的了解。

2） 自然灾难预警。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。

6.1.4 供应链管理

供应链管理是指识别和防范供应关系和供应活动中面临的安全风险，当供应链中断或部分失效时，能够保证业务系统持续稳定运行。

该指标包括以下内容。

a） 基本项。

1） 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产品时，应采购通过国家检测认证的设备和产品。可能影响国家安全的，要通过国家网络安全审查。

2） 关键产品及服务供应商资质备案。对于关键软硬件产品、设备与服务供应商，应建立证书

和资质备案制度。

3） 知识产权管理。提供满足业务持续稳定运行时限需求的软件产品或服务使用授权，包括但不限于许可证、产品序列号、开源许可协议等，并确保授权期内软件持续稳定可用。

b） 扩展项。

多供应商服务协议。强化采购渠道安全管理，制定从多个国家或地区获得关键产品及服务的方案，保证来源的多样性；对于重要组织或场景，建立供应商替代方案，防范供应链中断风险。

6.2 承受能力

6.2.1 应急响应

应急响应是指组织为应对突发/重大网络安全事件所做的准备，以及在事件发生后所采取的措施。

该指标包括以下内容。

a） 基本项。

1） 应急预案管理。基于关键业务、资产和服务的优先级，制定应急响应预案应符合GB/T 43269—2023的相关要求，并定期组织应急演练，保证网络安全事件发生时应急响应预案的有效执行。

2） 应急处置。采取必要应急调度手段，开展故障排查与诊断，对故障进行快速处理和恢复，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。

b） 扩展项。

有序响应。根据业务、资产与服务的优先级排序，对网络安全事件进行有序响应，并在预期时间目标和恢复点目标[6.3.3a)3)]内实现系统的恢复。

6.2.2 损失限制

损失限制是指限制网络安全事件在时间、网络资源或业务方面造成的损失或影响，降低网络安全级联事件发生的可能性和影响范围。

该指标包括以下内容。

a） 基本项。

1） 减小攻击面/收敛暴露面。减少系统输入/输出节点的数量，降低系统遭受攻击的可能性和影响的范围。

2） 分离关键业务和非关键业务。减少关键业务和非关键业务之间的连接，降低非关键业务风险影响关键业务的可能性，最小化非关键业务功能被利用来攻击关键业务的可能性。

3） IP地址受控访问。通过防火墙设定可访问的地址段或IP范围，或通过IP安全控制策略限制访问。

4） 分段与隔离。根据组织业务或业务的不同属性，对网络进行分段或隔离，实现对不同业务或不同属性的访问控制。例如：采用访问控制列表、MAC地址、协议类型等多种方式实现网络分段与隔离。

b） 扩展项。

缩短时间窗。限制网络安全事件持续的时间，降低网络安全事件造成的损失。

6.2.3 遏制

遏制是指当系统感知到攻击活动后，能够采取措施增加网络安全事件造成不利影响或后果的难度，阻止攻击方在预期的时间内达到预期的效果，提高攻击的成本。

该指标包括以下内容。

a） 基本项。

1） 动态隔离。当网络安全事件发生后，采用内部防火墙、网络边界隔离组件或杀毒软件，将

危险区域迅速关闭或与其他区域相隔离，将网络安全事件的影响限制在一组受限的资源，降低事件的影响。例如：将感染节点从网络中分离；或发现恶意代码后，将感染文件隔离。

2） 路由隔离。路由器能够识别报文异常情况，自动丢弃异常报文或更新报文，阻止路由异常报文的扩散。

b） 扩展项。

1） 延迟。采取措施增加网络安全事件造成不利影响或后果的难度和时间，遏制攻击活动的进展，增加攻击成本，降低系统风险。例如：设置网络安全防护机制时，考虑资产的分类分级管理机制，根据资产的重要性增加保护措施的数量和强度。

2） 重定向。可采用重定向功能，使攻击活动远离受保护的目标。例如：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。

6.2.4 生存性

生存性是指在攻击、失效、故障或中断发生的情况下，系统仍能运行基本业务功能，完成关键业务的能力。

该指标包括以下内容。

a） 基本项。

1） 安全失效模式。在极限场景下，或发生重大网络安全事件时，保证系统以可控的方式失效，保证失效事件不会对系统及其用户造成损失或尽量减小损失。

2） 降级模式。当发生重大网络安全事件时，系统能够采用比正常模式功能收缩、性能降低的模式运行，实现关键业务系统最小化运行，保证关键业务连续性。

注：最小化运行是指为了实现关键业务系统的生存性，需要保证运行的最少的基本业务功能集合。

b） 扩展项。

1） 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。

2） 吸收模式。可采用容错或鲁棒性等技术，吸收失效事件或设备故障，保证系统稳定运行。

6.3 恢复能力

6.3.1 灾难备份

灾难备份是指为了灾难恢复而对系统、基础设施、专业技术支持和运行维护管理能力进行备份的过程。

该指标包括以下内容。

a） 基本项。

1） 备份策略。明确备份策略，包括需要备份的重要数据和文件内容、备份方式、备份时间和备份地点，备份策略包括全盘备份、增量备份、差异备份 3 种策略。

2） 备份数据保护。对备份数据或文件提供必要的安全保护，确保备份文件是可用的、没有被篡改或破坏的。

b） 扩展项。

1） 重要数据备份加密保护。对于关键业务数据，采用适当的访问控制策略或符合国家密码管理相关部门要求的密码技术保护备份数据的保密性和完整性。

2） 安全库存与备份。对于重要硬件设备和软件，保证安全库存与备份。例如：保证备件数至少可平稳度过两个 MTPD 的数量。

6.3.2 业务连续性

业务连续性是指在中断发生期间，组织以预先确定的方式在可接受的时间范围内持续提供业务功

能的能力。

该指标包括以下内容。

a) 基本项。

1) 可用性目标。依据 GB/T 30146—2023,定义关键业务系统或服务的可用性目标,并在供应商 SLA 中约定。

2) 连续操作。当发生关键设备故障或重要服务中断时,具有手动操作、组件替换或切换等能力,保证基本业务功能的持续运行。

b) 扩展项。

1) 高可用性。对中断可能产生重大影响的关键业务,其可用性目标应达到 99.999%。

2) 系统还原或回滚。对于不期望的系统操作后果(特别是与关键业务相关的后果)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能力,以保证系统或数据的完整性,降低网络安全事件的影响。

