CAICT 中国信通院

全时域守护：网络运行安全保障体系的理论建构与实现路径

2026年10月30日 北京

PART

01

CHAPTER 01

《信息通信行业发展“十五五”规划》锚定工作方向

“十五五”规划在网络运行领域的核心要求

CAICT 中国信通院

《信息通信行业发展“十五五”规划》第 14 条重点任务：增强网络运行支撑保障能力

规划原文的九项举措，可归为五条主线：法治立基、标准定责、投入托底、风险前置、技术赋能 —— 把运行安全从「事后处置」前移到「事前可控」。

任务主线		规 划 举 措	解 决 什 么
01	**法治立基**	推进信息通信基础设施建设与保护立法 修订《电信网络运行监督管理办法》	保护义务法定化 2009 年的办法需重写
02	**标准定责**	推进网络运行安全标准化管理 强化「责任链」管理	要求进标准、进流程 责任可追溯到人
03	**投入托底**	加强安全投入保障	冗余、备份、备件与抢修力量是物质基础
04	**风险前置**	深化风险清单管理 构建国家通信网络运行极端事故场景试验验证能力	清单动态更新 用极限试验摸底
05	**技术赋能**	探索人工智能赋能网络运行管理	从人工巡检走向智能预警与自动处置

五条主线互为前提：规则不立则责任无据，投入不足则标准落空，风险不清则验证无从谈起。

网络运行安全保障的核心是什么？

CAICT 中国信通院

「网络不停、业务不断」

它管的不是信息会不会被窃取，而是网络能不能持续提供服务 —— 这是它与「网络安全」最本质的分界。

定 位

网络持续提供服务的能力

即网络基础设施运行的「本质安全」。衡量的是稳定、可靠、可用，而不是信息的保密与完整。

依 据

- 《安全生产法》《电信条例》；
- 《电信网络运行监督管理办法》。

边 界

《办法》第二条将网络攻击、入侵、病毒等防护措施划归「另有规定」，与网络安全防护分工管理。

抓 手

巡检维护、风险评估与隐患排查、故障预警与抢修、预案演练与应急处置。

威胁来源 • 现行《办法》界定的四类成因

- 突发公共事件
- 人为破坏
- 施工损坏
- 网络自身故障

管理方式 • 从「合规检查」到「工作评价」

过 去

合规检查

制度有没有、预案有没有、演练做没做

定性判断，依赖检查人员的经验

“十五五“

工作评价管理

用可量化指标评价运行保障能力

可比对、可排序、可问责

PART

02

CHAPTER 02

国际网络运行安全态势严峻

新发展形势诱发新风险 —— 暴露出的三类风险点

CAICT 中国信通院

设备层、网络层、操作层风险相互交织：新设备未经现网长期考验、云化融合放大故障影响面、集约化运维考验定位与处置能力。

01

设备层风险

- 大量新设备入网
- 软硬件解耦的持续推进
- 网络设备物理形态不断趋同
- 网络设备功能层面不断细分

一些新的技术和设备并没有在现网上进行长时间的考验，我们对于其运行安全性和可靠性的认知并不充分。

02

网络层风险

- 网络经营压力巨大
- 网络的融合化趋势
- 虚拟化技术快速发展
- 网络云化的步伐加快

网络的云化和融合化使得单一故障的影响面极易扩展，大面积网络运行故障的发生概率显著增大。

03

操作层风险

- 行业竞争加剧
- 网络集约化运维
- 网络运维管理更加便捷
- 人力投入得到有效控制

集约化运维如若管理不细、经验不足，发生故障后常常难以定位故障点，大大延迟故障应急处置的进程。

事故影响直达国计民生，网络运行安全是“生命线”

