EN ISO 13849-1

Allen-Bradley

Guardmaster®

安全标准参考指南

从标准EN954-1到
标准EN ISO 13849-1的过渡

LISTEN.
THINK.
SOLVE.®

Allen-Bradley · Rockwell Software

Rockwell Automation

简介

该出版物用于对应用机器安全的法规和标准近期和将来的变更作出说明。这主要是欧盟的要求，但是由于机器安全标准的发展在逐步全球化，许多内容也与世界其他地区有关。

机械与过程继续变得越来越快，越来越灵活，功能越来越强大。为了操作员与技师的持续安全，需要提供保护性措施，反过来说，即是为了与自动化日益增长的复杂性保持同步。传统上，安全系统在自动化系统中一直是单独实施，独立运行，并且经常与自动化系统平行运转。这样做有一个很好的理由，那就是安全系统必须一直保持可用状态。在机器的“正常”运行状态下，故障和无法预期的情况一定不能让安全保护措施发生降级或者妥协。

然而，随着自动化系统变得越来越智能化，因此要求必须有安全系统的支持，这是一个不可避免的事实。安全功能不断增长的要求取决于机器正在做的事情或者它所处的模式。在某种方式上，这意味着“安全”在与“正常”控制系统进行通讯。这表明我们需要重新考虑，我们如何实现安全系统的独立性以及完整性。其中最显著的一个表现便是新一代的标准通常都会参考功能安全标准。在本出版物中，我们将要考虑最为明显的问题之一：EN ISO 13849-1标准。除此之外，还有一个欧盟新的机械规范，也将有望成为最新工业环境中的法规。

对于供应机器或使用它们的人来说，被告知相关标准与管理机构要求是十分重要的。该出版物旨在协助相关任务，特别是与控制系统方面相关的任务。它并不是在标准和法规中描述过的详细研究具体规定的替代品。它的目的在于进行概述，希望它能有助于澄清有关要求的问题。

从标准EN 954-1到标准ENISO 13849-1的迁移

多年来，对安全系统进行分级最为通用的方法一直是使用标准EN 954-1的分类[或者是它的对应标准ISO 13849-1:1999]。在2009年12月末，EN 954-1将会被撤销[它的对应标准ISO 13849-1:1999已经被撤销]。这一做法的主要含义是说在该日期以后，这个标准已经不再用于表明其与机械规范的一致性。

代替EN 954-1的新标准已经出版。EN ISO 13849-1:2008，称为“机器安全 - 控制系统部件的安全”。还有可以使用的另外一种标准：EN/IEC 62061“机器安全 - 电气、电子和可编程电子控制系统的功能安全”。以上两种标准的任何一种可以表明与机械规范的一致性。在该出版物中，我们将会重新考虑两种相关标准之间的关系。选择哪一种标准由用户决定，但我们集中精力于标准EN ISO 13849-1:2008。它已被具体起草，为使用分类的系统设计者提供一个过渡，因此它很可能成为最为常用的机器安全系统标准。它可用在完整的系统中或用在一个子系统中。

标准EN 954-1和标准EN ISO 13849-1之间的基本差别

首先让我们来观察一下旧标准EN 954-1与新标准EN ISO 13849-1之间的基本差别。旧标准的输出为类别[B, 1, 2, 3或者4]。新标准的输出为性能[PL a, b, c, d或者e]。类别概念依旧保持，在PL要求一个系统之前，但有一些附加要求需要满足。

这些要求以基础表格的形式如下所示：

- 系统的架构 本质上，这会捕获到我们作为类别已经使用过的。
- 系统组成部分所需的可靠性数据。
- 系统所需的诊断覆盖率[DC]。这有效了表示系统中故障监控的数量。
- 保护免受通常原因导致的故障。
- 保护免受系统性故障
- 在相关之处，软件的具体要求。

稍后我们将更加深入地观察一下这些因素，但在此之前思考一下整个标准的基本目的和原则是大有帮助的。显而易见的是我们有许多新东西要去学习，但细节会让我们理解正在尝试所做的是什么事情，以及为什么去做这件事。

