ICS 25.040.01
L 67

中华人民共和国国家标准

GB 16655—1996

工业自动化系统
集成制造系统安全的基本要求

**Industrial automation systems—
Safety of integrated manufacturing systems—
Basic requirements**

1996-12-17发布　　1997-07-01实施

国家技术监督局　发布

中 华 人 民 共 和 国
国 家 标 准
工业自动化系统
集成制造系统安全的基本要求
GB 16655—1996
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电　　话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行　各地新华书店经售

*
开本 880×1230　1/16　印张 1¾　字数 49千字
1997年9月第一版　1997年9月第一次印刷
印数 1—500
*
书号:155066·1-14055　定价 14.00 元
*
标 目 317—49

目　　次

中华人民共和国国家标准

工业自动化系统
集成制造系统安全的基本要求

GB 16655—1996

Industrial automation systems—
Safety of integrated manufacturing systems—
Basic requirements

本标准等效采用 ISO 11161《工业自动化系统　集成制造系统的安全　基本要求》。

1　主题内容与适用范围

本标准规定了集成制造系统安全的基本要求准则。

本标准提出了集成系统的设计、构成、安装、编程、操作、维护、使用、修理等阶段有关安全的要求和建议(见图 1)。

本标准不包括单台设备的安全要求。

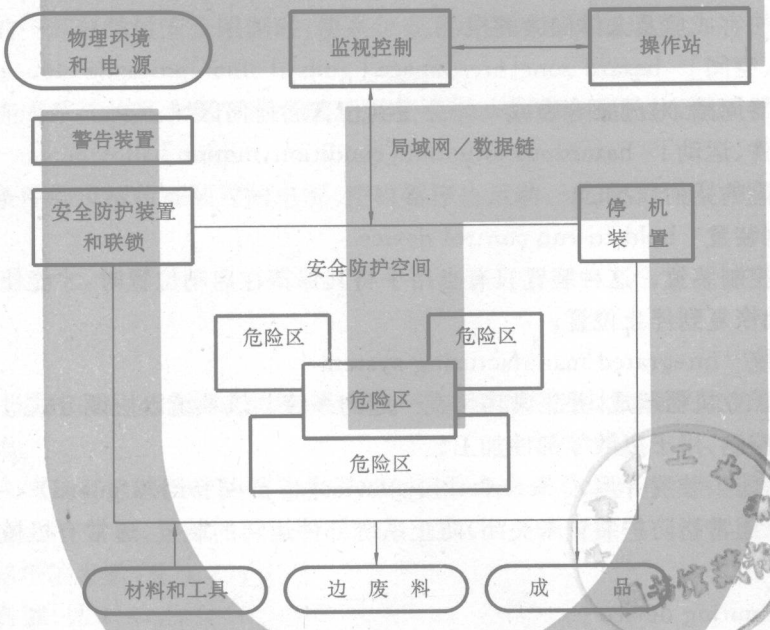

图 1　基本集成制造系统典型安全防护系统

2　引用标准

GB 2893　安全色

GB 2894　安全标志

IEC 204-1　工业机器的电气设备

ISO 6385　工作系统设计的人机工程学原则

国家技术监督局 1996-12-17 批准　　1997-07-01 实施

ISO/TR 8373 操作型工业机器人——词汇
ISO 10218 操作型工业机器人——安全
EN 418 机械安全——紧急停机设备

3 术语

3.1 屏障 barrier
危险区的物理边界。

3.2 示警屏障 awareness barrier
用物理接触报警，表示靠近将有或必有危险的一种辅助装置或屏障物。

3.3 控制停机 controlled stop
通过将命令信号降为0米停止机器运转。一旦0信号被确认，运转立即停止，但在停机期间机器的执行器仍保持供电状态。

3.4 使能装置 enabling device
一种手动操作装置，这种装置仅当在一个位置连续地操作时，才允许危险性的功能存在，但并不会启动，而在其他任何位置时，危险功能都被安全地停止。

3.5 防护装置 guard
一种专门用来起防护作用的物理遮挡式机械部件。按其结构可以分为防护罩、防护盖、防护屏、防护门、围栏等。

3.6 危险 hazard
可能导致人身伤害或危及人体健康的根源。

3.7 危险区[区域、空间] hazard zone[area, space]
机器内部或机器周围，对健康有害或人体会受到伤害的任何区域。

3.8 危险状况[条件、运动] hazardous situation[condition, motion]
会对人造成危险的任何状况。

3.9 握持运行控制装置 hold-to-run control device
一种手动启停控制装置。这种装置只有当用手将其保持在启动位置时，才能使机器保持运转，一旦手离开时，立即自动恢复到停止位置。

3.10 集成制造系统 integrated manufacturing system
由两台或多台工业机器组成，并正常连接在一起的系统。该系统以协调方式进行工作，由一台监控器或可编程控制器控制，用于离散零部件加工。

