ICS 29.020
CCS K 07

中华人民共和国国家标准

GB/T 41998—2022/IEC 62745:2017

机械电气安全　机械无线控制系统技术要求

Electrical safety of machinery—Safe technical requirements of mechanical wireless control system interface

(IEC 62745:2017,Safety of machinery—Requirements for cableless control systems of machinery,IDT)

2022-10-12 发布　　2023-05-01 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。

本文件等同采用IEC 62745:2017《机械安全　机械无线控制系统技术要求》。

本文件做了下列最小限度的编辑性改动:

——标准名称改为《机械电气安全　机械无线控制系统技术要求》;

——增加了资料性附录A,将国际标准IEC 62745:2017资料性附录A结构调整为“停止功能的逻辑”(见4.7.4)。

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:国家机床质量监督检验中心、深圳市轴心自控技术有限公司、合肥邦立电子股份有限公司、中联重科股份有限公司、环创(厦门)科技股份有限公司、琦星智能科技股份有限公司、中国石油大学(北京)、北京联华科技有限公司、广东求精电气有限公司、青岛诚信联合锻造机械有限公司、江门市乙丙丁机械有限公司、广东拓斯达科技股份有限公司、安徽沃弗永磁科技有限公司、福建大威科技有限公司、西安凯益金电子科技有限公司、西安新林达数字科技有限公司、义乌市宝能模具科技有限公司。

本文件主要起草人:黄祖广、薛瑞娟、王金江、于晓颖、吴文俊、王文浩、张凤丽、王本正、陈为民、郭子成、陈正茂、张正德、梁荣富、徐必业、余竹艳、刘步永、向梅、吴财政、张德银。

引　言

无线控制系统(CCS)广泛用于各类机械设备并为其提供操作界面。CCS的功能及与整个机械控制系统接口的方法直接影响到机械的安全性。

本文件提供与机械控制系统相连接或作为机械控制系统一部分的CCS的功能要求相关信息。

根据机械的风险评估,选择提供合适控制功能并具有适当安全完整性的CCS是很重要的。

本文件的目的是:

——保障人员和设备的安全;

——保证机械及其电气设备工作可靠;

——便于机械及其电气设备的使用和维护。

机械电气安全　机械无线控制系统技术要求

1　范围

本文件规定了无线(例如无线电、红外线)控制系统的功能和接口要求,它提供了操作员控制站和机械的控制系统之间的通信。具体要求包括在操作员可携带的操作控制站中。

注:作为操作员控制站的无线控制系统的部分有时称为"发送器",而与机械控制系统接口的部分有时称为"接收器"。然而,考虑到双向通信的可能性,本文件分别将这些单独的部分称为"远程站"和"基站"。

本文件不处理非操作员控制站之间的无线通信。

本文件的目的不是为了规定设计和构造无线控制系统所必需的所有要求。例如它不规定通信协议、频率或带宽方面,也不规定所有的构造要求,如抗冲击性、入口保护、电磁兼容性等。

本文件的规定适用于GB 5226系列相关电气设备的要求。

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 2423.7—2018　环境试验　第2部分:试验方法　试验Ec:粗率操作造成的冲击(主要用于设备型样品)(IEC 60068-2-31:2008,IDT)

GB/T 5226.1—2019　机械电气安全　机械电气设备　第1部分:通用技术条件(IEC 60204-1:2016,IDT)

ISO 13849-1　机械安全　控制系统的安全相关部件　第1部分:设计用一般原理(Safety of machinery—Safety-related parts of control systems—Part 1:General principles for design)

ISO 13849-2　机械安全　控制系统的安全相关部件　第2部分:验证(Safety of machinery—Safety-related parts of control systems—Part 2:Validation)

ISO 13850　机械安全　急停功能　设计原则(Safety of machinery—Emergency stop function—Principles for design)

IEC 60947-5-1:2016　低压开关设备和控制设备　第5-1部分:控制电路电器和开关元件　机电式控制电路电器(Low-voltage switchgear and controlgear—Part 5-1: Control circuit devices and switching elements—Electromechanical control circuit devices)

注:GB 14048.5—2017　低压开关设备和控制设备　第5-1部分:控制电路电器和开关元件　机电式控制电路电器(IEC 60947-5-1:2016,MOD)。

IEC 60947-5-5　低压开关设备和控制设备　第5-5部分:控制电路器件和切换元件　具有机械锁扣功能的电气紧急故障中断器件(Low-voltage switchgear and controlgear—Part 5-5:Control circuit devices and switching elements—Electrical emergency stop device with mechanical latching function)

IEC 61508(所有部分)　电气/电子/可编程电子安全相关系统的功能安全(Functional safety of electrical/electronic/programmable electronic safety-related systems)

IEC 62061　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)

