ICS 29.020
CCS K 09

中华人民共和国国家标准化指导性技术文件

GB/Z 302—2026/IEC TS 63074:2023

机械电气安全　与安全相关控制系统的功能安全有关的信息安全

Electrical safety of machinery—Security aspects related to functional safety of safety-related control systems

（IEC TS 63074:2023，Safety of machinery—Security aspects related to functional safety of safety-related control systems，IDT）

2026-10-30 发布

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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 5
4　功能安全和信息安全概述 …… 5
4.1　概述 …… 5
4.2　功能安全目标 …… 5
4.3　信息安全目标 …… 5
5　与功能安全相关的信息安全 …… 7
5.1　通则 …… 7
5.2　信息安全对抗(措施) …… 8
6　机械的网络安全和功能安全 …… 11
6.1　通则 …… 11
6.2　防损坏保护的有关方面 …… 11
6.3　防损坏的信息安全对抗(措施) …… 11
7　信息安全对抗(措施)的验证与维护 …… 13
8　给用户的机械信息 …… 13
附录 A(资料性)　与威胁和威胁建模方法有关的基本信息 …… 14
A.1　威胁评估 …… 14
A.2　与安全相关设备有关的威胁示例 …… 15
附录 B(资料性)　信息安全风险评估触发器 …… 17
B.1　概述 …… 17
B.2　事件驱动触发器 …… 17
附录 C(资料性)　设备供应商、机器制造商、集成商和机器用户之间的信息流通示例 …… 18
C.1　概述 …… 18
C.2　示例 1——机器的设计阶段 …… 18
C.3　示例 2——机器的使用阶段 …… 18
参考文献 …… 20

图 1　SCS 执行安全功能的威胁、漏洞、后果和信息安全风险之间的关系 …… 6

图 2　信息安全风险对 SCS 的可能影响 …… 7
图 A.1　与安全有关的可能入口 …… 16
图 C.1　设计阶段的通用信息流示例 …… 18
图 C.2　使用阶段的通用信息流示例 …… 19
图 C.3　IEC 62443-2-4 背景下使用阶段的信息流示例 …… 19

表 1　基本要求和可能对 SCS 的影响 …… 9

前　言

本文件为规范类指导性技术文件。

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。

本文件等同采用 IEC TS 63074:2023《机械安全　与安全相关控制系统的功能安全有关的信息安全》,文件类型由 IEC 的技术规范调整为我国的国家标准化指导性技术文件。

本文件做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《机械电气安全 与安全相关控制系统的功能安全有关的信息安全》。

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。

本文件由中国机械工业联合会提出。

本文件由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本文件起草单位:通用技术集团机床工程研究院有限公司、北京机床研究所有限公司、中国科学院沈阳计算技术研究所有限公司、沈阳中科数控技术股份有限公司、广州数控设备有限公司、科德数控股份有限公司、中国质量认证中心有限公司、山东国创微纳制造研究院有限公司、西安交通大学、西门子(中国)有限公司、北京凯恩帝机电技术有限公司、莱茵检测认证服务(中国)有限公司、深圳市意普兴科技有限公司、深圳市湾测技术有限公司、济宁科力光电产业有限责任公司、山东莱恩光电科技有限公司、皮尔磁工业自动化(上海)有限公司、北京北一机床有限责任公司、卡特彼勒技术研发(中国)有限公司。

本文件主要起草人:薛瑞娟、张颖、张培森、吴翟、尹震宇、吴怡然、于东、王楚婷、高知国、聂林、王江东、褚卫中、张南、康城玮、陈剑飞、王大伟、杨洪丽、姚坚、刘晓英、唐小辉、邵光存、胡进芳、刘吉泓、张佳琳、金葵娟。

引　言

工业自动化系统可能面临基于漏洞的信息安全威胁，其原因包括：

——控制系统存在被访问的可能性，例如对机器功能（包括安全功能）进行重新编辑；

——信息技术（IT）和工业系统之间的融合程度日益加深；

——嵌入式系统普遍采用操作系统，例如基于IP的协议正取代专有网络协议，这使得数据可直接从监控与数据采集（SCADA）网络传输至办公网络；

——软件开发过程中复用第三方现有软件组件；

——供应商的远程访问已成为运营/维护的标准方式，网络安全风险增加，例如未经授权的访问，可用性和完整性。

在机械领域，机器控制系统代表工业自动化系统。

与机器安全有关的控制系统是机器控制系统的一部分，因此也可能受到信息安全威胁，这些威胁可能导致机器丧失维持安全运行的能力。

注1：由于威胁态势的持续演变以及已知漏洞数量的不断增长，系统被攻击的风险显著增加。因此，信息安全目标主要围绕保密性、完整性与可用性确立，并通常通过基于风险的方法进行识别和优先级排序。

功能安全目标通过评估伤害的严重程度和伤害发生的概率考量风险。任何风险（危险事件）的影响决定了安全完整性的要求[根据IEC 62061适用于安全相关控制系统的安全完整性等级（SIL），或IEC 61508（所有部分）适用于电气/电子/可编程电子安全相关系统，或根据ISO 13849-1适用于控制系统安全相关部件的性能等级（PL）]。

就功能安全而言，信息安全威胁（内部或外部）会影响安全完整性和整个系统的可用性。

注2：为了确保信息安全目标，IEC 62443-3-3定义并建议了相关系统满足的信息安全要求（基本要求）。

注3：本文件并未涵盖整体的信息安全策略，进一步的信息参考IEC 62443（所有部分）或ISO/IEC 27001。

一些机械功能安全标准[例如IEC 61496（所有部分）和ISO 14119]提出了防止物理操作造成合理可预见的误用的措施。

注4：在IEC 62443（所有部分）中，通过物理操作防止合理可预见误用的措施与物理安全不同。

机械电气安全　与安全相关控制系统的功能安全有关的信息安全

1　范围

本文件明确了IEC 62443(所有部分)中有关信息安全威胁和漏洞的内容,这些信息安全威胁和漏洞,与可能导致机器安全运行能力丧失的安全相关控制系统(SCS)的设计和实施相关。

与SCS有潜在关系的机器的典型信息安全方面如下。

——SCS自身的漏洞,或通过机器其他部分间接产生的漏洞。这些漏洞可能被安全威胁利用,进而引发安全攻击(即信息安全漏洞)。

——影响SCS的安全特性及正确执行其功能的能力。

——典型用例的定义及相应威胁模型的应用。

本文件不考虑信息安全威胁和漏洞的非安全相关方面。

注:机器控制系统中与安全无关的部分也会受到信息安全威胁的影响,可能会影响机器的运行,如生产效率、性能或质量。有关这些方面,见IEC 62443(所有部分)。

本文件的重点是故意的恶意行为。然而,本文件没有考虑有意的硬件操作(例如接线、组件交换)或可预见的SCS物理操作(例如物理短路)的误用。

本文件不涵盖信息技术(IT)产品以及SCS中所用装置设计的安全要求(此类要求可参考产品特定标准,如IEC 63208)。

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。

IEC 62061:2021　机械安全　安全相关控制系统的功能安全(Safety of machinery—Functional safety of safety-related control systems)

注: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(IEC 62061:2005,IDT)

3　术语、定义和缩略语

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

资产　asset

对控制系统具有潜在或实际价值的物理对象或逻辑对象。

[来源:GB/T 35673—2017,3.1.1,有修改]