3.11 联锁装置(与防护装置并用) Interlocking device(as used with a guard)
在特定条件下(通常指防护装置未关闭)防止系统部件运转的装置。通常有机械的、电的或其他类型的。

3.12 限位装置 limiting device
一种防止系统或系统部件动作超过设计极限的装置。

3.13 局部控制 local control
系统或系统的一部分处于由各台单机的控制台或悬挂式操作盒对其进行操作的状态。

3.14 闭锁 lockout
隔能装置上的一种锁定装置。放在'OFF'或'OPEN'位置时，表明在解锁前隔能装置或设备正在受控不得操作。

3.15 暂停 muting
在正常运行中，将安全防护装置的保护功能暂时地自动停止。

3.16 操作停机 operational stop

在工作过程的某一点上，一旦进行至该点，加工过程便立即停止的动作。

3.17 悬挂式操作盒 pendant

连接到控制系统的一种装置，用以对系统或系统的一部分进行编程(或驱动)。

3.18 风险 risk

一个具体危险状态造成人身伤害的概率及其对人身伤害的程度。

3.19 保护装置 protective device

降低风险的装置(防护装置以外的)，可单独使用或同防护装置联合使用。

3.20 安全防护装置 safeguard

用于保护操作人员避免已出现或可能出现的危险的防护装置或保护装置。

3.21 安全防护 safeguarding

采用各种安全装置等专用安全技术手段，以保护工作人员免遭在设备设计上不能彻底排除或完全避免的危险。

3.22 安全防护空间 safeguarded space

由安全防护装置所确定的空间。

3.23 安全操作规程 safe working procedure

一种专门的规程，用以在执行指定任务时，减少遭受伤害的可能性。

3.24 任务程序 task program

为制造系统的专项作业而规定的动作和辅助功能的指令集。这类程序一般由用户编制。

3.25 跳闸装置 trip device

当人或其身体的一部分越过安全限制时，使系统或系统部件停机的装置。

3.26 故障查找 trouble shooting[fault finding]

顺序地判断系统或系统的某个部分不能执行预定任务或功能的原因的行为。

3.27 非控制停机 uncontrolled stop

切断引起故障条件的机械传动装置的电源，使机器停止运动。此时，所有的制动器和其他停机装置全部动作。

4 安全对策

4.1 总则

本章规定对一个系统确定安全要求的综合对策。这个对策将设计阶段采取的措施和要求用户执行的措施结合起来考虑。

首先是在保证系统具有能够接受的性能水平的前提下考虑系统设计中的安全对策。这包含以下几项：

a. 规定系统的极限参数(见 4.2)；

b. 制订安全对策(见 4.3)；

c. 具体列出所有的危险(见 4.4)；

d. 评估有关风险(见 4.5)；

e. 消除危险或尽最大可能限制风险。

如果采用以上措施，仍不可能将风险减小到能接受的程度，则在设计阶段必须考虑安全防护措施。这些措施必须是保持系统的灵活性而不减少系统的安全性。

此外，还必须提供那些难于识别的危险的有关信息(例如：编写说明书及警告标记)。

4.2 系统技术要求

系统技术要求至少应包括以下方面：

a. 功能描述；

b. 总体布局和/或模型；
c. 不同工作过程和手动操作相互联系的评述；
d. 包括手动交互作用在内的过程顺序分析；
e. 与传送装置或传输线之间接口的描述；
f. 过程流程图；
g. 设备基础方案；
h. 上料和下料装置的配置方案；
i. 上、下料所需的空间的确定；
j. 有用的事故记录；
k. 相似系统安装的研究。

设计者要有一个关于在现场中可能出现的人员的活动的规范化的书面意见，特别是：

a. 参观(出现与操作无关的第三者)；
b. 过程控制与监视；
c. 工件装卡；
d. 由操作者手动控制的设备检查验收；
e. 无需拆卸的调整和人工干预；
f. 安装；
g. 故障查找；
h. 维护。

基于上述，可使设计者制订出相应的、基于以下事项的工作程序：

a. 分析其他机组的过去及比较近期的有关情况；
b. 对生产性变化的影响的允许度(设备磨损、产品尺寸的改变等)；
c. 今后系统工作上有关系的人员介入。

4.2.1 系统设计准则

除功能描述外，在设计准则表中，还必须考虑确保安全操作所有的必要要求，包括有效地减少列在4.4中的各种危险的保护措施。

这样，系统设计才能最大限度地减少工程脱节现象，相应的步骤要求有：

a. 对人机接口的集成；
b. 先期确定在系统的各种工位(时间、空间)；
c. 先期考虑单机工作时的分断方式；
d. 环境状况的考虑(空气质量、光照条件、噪音等)。

系统设计，不仅是其工作性能的设计，还必须从使用和操作观点来考虑。

4.2.2 项目的组织

在规划、设计和建造集成制造系统中，各项安全措施，特别是有关各单机之间的相互作用的安全措施必须协调一致。这也适用于由不同供应商提供的分系统和/或单台设备组成系统的场合。