CAICT 中国信通院

一次网络运行事故，往往同时冲击应急指挥、金融支付、公共交通、政务服务与百姓生活 —— 网络运行安全已不再是企业的“内部问题”。

应急通信保障
911 / 112 中断

美国AT&T事故直接影响到911应急通信；丹麦运营商全国断网，紧急服务 112 不可用，公众无法联系警察、消防与救护人员。

金融与支付
250 万笔交易失败

新加坡 Equinix 数据中心故障持续 14 小时，造成 81 万次线上银行访问失败、250 万笔银行交易失败，近 600 万人受影响。

交通运输
全路网列车扣停

德国全境 GSM-R 铁路通信中断约 2 小时，全路网列车紧急扣停；俄罗斯 Rostelecom 断网致铁路票务与网约车平台瘫痪。

政务与公共服务
持续 22.6 小时

荷兰国防部系统故障波及政府、皇家宪兵队与海岸警卫队，埃因霍温机场航班大面积延误。

产业与民生
影响近半数居民

美国 AT&T 事故几乎覆盖全境（除阿拉斯加、夏威夷），持续 11 小时；澳大利亚 Optus 断网使近半数居民生活受到严重影响。

网络运行安全

已从企业运营问题，上升为国家安全、社会稳定与民生保障的重大问题。

网络运行安全工作极其重要

典型事故案例 1

2026-05-07 • 荷兰阿尔梅勒 • 数据中心火灾

事故基本情况

发生时间 2026 年 5 月 7 日上午约 8:45（当地时间）

运营企业 NorthC Datacenters，荷兰数据中心运营商，业务覆盖荷兰、德国、瑞士

事故分类 火灾，起火点位于建筑后部技术设施区域（含应急电源与备用发电机）

持续时间 扑救与处置约 14 小时；人员全部安全疏散，无人伤亡

处置与扑救时长

14 小时

08:45 起火 → 20:50 降为 GRIP 1

次日 00:35 降为 GRIP 0 并部分解封

救援：5 辆消防车、3 辆云梯车、1 台机器人

事故经过

08:45 建筑后部技术设施区域起火，启动安全协议、疏散人员；发布 NL-Alert 提醒居民关闭门窗通风

15:15 消防部门仍需数小时才能控制火势，起火原因与受损范围无法确认，一度无法进入建筑检查

18:30 情况未变，火势仍未得到控制，建筑尚未解封，恢复供电方案同步制定

20:50 火势被控制，降级为 GRIP 1，NL-Alert 撤销，当晚获准进入建筑初步检查

次日 00:35 降级为 GRIP 0，部分解封，团队进场清点损失并启动临时供电部署

典型事故案例 1

影响面与归因：一次园区火灾如何放大为多行业中断

事故影响

云服务	IBM Cloud 报告 Amsterdam 03 设施异常，IBM 正协调受影响客户
高校科研	乌得勒支大学网站与应用登录严重受影响，校内平台 DUB 离线，SURF 成员机构中断
公共交通	乌得勒支省的部分公交与有轨电车调度通信受扰，车载紧急按钮一度失效
公共服务	荷兰商会、水务机构及部分医疗机构出现服务故障
企业服务	TurboSMTP、Emailchef 全部服务一度不可用

对照项 • 阿尔梅勒 FlevoHospital（弗莱福医院） 因采用多数据中心冗余备份，且事故发生后业务倒换顺利，因此未影响医院正常运转。

事故原因

官方结论	起火原因与基础设施受损的确切范围尚未公布，NorthC 与主管部门的技术调查仍在进行
已知事实	火势集中在建筑后部的技术设施区域，涉及应急电源系统与备用发电机
行业关注	早期迹象指向技术设施（UPS / 电池区域），行业普遍强调电池实时监测与超期设备预防性更换
级联效应	多家第三方服务商因核心基础设施集中托管于该园区而整体中断