3 术语和定义、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

无线控制 cableless control

在操作员控制站和机械有一定距离的情况下,机械操作员命令传输无需任何物理连接。

3.1.2

无线控制系统 cableless control system;CCS

系统至少由一个远程站和一个基站组成,它们之间使用无线控制传输命令。

3.1.3

接收器 receiver

从发射机接收帧的无线控制系统的部分。

3.1.4

发射器 transmitter

将帧发送给接收器的无线控制系统的部分。

3.1.5

操作员控制站 operator control station

将一个或多个控制致动器(施加外部手动动作的装置部分)固定在同一外壳或同一面板。

注:操作员控制站也可以包含相关设备,例如电位计,信号灯,仪器,显示装置等。

3.1.6

帧 frame

在远程站和基站之间交换的信息"包",包括:

a) 地址码;

b) 操作命令;

c) 错误检测码;

d) 其他命令或信息。

注:"帧"有时称为"报文"或"信息"。

3.1.7

地址码 address code

使基站或远程站能够识别旨在向其传送命令的帧部分。

注:基站或远程站对被识别为具有相关地址码命令的响应。

3.1.8

操作命令信号 operating command signal

控制信号旨在启动、修改或维护机械功能。

3.1.9

错误检测代码 error detection code

附加信息添加到每个帧,以便检测传输错误。

3.1.10

中性帧　neutral frame

所有操作命令信号都处于这样的状态的帧，当它在基站被接收时，它不会激活任何用于控制机器危险操作的输出。

注1：中性帧可用于保持发射器和接收器之间的通信(即有效信号)，例如防止机械自动引发停止功能。

注2：中性帧传输旨在防止因建立或重新建立通信而导致机械的危险操作。

注3：中性帧可以包含数据，例如参数化数据和不会导致机械危险操作的命令。

3.1.11

汉明距离　Hamming distance

等长的两帧之间的比特位不同的位数。

3.1.12

远程站　remote station

无线控制系统的一部分，经由操作员接口与无线控制系统连接。

注1：无线控制系统的远程站有时称为“发射器”，但作为双向无线控制系统一部分的远程站将包括发射器和接收器。

注2：远程站构成无线控制系统的操作员控制站。

注3：远程站可以是便携式(由操作员操作)、移动式(例如与车辆或手推车上的机械分开安装)或固定式(例如安装在机械上或其附近)。

3.1.13

基站　base station

无线控制系统的一部分，在无线控制和机械控制系统的其他部分间形成接口。

注1：无线控制系统的基站有时称为“接收器”，但作为双向无线控制系统一部分的基站将包括接收器和发射器。

注2：基站可安装在静态或移动机械上。

注3：基站不一定是离散的物理实体，但它包括满足本文件为基站规定的要求的所有部件。

3.1.14

停止输出　stop output

基站的输出电路与机械控制系统相连接来执行停止功能。

注1：停止输出可以是安全相关的或非安全相关的，见表1。

注2：至CCS基站的现场总线端口的接口也可视为输出电路。

3.1.15

断开状态　OFF-state

基站的安全相关停止输出的状态，旨在用于引发机械的一个或多个停止功能。

3.1.16

安全相关停止功能　safety-related stop function

由CCS提供的导致关闭状态的停止功能，其失效可能导致风险立即增加。

3.1.17

主动停止　active stop

由停止信号从远程站到基站的传输而导致的停止。

3.1.18

被动停止　passive stop

由于基站无有效信号而导致的安全相关停止。

注：被动停止可以由例如超出范围条件、电池故障、电磁干扰引发。

3.1.19

自动停止　automatic stop

操作人员无需手动操动装置即可引发安全相关停止。

3.1.20

手动停止　manual stop

由操作员操动装置引发停止。

3.1.21

有效信号　valid signal

任何接收到的帧，包括中性帧，它被接收器的错误检查例行程序所接受并包含接收器的相关地址码。

3.1.22

禁用远程站　disabling of a remote station

故意使远程站不能向基站发送信号。

3.2　缩略语

下列缩略语适用于本文件。

ATS：自动停止(automatic stop)

CCS：无线控制系统(cableless control system)

EMS：紧急停止(emergency stop)

GSS：一般安全停止(general safe stop)

4　功能要求

4.1　概述

图1举例说明了CCS的主要元素及其与机械控制系统的交互。

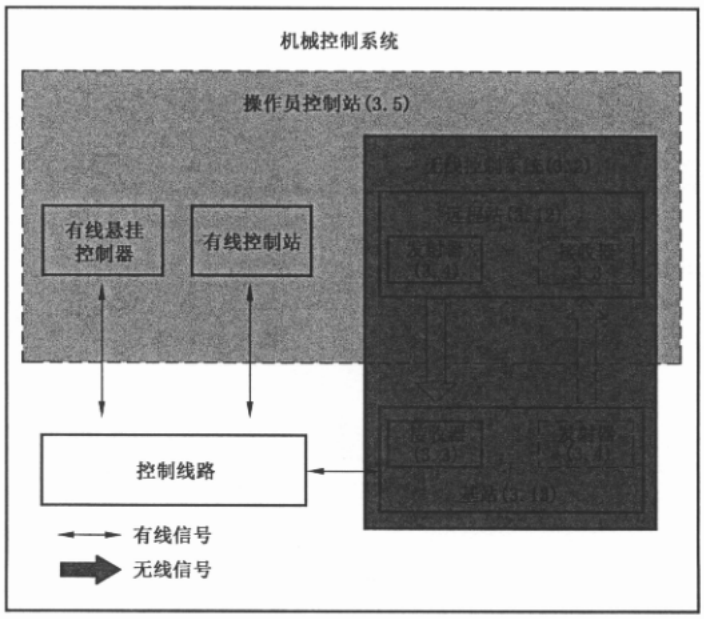

图1　无线控制系统的框图示例及其与机械控制系统的交互

注：本文件对GB/T 5226.1引用可能要满足GB/T 5226系列的其他相关部分要求。

4.2 操作预防措施

4.2.1 防止意外致动

远程站及其控制致动器的设计和布置应尽可能减少意外致动的可能性(例如由于跌落到地面上或撞击障碍物,电子设备故障而产生的意外危险命令)。

4.2.2 防止未经授权的操作

在必要的场合(例如预防机械危险操作),远程站应提供手段(例如钥匙开关、通路编码)以防止未经授权的使用。

4.2.3 防止意外命令

应采取措施确保操作指令信号:

——仅影响预期的基站或远程站(例如使用地址码);

——仅该基站或远程站引发预期功能。

这些措施应抵抗偶然或意外的变化。检测到功能失常或故障后,所有有关的安全相关输出应以适当的安全完整性控制到断开状态。

设备寻址使用硬件开关(例如 DIP)时,为了满足故障情况的要求,可能需要附加措施(如奇偶校验)。

注:典型的方法包括出厂设置编码,它比用户可配置的方法更健全,它们通常不能被用户(有意或无意)否决。

4.3 串行数据传输

串行数据传输应满足以下要求之一:

——应提供确保未被检测到的错误帧概率 $R(\mathrm{Pe})<1\times10^{-8}$(给定 $\mathrm{Pe}=10^{-3}$ 的输入错误概率)的手段,如果没有更好地输入比特错误概率可以被证明;

——汉明距离应为 4 或一帧中的总比特数除以 20,取其中较大者。

注 1:$\mathrm{Pe}=10^{-3}$ 的输入比特错误概率可被假定作为无线信道受到加性高斯白噪声(AWGN)和电磁干扰(EMI)的典型估计。

注 2:IEC 60870-5-1 定义了一组传输帧格式。

注 3:增加串行数据传输的可靠性只会降低传输介质中出现错误的可能性。

除 CCS 的安全相关功能外,每小时未检测到残余误差概率 Λ 应小于 CCS 各功能规定 PFHd 值的 1%。

每小时未检测到的残余误差概率 Λ 应按下式计算:

$$\Lambda(\mathrm{Pe})=R(\mathrm{Pe})\times v\times b[1/\mathrm{h}]$$

式中:

$\Lambda(\mathrm{Pe})$——与输入比特错误概率相关的每小时未检测错误的残余概率;

$R(\mathrm{Pe})$——与输入比特错误概率相关的每帧未检测错误的残余概率;

Pe ——输入错误概率。如果没有更好地输入比特错误概率可以证明,$\mathrm{Pe}=1\times10^{-3}$ 适用;

v ——每小时安全相关信息的最大数量;

b ——监听基站的最大数量。

注 4:$\mathrm{PFH_d}$ 的定义见 IEC 62061 或 ISO 13849-1。

注 5:$\Lambda(\mathrm{Pe})$的计算基于 IEC 61784-3;此方法适用于安全相关消息的循环传输。

注 6:当使用 CRC 作为散列函数时,可应用 GB/T 34040—2017 的公式(B.3)或公式(B.4),以确定 $R(\mathrm{Pe})$,输入错误码概率为 $\mathrm{Pe}=1\times10^{-3}$。

CCS 可配置传输可靠性指示器。

注 7：CCS 可配置传输可靠性指示器。没有必要为每个可能影响传输可靠性的条件提供单独的警告指示器。

4.4 取消远程站点传输

应提供迅速停止远程站传输的手段。这应通过以下一项或多项来实现：

——中断远程站传输电源的装置，这类装置应具有直接开路动作（见 IEC 60947-5-1:2016 中附件 K）；

——不使用工具即可取出电池；

——符合 IEC 61508（所有部分），IEC 62061 或 ISO 13849-1 和 ISO 13849-2 的专用传输移除功能，其完整性符合 4.7.2。

注：移除传输功率会导致自动停止。

4.5 传输和通信的建立和指示

远程站启动或重新建立通信（例如电源中断、远程站电池更换、信号丢失）不应激活用于控制机械危险操作的任何输出。引发或重新引发这些操作应要求采取有意动作（例如从其通电位置释放控制致动器，然后再次按压）。

基站不应响应可以激活用于控制机械危险操作输出的操作命令信号，直到接收到中性帧（即重新建立通信后）为止。

远程站传输开始时应在远程站上给出指示（例如通过指示灯、视觉显示器等）。

注：当基站从相关远程站接收传输时提供指示可能是有用的。例如为此目的，可在基站上指定一个或多个输出，和/或可将确认信号发送到远程站（如果双向通信可用）。基站未提供为指示而设计的手段，建议使用 CCS 的信息，包括关于如何实现功能的说明（例如使用基站停止输出）。