需协调的工作阶段包括(例如)：

a. 规划；
b. 设备选购；
c. 设备交付和总成；
d. 安装方法和试验步骤；
e. 分项验收及总验收；
f. 以完工单形式对系统的交付；
g. 系统验证(试车)，包括任何缺陷的校正和故障排除；

h. 可维修性；

i. 人机工程因素。

4.3 安全对策的应用

集成制造系统必须按照风险评估(见 4.5)设计并防护，使其确保能够正常发运、安装以及正确安全地使用和维护。为此，要考虑人为因素、工作任务、可能发生的事故和生产方法等之间的关系。

还必须考虑诸如噪音、有害物质、高温、低温、辐射以及物理运行环境的其他有害影响，以免造成对人身健康的损害。

系统或系统部件供应商必须说明：对物理环境的条件和外部电源的要求以及如何连接，以保证正常运行。用户应该保证满足这些条件，或者提供替代手段，并保证系统在按照技术条件要求的环境条件下运行。

4.3.1 设计与开发

在单机、分系统和全系统的开发中，一切有关安全的知识和经验都必须考虑，以便运用这些知识和经验避免人身事故和对健康的危害，或把其降低到一个可接受的水平。这包括全系统、分系统以及单机的可见性。特别是，在正常的操作员位置上，必须能充分地观察到生产流程和机器运行情况。有时，可辅以附加手段(如电视监视)。

操作和维护人员的正常位置必须易于出入，而且要处于危险区域之外。需要定期保养的部件(如加油点、定位机构)也要尽量安排在危险区之外。优先采用无危害器件，消除或减少危害，以达到所要求的安全水平。其次是通过改进工艺或过程顺序以获得更低的风险水平。

手动启停控制的设置方式必须做到明确地标志出了与之相关的危险区域。

4.3.2 安全防护

凡按照 4.3.1 中所述的措施不能或不完全能将风险减少到可接收的水平时，应按第 6 章提供安全防护装置。增加的这些安全防护装置后，不得使系统的操作和维护不必要的复杂化，并必须保持全系统、分系统和单机连接的清晰布局。

依据系统的设计和使用，可以使用一个单一的安全防护装置，也可使用几个不同的安全防护装置的组合。根据标识出的危险来选择安全防护装置。

安全防护措施应对所有操作模式保持有效(见 IEC 204-1 中 9.2.4 关于特定条件下安全防护的暂停)。

4.3.3 警告标记和个人防护用具

在 4.3.1 和 4.3.2 中所述的一些措施，在不能或仅部分能够起作用的场所，警告装置的警告标记应能表示难以防范的危险的出现。

下面的一些危险可能是难以防范的：

a. 意外动作所引起的危险；

b. 意外的能量效应(如超压、拉伸、旋转、超重、噪声、热、低温、辐射)所引起的危险；

c. 危险物质泄漏所引起的危险。

在必要的场所，应规定个人使用的防护用具。

4.4 危险识别

危险可能来自以下几个方面：

a. 系统自身；

b. 系统与其他机器或装置的相互作用；

c. 系统所在的物理环境；

d. 操作人员和系统的相互作用。

一些危险源的例子是：

a. 运动机械部件在：

1）危险区中单独地或与系统的其他部件或相关设备的正常运行；

2）意外运行状态（如：机械部件跌落、机器倾斜）。

b. 电源。

c. 能量积累。

d. 干扰：

1）电干扰（如：电磁干扰（EMI）、静电放电（ESD）、射频干扰（RFI）；

2）机械干扰（如：振动、冲击）。

e. 有害气体和物质：

1）易爆、易燃性的；

2）腐蚀性的；

3）辐射性的（如：电离或热）。

f. 失效或故障：

1）防护设施失效，包括被挪动、拆除或弃置；

2）部件、装置或线路故障；

3）电源或能源故障，包括脉动或扰动；

4）信息传输故障。

g. 人为差错：

1）设计、制造或修改中的差错；

2）操作系统、应用软件和编程中的差错；

3）使用和操作中的差错；

4）装卡差错，包括工件放置、夹持、刀具装卡等；

5）管理或用法差错；

6）维护和修理差错；

7）文件编写和培训/说明书差错。

h. 人机工程因素：

1）采光；

2）振动；

3）噪音；

4）气候条件；

5）操作员控制站的设计/布局。

4.5 风险评估

风险的评估是作为确定安全目标和安全措施的基础而进行的。

风险必须降低到一个可接受的水平。为此，本条对制订程序和计划提供这方面的指南，以便：

a. 建立一个安全的工作环境；

b. 确保人身安全和健康。

要把各种已经意识到的危险的风险都做评估，并且确定合理的安全措施及实施方案，以便把风险减小到最低程度。

要查明各单台装置的、各单台装置之间交互作用的、系统运转部件的，以及全系统的。一切设定的运行方式/条件下的危险；包括正常安全防护措施暂停使用的状态，如：编程、校验、故障查找、维护或检修等。此要求也适用于对系统的改造。