事故警示与对策建议

① 关键业务集中于单一园区

未采用冗余架构的机构在设施断电后立即失去服务能力，风险被单点放大

对策：核心系统跨园区、跨地域多活容灾，定期切换演练并验证备份可恢复性

② 高等级机房 ≠ 高可用架构

机房有内部冗余，但客户把关键服务集中在单一位置且恢复预案未经验证，风险依然存在

对策：将第三方托管设施的物理风险纳入业务连续性评估，明确可接受中断时长

③ 调度链路与生产同址

公共交通调度中心服务器位于受灾设施且未异地备份，直接导致调度通信与车载紧急按钮失效

对策：关键岗位配置独立通信链路；UPS / 蓄电池在线监测、超期设备预防性更换

典型事故案例 2

CAICT 中国信通院

2026-07-31 • 土耳其全国 • 固网宽带瘫痪

事故基本情况

发生时间 2026 年 7 月 31 日 11:15 起（当地时间）

运营企业 TurkNet，土耳其固网运营商，服务超过 110 万固网用户，主打 GigaFiber 千兆平台

事故分类 设备故障，互联网流量路由系统（BGP 路由）意外故障，流量黑洞

持续时间 约 5 小时；16:16 官方宣布故障已解决，访问逐步恢复

受影响固网用户

110 万

影响严格限定于 TurkNet 自有路由域内；同业运营商与移动网络未受波及，移动电话流量可用

事故经过

11:15

TurkNet 发生全国性网络瘫痪，故障仅影响其固网宽带用户

12:06

Downdetector 已记录 1,878 起报障，NetBlocks 独立确认全国性中断

故障期间

官方 App、在线客户门户与呼叫中心电话线路同步失效，用户失去全部信息渠道

16:16

官方宣布故障已解决，互联网访问逐步恢复；8 月 1 日凌晨全国互联无异常告警

一条错误路由，5 小时内即可把单一运营商的内部配置问题放大为全国性断网，且用户全程没有官方信息渠道。

典型事故案例 2

影响面与归因：单一运营商内部故障为何造成全域瘫痪

事故影响

影响范围 严格限定于 TurkNet 自有路由域内，服务超过 110 万固网用户

未波及同业 TurkTelekom、Superonline、Turkcell、Vodafone TR 未受影响，移动网络基本正常

业务受损 远程办公、企业专线、云应用与 Wi-Fi 通话受影响，部分用户视频会议中断

沟通瘫痪 官方 App 与客服系统同步失效，用户无法通过任何官方渠道获取进展信息

未波及互联 故障未波及国家核心互联节点，属单一运营商内部事故

对外部互联网无影响，但对本网百万级用户却是「全断」。

事故原因

官方定性 「互联网流量路由系统意外故障」，未披露具体根因

明确排除 非海底光缆断裂、非政府网络管制、非大规模网络攻击

直接原因 行业推断：核心路由器路由表转发异常，导致 BGP 路由收敛失败、形成流量黑洞

深层原因 行业推断：错误的路由策略推送或 BGP 属性配置失误，全网路由表被污染

冗余与隔离 行业推断：主备核心路由切换未按预期触发；App 与客服共用内部认证通道

事故警示与对策建议

① 骨干路由冗余不足

单一运营商事故虽未波及国家核心互联节点，但足以影响百万级用户

对策：BGP 策略与配置变更严格执行评审、灰度发布与回退；定期演练主备切换

② 管理平面耦合业务网

事故处置期间企业同时失去对外发声与信息收集能力，客观上延长并放大了社会影响

对策：建设带外管理（OOB）通道，与业务网络物理或逻辑隔离

③ 对外沟通无兜底通道

用户断网的同时无法获取任何官方进展信息，公众不满在信息真空中迅速累积

对策：建立不依赖自身网络的对外信息发布与客服通道

一个分享

2024.02.25 • AT&T 公开信

AT&T 总裁约翰·斯坦基就 2 月 22 日的网络中断事故公开致歉，并表明了对公司发展的信心。

> 这不是我们的第一次网络中断，也不会是我们的最后一次，这就是我们业务的现实。最重要的是我们如何做出反应、调整和改进，以提供客户需要和期望的服务。

—— 约翰·斯坦基 AT&T 总裁



AT&T

February 25, 2024

Addressing the February 22 outage

Thursday was a challenging day for our company. Our purpose is to connect people to greater possibility, and we fell short of what we typically do so well each and every day. I want to share the latest on the network outage we experienced and

Our initial review of the cause of Thursday's outage in execution of an incorrect process used while working investing billions to grow our network and deliver an e experience. This is both a point of pride and a challeng

The outage began in the early hours on Thursday, and our customers were able to access our network as the We prioritized FirstNet service restoration, in line with responders. The remaining customers were reconnect worked hard to successfully normalize the network by

No matter the timing, one thing is clear – we let down of you and your families. For that, we apologize.

