

网络运行安全完整性等级确定方法研究



Research on Method for Determination of Network Operation Safety Integrity Level

路晔绵/Lu Yemian, 郑梦青/Zheng Mengqing,
吴荣春/Wu Rongchun, 张治兵/Zhang Zhibing,
王晓颖/Wang Xiaoying

(中国信息通信研究院, 中国 北京 100191)
(China Academy of Information and Communications Technology, Beijing
100191, China)

DOI: 10.12142/ZTETJ.202604011

网络出版地址: <https://link.cnki.net/urlid/34.1228.TN.20260901.1347.004>

网络出版日期: 2026-08-28

收稿日期: 2025-09-25

摘要: 设备故障或系统失效经常引发大面积断网或业务暂停, 亟需引入安全完整性体系和新的安全完整性等级确定方法。通过分析总结现有多个领域中的安全完整性定级方法, 结合信息通信领域特点, 提出了网络运行安全完整性等级(NSIL)确定方法。通过实际案例分析, 验证了在信息通信领域引入安全完整性体系并确定关键设备或系统的NSIL等级的必要性, 为后续建立完善的信息通信领域网络运行安全完整性体系提供理论基础。

关键词: 网络运行事故; 安全完整性等级; 故障; 失效

Abstract: Equipment failures or system outages frequently cause large-scale network disruptions or service interruptions, underscoring an urgent need to introduce the safety integrity system and a new method for determining safety integrity levels. By analyzing and summarizing the existing determination method of Safety Integrity Level in multiple fields, combining with the characteristics of the information and communication field, a method for determining the network operation safety integrity level (NSIL) is proposed. Through practical case analysis, the necessity of introducing the safety integrity system in the information and communication field and determining the NSIL level of key equipment or systems is verified, providing a theoretical basis for establishing the well developed network operation safety integrity system in the information and communication field in the future.

Keywords: network operation accident; safety integrity level; fault; failure

引用格式: 路晔绵, 郑梦青, 吴荣春, 等. 网络运行安全完整性等级确定方法研究 [J]. 中兴通讯技术, 2026, 32(4): 72-78. DOI: 10.12142/ZTETJ.202604011

Citation: Lu Y M, Zheng M Q, Wu R C, et al. Research on method for determination of network operation safety integrity level [J]. ZTE technology journal, 2026, 32(4): 72-78. DOI: 10.12142/ZTETJ.202604011

数字经济时代, 信息通信网络已成为支撑社会正常运转的重要基石。然而近年来, 由网络设备、电源系统、空调系统等关键设备或系统的故障及失效引发的网络运行事故频发, 常常造成大范围网络中断或重要服务异常, 严重影响日常生产生活。目前, 在工业控制、机械、汽车等领域, 已广泛应用功能安全及安全完整性体系来应对故障和失效导致的安全风险, 其有效性已得到实际验证。因此, 有必要在信息通信领域引入安全完整性体系, 明确各类设备和系统应具备的安全功能及其安全完整性等级, 并达到相应等级的安全完整性要求, 以降低因设备或系统故障及失效导致的网络

运行事故概率。其中, 如何确定安全完整性定级方法是应用安全完整性体系时首要解决的问题。然而, 现有安全完整性定级方法主要基于故障失效风险对人身安全的影响划分等级, 而信息通信领域的故障和失效问题在绝大多数情况下并不会对人身安全构成威胁, 因此无法直接适用现有的方法。

本文通过分析工业控制、机械、汽车、轨道交通等领域中安全完整性等级的确定方法, 借鉴其设计理念, 并结合信息通信领域自身特点, 提出网络运行安全完整性等级(NSIL)的定级方法, 为后续构建网络运行安全完整性体系奠定基础。同时, 结合实际案例, 展示NSIL定级方法的应

用,验证了在信息通信领域引入安全完整性体系的必要性以及该方法的合理性。

1 技术现状

安全完整性属于功能安全领域的概念,在国际标准 IEC 61508-4^[1](对应中国标准 GB/T 20438-4^[2])中提出,指在规定条件和规定时间内,系统成功执行安全功能的概率。安全完整性与信息安全领域中的“完整性”极易混淆,后者在信息安全术语标准 GB/T 25069^[3]中被定义为“准确和完备的性质”,与安全完整性分属两个不同领域,是完全独立的概念。

