

ICS 45.020
S 62

TB

中华人民共和国铁道行业标准

TB/T 3482—2017

铁路车站计算机联锁安全原则

Computer based interlocking safety principles

2017-09-29 发布

2018-04-01 实施

国家铁路局 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总则 2

5 系统及硬件 3

6 软件 5

7 通信接口 6

8 继电接口 6

9 电子执行单元 7

10 其他要求 7

附录 A(规范性附录) 主要危害、安全功能和安全相关操作 8

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由北京全路通信信号研究设计院集团有限公司归口。

本标准起草单位：北京全路通信信号研究设计院集团有限公司、中国铁道科学研究院通信信号研究所、北京交大微联科技有限公司、卡斯柯信号有限公司。

本标准主要起草人：邱兆阳、张利峰、韩安平、黄翌虹、张松涛、季志均、张程。

铁路车站计算机联锁安全原则

1 范围

本标准规定了计算机联锁系统设备功能安全的原则要求,包括总则、系统及硬件、软件、通信接口、继电接口、电子执行单元及其他要求。

本标准适用于计算机联锁系统的研究、设计、制造。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 24339.1 轨道交通 通信、信号和处理系统 第1部分:封闭式传输系统中的安全相关通信(GB/T 24339.1—2009,IEC 62280-1:2002,IDT)

GB/T 24339.2 轨道交通 通信、信号和处理系统 第2部分:开放式传输系统中的安全相关通信(GB/T 24339.2—2009,IEC 62280-2:2002,IDT)

GB/T 28808—2012 轨道交通 通信、信号和处理系统 控制和防护系统软件(IEC 62279,IDT)

GB/T 28809—2012 轨道交通 通信、信号和处理系统 信号用安全相关电子系统(IEC 62425,IDT)

TB/T 3027 铁路车站计算机联锁技术条件

3 术语和定义

下列术语和定义适用于本文件。

3.1

危险侧输出 **dangerside output**

联锁计算机产生危及行车安全的输出。

[TB/T 3027—2015,定义 3.6]

3.2

危害 **hazard**

可能导致事故的一种状况。

[GB/T 28809—2012,定义 3.1.20]

3.3

非置信 **non-trusted**

没有专门的安全性预防措施。

[GB/T 24339.1—2009,定义 3.7]

3.4

安全相关操作 **safety related operation**

在人机对话层进行的某些操作,联锁的防护功能不存在或者减弱,错误进行安全相关操作,会危及行车安全。进行这些操作时,操作员需要对安全负责。

3.5

安全功能 **safety function**

计算机联锁设备中,失效会导致危险侧输出的功能。

3.6

随机故障 random fault

无法预测其发生的故障。

[GB/T 28809—2012, 定义 3.1.37]

3.7

安全完整性 safety integrity

在所有规定的条件和规定的运行环境下以及规定的时间内,安全相关系统完成指定的安全功能的能力。

[GB/T 28809—2012, 定义 3.1.48]

3.8

故障—安全 fail-safe

结合在产品内的一种观念,即发生失效事件时产品导向或维持在安全状态。

[GB/T 28809—2012, 定义 3.1.15]

3.9

组合式故障—安全 composite fail-safe

每个安全相关功能至少由两个对象来执行,各对象之间应相互独立,以避免共因失效。只有当必要数量的对象取得一致时,才允许进行非限制行为。应能检测出一个对象中的危害故障并在足够短的时间内加以拒绝,以避免第二个对象发生相同的故障。

3.10

反应式故障—安全 reactive fail-safe

允许一个安全相关功能由单个对象执行,前提是通过快速的危害故障检测和拒绝来确保它的安全操作。尽管只由一个对象实施实际的安全相关功能,但检查/测试/检测功能应被看作为第二对象。检查/测试/检测功能应是独立的,以避免共因失效。