For the portion of consumer and small business custo are automatically applying an account credit to compe experienced. Prepaid customers will have options avai are also working closely with our Mid-Market and Ente concerns as those discussions take place.

We all know that our customers receive tremendous v daily cost of our service, and outages sometimes have that may be greater than the face value of the credit. those customers for essentially a full day of service is impact to the business, I believe this approach is fully business objectives we have set for ourselves and our

Whenever a challenging or unexpected event impacts everyone to rise to the occasion and the last few days employees demonstrated expertise under pressure as action to restore service for our customers. Teams acr centers to product, marketing, communications, and t to live up to our commitment to serve customers first

the nation's critical infrastructure providers. I commend the effort and collaboration in this challenging moment, and I am appreciative of all the extra effort and hard work.

Moments like these are a test of resilience. This is not our first network outage, and it won't be our last – unfortunately, it's the reality of our business. What matters most is how we react, adapt, and improve to deliver the service our customers need and expect. Every AT&T customer deserves a connectivity experience they can feel confident in and that's exactly what we're going to deliver. While it is not unexpected to encounter challenges as we enhance and expand our network, we have processes and redundancies in place for a reason. We owe it to our customers and ourselves to do better, and I know that each and every one of you is committed to that goal.

These challenges provide opportunities to identify key learnings that will make us better, and I can tell you that we have already implemented changes to prevent what happened on Thursday. Knowing our plans for growth, resiliency, and customer focus, I am as positive and optimistic about the future as I have ever been. We have North America's largest wireless network and the nation's largest and fastest-growing fiber network. No company is better suited to answer the call for widespread connectivity than AT&T.

Thank you for everything you do to support our customers and move the business forward.

John

© 2024 AT&T Intellectual Property. All rights reserved. AT&T and the Globe logo are registered trademarks of AT&T Intellectual Property.

PART

03

CHAPTER 03

通信网络运行全时域保障体系

构建通信网络运行全时域保障体系

CAICT 中国信通院

现 状

当前工作中，各能力及其内含要素零散存在、各自为战，未系统性构建起保障体系。

目 的

把各家各自为战、协同不足、不成体系的现状，通过底层研究收敛成一套完整体系。

- **行业监管** 完善制度要求，让监管有统一标尺
- **企　业** 提供工作指导，让建设有清晰路径
- **支撑部门** 提供工作方向，让支撑有明确抓手

通信网络运行全时域保障体系 - 理论基础

CAICT 中国信通院

网络运行异常扰动

- 设备设施故障
- 自然灾害
- 人为操作
- 消安事件

外部与内部的随机扰动

网络运行脆弱性

网络自身局限

- 冗余设计不足
- 新技术未经考验
- 规划布局不合理
- 信息存在隔离
- 信息处理缓慢
- 信息沟通不畅

威胁认知不足

- 安全管理意识
- 底线红线思维
- 风险防范意识
- 管理力度有限
- 规章制度缺失
- 监管审批不严

网络运行风险

扰动暴露并利用系统中的脆弱性，从而引发服务中断或质量下降。

全时域保障策略 • 针对性形成三道防线

应急屏障	直接处置已发生的风险事件，快速恢复服务能力	网络故障处置 / 应急通信保障 / 应急服务支撑
免疫屏障	提升设施固有可靠性，削弱扰动对服务的影响	设施抗毁韧性 / 网络架构韧性
预防屏障	系统性预防管理机制，从源头消除脆弱性	扰动预防能力