6.3.3 数据与业务恢复

数据与业务恢复是指中断发生后,基于备份数据或文件,将业务系统从网络安全事件状态恢复到正常运行状态的能力。

该指标包括以下内容。

a) 基本项。

1) 恢复数据源。对于已经损坏或可疑的数据资源,要从干净的、受保护的备份中恢复。

2) 数据与业务恢复策略。明确数据和业务的恢复策略,例如:全盘恢复、个别文件恢复和重定向恢复。

3) 恢复目标。依据 GB/T 20988,采用适当的恢复策略,实现系统恢复目标,包括:恢复点目标 RPO、恢复时间目标 RTO。

b) 扩展项。

1) 网络恢复策略。网络遭受攻击后,通过节点修复和连边重构的方式快速恢复业务功能,例如:使用节点备份恢复策略或者节点接替恢复策略。

注:连边重构是指在网络某节点功能失效时,为实现网络路径的可用性,利用冗余节点重新构建网络节点间连边的过程。

2) 重续运行。灾难事件发生时,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 适应能力

6.4.1 自主管理

自主管理是指系统修复自身漏洞和缺陷,加固自身功能和结构,提高抵抗风险的能力。

该指标包括以下内容。

a) 基本项。

1) 自我修复和完善。系统能够学习已经识别或已经发生的网络安全事件相关知识,及时修复已知漏洞、功能失效、设备故障或失陷组件,实现自我修复和完善,消除网络安全风险隐患。

2) 清除受损数据。删除系统中不安全、不正确的或已经损坏的、可能造成损害的网络资源或数据,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,使该软件中植入的恶意代码被清除。

b) 扩展项。

1) 按需激活。创造条件降低网络安全事件产生的影响。例如:关键软件在需要时才组装或

激活，缩短关键软件被探测的时间窗口。

2） 积极防御。在适当情况下（例如：基于对即将发生的重大网络安全事件的预测），能够采取主动策略对威胁或攻击进行响应，避免重大网络安全事件的发生或产生影响，或降低网络安全事件发生的可能性和潜在损失。

6.4.2 重构

重构是指当组件发生损坏或失陷，或自身技术和运行环境发生变化时，能够利用可用资源，重构业务流程或功能的能力。

该指标包括以下内容。

a） 基本项。

1） 冗余。从安全角度考虑设置额外数量的系统单元，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。冗余可通过设置多重系统、单元或其他实现同一功能的设备来实现，例如：网络冗余、组件冗余、设备冗余、信道冗余。

2） 替换。系统能够自动识别受损组件或网络节点，并能够快速切换到未损坏的组件或节点，替换已经损坏的组件或节点。

b） 扩展项。

1） 动态资源调度。系统能够基于业务需求的变化，动态调整所调用的网络资源，快速重组系统功能，保证关键业务功能稳定运行，提高网络弹性。

2） 业务重排。能够基于业务需求，对业务流程进行重新编排或协调处理，避免引发级联故障或整体服务中断。

6.4.3 节点适应性

节点适应性是指通信网络中节点调整自身配置或状态，实现自我保护并适应环境变化的能力。

该指标包括以下内容。

a） 基本项。

1） 节点加固。网络节点具有识别特征已知的威胁、及时修复自身漏洞和缺陷，加固应用配置，避免遭受相同或类似的网络安全事件的能力。

2） 地址绑定与解绑的便利性。系统设计时，考虑 IP 地址与 MAC 地址或服务器的绑定和解绑的便利性，方便用户操作并实现节点保护。

b） 扩展项。

1） 节点优化。网络节点具有识别特征未知的威胁、自身技术和运行环境变化的能力，并采用容错或鲁棒性等方法吸收变化或优化自身配置，实现节点的自适应性，不断提高抵抗风险的能力。

注 1：容错是指在出现随机功能失效或故障的情况下，功能单元持续执行所需功能的能力。

注 2：鲁棒性是指结构能够承受环境干扰、输入异常、网络攻击等不利条件，输出正确运行结果，并保持其性能水平的能力。

2） 随机 IP 地址。采用随机 IP 地址生成器，或从限定类型或范围内随机选择 IP 地址，使 IP 地址具有弹性。

3） 虚拟 IP 地址。可采用虚拟 IP 地址，使所有发往这个虚拟 IP 地址的数据包最后都通过物理网卡到达目的主机，实现网络地址转换、容错和网络地址的可移动性。

6.4.4 网络适应性

网络适应性是指通信网络不断调整网络节点间连接关系，以适应环境变化的能力。

该指标包括以下内容。

a） 基本项。

1） 负载均衡。通过网络负载均衡策略，保证数据能够均匀分布到所有网络节点。
2） 路径多样性。根据系统实际需求，采用多样性技术实现网络路径的弹性。对于重要网络需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、浮动路由或带外通道。
3） 路由协议多样性。采用多种路由协议，提高路由协议的弹性。

b） 扩展项。
1） 数据与网络物理或逻辑上分离。将数据与网络在物理或逻辑上分离，避免数据与网络的耦合，并对关键业务数据设计备份或冗余，提高关键业务数据修改或网络配置的灵活性，降低系统重构的代价。
2） 路由算法弹性。可采用分布式路由算法或软件定义路由算法实现路由的弹性调度。