安全完整性等级(SIL)是在系统整体安全生命周期框架下构建的安全度量体系,是衡量安全系统降低故障或失效风险能力的有效途径。SIL等级越高,表明因系统故障或失效引发事故的概率或影响越低。通常情况下,需通过对系统进行危险与风险分析,以确定其所应实现的安全功能及对应的安全完整性等级。

作为安全完整性体系的基础标准,IEC 61508-5^[4](对应中国标准 GB/T 20438-5^[5])给出了几种基于定量和定性方法的安全完整性等级确定方法。周荣义等^[6]对包含这些方法在内的多个定级方法进行了对比分析,并给出了选择建议。总体而言,定量方法主观性最小,但需要大量已有故障数据作为计算支撑,在实际应用中难以获得,且系统性失效无法进行量化计算。因此,实践中使用较多的仍是定性方法,其中风险图方法是目前应用最为广泛的方法。

风险图方法选取危险事件的后果(C)、人员暴露于危险区域的频率/时间(F)、避免危险事件的可能性(P)以及不希望事件发生的概率(W)作为定级参数,对每个参数进行分级,并通过分支图确定不同参数等级组合所对应的SIL等级。该方法通过多因素综合分析,能较好地反映故障和失效的危险程度,因此被许多领域借鉴和采用。例如,过程工业领域功能安全标准 IEC 61511-3^[7](对应中国标准 GB/T 21109.3^[8])基本沿用了IEC 61508中的风险图方法,仅对参数赋值进行了校准;机械领域标准 IEC 62061^[9](对应中国标准 GB 28526^[10])选择了与风险图方法类似的参数,但对完整性等级的推导方式作了修改;而机械领域标准 ISO 13849^[11](对应中国标准为 GB/T 16855.1^[12])则在风险图方法基础上删去W参数,从严定级,仅考虑最坏情况下发生危险事件的可能性。

汽车领域根据其产品特点,在标准 ISO 26262-3^[13](对应中国标准 GB/T 34590.3^[14])中定义了自身的安全完整性等级(ASIL)定级方法,考虑3个参数,即危害的严重性等级(S)、暴露在危害中的概率(E)和危害的可控性(C)。在

参数赋值设计中,ASIL定级方法充分考虑了汽车领域应用场景的独特性,使定级结果更具适用性,例如以驾驶员的可控性来评估危害可控性。在完整性推导阶段,ASIL定级方法采用三元素矩阵划分方式,ASIL等级随3个参数等级的递增而逐级升高。

轨道交通领域功能安全相关的标准中并未明确推荐SIL定级方法,但产业界和学术界均对此展开了广泛研究。欧洲轨道交通技术项目 MODSafe 提出了一个半定量的SIL定级方法——EPC方法^[15]。该方法中,安全功能失效导致后果的严重程度(THR)作为原始风险数值,而风险群体成员(如乘客)暴露的可能性(E)、减少事故的可能性(P)和减轻后果的可能性(C)3个参数分别对应其他情况或措施对原始风险的降低效果。通过将THR值除以E、P、C3个参数的值,可计算安全相关系统所需达到的风险降低能力,进而对应至SIL等级。EPC方法属于半定量方法。

在学术界,张冬梅^[16]、杨娟^[17]、李葛亮^[18]、白春光^[19]等提出了类似的方法。俞杭华^[20]和刘亚妮^[21]等对不同SIL定级方法在轨道交通领域的适用情况进行了分析,其中后者还通过实际案例验证了EPC方法与风险图方法定级结果的一致性。

以上几个领域的安全完整性定级方法在参数选择上具有较高的相似性,均考虑了危险事件的后果、人员暴露于危险区域的频率/时间,以及避免危险事件的可能性3个参数。然而,现有方法在评估危险事件后果时,均从对人身安全构成威胁的角度出发,而网络运行事故在绝大多数情况下并不会危及人身安全,而是影响其上承载的业务,进而波及社会生产生活。由于影响对象不同,现有的安全完整性定级方法无法直接应用于信息通信领域,因此有必要设计针对网络运行安全的、具有领域特色的安全完整性等级确定方法。

2 NSIL定级方法设计

基于上述对工业控制、机械、汽车等领域安全完整性定级方法的分析,定级方法的设计需从3个层面展开:首先选择合适的定级参数,然后根据各领域特点确定各参数的赋值,最后明确不同参数赋值所对应的安全完整性等级,即完整性推导规则。NSIL定级方法也将遵循这一框架进行设计。