3.11

内在式故障—安全 inherent fail-safe

允许一个安全相关功能由单个对象执行,前提是假定对象的所有可信失效模式均为非危害的。

4 总则

4.1 计算机联锁设备在无故障时、故障时以及受规定的外界环境影响时,系统应满足规定的安全要求。

4.2 计算机联锁设备在发生故障时,应使其处于受控的、可预知和预先定义好的状态。

4.3 计算机联锁设备发生任何单一随机故障时应确保满足规定的容许危害率,发生可识别的单一随机硬件故障时,不应导致危险侧输出。被证明其影响可以忽略的故障可以不予考虑。

4.4 只要可行,应将计算机联锁的安全相关功能与非安全相关功能清晰地分离开,由不同的子系统各自执行;否则子系统所有相关的软硬件部分都应被视为安全相关的,除非能够表明这些未分离的安全相关功能和非安全相关功能的实现是充分独立的,即非安全相关功能的失效不会引起安全相关功能的危险失效。

4.5 计算机联锁与其他系统的接口不应降低自身的安全完整性。

4.6 计算机联锁的设计变更、数据制作、测试、安装、运营维护过程的活动不应降低其安全完整性。

4.7 计算机联锁实现安全性要求时,应同时满足可用性要求。

4.8 计算机联锁设备在规定的使用条件及运行环境下和预期寿命阶段内,每安全功能每小时容许危害率应小于 1×10^{-8} 。

4.9 计算机联锁安全功能的安全完整性应符合 GB/T 28809—2012 规定的安全完整性等级 4 级

(SIL4)的要求。

4.10 计算机联锁应对表 A.1 的危害进行防护,并实现表 A.2 中的安全功能。

4.11 计算危害发生率时,只计算计算机联锁设备本身的失效。

4.12 对于每小时容许失效危害率大于 1×10^{-5} 的功能,虽然没有直接的安全完整性要求,同样对安全性提升有很大的帮助,只要合理可行,应通过这些功能为安全功能提供二次防护,以减轻安全功能失效后果的严重性,如人机对话层的报警和提示。

5 系统及硬件

5.1 总体要求

5.1.1 计算机联锁系统划分为联锁运算层、执行表示层和人机对话层。

5.1.2 计算机联锁应在系统规定的时间内完成安全功能和故障检测。

5.1.3 计算机联锁上电后执行安全功能之前,应进行自检并在整个工作期间内进行周期性的自检。

5.1.4 在发生故障时,计算机联锁应自动进入或保持在安全状态。可以通过以下的一种或几种设计原则实现:

- a) 组合式故障—安全;
- b) 反应式故障—安全;
- c) 内在式故障—安全。

5.1.5 第一个故障单独或与第二个故障组合可能导致危险侧输出时,应在足够短的时间内被检测到并强制进入安全状态以实现规定的量化安全目标。

在组合式故障—安全条件下,上述要求意味着应在足够短的时间内检出第一个故障,并强制达到安全状态,以确保在检测和拒绝期间出现第二个故障的风险小于规定的概率指标。

在反应式故障—安全条件下,上述要求意味着检测和拒绝所需最大时间不应超出规定的有潜在危害的瞬间输出持续时间限制。

检测出第一个故障并进入安全状态后,后续故障不能使系统退出安全状态。允许的修复时间内,如果故障进一步发生,系统应具有保持在安全状态的能力。

5.1.6 应及时检测可能直接造成危害或与继发故障组合后造成危害的多重故障,并且强制达到一个安全状态。这一时间应足够短以满足规定的安全指标。应进行共因失效分析以确保多重故障只在多个随机单一故障组合情况下发生,而不是一个共因故障的结果。

5.1.7 对安全性有影响的设备,错误的插入或替换不应导致危险侧输出。包含软件的设备应采取校验措施,降低版本不匹配带来的安全风险。

5.1.8 实现安全功能的电路,供电电源的故障或干扰不应导致危险侧输出。

5.1.9 实现安全功能的电路部件应尽可能降额(元器件使用中承受的应力低于其额定值)使用。

5.1.10 计算机联锁设计时应降低下列人为失误导致危险侧输出的可能性:

- a) 调整设备以及调节装置;
- b) 卸下元件和装置;
- c) 不正确地装配设备;
- d) 没有按照建议进行维护。

5.1.11 计算机联锁内部的各安全单元间通信故障时,应及时将相关信息处理为安全侧。由于通信故障导致的错误数据漏检率应满足相应安全功能要求。

5.1.12 计算机联锁内部的各部件应有正确地址标识,避免信息传输对象错误,发现冲突或重复地址标识时,应及时采取安全措施。

5.1.13 计算机联锁各层间应保持独立性,任何一层的故障不应对其他层的安全性造成影响,并不应降低整个系统的安全性。

5.1.14 计算机联锁内部各层安全侧定义如下：

- a) 联锁运算层的安全侧定义为对外无发送数据,或发送预先定义的数据;
- b) 执行表示层驱动单元安全侧定义为对外无输出或预先定义的输出;
- c) 执行表示层采集单元安全侧定义为采集状态无效或预先定义的采集状态;
- d) 人机对话层安全相关操作安全侧定义为操作不执行。

5.1.15 计算机联锁与其他系统结合时安全侧定义如下：

- a) 采用通信方式接口时,发送安全侧定义为对外无发送数据或发送预先定义的数据;
- b) 采用通信方式接口时,接收安全侧定义为通信中断或预先定义的数据;
- c) 采用继电方式接口时,输出安全侧定义为令继电器落下;
- d) 采用继电方式接口时,采集安全侧定义为接点断开或无效。

5.2 联锁运算层

5.2.1 联锁运算层应根据采集和通信数据及内部状态,依据联锁规则进行运算,产生输出命令和数据。

5.2.2 联锁运算层发生可能危及行车安全的故障时,应及时采取安全措施。

5.2.3 联锁运算层与执行表示层或其相连接的安全设备失去联系时,应及时将相关接收信息处理为安全侧。

5.2.4 联锁运算层加电或启动复位后,在联锁软件(用于实现联锁功能的软件)产生运算输出前仅允许安全侧输出。

5.2.5 联锁运算层采用可靠性冗余结构时,应防止由于冗余单元输出不一致导致危险。

5.3 执行表示层

5.3.1 执行表示层驱动单元应根据联锁运算层的命令进行输出,当该单元与联锁运算层失去联系或发生危及行车安全的故障时,应及时导向安全侧。

5.3.2 执行表示层采集单元应采集信号设备状态信息并传送给联锁运算层,当该单元发生可能危及行车安全的故障时,应及时采取安全措施。

5.3.3 执行表示层驱动单元加电启动或复位后,与联锁运算层建立联系前,输出应维持在安全侧。

5.3.4 执行表示层检测电路应满足以下要求：

- a) 检测电路宜采用闭环控制方式;
- b) 检测电路故障,使危险侧采集故障或输出故障不能被及时发现时,应及时采取安全措施;
- c) 应避免检测对象状态长期无变化时可能产生的故障隐藏;
- d) 检测电路的检测性能不应由于主电路工作状态变化而降低,造成故障累积。

5.3.5 执行表示层输入输出电路,应采取措施降低以下情况对安全性的影响：

- a) 寻址错误;
- b) 断路、混线和短路;
- c) 存在有害的潜在通路(是一个潜在的电路路径或条件,在某种条件下,导致不希望的功能发生,或阻止希望的功能,它与组件失效无关,而是设计者无意地设计进系统的一种潜在状态);
- d) 输入、输出电流和电压超出规定值;
- e) 保护电路动作或故障时;
- f) 电源电压异常或波动超限;
- g) 软件运行停止。