对于正常运行条件中，显然人工干预也作为生产过程的一部分时，运行风险同样要进行评估。如果存在危险，则正常生产就应避免人工的干预。

对于显然必需人工直接干预的局部生产过程的风险也要考虑（如：清除阻塞、装卡、编程/示教、故障

查找、维护等)。应认识到,在某些情况下,正常的控制顺序以及某些甚至全部正常安全防护装置可能暂停。在此种情况下,必须投入备用的安全系统作为对局部的控制和安全防护的专门保障(如闭锁)。

对系统中人员可能进入的每个区域可能发生的危险,要有危险标记,以便识别。

4.6 人机工程考虑

4.6.1 人机接口

下列措施设计用来方便自动化系统监视和数据处理。

4.6.1.1 运行的直接观察

场地的设计要便于与系统敏感点有关的信息的探测,应特别重视观测点或观测区的布局(可使用反射镜、视频系统等辅助观测手段)。

4.6.1.2 显示信息

应能让使用者获得生产循环过程实际状况的全部必要信息。全部的关于系统状况的信息应都可从人机接口界面得到,应特别重视,选定在界面上应显示的信息,及可由系统操作员请求读取的信息。

信息的表达语言要考虑系统操作人员的动作习惯和技术文化。对于信息显示的格式和外观要遵守下列要求:

a. 信号和控制的物理特征应适合于所有操作员的观察和操作能力;

b. 对给定动作及监测其结果有关的控制和信息的位置应相互靠近;

c. 信息的组成应能支持诊断(即便于识别技术系统的重要配置);

d. 提供校验显示器可靠性的信息应安排在显示器附近;

e. 所有装置的颜色、缩写、螺旋方向、图形的朝向等采用的约定要互相一致;

f. 显示系统的设计应能进行显示系统故障检测及维修;

g. 装置能力要有裕度,以适应生产和用户面的扩展;

h. 重复:通常需要把同一个信息显示在现场上的几个部位上。

在现场设计阶段要考虑在存储器中用户存入重要事件(安装、换油、偏差、偶然事件、事故等)的可能性。存储器中的这些内容便于使用户跟踪系统的历史。

再者,通过不同接口传送的信息应互连,尤其是当使用冗余原理时,以确保信息的一致性。

4.6.1.3 手动操作控制装置

手动操作控制装置的设计和安装位置应该是:

a. 确保从手动控制装置的位置上能看见动力驱动设备的状态;

b. 确保装置的功能及状态能对操作员明确地定义及显示出来;

c. 通过确保系统不同控制部件之间的统一,使手动操作装置的名称、方位等一致;

d. 控制装置的操作机构的形状、尺寸要适当选配,以确保车间操作员能正确无误地操作它们。

任何手动控制装置的动作效果应定义清楚。手动控制装置的操作状态必须清晰明显。

4.6.2 人工干预

4.6.2.1 控制和维护作业

划定及安排干预区域,以保证足够的动作空间以最小风险执行预定任务。

特别对以下部位要采取保障措施:

a. 对系统进行控制和维护作业的动作区域,应尽可能避免高度的改变和过长的移动,并对交叉部位要采取防范措施;

b. 对于长时的、频繁的或举高作业的干预空间或平台应考虑人身姿态、体型、环境和作业诸方面问题;

c. 接口配置:中央及分布控制台(固定的或移动的)配置,应能观测到操作部件;并能将操作员间通信时间制约及通信障碍的危险减小到最低程度;

d. 工作区及要求专门监视的现场区域的光照度要适于操作。并应注意可见度不受眩光或反光的

干扰。在某些场合，还应提供调整光照条件(光的强度和方向)的保障；

e. 设备的吊环或其他起吊装置和/或现场成形部件以及专用装卸工具的用法，都要便于系统的组装和拆卸。

4.6.2.2 主要的手工作业

应用人机工程方法和数据资料，使操作更加容易，，并减少干预(修理、维护、检查、编程、操作等)时的人为差错，以提高安全水平。存在人工干预的各部分的系统部件的设计，应考虑人体特征。诸如：体型、姿态、体力、动作和体能(ISO 6385)。