2.1 定级参数选择

从各领域的安全完整性定级方法可以看出,安全完整性的定级通常需考虑设备或系统故障或失效时可能造成的危害后果严重性、影响对象暴露于危险的可能性、避免危险事件

发生的可能性,以及减轻后果的可能性等因素。

在其他领域中,危险事件的影响客体是人体,危害后果为人员伤亡;而在信息通信领域,危险事件的影响客体通常并非人体,所造成的危害后果体现为业务性能下降或中断后对社会、经济等方面产生的影响。由于信息通信网络上承载的业务类型多样,不同类型的业务对社会、经济的影响程度各异,因此需要结合业务类型与故障危害类型来评估受影响业务对社会的危害程度,同时根据目标业务的用户范围评估危险事件可能的影响范围。基于此,NSIL定级方法可将危害后果严重性因素细化为业务重要性(I)、故障危害类型(T)和业务影响范围(S)3个参数。

对于影响对象暴露在危险中的可能性因素,由于依托信息通信网络运行的业务均不间断持续运行,网络发生故障时其上业务必然受到影响,无须分级别讨论,因此在NSIL定级方法中不再将该因素纳入考虑范围。

对于避免危险事件发生的可能性和减轻危害后果的可能性因素,信息通信网络建设中通常会部署各类措施以预防危险事件发生或减轻其后果,例如通过异地备份帮助业务从机房故障中快速恢复。然而,信息通信领域中许多措施既能一定程度上避免危险事件发生,也能减轻危害后果。为防止重复考虑这些措施而影响完整性推导结果的合理性,我们将上述两个因素合并为一个因素进行考虑,并根据具有这两类效果的相互独立措施的数量对该因素进行分级。

综上所述,在网络运行安全完整性等级(NSIL)定级方法中,将考虑以下两类共4个参数:

- 1) 危害后果严重程度(C),细分为3个子参数:业务重要性(I)、业务影响范围(S)、故障危害类型(T);
- 2) 避免危险和减轻后果的可能性(P)。

2.2 参数赋值设计

2.2.1 业务重要性(I)赋值设计

信息通信网络承载种类丰富的业务。当发生网络故障造成各类业务中断或者业务性能劣化时,不同业务对社会和经济发展产生的影响亦有所不同。因此,需要结合业务本身的属性,完成业务重要性的等级赋值。本文参考《电信网络运行监督管理办法》^[22]中对网络运行事故的分级规则,设计业务重要性(I)的赋值规则,具体如表1所示。

2.2.2 业务影响范围(S)赋值设计

业务影响范围可从两个维度衡量:一是根据行政区域范围衡量,适用于直接搭载在运营商网络上运行的业务,如基础电信业务(语音通话等)及区域性党政机关业务等;二是

根据影响用户数量衡量,适用于运行于上层互联网的业务,如社交应用、电商服务平台等。这类业务通常部署在互联网数据中心,可能面向全国提供服务,但其实际影响范围仅限于使用该类业务的目标用户。不同业务的用户数量差异悬殊,从几万到上亿不等,此时若采用行政区域范围衡量,易产生较大偏差,因此宜使用影响用户数量作为衡量依据。

本文参考《电信网络运行监督管理办法》中对网络运行事故的分级规则,确定行政区域范围的划分方法;依据《互联网平台分类分级指南(征求意见稿)》^[23],确定影响用户范围的划分标准。在用户数量分级上,本文将互联网超级平台用户数量(5亿)的十分之一作为影响用户范围的最高等级,后续依次递减。最终设计业务影响范围(S)的赋值规则如表2所示。

由于互联网业务广泛采用异地备份,单点故障未必会导致其原有影响范围内的全部用户受损,因此,在明确知晓业务已实现异地备份的情况下,可将业务影响范围等级下调一个级别。

2.2.3 故障危害类型(T)赋值设计

信息通信网络设备或系统的故障或失效对业务造成的危害类型相对集中,主要可从响应性能下降和业务中断两个方面加以考察。

然而,并非所有业务都对性能下降敏感。本文从网络运行事故所引发的社会、经济影响角度出发,仅关注性能下降

表1 业务重要性(I)参数赋值规则

赋值	说明
I3	党政领导机关业务,电力、燃气、水利、交通、公共服务、金融等基础民生业务
I2	固话及移动电话语音通信业务、卫星通信业务、国际通信业务
I1	短消息业务、数据业务及其他增值业务,一般行业业务(不属于I3范围的其他行业业务,如线上教育)