5.3.6 执行表示层采取安全措施停止危险侧输出时,应采用基于故障安全的输出切断方式,主电路和检测电路的故障不应影响输出切断功能。

5.3.7 执行表示层采用可靠性冗余结构时,冗余单元故障或失去同步时,不应产生危险侧输出。

5.4 人机对话层

5.4.1 人机对话层进行安全相关操作应进行人工确认。安全相关操作在表 A.3 中规定。

5.4.2 人机对话层与联锁运算层失去联系时,应有明确的提示。

5.5 通信前置机

5.5.1 设置通信前置机时,不应降低计算机联锁系统与其他安全系统通信的安全性。

5.5.2 设置通信前置机时,通信前置机引入的额外延时不应对整个通信安全性产生影响。

5.5.3 通信前置机承担安全功能时,应满足联锁运算层的安全设计原则和要求。

6 软件

6.1 总体要求

6.1.1 计算机联锁中承担安全功能的软件,其安全完整性等级应与系统的安全完整性等级一致,满足 GB/T 28808—2012 的要求。

6.1.2 用于实现安全功能的处理,应由联锁运算层或执行表示层执行。

6.1.3 应采取技术措施防止软件在存储过程中产生损坏以及在下载安装中出错导致危险侧输出。

6.1.4 应有措施防止远程进行软件修改。

6.1.5 应采取措施防止编译器等工具软件引入的错误导致系统产生危险侧输出。

6.1.6 应对安全软件(实现安全功能的软件)的运行时间进行监测,当软件运行时间不满足设定的范围时,应及时采取安全措施。

6.1.7 应采取措施防止安全软件任务执行顺序和执行次数错误产生危险侧输出。

6.1.8 在安全软件中设置软件监视逻辑时,逻辑监视软件应与被监视软件保持独立性。

6.1.9 安全软件停止运行后,应采取措施防止中断意外响应导致危险侧输出。

6.1.10 运行安全软件的目标系统中还有其他软件同时运行时,应有措施防止其他软件失效破坏安全软件的安全完整性。其他软件包括采购的商用软件和自行开发的既有软件。

6.1.11 安全软件应采取措施防止程序代码和静态数据(软件运行时数值不会改变的数据)畸变时导致危险侧输出。

6.1.12 程序和配置数据分离时应对配置数据的版本和适用性进行检查,并对配置数据的正确性进行检查。该检查在程序载入和运行时都应执行。

6.1.13 应采取措施降低安全软件中安全关键变量由于硬件故障或软件意外改写时导致的风险。

6.1.14 安全软件应对来自外部数据的有效性进行检查。

6.1.15 安全软件应采用防御性编程技术。

6.1.16 计算机联锁对涉及安全相关功能的全部安全关键变量的使用,都应遵循持续动态更新的命令/状态生成原则;并应尽可能地采用对非限制性命令/状态/信息“一次性有效”的使用及校验原则,特别是在跨模块尤其是跨边界模块的交互中,避免非预期的保持带来的风险。

6.1.17 仿真软件(专门用于仿真测试的软件)不应控制现场设备,现场运行的软件应经过特殊操作才能进入仿真状态。

6.1.18 安全软件应制定相应编程语言的编程规范并严格执行,编程规范应针对铁路信号失效—安全要求及安全侧明确的特点,严格规定采用非限制性代码唯一的安全侧对应编码及判别原则。应依据系统安全侧的定义明确安全软件中安全相关数据、状态的安全侧。

6.1.19 联锁运算层软件应采取措施防止以下情形对安全性的影响:

- a) 联锁运算层可靠性冗余单元间的输入不一致,如联锁双系输入数据不一致;
- b) 联锁运算层可靠性冗余单元间用于同步判断的条件不充分出现伪同步现象;
- c) 联锁运算层可靠性冗余单元间故障传播。

6.2 联锁软件要求

6.2.1 联锁软件初始化和非同步系切换时应采取安全锁闭措施。

6.2.2 联锁软件在命令不具备执行条件时,或命令执行后在规定的时间内未得到正确响应时,应及时采取措施防止危险侧输出。

6.2.3 计算机联锁检测到非预期的驱采状态,影响安全时,应采取安全措施。

6.2.4 联锁软件内部同一设备状态和运算结果,需要对外驱动以及给多个外部系统发送时,对外驱动以及给各系统发送的信息含义应一致。

7 通信接口

7.1 总体要求

7.1.1 在传输安全相关的信息时,封闭式传输系统按 GB/T 24339.1 的要求采取防护措施,开放式传输系统按 GB/T 24339.2 的要求采取防护措施。