故障、人为失误等异常扰动暴露并利用系统脆弱性而引发风险；保障策略针对性形成三道防线 —— 从被动响应到主动免疫，再到源头预防，构成闭环防护体系。

通信网络运行全时域保障体系 - 三屏障模型

CAICT 中国信通院

三大屏障协同作用，构建覆盖“事前预防、事中抗扰、事后恢复”的全流程防御体系，共同提升通信网络的可靠性与服务连续性。

预防屏障 PREVENT	降低扰动发生概率	有效	扰动被拦截，网络保持常态运行
		失效	扰动注入系统，进入免疫环节
免疫屏障 IMMUNE	扰动发生时维持服务连续性	有效	服务不中断，业务持续可用
		失效 / 部分失效	服务中断，转入应急环节
应急屏障 EMERGENCY	中断后快速恢复，缩短时长	能力强	高效服务：网络能力与应急通信快速恢复
		能力弱	低效服务：长时间未恢复、应急通信长时间未建立

扰动来源

人为因素、管理因素、产品质量、极端自然灾害、社会突发事件……

预防保障 | **可靠性保障** | **应急保障**

通信网络运行全时域保障体系 - 总体框架



体系以“全时域覆盖”为核心逻辑，由六大核心保障能力构成保障效能的直接载体，形成从风险前置防控到应急处置的完整闭环。

PART

04

CHAPTER 04

网络运行安全保障工作管理思路

管理提升思路

CAICT 中国信通院

企业要筑牢网络运行安全保障“三项基础”