表2 业务影响范围(S)参数赋值规则

赋值	说明
S4	1)两个及以上省(或自治区、直辖市)的用户业务受到影响,或全国的用户业务受到影响 2)影响超过5 000万用户
S3	1)两个及以上地市的用户业务受到影响,或一个省(或自治区、直辖市)的用户受到影响 2)影响超过500万用户
S2	1)两个及以上县(区)的用户业务受到影响,或一个地市的用户受到影响 2)影响超过100万用户
S1	1)一个县(区)的用户业务受到影响 2)影响超过20万用户

超过50%、显著影响业务质量的情形。将性能下降比例阈值设为50%，是考虑到若存在一个负载均衡设备/系统或冗余备份设备/系统，当一个设备/系统因故障停止运行时，所能造成的最坏影响即为性能损失一半的情况。

对于业务中断，考虑到并非所有设备/系统故障都会立即引起中断，当故障经过一段时间后才导致中断时，系统或操作人员在中断发生前有机会发现异常并采取补救措施。因此，本文将中断类型分为延时中断和立即中断两种情况。此外，对于时效性要求较高的业务，显著的性能下降也可按延时中断处理。

另外，由于业务影响范围(S)的赋值设计中已纳入异地备份的修正因素，故在故障危害类型(T)的分级设计中不再重复考虑该因素，而是以业务无异地备份作为不同级别赋值的前置假设条件。

本文设计的故障危害类型(T)赋值规则如表3所示。

2.2.4 避免危险和限制伤害的可能性(P)分级设计

信息通信网络建设中通常会部署各类措施以预防危险事件发生或减轻其后果，相互独立的安全措施数量直接影响这些措施综合产生的避免或减轻效果。因此，本文根据具备明确效果的独立安全措施数量来确定避免危险和减轻后果的可能性(P)，并设计其赋值规则如表4所示。该设计与轨道交通领域EPC方法的理念相符。

表3 故障危害类型(T)参数赋值规则

赋值	说明
T3	在不考虑其他保护措施(例如业务异地备份)存在的前提下,故障发生后立刻造成业务中断(或无法正常提供服务)
T2	1)在不考虑其他保护措施存在的前提下,故障发生一段时间后才可能造成业务中断(或无法正常提供服务) 2)高时效要求的业务,其性能显著下降,显著影响业务质量
T1	性能下降超过50%,显著影响业务质量

表4 避免危险和限制伤害的可能性(P)参数赋值规则

赋值	描述	判定
P1	不可能	没有额外的措施来减轻危害变成事故的概率或避免风险业务可能遭受某种危害后果的伤害
P2	有一定可能	只有一种措施能明确地降低危害演变成事故的概率或避免风险业务遭受某种危害后果的伤害
P3	有较大可能	有两种及以上独立的措施能明确地降低危害演变成事故的概率或避免风险业务遭受某种危害后果的伤害

2.3 完整性推导

在完整性推导阶段，本文首先根据业务重要性(I)、业务影响范围(S)和故障危害类型(T)推导出危害后果严重程度(C)，再结合避免危险和减轻后果的可能性(P)推导出最终的NSIL等级。NSIL与SIL等级保持一一对应关系。

2.3.1 危害后果严重程度(C)推导

危害后果严重程度(C)参考《电信网络运行监督管理办法》划分为C1至C4共4个等级；同时，为提升场景覆盖能力，增设C0等级以涵盖可能造成较低危害的情形。各等级的具体描述如表5所示。

在根据业务重要性(I)、业务影响范围(S)和危害类型(T)推导危害后果严重程度(C)时，本文采用三元素矩阵的推导方式，以尽可能保证推导结果符合实际情况。相应推导规则如表6所示。

鉴于同一信息通信网络上可能同时运行多个重要业务，一个设备或系统故障可能同时影响多个业务，因此有必要对该场景下的危害后果严重程度进行修正，需综合考虑受影响业务的数量及其各自的重要程度等级，以判定最终等级。

假设同时影响的业务数量为 n ，危害后果严重程度等级

表5 危害后果严重程度(C)等级描述

危害后果严重程度等级(C)	描述
C0	对公共利益、社会经济和秩序造成较低危害
C1	对公共利益、社会经济和秩序造成一般危害
C2	对公共利益、社会经济和秩序造成较大危害
C3	对公共利益、社会经济和秩序造成重大危害
C4	对公共利益、社会经济和秩序造成特别重大危害