计算机联锁通过通信方式与其他系统结合时,不应由于信息重复、插入、删除、重排序、损坏、延时和伪装等而产生危及行车安全的后果。

7.1.2 安全相关通信应满足以下要求:

- a) 非置信传输系统传输质量严重劣化时安全相关传输系统残留的数据错误率要低于规定值;
- b) 非置信传输系统由于故障导致双向通信变成单向通信时不应对安全产生影响;
- c) 非置信传输系统以最大可能的报文频率接收错误报文时,安全相关传输系统残留的数据错误率要低于规定值;
- d) 非置信传输系统中包含存储器时,在某个错误时间再次发送的安全报文不应被错误使用;
- e) 由于报文发送和接收频率不一致等原因导致的长期缓慢累积延时不应影响安全性。

7.1.3 以下情况下应采取必要的防护措施保证通信安全性:

- a) 传输系统改变导致威胁种类或严重程度增加时;
- b) 应用或传输内容改变导致已进行的风险分析不适用时。

7.1.4 计算机联锁采用通信方式与其他安全系统接口时,涉及安全的通信信息应有明确的安全侧定义,当通信故障时,须在规定的时间内将接收数据导向预先定义的安全侧。

7.1.5 对通信协议的处理应包含对对方协议版本号的匹配校验控制。

7.2 应用相关

7.2.1 使用固定周期传输全体信息的通信方式时,以下因素不应对安全性产生影响:

- a) 通信中断延迟时间内忽略的设备变化;
- b) 全体信息掩盖的信息变化顺序。

7.2.2 对经由不同通道传输的数据,采用“逻辑或”的方式进行处理时,应确认这些数据具有相同的含义。

7.2.3 来自其他安全系统的通信数据,如果经安全校验后数据出现非预期或矛盾的结果,计算机联锁系统应采取安全措施。

7.2.4 经由网络传输的信息与本地直接采集的信息组合使用时,应采取避免由于本地采集数据与网络采集数据延时不同导致的风险。

8 继电接口

8.1 计算机联锁以开关量采集或驱动方式与继电接口应符合故障—安全原则。

8.2 使用具有机械或磁性保持的继电器,应采取降低直接使用其采集状态的风险。

8.3 对计算机联锁控制的继电器,其他设备不宜同时控制。

8.4 对计算机联锁控制的继电器,应采取降低其控制状态与控制预期不一致时的风险。

8.5 计算机联锁控制的继电器,其接点状态不直接回采时,宜通过其关联动作的继电器或其他方式确认其受控状态。

8.6 对计算机联锁控制的继电器,应采取措施降低驱动混线造成继电器误吸起的风险,如采用偏极继电器防护、输出采用双断方式、驱动电路串接防护继电器、对继电器的状态进行回采确认等。

8.7 应采取措施降低关键继电器采集混线带来的风险,如采用前后接点采集、双接点采集、条件串接采集等,并对采集结果加以校核;校核有误时应及时采取安全措施并报警。

8.8 计算机联锁的开关量采集和驱动电路接口电路,应采取措施降低以下情况对安全性的影响:

- a) 采集或驱动电源通、断或波动;
- b) 采集或驱动回路上存在干扰时;
- c) 采集或驱动回路短路、接地时;
- d) 采集或驱动回路保护电路动作或故障时;
- e) 采集对象状态不稳定时。