4.6 CCS 的安全相关功能

对于安全相关应用的 CCS 的功能应具有适当的安全完整性。应符合 IEC 62061 和/或 ISO 13849-1，ISO 13849-2 的要求。

在检测到故障时，所有有关的安全相关输出应控制在断开状态。此外，在远程站中检测到可导致安全相关功能丧失的故障时，应停止传输。

注：有关控制功能安全相关方面设计的更多信息在 ISO 12100 和 IEC 61508（所有部分）中给出。

4.7 CCS 的停止功能

4.7.1 概述

CCS 应提供自动停止（ATS）功能和至少一个停止功能，该功能由控制装置上专门为此目的提供的故意动作引发。

有关停止功能逻辑如 4.7.4 所述。

注：在大多数应用中，这种手动引发停止功能是 GSS 或 EMS（见 4.7.3）。

4.7.2 CCS 的安全停止功能

CCS 的每个安全相关的停止功能应在基站引发相关停止输出的断开状态。

CCS 中执行安全相关停止功能的部分是一个安全相关控制系统。其安全相关停止功能的 SIL/PL 应取决于风险评估，但不应低于 SIL1/PLc。

此外，CCS 任何部分的单一故障不应导致任何安全相关停止功能的缺失，并且在合理可行的情况下，应在对安全相关停止功能下一次要求之时或之前检测到单一故障。

4.7.3 停止功能分类

4.7.3.1 概述

CCS 的停止功能分类为：

——控制停止；

——一般安全停止(GSS)；

——紧急停止(EMS)；

——自动停止(ATS)。

表 1 描述了不同停止功能的特性。

表 1 CCS 停止功能概述

功能	章条编号	安全相关功能	停止形式（见图 2）	对 CCS 作用	可用性和可操作性	控制致动器	
						形式	颜色
控制停止	4.7.3.2	任何	主动，被动或主动，然后被动	规定的停止输出状态，或与释放保持运转控制致动器相联的其他输出或如果安全相关：安全相关停止输出的断开状态	当 CCS 在控制机械时操作	见 GB/T 5226.1—2019	黑 白 灰
一般安全停止（GSS）	4.7.3.3	是	被动，或主动，然后被动	安全相关停止输出的断开状态	当 CCS 在控制机械时操作	见 4.7.3.3	黑色优先可以用红色，但是不应有黄色背景
紧急停止（EMS）	4.7.3.4				全部时间操作	装置符合 IEC 60947-5-5	红色带黄色背景
自动停止（ATS）	4.7.3.5				当 CCS 在控制机械时操作	不用	不用

4.7.3.2 控制停止功能

控制停止功能始终由操作员手动引发，且仅在 CCS 控制机械时可用。

控制停止功能应按照 GB/T 5226.1—2019 中 9.2.3.3 设计。

注：控制停止功能的引发可以通过释放保持运转控制致动器或通过不在运行位置的使能装置。

4.7.3.3 一般安全停止(GSS)功能

CCS 的 GSS 功能是安全相关的控制功能。

在 CCS 上提供 GSS 功能的位置，远程站应包括一个单独的、清晰可识别的手动启动此功能的方式，该方式应导致基站安全相关的停止输出处于断开状态。见表 1。

引发 GSS 功能的装置应具有直接开路动作(见 IEC 60947-5-1:2016 中附录 K)。

当致动器的主动操作在GSS功能引发后停止时，应通过装置的连接来维持命令的作用，直到它通过远程站的手动操作复位。致动器不锁定时不应产生停止命令，无停止命令产生时，不应出现致动器的锁定。如果锁定机构发生故障，无论致动器是否锁定，装置的致动器应产生停止命令。

当引发GSS功能后，控制致动器的主动操作停止时，命令的作用应通过装置的接合来维持，直到通过远程站点的有意的人工操作使其脱开。

注1：通过风险评估确定，由GSS功能产生的信号预期用于按照GB/T 5226.1引发机械的0类停止或1类停止。

注2：在传输中断之前，CCS通过发送停止命令来执行GSS功能（即主动停止），而其他仅传输中断（即被动停止）。主动停止可以向机械控制系统更快地传递停止命令，因为在引发自动停止命令之前识别有效信号丢失相关的时间延迟不存在。

4.7.3.4 紧急停止（EMS）功能

提供EMS功能的CCS应符合4.7.2，4.7.3.3的要求和下列附加要求（也见表2）：

a) 作为紧急停止装置的致动器应标志和/或标记（见GB/T 5226.1—2019中10.2.1，并应符合IEC 60947-5-5）；

b) 无论机械的操作模式（例如自动/手动、远程/本地）紧急停止功能始终可用和可操作；

c) EMS功能的引发应导致基站所有安全相关的停止输出处于断开状态；

d) 符合ISO 13850的相关要求；

e) 使用信息（见第6章）应说明将CCS并入机械控制系统中的系统集成商确保符合本条的要求；

f) 多个远程站同时与单个基站通信的情况下，单个远程站的禁用（禁用远程站的EMS功能不可用）将引发自动停止（ATS）功能。

注：在远程站点上提供紧急停止可用和可操作的指示应是有用的，使双向通信更加便利。

4.7.3.5 自动停止（ATS）功能

CCS的ATS功能应引发基站的相关停止输出的断开状态，以防止机械的危险操作。见表2。

注1：受ATS功能影响的停止输出可能与通过GSS功能和/或EMS功能导致的断开状态的停止输出相同。

CCS的ATS功能是安全相关的控制功能。ATS功能应具有不低于任何CCS提供的其他安全相关停止功能的最高安全性能。

CCS的ATS功能在包括但不限于下列条件下，应自动引发。

——在CCS中，当检测到可能导致危险情况的故障时。

——在CCS制造商声明的时间段内，在基站没有检测到有效信号（必要时根据双向通信CCS远程站的风险评估）。这段时间应由机械的风险评估确定，但通常不宜超过0.5 s。