表6 危害后果严重程度(C)推导规则

业务重要性(I)	业务影响范围(S)	故障危害类型(T)		
		T1	T2	T3
I1	S1	--	--	C1
	S2	--	--	C1
	S3	--	C1	C2
	S4	C1	C2	C3
I2	S1	--	--	C1
	S2	--	C1	C2
	S3	C1	C2	C3
	S4	C2	C3	C4
I3	S1	--	C1	C2
	S2	C1	C2	C3
	S3	C2	C3	C4
	S4	C3	C4	C4

最高的业务等级为 C_x (其中 x 可选值为 1、2、3、4, 为危害后果严重程度 C 的具体等级数值, 下文 y 、 z 、 m 同), 次高为 C_y , 第三高为 C_z , 整体严重程度等级为 C_m , 其中需满足 $1 \leq z \leq y \leq x \leq 4$, 则修正规则如表 7 所示。

2.3.2 NSIL 推导

在获得危害后果严重程度 (C) 的等级后, 即可结合避免危险和减轻后果的可能性 (P) 的赋值推导出最终的 NSIL 等级, 具体推导规则如表 8 所示, 其中 NSIL 4 为最高等级。

NSIL 1—NSIL 4 可对应 IEC 61508 中 SIL 1—SIL 4, 适用相关等级的安全完整性要求。NSIL 0 可进行质量管理和基本的安全维护要求。

3 NSIL 定级方法验证

本文以某数据中心空调子系统为例, 结合 NSIL 定级方法与 IEC 61508 中的安全完整性要求, 对该系统进行安全分析, 识别其中的安全隐患, 从而验证 NSIL 定级方法的合理性与必要性。

根据 Uptime 发布的 2024 年数据中心运行事故原因统计报告^[24], 空调系统故障已成为网络运行事故的第二大诱因, 且易造成大面积影响。对空调系统开展安全完整性定级与要求制定, 对于提升数据中心网络运行安全能力具有重要意义。然而, 其他领域的安全完整性定级方法仅从人身安全角度出发, 难以反映空调系统故障对数据中心网络运行安全能力的影响。因此, 有必要采用本文提出的 NSIL 定级方法对该数据中心的空调子系统进行分析。

该数据中心承载了多个知名互联网业务, 如电商平台、

社交平台等。数据中心中央空调配备 8 台冷机, 其中 2 台既可用于制冷, 也可用于蓄冷。冷冻水系统管道与蓄冷池管道在与两用冷机连接时存在一段共用管道, 需要通过几个阀门的启闭来控制当前水系统与两用冷机的连接状态。该架构的简化示意图如图 1 所示, 其中 F1、F2、F3、F4 为控制冷冻水系统管道与蓄冷池管道隔离的关键阀门, 图中箭头标注了各管道的水流方向。空调 BA 系统在下发制冷或蓄冷指令时, 会相应调整阀门的启闭状态, 以使管道连接满足当前工作模式的需求。

在该数据中心空调子系统中存在一个安全隐患: 若阀门因故障未按 BA 系统指令正确启闭, 可能导致冷冻水系统管道与蓄冷池管道相连, 造成冷冻水流失、空调系统停机、机房温度升高, 最终引发服务器停机。因此, 需实现一项安全功能 (目标安全功能), 即在启动制冷或蓄冷模式前及运行期间, 对各个关键阀门的启闭状态进行检查, 以确保系统始终运行在正确状态。由于制冷、蓄冷模式由 BA 系统触发, 且 BA 系统可查看并控制各阀门状态, 因此由 BA 系统实现该安全功能的执行逻辑, 将阀门状态检查纳入制冷、蓄冷模式的启动流程中。

下面本文将使用所提方法分析 BA 系统的目标安全功能需达到的 NSIL 等级, 并对照 IEC 61508 中对应 SIL 等级的软件安全要求, 检验 BA 系统在设计实现过程中是否已应用相应的技术和措施。

3.1 NSIL 定级推导

1) 危害后果严重程度 (C) 推导

表 7 危害后果严重程度(C)修正规则		
参数取值		C_m 取值
$n = 2$	$x < 4$ 且 $x = y$	$C_m = C(x + 1)$
$3 \leq n < 10$	$x < 4$ 且 $x = y$, 或 $x < 4$ 且 $y = z = (x - 1)$	
$n \geq 10$	$x < 4$	
其他情况		$C_m = C_x$