7 评价方法

对网络弹性进行评价时，参考附录C对系统的网络弹性需求进行分析，并按照附录A逐一对网络弹性指标进行评价，评价结果包括符合、不符合、不适用。其中，单项指标评价结果为符合则得分为1分，不符合为0分，不适用项不计分。裁定标准如下：

a） 符合：指标的内容全部得到了满足；
b） 不符合：指标的内容未全部得到满足；
c） 不适用：指标的应用场景或评价方法不适用于评价对象。

按照对网络弹性的重要性，将评价指标分为基本项和扩展项两种类型，对两类指标的得分分别进行汇总。

网络弹性评价分值计算如下：

基本项指标分值＝基本项指标单项评价总分/总适用项×100％

扩展项指标分值＝扩展项指标单项评价总分/总适用项×100％

根据网络弹性评价分值，确定网络弹性等级。网络弹性等级由高到低依次为3级、2级、1级，其划分原则见表1。

表1 网络弹性等级划分

评价等级	指标分值
3级	基本项指标总分达到100％ 扩展项指标总分≥90％
2级	基本项指标总分达到100％ 扩展项指标总分≥60％
1级	基本项指标总分达到100％

附 录 A
（规范性）
网络弹性评价表

网络弹性指标与评价方法如表 A.1 所示。

表 A.1 网络弹性评价表

一级指标	二级指标	指标类型	三级指标	评价方法	符合性	得分
6.1 预防能力	6.1.1 态势感知	a）基本项	1）检测	是否建立本单位网络安全全景图并保持为最新		
			2）重大风险源监测	① 是否对关键业务系统所依赖的重要资产和服务的安全状态或主要设备故障进行检查和监测； ② 关键业务系统中重要服务和主要设备部署安全控制和传感器监控的比例是否能够满足需求		
			3）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		
			4）特征已知威胁检测	针对特征已知威胁的检测成功率是否达到 100%		
		b）扩展项	特征未知威胁检测	针对特征未知威胁是否具备检测、发现的能力		
	6.1.2 检查分析	a）基本项	1）重大网络安全威胁分析	提供包括网络安全事件的漏洞利用、触发条件和脆弱点模式的重大网络安全威胁分析报告，例如：某 APT 攻击分析报告		
			2）重大风险源分析	是否识别了重要资产和服务或主要设备的脆弱性、失效模式和故障模式，分析了潜在损失和影响的范围		
		b）扩展项	级联事件分析	对可能存在级联效应的网络安全事件，是否在物理拓扑结构下计算网络安全事件潜在损失，对极端网络安全事件采取了预防措施		
	6.1.3 协同防御	a)基本项	1）协同防御策略	是否具备协同防御策略，能够借助群体防御力量，抵御未知威胁和攻击		
			2)情报共享	是否对接国家威胁情报共享平台		
		b)扩展项	1)自建内部威胁情报库	是否建设内部威胁情报库		
			2）自然灾害预警	是否建设自然灾害历史数据库或对接国家自然灾害预警系统		
	6.1.4 供应链管理	a）基本项	1）关键设备采购清单	① 采购网络关键设备和网络安全专用产品目录中的设备和产品时，应采购通过国家检测认证的设备和产品；可能影响国家安全的，要通过国家网络安全审查； ② 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		
			2）关键产品及服务供应商资质备案	① 关键软硬件产品、设备及服务供应商是否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了备案； ② 是否具有长时间不录用机制		
			3）知识产权管理	① 软件产品或服务使用授权是否满足业务持续稳定运行时限需求，包括但不限于许可证、产品序列号、开源许可协议等； ② 授权期内软件是否持续稳定可用		
		b）扩展项	多供应商服务协议	对于关键设备或服务，是否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		

表 A.1　网络弹性评价表（续）

一级指标	二级指标	指标类型	三级指标	评价方法	符合性	得分
6.2 承受能力	6.2.1 应急响应	a）基本项	1）应急预案管理	是否制定了符合 GB/T 43269－2023 相关要求的应急预案，并定期开展应急预案演练，能提供系统演练记录		
			2）应急处置	是否具备必要应急调度手段支撑开展故障排查、诊断、处理和恢复		
		b）扩展项	有序响应	根据业务、资产与服务优先级排序，对故障进行有序响应和恢复		
	6.2.2 损失限制	a）基本项	1）减小攻击面（收敛暴露面）	① 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； ② 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		
			2）分离关键业务与非关键业务	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		
			3）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		
			4)分段与隔离	① 是否根据关键业务不同属性对网络进行分段或分区管理； ② 不同网络分区或网段之间是否具备相互隔离能力		
		b）扩展项	缩短时间窗	① 应急事件被识别至故障排除时间是否能够被接受； ② 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，或在预期时间内从异常状态恢复到正常状态的能力； ③ 是否具备相应的故障切换预案等		
	6.2.3 遏制	a）基本项	1）动态隔离	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，以及隔离记录		
			2）路由隔离	路由器能否识别并丢弃异常的路由更新报文，从而阻止路由异常报文的扩散		
		b）扩展项	1）延迟	是否能够根据资产重要度提供不同安全等级的防御措施，增加重要资产的攻击成本		
			2）重定向	是否具备对攻击活动的重定向机制及重定向记录，并验证重定向是否有效		

表 A.1　网络弹性评价表（续）

一级指标	二级指标	指标类型	三级指标	评价方法	符合性	得分
6.2 承受能力	6.2.4 生存性	a）基本项	1）安全失效模式	① 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，控制和减少对系统自身及其用户造成伤害； ② 是否对重要功能进行了失效模式分析，识别了导致系统重要功能失去执行能力的潜在风险因素并加以控制		
			2）降级模式	① 是否清晰识别关键业务系统的最小运行集，确定哪些基本业务功能或服务在降级模式下应得到保证，例如：参考日志级别设置预案的能力； ② 是否具备系统切换并以降级模式运行的能力		
		b）扩展项	1）防故障模式	① 是否具备常见故障类型清单及防故障处置方案； ② 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		
			2）吸收模式（鲁棒性、容错）	① 当系统内部功能运行出现偶然故障，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； ② 当系统偶然输入了错误信息，是否具备反馈控制机制保证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； ③ 删除少量网络节点后（低于 10%），网络拓扑结构的整体联通度是否仍然能够实现业务连续性目标		
6.3 恢复能力	6.3.1 灾难备份	a）基本项	1）备份策略	① 重要数据资产是否具备确定的备份策略（包括备份内容、备份方式、备份时间和备份地点）并正确执行； ② 是否基于系统或业务数据的重要性，提供异地灾难备份功能，利用通信网络将重要数据实时备份至备份场地； ③ 备份结果是否与备份预期目标一致		
			2）备份数据保护	是否对备份数据采取必要的保护措施，保证其不被篡改和破坏		
		b）扩展项	1）重要备份数据加密保护	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和完整性		
			2）安全库存与备份	关键设备备件数是否足够平稳度过两个 MTPD 的数量		