——当传输停止时（见4.9）。

注2：机械控制系统设计者或制造商宜考虑在这段时间内丧失控制机械能力的潜在后果以及对机械整体停止时间的影响。

4.7.4 停止功能的逻辑

CCS的停止功能能够手动或自动启动，也能通过主动停止和/或被动停止执行。

注：主动停止可以自动跟随被动停止。

图2显示了CCS停止功能的典型逻辑顺序。箭头旁边的数字1至5对应顺序。

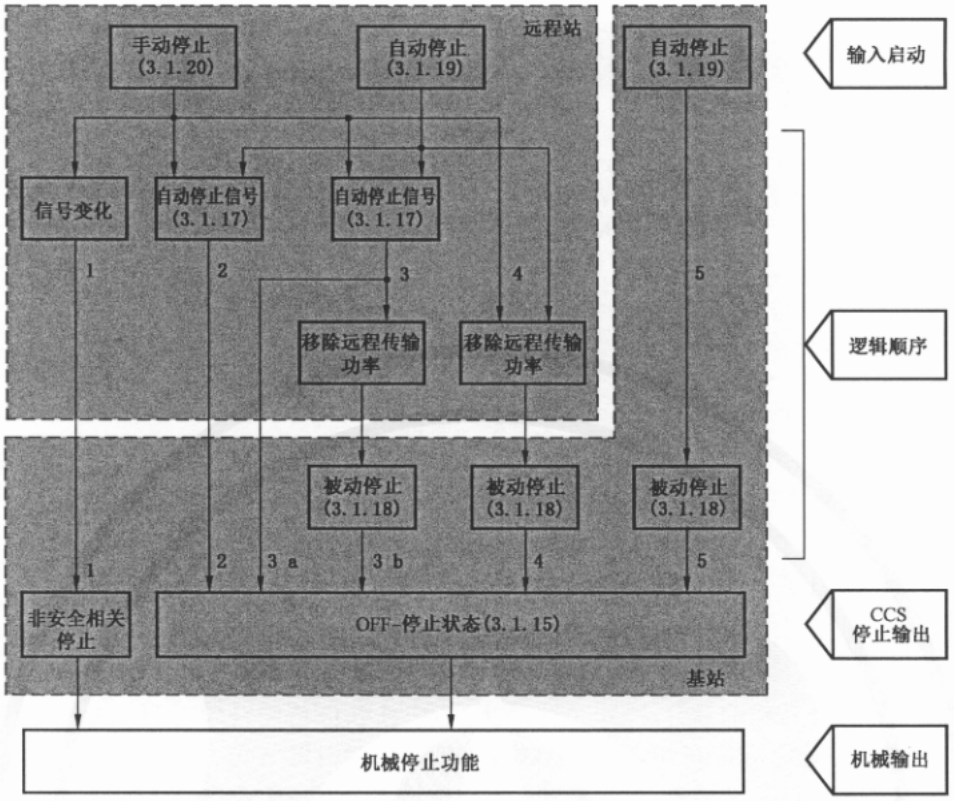

图 2　停止功能的逻辑

顺序 1 表示手动引发的停止，其导致 CCS 非安全相关的控制停止。例如，释放保持运行的控制致动机构会导致 CCS 执行控制停止功能，从而导致机械的相关运动停止。基站不引发断开状态。

顺序 2、3 和 4 表示各种类型的手动停止(3.1.20)或自动停止(3.1.19)，所有这些都最终导致基站处于断开状态。

a)　顺序 2——仅限主动停止：

- 手动停止(3.1.20)示例：激活 STOP 致动器会引起远程站发送停止信号，从而在基站产生断开状态。远程站传输功率不会被消除。
- 自动停止(3.1.19)示例：响应特定情况，远程站发送停止信号，该信号在基站产生断开状态。远程站传输功率不会被消除。

b)　顺序 3——主动停止，随后自动消除远程站传输功率。基站通过主动停止(3 a)和被动停止(3 b)引发断开状态。即使主动停止(3 a)无效，被动停止(3 b)也会引发断开状态：

- 手动停止(3.1.20)示例：激活 STOP 致动器会引起发送停止信号，然后也会消除远程站的传输功率。当接收到停止信号时，或当随后检测到有效信号缺失时，基站引发断开状态。
- 自动停止(3.1.19)示例：响应特定情况，远程站在传输功率被消除前发送停止信号。当接收到停止信号时，或者当随后检测到有效信号缺失时，基站引发断开状态。

c)　顺序 4——由于移除远程站传输功率导致的被动停止：

- 手动停止(3.1.20)示例：激活 STOP 致动器取消远程站传输功率。当基站检测到没有有效信号时，引发断开状态。
- 自动停止(3.1.19)示例：响应特定情况，在远程站中触发消除传输功率。当基站检测到没有有效信号时，引发断开状态。

顺序 5 表示另一种自动停止(3.1.19)的类型，其中被动停止和由此产生的断开状态在基站被自动

引发。例如,远程站被移动到工作范围之外,即离基站太远,由于无有效信号,自动引发基站的断开状态。

4.8 复位

远程站引发安全相关停止功能后复位,在用于控制机械危险操作的输出激活前应要求在远程站(以及每个引发安全相关停止的远程站)上采取有意动作。

如果锁定的 GSS 或 EMS 装置脱开导致通信重新建立,则可能需要在远程站上进行额外的手动复位操作。

注:依据风险评估,除了远程站的复位动作外,考虑在人员可以清楚观察危险区的位置添加一个或多个辅助固定复位装置(例如按钮)可能是合适的。

当远程站是移动或便携式的,给予特别考虑是必要的。

电源的中断和重新连接(在远程或基站处)或 CCS 任何部分的单一故障不应导致先前引发安全相关的停止功能(如 GSS 或 EMS 功能)的复位。

当检测到 CCS 内部存在故障时,应不能进行复位。

制造商提供的信息见 6.2 q)。

4.9 远程站停止传输

CCS 提供自动停止传输的场合,操作命令停止后,中性帧应传输一段时间。中性帧传输持续时间应由 CCS 制造商规定。CCS 应在预定的中性帧传输期结束时引发 ATS 功能。