务必要保证操作人员：

a. 保持正常体位；

b. 可联络(视觉地及口头地)。

4.7 标志

系统应提供专用标识，至少应具有以下信息：

a. 制造商/供应商的名称和地址；

b. 系统标识；

c. 适用证书(有要求的场合)。

4.8 文档要求

系统文件应按订货时用户和供应商一致同意的语种编写，并(至少)包括以下内容：

a. 清楚详尽的系统说明及安装说明包括设备安装和外部电源连接；

b. 在系统上可见到的标志的副本(见4.7)；

c. 系统性能规范；

d. 外部电源规范；

e. 物理环境规范(例：光照、振动、噪声声级、大气污染度等)；

f. 潜在危险条件的说明和如何避免的方法(如：闭锁、阻塞、锁住)；

g. 非正常特征如何识别和纠正方法；

h. 下列有关信息：

1) 编程，

2) 操作，

3) 检测周期，

4) 功能测试的周期和方法，

5) 有关系统的修理和维护指南以及它的安全防护装置；

i. 维护工作程序记录，以帮助操作者在操作或故障查找时用的推荐性规程；

j. 提供各种安全防护装置、相互作用的功能部件的说明，以及危险动作的联锁防护装置的说明，尤其是相互作用的设备的联锁防护装置的说明(包括各种接线图)；

k. 当原有安全防护装置暂停时，应采取的安全防护措施和方法的说明；

l. 控制电路及电源电路连接的接口说明(包括图样)；

m. 限位装置调整规程。

系统的操作使用手册应包括其各构成部分的专用操作使用手册。

5 控制系统安全性能设计要求

5.1 概述

下述要求适用于集成制造系统控制的各个方面(电器、液压、气动、机械等)。

控制系统的设计制造必须做到无论在自动操作或手动操作时，只要按照技术条件使用，就不会出现人身安全事故。此要求也适用于总控制系统与单台控制之间的交互作用以及单台控制系统相互之间的

关系。

控制系统中的电器设备必须符合 IEC 204-1，特别是其中的第 9 章的规定。

电源及接地必须按照供货单位推荐的标准。

5.2 干扰

控制系统的设计与安装必须具有能保证控制功能与控制系统不受干扰源影响的良好的工程措施。如果能预知风险是干扰引起的，则必须采取隔离措施以确保对控制功能的干扰在机器工作的任何时刻均不会造成危害。

干扰源举例如下：

a. 电磁干扰；

b. 静电放电；

c. 射频干扰；

d. 振动/冲击；

e. 空间噪声；

f. 光照；

g. 辐射。

5.3 故障对安全性影响的限制

控制系统的设计、组装、安装、使用虽无法避免系统内的单个控制部件失效而产生停机动作，但是应保证在故障排除之前，系统不再启动或继续运行。

此项要求不适用于其失效不会引发危险状态的部件。

当分析故障时，必须按照下列规定(见图 2)：

a. 每次故障不得引发任何人身事故。

b. 第一个故障未被识别又连带第二个故障也不得引发任何人身事故。

假设两个独立的故障不可能同时出现，但设计人员必须考虑各种常见失效类型。

考虑失效是为了在出现失效时保证安全，及/或对某些类型的故障的监测。因此，研究与评估(故障分析)必须在各种部件的各种失效模式的设定基础上进行。

5.4 安全措施

5.4.1 控制的安全措施

除 5.3 的要求外，还必须考虑采用成熟的线路和部件，以及下列一项或多项的安全措施。

a. 部分或全部地冗余

电器、电子或液压系统的控制部件的失效保护，通常采用多部件或多路的并联或串联来实现。控制部件的失效保护不应仅依赖简单冗余。

部件冗余是使用两个或多个的控制部件并联或串联起来，用以确保可靠运行。因此，冗余器件中某个失效可能未被监测到，表面上仍在安全运行。如果冗余部件逐次失效，仍可能出现不安全状况。对此种单个器件失效的监测和对策是十分重要的。

b. 采用分布控制方式(按 IEC204-1 的 9.4.2.3)

c. 降低危险动作的速率(功率)

采用“减速法”是基于事故出现时，人员能及时从危险区内退出。当没有剪、挤危险时，可以设定危险动作速度不超过 15 m/min；当有剪、挤危险时，危险动作速度不超过 2 m/min。此数据对减速使用的使能装置也适用。

d. 监测控制功能

采用“监测控制功能”措施(也可用仿真实现)为的是，在确定方式下用固定的时间间隔监测，以决定如何从风险评估的考虑来识别故障，并当发现故障时应能发出一个安全信号(大多是停止信号)。