表 A.1　网络弹性评价表（续）

一级指标	二级指标	指标类型	三级指标	评价方法	符合性	得分
6.3 恢复能力	6.3.2 业务连续性	a）基本项	1）可用性目标	是否按照国家、行业、企业等多维度规定，基于业务重要程度，提供可用性验证文档（测试文档等），系统的可用性、设备组件的可用性是否满足规范或用户要求		
			2）连续操作	是否具有手动操作、组件替换或切换等方式，保证关键业务功能或重要服务不中断的能力		
		b）扩展项	1）高可用性	中断可能产生重大影响的关键业务，可用性是否达到 99.999%		
			2）系统还原或回滚	对关键业务，是否具备系统还原或数据回滚机制及回滚测试记录		
	6.3.3 数据与业务恢复	a）基本项	1）恢复数据源	通过完整性检查、行为确认等方法判断恢复数据源是否完整		
			2）数据与业务恢复策略	① 是否具有明确的数据和业务的恢复策略，例如：全盘恢复、个别文件恢复和重定向恢复策略； ② 恢复测试记录是否能够证明数据恢复的正常进行		
			3）恢复目标	① 从业务需求角度评估 RPO、RTO 是否在可接受范围内； ② 系统恢复测试中，是否达到了 RPO、RTO 的要求		
		b）扩展项	1）网络恢复策略	① 是否具备节点备份恢复策略或节点接替恢复策略； ② 当网络平面受到破坏，是否能够基于运行数据备份快速恢复网络		
			2）重续运行	遭受重大网络安全事件时，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		
6.4 适应能力	6.4.1 自主管理	a）基本项	1）自我修复完善	是否能够及时修复已知系统漏洞、缺陷、功能失效和设备故障		
			2）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潜在风险因素，包括但不限于定时任务、静态数据、暂态数据		
		b）扩展项	1）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发生		
			2）积极防御	发现重大网络安全威胁时，是否能够采取主动策略，防止重大网络安全事件的发生		
	6.4.2 重构	a）基本项	1）冗余	① 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； ② 是否存在适用的设备备用站点		
			2）替换	是否具备组件替换记录，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价		
		b）扩展项	1）动态资源调度	① 是否能够针对业务优先级采用不同调度策略或调度算法； ② 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		
			2）业务重排	是否具备不同层次或不同位置的业务重排记录或基于事件的决策机制		

表 A.1　网络弹性评价表（续）

一级指标	二级指标	指标类型	三级指标	评价方法	符合性	得分
6.4 适应能力	6.4.3 节点适应性	a）基本项	1）节点加固	① 节点是否具有针对网络安全事件的检测和抵御能力； ② 是否能够对设备故障和应用程序漏洞进行及时有效地修复； ③ 是否能够对节点应用程序、配置进行加固，消除不必要的程序和账户，获得更稳定的配置和更透明的环境		
			2）IP 地址绑定与解绑便利性	基于简单配置绑定 IP 到 MAC 地址或服务器，方便用户解绑操作		
		b）扩展项	1）节点优化	① 网络节点具有识别特征未知的网络安全事件、自身技术和运行环境变化的能力； ② 是否采用容错或鲁棒性等方法，具有吸收变化或优化自身配置的能力		
			2）随机 IP 地址	① IP 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； ② 网络环境是否具备弹性 IP 地址分配池及管理算法		
			3）虚拟 IP 地址	① 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； ② 关键路由节点是否采用虚拟浮动地址		
	6.4.4 网络适应性	a）基本项	1）负载均衡	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均衡的方法		
			2）路径多样性	① 具备多个运营商提供的广域网通信链路，或提供多条冗余路径； ② 关键设备/系统至少具备一个带外通道，并提供多个独立命令、控制和通信路径供选择； ③ 关键路由器（如网络出入口路由器）可配置快速切换冗余备份路径		
			3）路由协议多样性	对于重要网络路由设备，是否采用 3 种以上路由协议（如 RIP/OSPF/ISIS/BGP 等）		
		b）扩展项	1）数据与网络物理或逻辑上分离	① 存储单元与控制单元是否隔离在不同的网络平面； ② 是否具备数据的弹性设计，例如：数据备份和恢复等，提高关键业务数据修改或网络配置的灵活性		
			2）路由算法弹性	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		

附 录 B
（资料性）
极限场景、极端网络安全事件下网络弹性指标示例

弹性的概念是风险管理和灾难管理的里程碑。网络弹性更多地被应用于极限场景、极端网络安全事件以及灾难事件的风险管理中。其中：

极限场景是指在时间和空间属性上突破传统网络和信息系统应用范畴，或者系统资源使用率远远超过正常使用基线的场景。极限场景下，需要采用创新解决方案，才能保证关键业务系统的生存性。极限场景的示例见表 B.1。

表 B.1 极限场景示例

极限场景	极限场景示例
重大自然灾害或人为灾难	干旱、洪水、飓风、地震、海啸、流行病、极端气候条件等重大自然灾害 火灾、爆炸、断电、断网等人为灾难
极端的网络压力	重要信息基础设施遭遇有组织的、大规模、持续时间长的网络攻击 网络瞬时并发访问数量超过 100 万人以上的公共信息服务系统 云计算、数据中心和大数据交易平台遭遇破坏性的攻击 电子支付、结算系统、信用信息系统遭遇大规模信息盗窃、高价值身份被假冒、欺骗 物联网大量末端传感器管控、时钟同步