没有提供自动停止传输的场合,中性帧应一直被传输直至下一个操作命令信号。

注:如果中性帧传输时间不够时传输自动停止,将引起停止输出(例如机械的主接触器)频繁地进入断开状态,这将增加停止输出的切换操作次数以及它切换的任何部件。

4.10 锁定控制功能

由于人类工效学和功能的原因,对于某些 CCS 控制功能来说,在远程站或基站中实现锁定能力(即不保持运行)可能是有用的。

注 1:通过远程站的控制致动器(例如双稳态开关或电位计)或基站的控制逻辑可实现特定控制功能的锁定。

锁定远程站的控制逻辑应只能用于预期控制机械非危险操作的输出。

除非风险评估支持,基站的锁定控制功能不应用于维持机械的危险操作。对此限制的信息应在 CCS 使用说明中提供(见第 6 章)。

注 2:在某些情况下,例如当 CCS 用于控制磁性或真空提升装置时,在基站中锁定命令的能力可以是有用的特性。

4.11 电源损失的行为

CCS 电池电压或电源的变化不应引起基站的意外输出命令。

当电池电压变化超过规定限值时,应向操作人员发出视觉和/或听觉警告。在这种情况下,CCS 应在使用信息中所规定时间内保持功能。

注:CCS 宜在足够长时间内保持功能来确定机械进入非危险状态。如果用户或系统集成商未规定时间要求,一般 10 min 为准。这段时间可能随着电池老化和温度等环境因素而变化。

当电池电压变低以至于无法保证可靠的传输时,应根据 4.7.3.5 引发自动停止。直到电池电压恢复到可接受的水平并进行手动复位操作(见 4.5 和 4.8),远程站才应继续传送帧。

如果配置数据或地址代码等信息存储在 CCS 中(见 4.15),电源电压的存在或缺失不应影响这些数据的保留。

4.12 多远程站

如果 CCS 配备多个远程站,则 CCS 的设计应使任何一个远程站被使用时不允许再使用其他站,引

发 EMS 功能和其他停止功能除外。

注：此要求不适用于不在服务中的远程站。

宜有指示哪个远程站在控制基站的方法(见 4.5)。

将控制权从一个远程站转移到另一个远程站时，应要求为此目的专门设计的有意动作，以最大限度减少由此类转移可能导致的危险情况。

4.13 多基站

当远程站可用于与几个基站中的一个通信时，应在远程站上提供选择欲连接基站的方法。选择连接到特定基站本身不应导致该基站的控制命令。

当远程站可用于控制多个基站时，在基站和/或远程站上应提供指示，以确认哪个基站处于远程站的控制之下。

4.14 暂停 CCS 控制

暂停模式可以提供允许机械地控制从 CCS 切换到另一个操作员控制站，而不激活基站停止输出，见 4.13。

注：当远程站断开，机械可以运行的典型模式，例如为了保持电池充电，或当机械由其他操作员控制站或控制系统控制时(例如自动模式)。

远程站退出机械控制应要求用户执行为专门此目的设计的有意动作。例如，使用指定开关或钥匙开关的特殊任务。在该任务完成后，远程站不再控制机械且自动停止功能不被引发。

远程站重新获得机械控制应要求远程站再次执行为专门此目的设计的有意动作。例如使用指定的开关或钥匙开关登录基站。该任务结束后，远程站控制机械。远程站宜显示 CCS 的控制状态。

暂停应：

——在远程站上显示；

——在基站激活机械控制系统的输出信号。这种模式可用时，远程站不允许使用 EMS。

4.15 可配置性保护

应采取措施，确保 CCS 的任何可配置功能受到保护以防止未经授权的修改。例如，中性帧传输的持续时间(见 4.9)，或远程和基站的通信配对，包括控制致动器对输出的配置(见 4.2.3)。

5 验证

5.1 概述

CCS 及其与机械控制系统的接口的特定要求应通过目视检查、分析(即计算)和/或测试(即型式试验、验收/常规试验、功能试验和集成试验)，由 CCS 制造商和/或系统集成商进行适当的验证和确认(即如 CCS 制造商提供的使用信息中所规定的)。

注：某些验证活动与 CCS 本身的特性有关，而其他验证活动与 CCS 的正确配置以及与机械控制系统接口的适用性有关。

如果制造商修改了 CCS 的设计配置或 CCS 与控制系统的接口的任何方面，应进行适当的重复验证。

5.2 标签和标记

应验证在 CCS 远程站和基站上有明确的标识，每个铭牌至少包含第 7 章中规定的信息。

5.3 文件

验证 CCS 符合使用信息(见第 6 章)。

5.4 功能验证

符合第 4 章规定的功能要求应通过适当的试验进行检查;如果分析证明 CCS 能够通过试验,则试验可以省略。表 2 提供了要求验证的 CCS 的功能要求摘要,其中还包括适用于与机械控制系统 CCS 接口的系统集成商的验证程序,如在使用信息中规定的,见 6.2。