表 8 NSIL 推导规则			
危害后果严重程度等级(C)	避免危险和减轻后果的可能性(P)		
	P3	P2	P1
C0	NSIL 0	NSIL 0	NSIL 0
C1	NSIL 0	NSIL 0	NSIL 1
C2	NSIL 0	NSIL 1	NSIL 2
C3	NSIL 1	NSIL 2	NSIL 3
C4	NSIL 2	NSIL 3	NSIL 4

NSIL: 网络运行安全完整性等级

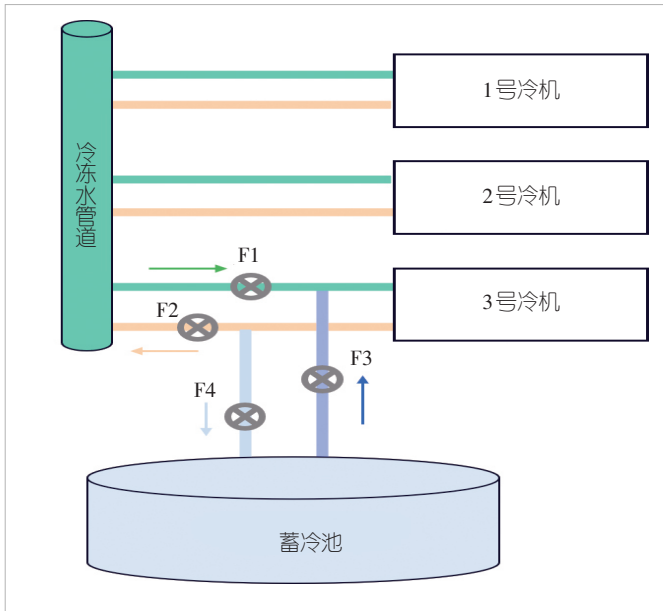


图1 某数据中心空调系统部分架构图

该数据中心承载多个业务,其中最为关键的包括一个知名电商平台和两个知名社交平台。各业务对应的危害后果严重程度推导分别如下:

(1) 知名电商平台业务的危害后果严重程度推导

在业务重要性方面,该电商业务属于一般行业业务,依据表1取值为I1。在业务影响范围方面,该电商平台在本地数据中心承载的业务为全国性业务,且用户数量超过8 000万,依据表2取值为S4。在故障危害类型方面,该安全隐患导致空调系统停机,一段时间后机房温度升高,服务器因过热宕机,进而引发业务中断,依据表3取值为T2。根据表6, I1、S4、T2组合对应的危害后果严重程度为C2,即前述故障对该知名电商平台业务造成的危害后果严重程度为C2。

(2) 知名社交平台业务的危害后果严重程度推导

两个社交平台业务同属一家公司,情况相似,此处以其中一个为例进行推导。

在业务重要性方面,社交业务属于一般行业业务,依据表1取值为I1。在业务影响范围方面,该社交平台在本地数据中心承载的业务为全国性业务,用户数量超过1亿,依据表2取值为S4;同时,该公司的社交平台业务均存在异地备份,因此将影响范围等级修正为S3。在故障危害类型方面,与电商平台案例一致,依据表3取值为T2。根据表6, I1、S3、T2组合对应的危害后果严重程度为C1。另一社交平台业务情况相同,危害后果严重程度同为C1。

(3) 总体危害后果严重程度推导

由于存在1个C2等级的业务和2个C1等级的业务,因此根据表7中所示的修正规则, $n=3$, $x=2$, $y=z=1$, $C_m=C(x+1)=C3$ 。即该数据中心空调子系统BA系统的总体危害后果严重程度(C)至少为C3。

2) 避免危险和限制伤害的可能性(P)判定

该数据中心配有冰块降温措施,可在空调系统报警后延长服务器过热宕机前的响应时间,有利于及时排查故障,提高阻止事故发生的可能性,降低危害演变为事故的概率。因此,依据表4,避免危险和减轻后果的可能性等级确定为P2。