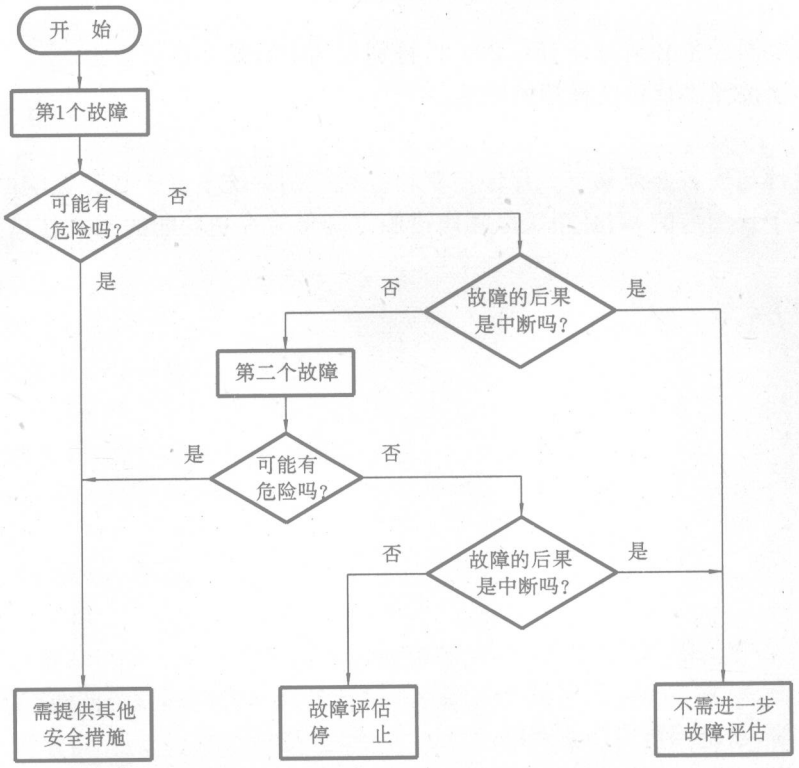

图 2 故障评估

e. 使能装置(见 6.5)

采用"使能装置"措施为的是,使用使能装置的人员能发现危险并及时采取直接行动防止事故。

f. 利用可解锁的单向阀、不经常动作的滑阀的周期性转换动作、压力阀、无弹性作用的脉冲阀。

在液压或气动系统中可能蓄有可观的能量。必须确保它们不致引起危险动作。积蓄的能量可以被引发安全功能(如复原动作)。如有必要,应提供防止后继危险(如由于压力下降、主管路关闭、泄漏、管路破裂等所引起的危险)的附加措施,如机械力锁定,可解锁单向阀等。

5.4.2 附加安全措施

当单纯的控制上的安全措施不足以防止危险性故障的后果时,必须采取诸如机械安全保护、备用照明等补充措施。

5.4.3 安全措施的组合

通常需要把多种安全措施组合使用。安全措施在集成制造系统的每个单机的控制系统设计中确定,它必须满足安全性并经过风险评估(见 4.5)。当系统部件组合中又出现新的安全要求时,应在系统层加以解决。

5.5 手动操作控制装置

各种手动控制装置必须是可迅速找到、易识别、有适当标记或标签的。这些关系到安全的措施必须安放在能果断、迅速无误地安全操作的位置上。这些装置必须安放在危险区之外,除非是作为安全措施的某些装置(如急停装置、使能装置等)。

5.6 状态显示器

状态显示器显示系统或系统的特定区域的运行状况。

5.7 系统运行方式的选择

控制设备至少应提供下列几种运行方式:

a. 正常(生产)方式:所有正常安全防护装置已连接并投入运行;

b. 某些正常安全防护装置暂停的运行；

c. 系统启动或遥控手动启动引发的危险状态已禁止的运行(如：局部操作、电源隔离或危险状况的机械锁定)。

运行方式的选择使某些操作(如：编程、校验、维护)可在监控下进行。对操作条件可能带来危险状态的部位，必须联锁进入危险区的通路。

5.8 安全防护装置暂停的控制措施

当

——设置(见 8.4.2a)

——编程(见 8.4.2a，8.5)

——程序校验(见 8.4.2b，8.6)

——故障检查(生产周期的故障查找、观测)(见 8.4.2b，8.7)

——维护(见 8.8)

这样的控制方式在安全防护空间以外不能执行操作时，相关的安全防护装置可以暂停，以允许人员进入危险区。安全防护装置的暂停必须有时限(如 10 s)。暂停可以通过可锁定的选择装置，或通过其他具有同等安全级的装置实现。

通过其他措施比只采用可锁定的选择装置能达到足够的安全级。

当人员需要进入危险区时，在控制系统中必须按照第 8 章的要求提供以下的安全措施：

a. 握持运行；

b. 使能装置；

c. 减速；

d. 减少功率；

e. 手提式紧急停机。

如上所述，安全防护装置暂停时，不会由危险区外引发危险状态。

当安全防护装置的防护作用重新恢复后，才有可能进行正常的生产。

在安全防护装置暂停时为了要给操作人员以帮助，可考虑的方法如下：

a. 显示与安全有关的能产生危险的功能元件、线路和执行器的状态；

b. 显示重要要素的状态(例如：工作运行状态、设备器件的位置参数、温度)。

5.9 局部操作

在危险区中进行设备的局部操作时，必须把此状况通知系统的其余部分。局部操作的方法应设计成为，允许操作者或其他人在特定区域中局部地操作该区中的设备，但是要能防止任何外部方式驱动该区域中的任何设备。