极端事件是指一个系统内可量化的小概率、具有持续严重影响的事件。

注 1：在新型复杂网络环境下，系统级联效应可能产生链锁反应从而造成重大的影响。网络安全级联事件属于极端事件，但极端事件不一定是网络安全级联事件。

灾难事件是指由于人为或自然的原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

判断一个事件是否是极端事件，通常根据事件发生的概率和后果的影响。假设网络安全事件发生的概率符合正态分布，选取某个长期序列的固定百分位数作为阈值，例如 95%和 5%分位数，那么超出这一概率阈值范围、并且产生严重影响的重大事件就可以被认为是极端事件。判断一个事件是否是灾难事件通常以是否需要切换到灾难备份中心运行为标准。

其中，具有严重影响的重大事件的判定可依据 GB/T 20986—2023，指事件发生在特别重要或重要的事件影响对象上，并且：

a） 导致特别重要或重要的事件影响对象遭受严重的业务损失，或

b） 造成重大的社会危害。

在极限场景下或发生极端网络安全事件或灾难事件时，关注以下重点问题。

a） 极限生存。以业务风险控制为核心，分析关键业务系统运行中断或主要设备功能故障而导致重大网络安全事件的风险。保证在极限场景下或发生极端网络安全事件或灾难事件时，系统仍能提供基本业务功能的能力，保证关键业务系统的生存性，保证关键业务的连续性。

注 2：业务风险是指组织在运营活动中存在的风险，可表示为业务所涵盖的系统资产的风险值。

b） 协同防御。面对层出不穷的网络攻击新模式，通过态势感知、检查分析、威胁信息共享、自建威胁情报库、对接国家自然灾害预警系统等措施，积极防范化解重大网络安全风险。

c） 响应恢复。促进应急响应和恢复能力的提升。对网络安全事件采取应急响应、损失限制措施，并采取适当的恢复或重构策略实现业务的恢复目标。

d） 能力提升。采用自主管理、重构、节点适应性和网络适应性等措施，提高系统适应能力。本文

件基于系统内在结构决定外在功能的基本原理，给出一个网络弹性架构设计参考（见附录D），以确保功能和结构的统一，为网络弹性设计提供指导。

表B.2例举了部分典型公共服务场景下极端网络安全事件或灾难事件及相关网络弹性指标示例。

表B.3给出了一个极端网络安全事件情景下的网络弹性指标评价示例，为网络弹性评价提供参考。

表B.2　极端网络安全事件或灾难事件及相关网络弹性指标示例

典型公共服务系统	极端网络安全事件或灾难事件示例	相关网络弹性指标示例
公共网络通信系统	受DDOS攻击导致大规模的网络服务宕机 电力供应中断导致通信网络服务中断 路由器技术故障、路由器被部署恶意软件导致大规模宕机 通信线路被物理破坏，例如被剪断	预防、承受、恢复 电力供应冗余 关键设备冗余、防故障模式 骨干网需配备第三种通信模式
供电系统	网络被DDOS攻击导致供电系统服务中断 网络中重要设备设施故障导致供电系统服务中断 机器损坏导致服务故障、关键服务被杀死	预防、应急响应、恢复 关键设备冗余、备份、供应链管理 防故障模式、业务连续性
能源供应系统	供应链服务系统受攻击导致大量客户信息泄露，系统服务中断 加油站管理系统被攻击、数据被破坏导致大面积宕机	预防、承受、恢复、适应
智能交通系统	自动驾驶系统存在漏洞导致系统被远程控制、网络被攻击 车联网系统被攻击，导致交通指挥系统被干扰 航空指挥调度系统服务中断与故障	安全失效模式、防故障模式、吸收模式、高可用性、低时延、高带宽
金融服务系统	电子支付系统被攻击导致服务中断、资金被恶意转账 信用系统数据库被攻击、被破坏，重要数据被泄露	预防、承受、恢复、适应
教育系统	在线授课、考试系统被攻击导致服务中断、系统被破坏	预防、承受、恢复、适应
电子政务系统	电子政务网上服务系统被攻击、破坏，造成严重社会影响	预防、承受、恢复、适应
工业生产服务系统	工业控制系统突破物理隔离的限制，系统被远程控制 工业互联网受DDOS攻击，导致系统宕机 工业软件0day漏洞被利用，被勒索病毒攻击 内网移动办公系统受攻击导致大面积服务中断 主要设备设施故障，如出口防火墙故障导致大面积网络中断	隔离、访问控制 预防、承受、恢复、适应 供应链管理、备份 检测、检查分析、监测预警 主要设备冗余、备份、防故障模式
供应链系统平台	勒索病毒攻击、APT攻击、黑客攻击等导致供应链服务系统被攻击、服务器数据被泄露、被破坏	预防、承受、恢复、适应 供应链管理、备份
	重要网络资源或设备存在漏洞，如芯片漏洞、操作系统漏洞、编译器漏洞、打印机漏洞等，漏洞被利用攻击关键业务系统	供应链管理
云计算平台	恶意程序攻击，例如：DDOS攻击，资源池单IP被DDOS，或资源池IP段（C段）被DDOS，导致资源池入口被打满	检测、监测预警、生存性、业务连续性
	路由器故障或下线导致网络风暴或RIP风暴；网络专线故障导致专线业务中断；网络入口故障导致整个资源池断网；服务器故障导致宿主机承载虚拟机故障；存储设备故障导致资源池I/O异常；机房空调故障导致集群性能下降，严重时资源池集体掉线；机房电路故障、UPS未启动、发电机未启动，导致资源池全部设备关机；系统故障导致业务系统受损	冗余 路由控制机制弹性 网络路径弹性 物理位置的弹性
	洪水、地震、台风、冰冻等自然灾害导致部分或全部主机故障	协同防御、灾难备份、业务连续性、数据与业务恢复、物理位置的弹性
数据中心	数据中心被攻击、被勒索导致大量数据被泄露、被破坏	灾难备份、恢复、数据加密