8.9 计算机联锁采集和驱动单元采用冗余配置时,应采取措施避免由于冗余配置的并联工作和交叉故障导致危险侧输出或危险侧采集状态。

9 电子执行单元

9.1 电子执行单元安全完整性等级要求与联锁执行表示层相同,应满足执行表示层的安全设计原则和要求。电子执行单元不应产生危及行车安全的驱动和信息输出。

9.2 电子执行单元与联锁运算层的联系中断时,应及时采取安全措施。

9.3 电子执行单元连接的室外设备和结合电路的线缆发生断线、短路、接地、一处混线时,不应产生危险侧输出,检测到上述故障时应及时报警。

9.4 电子执行单元应根据应用环境采用适当的防雷和电磁干扰的防护措施。

9.5 电子执行单元与室外设备连接电缆上的干扰(分布电容、牵引电流等)不应使电子执行单元产生危险侧输出或危险侧采集状态。

9.6 电子执行单元具备室外信号设备运行参数采集功能时,采集功能不应影响安全性。

10 其他要求

10.1 计算机联锁的配置数据应经过完整的测试和确认,配置数据的检查流程应与系统的安全完整性等级要求相适应。

10.2 计算机联锁应优先采用已经经过验证的模块,但应对模块的应用环境进行适用性分析。

10.3 计算机联锁内部的硬件、固件、软件和数据变化时,应变更相应部分的版本号。

附录 A
(规范性附录)

主要危害、安全功能和安全相关操作

计算机联锁的主要危害和安全功能见表 A.1 和表 A.2。安全相关操作见表 A.3。

表 A.1 计算机联锁主要危害

序号	危 害	对应安全功能
1	错误开放信号或未及时关闭信号	信号控制、非进路调车、进路表示器
2	错误转换道岔	道岔控制、到发线出岔、结合电路、非进路调车
3	进路错误解锁	进路功能、延续进路、平面溜放、到发线出岔
4	道岔错误解锁	道岔锁闭、到发线出岔、上电锁闭、非进路调车、结合电路
5	给结合电路发送错误的可能会危及行车安全的条件	上电锁闭、结合电路
6	给其他系统发送错误的可能会危及行车安全的信息	上电锁闭、信号系统接口

表 A.2 计算机联锁安全功能

序号	功能项	功能说明(对应 TB/T 3027 的功能部分要求)
1	进路功能	进路锁闭,进路解锁
2	信号控制	信号开放,信号关闭,点灯控制
3	道岔控制	进路选动和带动,单独操纵
4	道岔锁闭	进路锁闭,区段锁闭,单独锁闭,人工封锁,道岔总锁闭
5	延续进路	进路锁闭,进路解锁
6	到发线出岔	分歧道岔锁闭和解锁
7	平面溜放	溜放进路锁闭和解锁
8	上电锁闭	上电安全锁闭和解锁
9	非进路调车	相关道岔锁闭、解锁和信号开放、关闭
10	进路表示器	进路表示器开放和关闭
11	结合电路	与区间闭塞结合、场间联系、与机务段结合、局部控制道岔、车站电码化、与灾害监控系统结合
12	信号系统接口	与无线闭塞中心、列控中心的结合,计算机联锁系统之间的通信联系

表 A.3 安全相关操作

序 号	操 作
1	引导总锁
2	上电解锁
3	坡道解锁
4	人工解锁

表 A.3 安全相关操作(续)

序 号	操 作
5	区段故障解锁
6	引导信号
7	64D 事故复原
8	非进路调车故障恢复
9	区间辅助改方操作
10	区间允许改方
11	关灯操作
12	非常站控



中 华 人 民 共 和 国
铁 道 行 业 标 准
铁路车站计算机联锁安全原则
Computer based interlocking safety principles
TB/T 3482—2017

*

中国铁道出版社出版、发行
(100054,北京市西城区右安门西街8号)
读者服务部电话:市电(010)51873174,路电(021)73174
中国铁道出版社印刷厂印刷
版权专有 侵权必究

*

开本:880 mm×1 230 mm 1/16 印张:1 字数:19 千字
2018年3月第1版 2018年3月第1次印刷

*



定 价: 10.00 元