表 2 功能要求的验证

章条编号	要求	方法(一个或多个指定的方法适用)			附加的验证要求
		分析	测试	目视检查	
4.2.1	防止意外致动	—	X	X	当 CCS 处于操作就绪状态时,便携式远程站应按照 GB/T 2423.7—2018 的 5.1(倾倒和翻倒)和 5.2(自由跌落方法 1)试验,除了 GB/T 2423.7—2018 第 6 章中定义的最终检查外。在这些试验过程中不应有任何信号变化,除了对应 GSS,EMS 或 ATS 的功能外功能
4.2.2	防止未经授权的操作	—	X	X	—
4.2.3	防止意外命令	X[a]	X[a]	—	—
4.3	串行数据传输	X	X	—	为了测试帧的不正确寻址和损坏,例如造成干扰
4.4	取消远程站点传输	X	X	—	—
4.5	传输和通信的建立和指示	—	X	X	—
4.6	CCS 的安全相关功能	X	X	—	—
4.7	CCS 的停止功能	X	X	—	—
4.7.3.4	紧急停止(EMS)功能	X[a]	X[a]	X[a]	—
4.8	复位	—	X	X	—
4.9	远程站停止传输	—	X	—	—
4.10	锁定控制功能	X	X	—	—
4.11	电源损失的行为	—	X	—	—
4.11	电池供电的远程站	—	X	X	按照制造商的建议电池最初应充满电。在试验期间,充电电源应与远程站断开,远程站应与最多数量的基站连接通信及试验期间远程站应持续传输

表 2　功能要求的验证（续）

章条编号	要求	方法(一个或多个指定的方法适用)			附加的验证要求
		分析	测试	目视检查	
4.12	多远程站	—	X	X	—
4.13	多基站	—	X	X	—
4.14	暂停 CCS 控制	X	X	—	—
4.15	可配置性保护	—	X	—	—
注：X——需进行的功能要求的验证。					
* 所有标记的方法都适用于此验证。					

6　使用信息

6.1　概述

CCS 的识别、运输、安装、使用、维护和停止使用以及处置所需的全部信息应以适当的格式提供，例如图纸、示意图、图表、表、说明等。

注 1：CCS 提供的技术文件将构成机械整体文件的一部分。

注 2：在一些国家，使用规定语言的要求受法律保护。

6.2　提供的信息

提供给用户的文件应包含以下信息。

a) 制造商的名称(商标名称、原产地标志)和完整地址。

b) CCS 的一般描述。

c) CCS 预期使用的环境和工作条件(温度、湿度等)。

d) 传输输出功率或发射电平。

e) 额定工作电压(直流、交流、频率)和功耗的详细信息，包括电池的下列详细信息：

- 如果用户可更换，推荐远程站的电池规范；
- 单个电池充电的典型工作持续时间及其参考条件；
- 电池更换和充电的程序；
- 电池低电量警告和引发远程站关机之间的近似时间以及可能影响此时间的因素(例如电池老化或发热)。

f) 在自由视线内的正常工作的距离范围。

g) 关于如何解决 CCS 和其他在该位置使用的系统之间可能存在的干扰问题的说明。

h) 控制致动器及其相关控制功能的所有细节，包括每个控制功能的最大响应时间。

i) 在适用场合，对不同远程站之间的控制转移的说明。

j) 是否提供自动断电(消除传输功率)，以及提供中性帧传输的最大持续时间。

k) 基站的任何控制功能和相关输出是否有用户可配置或工厂预设的锁定功能(见 4.10)，适当时，提供配置说明。提供对于控制机械危险操作有关限制使用锁定功能的说明，包括传输情况下的功能，例如通电(启动)或重新建立通信。

l) 远程站和基站之间的通信配对是出厂预设还是用户可配置的，适当时，提供配置说明。

m) CCS 支持的每个安全相关控制功能(包括停止功能)的功能规范,包括:
- 功能描述;
- 误测时的反应;
- 定时信息,包括 EMS、GSS 和 ATS 功能的安全相关输出接口(例如触点)的任何延迟时间。

n) 对于 CCS 的 ATS 功能(见 4.7.3.5),指定:
- 导致其引发的所有条件;
- 有效信号丢失与其引发之间的时间间隔;
- CCS 内的最大响应时间;如果因不同的原因有不同的时间,每次都应声明。

o) 对于每个安全相关的控制功能,其安全完整性的规范如下:
- 按照 IEC 61508(所有部分)或 IEC 62061 设计 SIL;和/或
- 如果符合 ISO 13849-1 设计的 PL。