表 B.3　极端网络安全事件相关网络弹性指标评价示例

网络安全事件描述	某系统关键服务监控功能被杀死导致关键业务中断风险
网络弹性需求分析	明确网络弹性目的，包括如下。 a)　关键业务连续性目标： 1)　关键业务及其重要资产和服务的优先级排序：对系统中所运行的服务进程设置优先级，分为：非常高、高、中、低 4 个级别； 2)　服务可用性目标：保证关键业务的高可用性，即关键服务进程的可用性达到 99.999%； 3)　最大可容忍中断时间：关键服务进程的最大可容忍中断时间为 30 s。 b)　关键业务生存目标： 1)　极限场景或发生重大网络安全事件时的风险控制目标：保证优先级为非常高的关键服务进程不中断； 2)　系统主要设备防故障目标：防止设备设施故障导致关键服务进程中断； 3)　识别最小化运行功能集，确定重大网络安全事件发生时系统降级运行模式目标：当资源不足时，优先级为非常高的关键服务进程能够生存下来，即为最小运行集，其他级别的进程依照资源的使用情况可关闭。 c)　网络弹性能力目标： 1)　预防能力：系统能够检测关键服务进程中断； 2)　承受能力：系统自身具有防故障功能； 3)　恢复能力：中断时，系统能在 30 s 时间内恢复关键服务进程； 4)　适应能力：系统能够适应内、外部环境变化，不断提高抵抗风险的能力
网络弹性指标评价	预防能力： a)　检测：系统能够基于指示器信息，检测关键服务进程中断风险； 评价结果：符合； b)　重大风险源监测：对进程进行实时监控，及时发现异常； 评价结果：符合； c)　监测预警：建立了系统进程运行基线，发现异常及时告警； 评价结果：符合。 承受能力： a)　降级模式：当系统资源受限时，进程管理器按照优先级低、中、高的顺序关闭服务进程，保证优先级非常高的关键服务进程持续运行； 评价结果：符合； b)　防故障模式：优先级为非常高的进程具有最高的资源占用权，保证优先级非常高的关键服务进程无法被杀死； 评价结果：符合。 恢复能力： 恢复目标(RTO)：当由于突发事件导致关键服务进程中断时，进程管理器会在 30 s 内自动将死掉的关键服务进程重启，保证关键服务进程的持续运行； 评价结果：符合。 适应能力： a)　自我修复和完善：目前还无法做到从机理上对故障进行修复，避免故障的再发生； 评价结果：不符合； b)　动态资源调度：当关键服务进程中断时，进程管理器能够识别系统中低、中、高级别的服务进程，并将其关闭，保证关键服务进程的资源需求优先得到满足； 评价结果：符合。

附 录 C
（资料性）
复杂信息系统网络弹性需求分析

C.1 概述

对于多业务协同的复杂的网络信息系统，可依据下面介绍的方法，对系统进行分析，清晰地识别系统中关键业务、所依赖的重要资产、服务和主要设备，并对其优先级进行排序，分析系统的脆弱性、重要功能失效和主要设备故障模式，制定适合自身需求的网络弹性目的和需求。

C.2 识别关键业务

识别关键业务包括：

a） 根据 3.2 关键业务的定义，清晰地识别系统关键业务、业务系统运行环境以及可能存在的极限应用场景；

b） 识别系统中包含的关键业务、非关键业务和相关外部业务，分析关键业务对非关键业务和相关外部业务的依赖关系；

c） 对业务优先级进行排序。

C.3 识别重要资产和服务

识别重要资产和服务包括：

a） 识别支撑关键业务的重要网络资产和服务，输出重要资产和服务的分布和运营情况；

b） 分析关键业务系统的最小化运行功能集，明确系统降级模式运行时需要保证的最少的基本业务功能集合，保证遭受重大网络安全事件时关键业务系统的生存性，保证关键业务的连续性。

注：资产是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。服务包括了对象系统提供给客户的服务（产品），也包括为了实现业务功能，而由第三方服务机构提供给业务系统的服务。

C.4 风险分析

依据 GB/T 20984—2022 等风险评估标准，开展风险分析，包括：

a） 分析关键业务系统的网络安全风险，识别系统的脆弱性，分析可能面临的“不利条件、压力、攻击或失陷组件”等威胁，识别重大风险源，分析重大网络安全事件风险；

b） 分析关键业务系统重要功能失效模式和主要设备故障模式，分析可能产生的后果，以设计并开发安全失效模式和防故障模式。

C.5 约束与限制条件

基于组织风险管理策略和网络安全法律法规需求，识别约束与限制条件。包括以下内容。

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网络安全事件相关的限制要素，例如：对特定技术的承诺，与其他系统的交互需求等。