对于进行局部操作的系统或区域，可选择的方式应是：

a. 位于危险区域以外；

b. 能够由操作者或者其他指定人员所控制(例如：用钥匙开关或存取密码)。

处于局部操作中的机器和有关设备必须在系统操作员的直接控制之下。当局部控制时，决不允许由遥控或外部操作而引发危险状况。

局部和遥控或外部操作的转换开关自身应不能产生任何危险的状态。

5.10 启动

只有当与保护区有关的所有安全防护装置已到位并功能化，而且全部正常的操作条件均已满足时，才能由位于保护区之外的一个控制站启动系统或在系统操作区内的机器或者有关设备。

当系统(或特定区)要求由几个控制站同时启动时，启动方式必须是联锁的，以防止未达到规定的控制站数时的误启动。

反之，当由于安全的原因，系统的某个特殊区域要求是单控制点启动时，其他启动控制应设计成为

不能启动系统的其他区域，或该区域不能由其他部位启动。

5.11 停机

每个系统或系统内的区域，至少要具有两级停机：一级是与安全措施有关；另一级是与正常操作的条件有关。正常操作条件包括所有安全措施。停机功能的实施基于风险评估。

5.11.1 停机功能

停机功能不考虑相关的启动功能。停机功能必须根据风险评估，按下列类型选择。

三种停机类型如下：

a. 类型 0：直接切断产生危险状况的执行器电源停机（即非控制停机——见 3.30）；

b. 类型 1：对产生危险状况的执行器保持供电的控制停机（见 3.3），停机后再切断电源；

c. 类型 2：对产生危险状况的执行器保持电源的控制停机。

类型 0 和类型 1 应按照 5.3 设计。

根据风险评估，每个区域都将配置类型 0 或 1（或两者都要），按类型 0 或 1 停机后，重新恢复正常供电应不引起危险状况。

5.11.2 紧急停机

系统应提供一个或多个紧急停机功能，这些功能可适用于整个系统或系统内可清楚分界的区域。

在系统内可清楚分界区域情况下，各区应有仅供本区使用的紧急停机功能。一个或多个区域处在急停状态时，此状态应报告给系统（或系统其余部分）。由于清楚分界，一个急停装置动作后，该区域和系统其他区域之间的接口处不得有任何危险存在。

凡是急停功能通过电路实现的，必须符合 IEC 204-1 的规定，而使用液压驱动实现的，还须符合 EN 418 规定。

急停电路复位由指定人员进行干预。急停的复位不得引发或重新启动任何危险运动或产生任何危险状况。

每个控制站必须有手动急停装置，这种急停装置与可清楚分界的区域相连。手动急停的执行器应符合 IEC 204-1 规定。

5.11.3 安全防护装置产生的中断

安全防护装置（即跳闸装置或联锁保护装置）应与类型 0 或类型 1 停机功能相连，在多数情况下，这些安全防护装置的作用，是系统工作规程的一部分。所以，这种停机功能必须能使系统或其停机部分很容易重新启动，这一点是很重要的。这一要求根据生产工艺规程不可能实现时，需要有一个操作停机功能，它可在安全防护装置动作之前动作。操作停机功能应设计为：在生产过程的自然停止点上停机，以避免影响机器、工件和工艺规程。

当提供操作停机时，由于安全的原因不可能在任一个生产周期或其中间停止工艺过程时，则必须使用带有保护锁定的电联锁保护作为安全防护，以防止人员进入危险区，直到生产周期结束和所有危险情况均排除为止。