注:其他相关数据(例如 PFH_d、$MTTF_d$/$B10_d$、DC、SFF)可便于 CCS 集成到机械控制系统中。

p) CCS 停止功能的所有启动器的详细信息,包括每个停机命令包括是否会产生主动,被动,主动然后被动的停机命令和 CCS 内的最大响应时间。

q) 执行下列操作的说明:
- 在引发任何安全相关停止功能后复位;
- 失去通信或远程站/基站失效或故障后恢复。

r) 提供 EMS 功能的使用和可用性说明,包括便携式或移动式远程站的紧急停止装置不应作为引发机械 EMS 功能的唯一手段的说明。

s) 在便携式或移动式远程站引发 EMS 功能后,只有当可以看到引发的原因已经解决,并且需要使用附加固定复位装置时,才应有可能复位。

t) 指定只有在接收中性帧(或在重新建立通信后没有收到中性帧)时,才能激活基站的哪些输出,并提供有关它们用于控制机械危险操作的警告。

u) 关于防止未经授权措施的说明。

v) 错误代码处理和建议的操作员反应的描述。

w) 如果提供了 EMS 功能,则无论机械的操作模式如何(例如自动/手动、远程/本地),应指定该功能始终可用和可操作。

x) 当 CCS 集成到机械的电气设备中时,系统集成商执行所有验证活动的细节(见表 3 和 5.4)。

表 3 系统集成商要执行的验证清单

功能要求
防止意外致动
防止未经授权的操作
防止意外命令
取消远程站点传输
传输和通信的建立和指示
CCS 的安全相关功能
CCS 的停止功能
复位
锁定控制功能

表 3　系统集成商要执行的验证清单（续）

功能要求
电源损失的行为
电池供电的远程站
多远程站
多基站
响应时间
暂停 CCS 控制

7　标签和标志

每个 CCS 基站和远程站应有清晰、耐久的铭牌，能承受应用（环境等）和预期用途。基站和远程站的铭牌至少应包含下列信息：

——供方的名称或商标；

——认证标志（必要时）；

——顺序号和型号；

——工作频段；

——额定电压。

并在相关时：

——电池类型和等级；

——必要时附加标记以识别远程站和基站的匹配。

附 录 A
（资料性）
机械的无线控制系统（CCS）示例

A.1 概述

本条涉及使用无线技术（例如无线电、红外线）控制系统的功能要求，用于操作控制站和控制系统其他部分之间传输控制信号和数据。

依靠数据传输（例如有关安全的有效停止、运动命令）的无线控制系统（CCS）的安全功能，其传输可靠性要求可能是必要的。CCS 应有适合基于风险评估所要求的功能和响应时间。

A.2 无线控制系统对控制机械的监控能力

无线控制系统（CCS）所具备的控制机械的能力应能实施自动监控或连续监控或定时监控。这种能力状况应清晰标明（例如采用指示灯、视觉显示器指示等）。

如果通信信号降级（例如降低信号电平、电池电量低）可能降低 CCS 控制机械的能力，应在 CCS 控制机械能力降低前向操作者提出警告。

当 CCS 的控制机械的能力下降至风险评估所确定的时间时，应引发机械的自动停止。

恢复 CCS 控制设备的能力不应使设备重新启动。重新启动应要求一系列预定的操作，例如，手动操作启动按钮。

A.3 控制限制

应采取措施（例如编码传输）防止机械响应非预定无线操作控制站发出的信号。无线操作控制站应只控制预期使用的机械和只影响预期使用的机械功能。

A.4 使用多无线操作控制站

当控制一台机械的无线操作控制站多于一个时，则：

——除非机械操作有需要，在同一时间内只有一个无线操作控制站起作用；

——当一个无线操作控制站的控制权转移至另一个时，应要求有控制权的控制台进行慎重的手动操作；

——在机械运行期间，只有在两个无线操作控制站设定相同的机械运行模式和/或机械功能时才有可能实现控制权的转移；

——控制权的转移不应改变选择的机械运行模式和/或的机械功能；

——每个取得机械控制权的无线操作控制站应提供其取得控制权的指示（例如指示灯、视觉显示器）。

A.5 便携式无线操作控制站

便携式无线操作控制站应提供措施（例如使用钥匙操作开关、访问代码）防止未经授权使用。

每台机械当其处于无线控制时要有指示。

当便携式无线操作控制站可以连接至数台机械中的一台或多台时，应在便携式无线操作控制站上提供选择连接至哪一（几）台机械 DE1 手段。选择要连接的机械不应引发控制命令。

A.6 禁用便携式无线操作控制站

控制时，如果处于禁用的无线操作控制站，相关的受控机械应满足 A.2 所述 CCS 丧失控制机械能

力的要求。

对需要禁用便携式无线操作控制站而不中断机械操作的场合，应提供手段(例如在便携式无线操作控制站上)将控制权转移至其他固定或便携式控制站。

A.7 位于便携式无线操作控制站上的紧急停止装置

位于便携式无线操作控制站上的紧急停止装置不应是设备上启动紧急停止功能的唯一手段。

应通过恰当的设计和使用信息避免主动和被动紧急停止装置之间相混淆。

A.8 紧急停止复位

在失电、去除使能、重新使能、通信丢失或 CCS 部件故障后，无线控制的重新启动不应导致紧急停止状态的复位。

使用说明书应说明，应在已查明便携式无线操作控制站引发紧急停止的原因后，紧急停止状态方可复位。

除了可在便携式无线控制站上对紧急停止执行机构复位，还应根据风险评估，补充提供一个或多个固定复位装置。

参 考 文 献

[1] GB/T 34040—2017 工业通信网络 功能安全现场总线行规 通用规则和行规定义

[2] ISO 12100 Safety of machinery—General principles for design—Risk assessment and risk reduction

[3] IEC 60870-5-1 Telecontrol equipment and systems. Part 5: Transmission protocols—Section one: Transmission frame formats