c） 识别依赖关系。厘清重要资产和服务的内外部依赖关系，理解网络安全事件的影响因素和作用机制，以利于风险决策。包括：

1） 识别重要资产和服务的内部依赖关系，例如：时序关系、并行关系、顺序关系等；

2） 识别重要资产和服务的外部依赖关系，例如：硬件设备是否到位，软件供应商是否开发了系统补丁程序等。

C.6 明确网络弹性目的和需求

基于关键业务、重要资产和服务、风险分析和约束与限制条件的分析结果，明确网络弹性目的，包括3个目标，10个子目标。

a） 关键业务连续性目标。包括：

1） 关键业务及其重要资产和服务的优先级排序；

2） 服务可用性目标，例如：高可用性通常为99.999%；

3） 最大可容忍中断时间MTPD、最小业务持续时间MBCO等。

b） 关键业务生存目标。了解极限场景，可能面临的重大网络安全威胁和重大网络安全风险隐患，保持系统对于重大网络安全事件的准备和预防状态，包括：

1） 极限场景或发生重大网络安全事件时的风险控制目标；

2） 系统重要功能的安全失效和主要设备防故障目标；

3） 识别最小化运行功能集，确定重大网络安全事件发生时系统降级模式目标。

c） 网络弹性能力目标。了解网络安全状态和面临的威胁，确定“预防、承受、恢复、适应”目标，包括：

1） 预防能力目标；

2） 承受能力目标；

3） 恢复能力目标；

4） 适应能力目标。

从上述网络弹性目的和目标出发，以终为始，为设计更适合系统业务需求的网络弹性提供指导。

附 录 D
（资料性）
网络弹性架构设计方法

D.1 概述

为指导网络弹性建设，本文件给出一个网络弹性架构设计方法，包括逻辑架构、物理架构和通信网络架构3个方面，如图D.1所示。

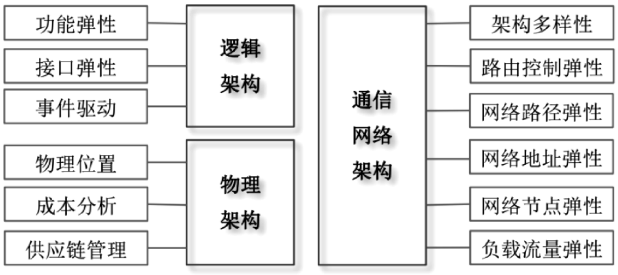

图 D.1 网络弹性架构设计

D.2 逻辑架构

D.2.1 功能弹性

D.2.1.1 软件定义弹性

可基于软件定义的思想，将软件功能需求和非功能需求（如质量属性、安全性、可靠性、弹性等）相分离，根据需求的变化对软件功能进行重组，实现关键业务连续性目标。包括：

a） 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；

b） 根据业务功能需求变化对软件功能进行重组。

D.2.1.2 业务流程弹性

关键业务流程或所依赖的重要网络资源宜具有适当的冗余，保证当某一个关键业务流程发生故障时，系统关键业务仍能够持续运行。

D.2.2 接口弹性

D.2.2.1 弹性网络接口

实体网络设备或虚拟网络设备的物理层弹性网络接口、数据链路层交换接口、网络层路由接口以及应用层各种服务协议接口等具有弹性，保证当一个网络接口组件出现故障时，有其他网络接口组件可接替其工作。

D.2.2.2 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。

D.2.2.3 匿名系统接入的验证机制

对于匿名系统服务或设备，可通过多种动态验证机制，提高网络接入验证的弹性。例如：对匿名接入系统，至少提供2种不同类型的验证机制，如基于口令、生物特征以及令牌、短信等验证机制。

D.2.3 事件驱动

D.2.3.1 基于事件的决策

系统能够根据当前时间节点的事务处理状况进行决策，调用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，可提供基于事件优先级的处理方式。

D.2.3.2 资源的调度

系统能够基于业务需求的变化，动态调整所调用的网络资源。包括：

a) 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) 能够根据事件的处理数量、处理优先级、计算与存储资源的需求和 I/O 消耗量动态调度相应的资源。

D.2.3.3 事件处理效率

采用基于事件的决策方法，动态调用资源，提高资源的使用效率，提高单位时间内完成的事件数量。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和分析事件处理效率。

D.3 物理架构

D.3.1 物理位置

D.3.1.1 节点地理分布、物理环境、位置约束

基于位置的系统实际物理拓扑结构，分析节点的地理分布、物理环境、位置约束，识别物理环境风险，并遵从适当的物理安全标准和规范，保证物理位置安全和弹性。包括：

a) 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符合 GB/T 2887—2011 等相关标准。

D.3.1.2 硬件、软件或网络弹性

对于重要网络设备，采用备份和冗余等策略，保证重要设备发生故障时，能够迅速替换或切换到备份或冗余设备，保证关键业务的持续运行。包括：

a) 硬件：不存在单点故障，至少有一个冗余设备可接替故障设备继续工作，例如：5G 基站等重要设备设施宜设计冗余；
b) 软件：无论是组件、节点、进程还是模块，均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都可以由另一网络平面来承接其工作；
d) 网络中物理设备被干扰或中断但没有导致关键业务系统崩溃或功能丧失的比例，即被干扰/中断设备的数量：总设备数量，是否达到预期。

D.3.1.3 数据与网络物理或逻辑上分离与冗余

将数据与网络在物理或逻辑上分离，避免数据与网络的耦合，并对关键业务数据设计备份或冗余，提高关键业务数据修改或网络配置的灵活性，降低系统重构的代价。包括：

a) 存储单元与控制单元宜隔离在不同的网络平面；
b) 运营数据宜采用弹性设计，如数据备份和恢复等，保证数据备份和恢复的灵活性。

D.3.2 成本分析

D.3.2.1 直接损失成本

在物理拓扑结构下分析网络安全事件产生的直接损失成本，包括物理资产、数据资产与服务中断损

失评估，帮助确定网络中重要设备或组件的备份或供应链管理策略。

D.3.2.2 间接损失成本

在物理拓扑结构下，计算与环境的依赖关系造成级联事件而产生的间接损失成本。包括：

a) 第一方人身伤害，第三方硬件设备、软件、数据等信息资产损失和人身伤害损失；
b) 组织品牌、声誉等无形资产损失。

D.3.2.3 人工成本

数据备份与恢复、节点设备与组件替换所需要的人工成本。例如：硬件设备、软件安装及数据重新加载配置所需要的人工成本。

D.3.3 供应链管理

D.3.3.1 关键设备采购清单

采购网络关键设备和专用网络安全产品时，采购通过国家检测认证的设备和产品。可能影响国家安全的，要通过国家网络安全审查。

D.3.3.2 多供应商服务

对于关键业务依赖的重要设备或服务，可以合同的形式与多家有保障的供应商签订服务协议，保证在供应链系统发生部分失效时，仍能持续提供产品和服务，并快速恢复到正常供应状态。

D.3.3.3 安全库存与备份

对于重要硬件设备、软件和数据，实行备份制度，保证安全库存与备份。包括：

a) 有足够的库存和备用设备来应对突发的重大网络安全事件，例如：备件数至少准备可平稳度过两个 MTPD 的数量；
b) 库存和备用设备宜保存在设计安全距离内。

D.3.3.4 供应商资质备案

对于关键软硬件产品、设备与服务供应商，具备证书和资质备案制度。包括：

a) 关键软硬件产品、设备服务供应商是否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) 是否有长时间不录用机制。