从主要负责人到一线员工，把安全责任、制度规程、教育培训与应急处置落到每一个岗位。

控得住

企业主要负责人

- 全员网络运行责任制
- 网络运行规章制度和操作规程
- 网络运行安全教育和培训计划
- 网络运行事故应急处置预案



抓得紧

运行安全管理人员

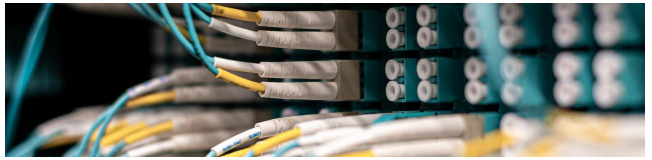
- 规章制度、操作规程和应急处置预案
- 教育和培训
- 应急演练



做得好

企业员工

- 网络运行知识
- 本岗位的操作技能
- 事故预防和应急处置能力
- 严格执行规章制度和操作规程



组织保障 合理、完善的安全管理组织机构搭建

机制保障 责任明确、管理制度体系搭建、应急演练有效……

管理提升思路

CAICT 中国信通院

重视预防：压茬推进监督检查，落实双重预防机制

借鉴事故教训，总结易发问题环节，压茬推进网络运行监督检查；完善双重预防机制 —— 周期性全覆盖推进网络运行风险评估。

压茬推进监督检查

01

开展全行业压茬式电信网络运行安全监督检查

全面深入排查治理各类安全风险隐患，杜绝问题整改不到位、不彻底、虚假整改、死灰复燃等问题，有效防范和遏制重特大事故发生。

02

监督检查与安全考核评价相结合

将网络运行安全情况纳入企业绩效考评指标，压实主体责任，提升管理水平、夯实安全基础。

03

深化精准监督检查，细化检查项目

重点检查同局址、同节点、同路由情况；设备超期、超负载、超容量情况；变更操作管理与容灾倒换演练。

完善双重预防机制

01

扩大评估范围

从 5G 扩展至整个通信网络，涵盖 4G 核心网、IMS，以及近期事故多发的承载网、基础设施、时间同步网等。

02

系统组织评估

制定年度和三年工作规划，在三年内完成覆盖全省通信网络的全面评估。

03

关注新业务风险

探索开展针对通信网络新场景、新业态（车联网等）的风险评估，防控新型业务运行安全风险。

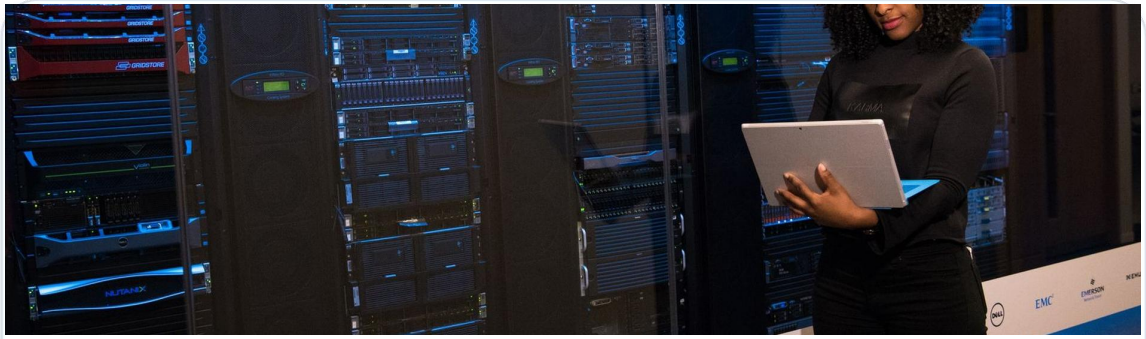
04

关注重大基础设施风险

强化重要通信机房、大型数据中心、通信线路、卫星通信、域名解析、国际通信设施的登记与风险评估。

管理提升思路

建设队伍：全面提升人员能力



监管层面 监管侧能力

01 监管支撑队伍

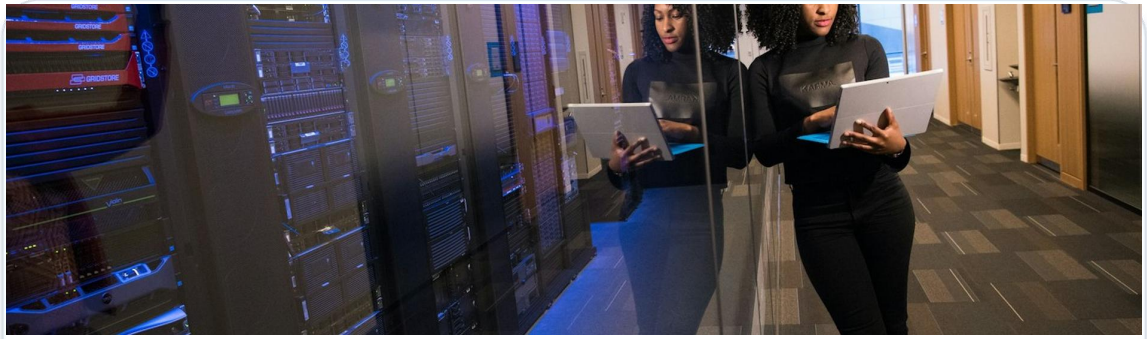
建立专门的网络运行安全监管支撑队伍，更系统、更全面、更细致地协助监管部门做好规划、落实执行。

02 专家库

遴选技术专家、管理专家组建专家库，评估发布网络运行安全态势，指导提升运行安全水平。

03 故障处置指导

牵头处置网络运行安全故障事故，提供技术判断、资源协调与处置指导。



企业层面 企业侧能力

01 专业人员资质评定

全面推进网络运行专业人员资质评定，建立岗位能力的统一基准。

02 行业企业协同

行业、企业协同发力，共享运行经验、典型案例与最佳实践。

03 专业化人才梯队

打造分层分类的专业化人才梯队，让体系运转有人可用、有序接续。

管理提升思路

CAICT 中国信通院

保障网络运行安全，要做到三个坚持

1 坚持预防为主

认清价值

事中响应、事后补救 → 事前预防、风险前置

“事前 1% 的预防胜过事后 99% 的补救”

- 网络运行安全是网络运营企业的“生命线”
- 安全投入不是成本消耗，而是价值投资
- 落实全网络全生命周期管理

2 坚持高位推动

有力监管

运动式管理 → 系统式管理

- 建立系统化的多维度监管机制
- 聚焦关键设备、高危操作、极端场景，推动风险评估持续开展
- 开展压茬式监督检查，建立监督检查考评制度

3 坚持与时俱进

持续创新

基础电信企业 → 基础电信企业 / 增值电信企业 / 大型互联网平台

信息传递媒介 → 千行百业（传统、新兴）

- 传统行业数字化、智能化改造对网络运行安全要求不断提升
- 网络运行安全性需与物联网、工业互联网、车联网等新兴业态相适配

“安全依赖多层次、差异化的防御体系，而非单一措施。”

CAICT 中国信通院

感谢观看

THANKS

www.caict.ac.cn