3) NSIL判定

根据表8, C3、P2对应的NSIL等级为NSIL 2,即该数据中心空调子系统BA系统的目标安全功能需至少达到NSIL 2等级要求。

3.2 安全分析

IEC 61508-3^[25]对软件安全生命周期各环节应采取的技术和措施进行了详细介绍。受篇幅所限,本文以软件模块测试环节中的相关要求为分析对象。

在本案例中,BA系统需实现的安全功能与异常检测相关,因此选取SIL 2(对应NSIL 2)动态分析和测试中的“根据错误推测执行测试用例”要求作为切入点。根据IEC 61508-3及IEC 61508-7^[26]中的相关解释,该要求在测试用例设计时需考虑哪些特殊值或值的组合容易出错,并据此设计测试用例,以检验系统是否能正确处理这些异常情形。

对应本案例,根据图1所示的架构图,BA系统在实现功能时需考虑F1、F2、F3、F4这4个阀门的不同启闭组合,识别其中会导致不安全状态的组合,并在启动制冷、蓄冷模式前检查是否存在此类组合,进行相应处理;在产品测试验证环节,设计的测试用例也应覆盖所有不安全状态组合,以检验BA系统是否能正确处理。

经分析,在实际实现中,BA系统在启动蓄冷模式前会首先检查F1、F2阀门状态,确保两个阀门均关闭再启动蓄冷模式。然而,由于编程疏忽,BA系统实际实现的逻辑却变为:仅当F1、F2中有一个处于关闭状态时,即判断为安全状态,从而允许启动蓄冷模式。同时,在测试验证阶段也未考虑所有异常情况的检测,导致该安全隐患未被发现和处理。在某次BA系统启动蓄冷模式时,F1阀门意外处于开启状态,BA系统未能检测到该异常,正常执行蓄冷操作。蓄冷命令下达后,冷冻水系统与蓄冷池系统连通,导致冷冻水流失,空调系统停机,服务器过热宕机,进而造成该数据中心承载的业务中断,产生了严重的社会影响。

由此可见,在信息通信领域引入安全完整性体系,明确各安全功能的安全完整性等级及对应等级所应采取的技术和措施,将有助于提前发现安全隐患,提高信息通信网络运行环境的安全性,降低网络运行事故发生的概率。

4 结束语

本文分析了在信息通信领域引入安全完整性体系的必要性。通过分析过程工业、机械、汽车、轨道交通等领域的安全完整性定级方法,并结合信息通信领域自身特点,提出了NSIL定级方法。结合实际案例,验证了在信息通信领域引入安全完整性体系的必要性以及本文所提NSIL定级方法的合理性。

NSIL定级方法的提出仅为安全完整性体系在信息通信领域应用的第一步。文中的案例分析借鉴了IEC 61508中的安全完整性要求,但该标准主要面向工业控制领域,面对的系统相对简单且封闭,部分技术和措施并不完全适用于信息通信领域的设备和系统。因此,后续仍需结合信息通信领域的特色,制定网络运行安全完整性体系标准,明确各NSIL等级对应的技术和措施要求。