D.3.3.5 知识产权管理

提供满足业务持续稳定运行时限需求的软件产品或服务使用授权，包括但不限于许可证、产品序列号、开源许可协议等，并确保授权期内软件持续稳定可用。

D.4 通信网络架构

D.4.1 架构多样性

D.4.1.1 异构系统

对于复杂连接的网络，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。例如：对于关键业务系统可部署 2 种或 2 种以上操作系统、通信协议或网络模态。

D.4.1.2 分布式系统

对于分布式系统，可通过网络资源的冗余和自动故障转移实现高可用架构。

D.4.2 路由控制机制弹性

D.4.2.1 路由算法

可采用分布式路由算法或软件定义路由等方法实现弹性路由调度，降低网络拥塞。

D.4.2.2 路由协议多样性

可采用多种路由协议，提高路由协议的弹性。例如：对于重要网络路由设备，可采用 3 种以上路由协议（如 RIP/OSPF/ISIS/BGP 等）。

D.4.2.3 网络负载均衡

通过网络负载均衡策略，保证数据能够均匀分布到所有网络节点。

D.4.2.4 隔离性

路由器可采用访问控制列表、MAC 地址、协议类型等多种方式实现网络隔离。包括：

a) 不同虚拟网络之间的路由表具备相互隔离能力；
b) 路由器能够识别并丢弃异常的路由更新报文，从而阻止路由异常报文的扩散。

D.4.2.5 适应性

当网络中有新节点加入，路由算法可自动调整，重新分配数据，原有节点数据不变。包括：

a) 路由控制机制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，使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。

D.4.3 网络路径弹性

D.4.3.1 路径多样性

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。对于重要网络需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、浮动路由或带外通道。包括：

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不能过高；
b) 采用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，并提供多个独立命令、控制和通信路径供选择；
d) 网络中关键路由器（如网络的出入口路由器）是否配置可快速切换的冗余备份路径。

D.4.3.2 路径综合可用性

可采用网络容错技术，保证网络路径整体可用性。例如：采用冗余或者容错技术，使端到端路径的整体可用性达到 99.999%。

D.4.3.3 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的业务连续性目标。例如：删除少量网络节点后（低于 10%），网络整体连通度的下降程度宜低于 50%。

D.4.3.4 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，宜≤20%。

D.4.3.5 链路失效率

单位时间内失效的链路数占总链路数的比例，宜≤20%。

D.4.4 网络地址弹性

D.4.4.1 随机 IP 地址生成技术

采用随机 IP 地址生成器，或从限定类型或范围内随机选择 IP 地址，使 IP 地址具有弹性。包括：

a) 网络环境具备弹性 IP 地址分配池及管理算法；

b) 检查 IP 地址能够通过随机方式生成，包括但不限于 DHCP 分配、代理分配、虚拟专网分配等。

D.4.4.2 IP 地址受控访问

通过防火墙设定可访问的地址段或 IP 范围，或通过 IP 安全控制策略限制访问。例如：关键服务节点可采用地址隐藏、跳变等受控访问机制。

D.4.4.3 虚拟 IP 地址

一种不与特定计算机或特定网卡相对应的 IP 地址，所有发往这个 IP 地址的数据包最后都会通过物理网卡到达目的主机。虚拟 IP 地址主要用于网络地址转换、容错和网络地址的可移动性。包括：

a) 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) 关键路由节点可采用虚拟浮动地址。

D.4.4.4 地址绑定与解绑的便利性

为方便用户操作，系统设计需要考虑 IP 地址与网络设备物理地址(MAC 地址)或服务器绑定和解绑的便利性。

注：将 IP 地址与网络设备物理地址(MAC 地址)绑定，可实现静态 IP 地址，防止 ARP 攻击。

D.4.5 网络节点弹性

D.4.5.1 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。

D.4.5.2 自动识别并替换受损组件

网络节点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。

D.4.5.3 感知并抵御已知威胁

针对特征已知的威胁的感知及抵御成功率。例如：抵御成功率是否达到 100%，可结合节点设备或系统安全测试报告进行评估。

D.4.5.4 感知并抵御未知威胁

针对特征未知的威胁(如利用 0day 漏洞的网络攻击)，具备感知和发现的能力。

D.4.6 负载流量弹性

D.4.6.1 吞吐量

单位时间内网络、设备、端口、虚拟电路或其他设施成功完成的任务数或传输数据的数量。例如：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。

D.4.6.2 传输速率

单位时间内由通信信道传输数据的数量。例如: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。

D.4.6.3 带宽

单位时间内网络或通信信道的最高传输速率。可在供应商SLA中约定,以满足业务高峰期服务的需求。

D.4.6.4 时延

数据从网络的一端传输到另一端所需要的总时间。例如:在网络轻、重负载时,关键业务时延的上升幅度宜≤100%。

D.4.6.5 丢包率

网络传输过程中丢失数据包的数量/发送数据包的总数量。例如:

a) 在网络重负载时,网络通信丢包率宜控制在≤5%;

b) 设备正常负载的丢包率宜≤10^{-6}。

参 考 文 献

[1] GB/T 2887—2011 计算机场地通用规范

[2] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[3] GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南

[4] GB/T 42453—2023 信息安全技术 网络安全态势感知通用技术要求

[5] ISO/IEC/IEEE 24765:2017 Systems and software engineering—Vocabulary

[6] 工业互联网产业联盟. 面向行业的 5G 网络 SLA 定义及需求白皮书

[7] T/SIA 031.1—2021 系统安全工程 网络弹性构建指南 第 1 部分:概述

[8] T/SIA 031.2—2021 系统安全工程 网络弹性构建指南 第 2 部分:网络弹性工程框架

[9] T/SIA 031.3—2021 系统安全工程 网络弹性构建指南 第 3 部分:网络弹性构建过程

[10] T/SIA 031.4—2022 系统安全工程 网络弹性构建指南 第 4 部分:网络弹性技术

[11] T/SIA 031.5—2022 系统安全工程 网络弹性构建指南 第 5 部分:网络弹性设计原则

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

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

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

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

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

[17] Nii O. Attoh-Okine. Resilience Engineering. Models and Framework. Cambridge University Press. 2016