5.11.4 操作停机

操作停机功能是类型 2 的停机，必须符合 IEC 204-1 的规定。这一级停机是作为功能性或操作性的停机，而并不是作为安全措施。

5.12 应急动作

必须提供在紧急状态下系统器件的动作方式。举例如下：

a. 在断电条件下：

——打开溢流阀，使系统减压；

——手动松开机械制动器，防止产生附加的危害。

b. 在供电条件下：

——手动：用先导阀/驱动器手动控制各种设备；

——使设备开始反向运转。

5.13 电源中断或脉动

任何电源的中断或脉动应不发生任何危险状态，或者应启动一个直接停机动作。电源的自恢复也不应产生任何危险状况或者重新启动系统。

5.14 电源断开

必须提供所有外部电源的断开方式，并应加以标志或标签，以便识别。外部电源应具有带锁定功能的断开方式。

整个系统或系统中可清楚分界的区域，应有断开它的各种电源中的每一个源的手段，这些手段应以使人不受危险的影响和必须具有锁定能力的原则来设置。

供电设备断开装置的要求见 IEC 204-1。

5.15 积蓄能量

必须提供能够产生危险状态的积蓄能量的隔离、封闭或者控制释放的措施。

5.16 有关安全的参数

如果超出了有关安全参数的预设限值，控制系统应采取适当的措施来消除或减少危险。有关安全参数例如：位移、速度、温度和压力等。

6 系统的设计和安全防护

6.1 总则

下述安全防护装置，只要能满足 5.3 条的要求，均可用于人身安全防护：

a. 固定或可移动的防护装置；

b. 配有联锁装置（光束/挡板，压敏垫/压敏块，触觉传感器等）的跳闸装置；

c. 与人员位置有关的安全措施（如：双手控制，使能装置等）。

此外，可用诸如示警屏障、示警装置及信号、警告标记和符号、安全标记，以及安全工作须知等措施。但这些措施除非经风险评估确定，否则不能作为替代防护的措施。

6.2 安全防护要求

本条规定系统的安全防护的各项要求。

6.2.1 周界的识别

必须划定或标出系统的周界或系统内各区域的周界。如在周界内存在危险区，则应设置安全防护措施，以监测或防止人员偶然地进入危险区。入口监测应能防止危险区内的危险性动作的启动，或在人员遭到危险之前，使危险性动作停止。

从周界外进出系统的各种通道，应能防止有人偶然地进入危险区。

6.2.2 系统内部的安全防护

在单机间以及单机与系统其他部件之间有危险之处：

a. 应设置防护装置，以防止人员进入危险区域；或

b. 应设置跳闸装置，以监测人员进入危险区域。

监测装置应能防止危险状态的启动，使危险区内产生危险状态的动作立即停止（见 5.11.3），或防止进入危险区而引起危险状态。

6.2.3 在单台机器处的安全防护

系统内能使工作人员处于危险之中的工业机器或其他设备，均应按照有关的标准提供安全防护措施。无标准者，应按照本标准，设置附加的安全防护措施。

6.2.4 手动操作的安全防护

在调整、编程、程序校验、故障查找、维护及检修工作中，均应提供相应的安全防护。

在调整、维护以及检修工作时，危险区内的危险状态应由局部控制。

6.3 防护装置

制定系统的安全防护措施时，应考虑以下各种防护装置形式：

a. 固定的，只能用工具才能拆除的；

b. 移动的(如可调的、插入式的、双向的等)；

c. 带或不带门或通道口(例如：上料/下料)的周界。

注：防护装置可以单独工作；只有当它与联锁装置或与带有防护锁定的联锁装置一起闭合时才有效。在此情况下，即能确保安全防护。

固定防护装置安装方式应是：

a. 永久地(如：焊接)；或

b. 用紧固件固定，必须用工具才能拆除。

移动式防护装置是用机械方法(如用铰链或滑板等)与机架或邻近的固定器件连接，无须工具即可拆除。防护装置应联锁，以便启动危险状况的停机装置，防止防护装置开启时危险状况的出现。

可移动式防护装置必须是：

a. 其安装位置使入口通向无危险区；

b. 危险状况消除前，能阻止人员进入危险区域；

c. 装置打开时，应能阻止危险状态启动，或应使危险区内的危险状态紧急停机起作用，或能防止人员进入，而引起危险状态；

d. 不禁止人员从系统内退出。

保护人员免遭与系统有关的危险的防护装置的设计、制造和应用，应能：

a. 防止人员无意地从防护装置上方、下方，绕过或穿过防护装置进入危险区域；

b. 防护装置本身或与系统的其他部件，不会构成对人员的危害；

c. 有明确地确定的保护状态位(如：使用铰链、挡块、轨道等)；

d. 提供对工作区域的可见性，以适应特殊操作；

e. 防护装置其安装方式应使其不能轻易地移动，并应连接到固定的表面上；

f. 设计采用的材料及强度可保护人员脱离与系统使用有关的危险，并能经受住正常的操作和环境力。

6.4 联锁和保护跳闸装置

6.4.1 联锁装置

联锁装置应按5.1条款要求设计制造。与防护装置一起工作的联锁装置在使用时，应按如下安装和调整：

a. 控制系统通过联锁装置，在防护装置闭合之前，或必要时在复位前(见6.4.3)，应能禁止系统或由联锁装置控制的部分系统的正常运行。

b. 联锁装置闭合应不启动正常操作。启动应是操作者的周密考虑后的操作(见5.10)。

c. 在危险已消除，防护装置处于闭合锁定前(带防护锁定的联锁保护)；或是系统正在工作时打开防护装置，均给出类型0或类型1停机功能(联锁防护)。

d. 重新建立联锁后，只有当重新启动不会引起其他危险时，才能从停止状态重新启动系统或部分系统。

e. 在可能接近危险之前，电源中断足可以消除危险。在如电源中断还不能立即消除危险时，联锁系统应备有保护锁定或制动装置。

f. 在可能全身进入安全防护空间，且又不能安装复位装置之处，必须有一个能证实确实无人处在安全防护空间内的良好的可见性附加措施，以防止有人在安全防护空间内时重新启动。

g. 用来防止一种危险的联锁功能(如该危险状态的停机)不得引起不同的危险，如将有害物质释放到工作区内。