参考文献

- [1] IEC 61508-4-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - part 4: definitions and abbreviations [S]
- [2] GB/T 20438.4-2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语 [S]
- [3] GB/T 25069-2022 信息安全技术 术语 [S]
- [4] IEC 61508-5-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - part 5: examples of methods for the determination of safety integrity levels [S]
- [5] GB/T 20438.5-2017 电气/电子/可编程电子安全相关系统的功能安全 第5部分:确定安全完整性等级的方法示例 [S]
- [6] 周荣义, 钟岸, 任竟丹, 等. 安全系统安全完整性等级确定方法比较研究 [J]. 中国安全生产科学技术, 2014, 10(3): 67-73. DOI: 10.11731/j.issn.1673-193x.2014.03.011
- [7] IEC 61511-3-2016 Functional safety - safety instrumented systems for the process industry sector - part 3: guidance for the determination of the required safety integrity levels [S]
- [8] GB/T 21109.3-2007 过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南 [S]
- [9] IEC 62061 CORR 1-2015 Safety of machinery - functional safety of safety-related electrical, electronic and programmable electronic control systems (edition 1.2) [S]
- [10] GB 28526-2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全 [S]
- [11] ISO 13849-1-2015 Safety of machinery - safety-related parts of control systems - part 1: general principles for design (third edition) [S]
- [12] GB/T 16855.1-2018 机械安全 控制系统安全相关部件 第1部分:设计通则 [S]
- [13] ISO 26262-3-2018 Road vehicles - functional safety - part 3: concept phase (second edition) [S]
- [14] GB/T 34590.3-2022 道路车辆 功能安全 第3部分:概念阶段 [S]
- [15] European Commission. Analysis of safety requirements for MODsafe continuous safety measures and functions [EB/OL]. (2011-01-21) [2025-03-20]. http://www.modsafe.eu/fileadmin/documents/deliverables/DEL_D4_2_UITP_WP4_110121_V2_0.pdf
- [16] 张冬梅, 刘伟. 基于风险矩阵的轨道交通车辆安全完整性等级分析 [J]. 城市轨道交通研究, 2020, 23(8): 62-65. DOI: 10.16037/j.1007-869x.2020.08.015
- [17] 杨娟, 张小林. 基于EPC因子的有轨电车信号系统安全完善度等级(SIL)评估 [J]. 城市轨道交通研究, 2018, 21(4): 57-60+65. DOI: 10.16037/j.1007-869x.2018.04.014
- [18] 李葛亮, 刘明, 吕远斌. 城市轨道交通列车关键子系统的安全完整性等级分析 [J]. 城市轨道交通研究, 2021, 24(7): 98-101. DOI: 10.16037/j.1007-869x.2021.07.021
- [19] 白春光. 基于安全完整性级别分析的全自动驾驶地铁列车安全功能设计 [J]. 铁道技术监督, 2021, 49(4): 53-57
- [20] 俞杭华, 胡宗福, 薛小平. 城市轨道交通信号系统安全完整性研究 [J]. 大连交通大学学报, 2008, 29(6): 34-39
- [21] 刘亚妮, 王大平, 李梁, 等. 轨道车辆常见安全完整性等级确定方法研究 [J]. 电力机车与城轨车辆, 2023, 46(2): 108-112. DOI: 10.16212/j.cnki.1672-1187.2023.02.023
- [22] 电信管理局. 关于印发《电信网络运行监督管理办法》的通知 [EB/OL]. (2009-05-12) [2025-11-20]. https://www.miit.gov.cn/jgsj/xgj/gzzd/art/2020/art_01e36db302234d8b8b460e92a9889540.html
- [23] 网络交易监管司. 互联网平台分类分级指南(征求意见稿) [EB/OL]. (2021-10-29) [2025-11-28]. https://www.samr.gov.cn/cms_files/filemanager/1647978232/attach/20233/P020211029613134705.doc
- [24] Uptime Institute. Annual outage analysis 2025 [EB/OL]. (2025-05-06) [2025-11-20]. <https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2025>
- [25] IEC 61508-3-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - part 3: software requirements [S]
- [26] IEC 61508-7-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - part 7: overview of techniques and measures [S]

作者简介



路晔绵, 中国信息通信研究院高级工程师; 主要从事智能终端/信息通信设备网络安全、网络运行安全等方面的研究和测试评估工作; 参与制定国家标准2项, 牵头制定通信行业标准和团体标准14项, 参与制定行标和团标25项, 发表论文6篇, 拥有专利2项、软著1项。



郑梦青, 中国信息通信研究院工程师; 主要从事网络运行安全、网络安全、信息通信网络检测认证相关研究; 牵头制定通信行业标准和团体标准4项, 发表论文3篇, 拥有专利1项。



吴荣春, 中国信息通信研究院工程师; 主要从事网络安全研究和攻防测试评估相关工作; 参与多项安全领域国家重点研究项目, 在设备安全检测、网络安全评估、渗透攻防测试等领域拥有丰富经验; 参与编写国家标准5项、电力行业标准2项、通信行业团体标准6项, 牵头完成重点重大课题10余项, 发表论文6篇, 拥有专利2项。



张治兵(通信作者), 中国信息通信研究院泰尔系统实验室副总工, 高级工程师, 同时担任电信终端产业协会(TAF)网络设备技术与安全技术组组长、中国通信标准化协会(CCSA)网络关键设备工作组组长; 长期从事通信安全领域研究工作, 在网络运行安全与通信安全生产、网络与信息安全、通信产品检验检测等方面有多项研究成果; 牵头研究制定国家标准5项、通信行业标准和团体标准32项, 拥有发明专利4项, 发表论文15篇, 出版专著2项。



王晓颖, 中国信息通信研究院工程师; 主要从事信息通信行业安全生产、网络运行安全等研究工作; 参与通信网络相关科研课题5项, 发表论文2篇。