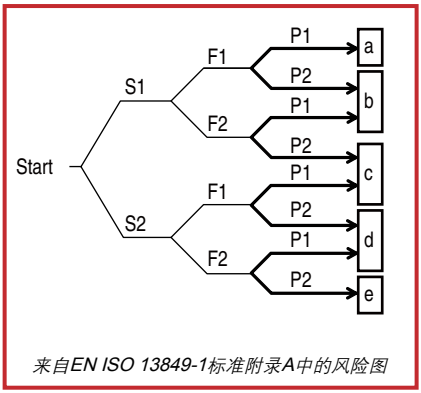
首先，我们为什么需要新的标准? 很显然，过去十年间机器安全系统中所用的技术已经前进并且有相当程度的更改。相对而言，最近的安全系统所依靠的“简单”设备带有可预见到的以及可预测的故障模式。最近一些时间内，我们观察到安全系统中更加复杂的电子和可编程设备的使用正在增长。这在成本、灵活性与兼容性方面给予了我们极大好处，但它也意味着之前存在的标准已经不再胜任。为了理解安全系统是否已经足够好，我们需要知道更多有关信息。这就是新标准需要更多信息的原因所在。由于安全系统开始使用更为“黑盒子”式的方法，我们开始更加依赖标准的一致性。因此这些标准需要能够合理质问该技术。为了实现这一目标，他们必须提到基础因素，如可靠性、故障检测、架构完整性和系统完整性。这就是标准EN ISO 13849-1存在的目的。

为了规划标准的逻辑方式，重要的是要意识到它在功能上有着两种不同的用户类型： 安全子系统设计者与安全系统设计者。通常子系统设计者[典型上称为安全部件生产商]会倾向于高等级的复杂性。他们需要提供所需数据，这是为了系统设计者能确保系统的充足完整性。通常这将会需要一些测试、分析和计算过程。结果将会以标准需要的数据格式表示出来。

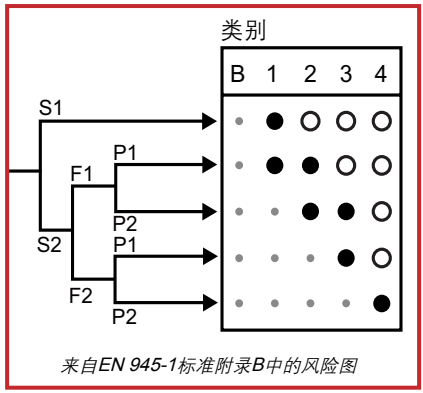
系统设计者[典型上称为机器设计者或集成商]将会使用该数据，执行一些相对而言简单计算，以确定系统的整体性能等级[PL]。

为了确定PL所需的[PLr]，标准提供风险图，使之进入损坏严重性、接触次数和避免可能性的应用因素为输入。

输出为PLr。旧标准EN 954-1的用户将会熟悉这种方式，但是现在请注意S1线在旧的风险图位置进行细分。请注意它意味着在较低风险等级进安全措施的完整性可能会进行重新配置。



来自EN ISO 13849-1标准附录A中的风险图



来自EN 945-1标准附录B中的风险图

现在，我们可以观察到系统的PLr[来自风险图]与通过系统获得的PL[通过计算]之间的直接关系。

然而，有一样非常重要的零件需要覆盖。我们现在可以区分系统需要多么好的标准，并且如何确定它有多好，但是我们不知道它应该做些什么。我们需要确定安全功能是什么。很明显，安全功能一定对任务是合适的，我们怎么提供? 标准怎样帮助我们?

意识到所需功能只能通过考虑特性战胜实际应用的方法来进行确定，这是十分重要的。这可以被视为安全概念设计阶段。它不能被标准完全覆盖，因为标准不了解具体应用的全部特性。这也经常应用在机器制造商，它们制造机器但不一定解它会使用的准确条件。

列出通常使用的安全功能，标准会提供一些帮助，并且给出了一些正常的要求。其他标准，例如EN ISO 12100： 基础设计原则和EN ISO 14121： 风险评估在此阶段强烈推荐使用。也有大型范围的机器具体标准，将会提供具体机器的解决方案。在欧洲EN标准中，他们被定义为C类型标准，它们中的大多数在ISO标准中都有对等的标准。

因此我们现在可以观察到安全概念设计阶段是由于机器类型和应用特性以及使用环境决定的。机器制造商预计到了这些因素，为了能够设计安全概念。使用特定的[即预期的]条件在用户手册可以找到。机器用户需要检查比较他们的实际使用情况。

因些我们现在需要描述一下安全功能。从标准的附录A中，我们可以得到控制系统[SRP/CS]的安全零件所需的性能等级[PLr]，该系统将会用于实施该功能。现在我们需要设计系统，确保它符合PLr。

在决定使用标准[EN ISO 13849-1或者EN/IEC 62061]的明显因素之一便是安全功能的复杂性。在大多数情况下，对于机械而言，安全功能相对而言是简单的，标准EN ISO 13849-1将会是最为适宜的。为了评估PL，它利用了已经提及的因素：可靠性数据、诊断覆盖率[DC]、系统架构[类别]以及相关位置、软件要求等。

这是一种简单的描述，意味着的只是概述。理解标准结构中必须应用的全部条款是十分重要的。不过，帮助垂手可得。有一种优秀的软件工具可以帮助我们计算方向。这种软件工具被称为SISTEMA。由在德国的BGIA公司生产。使用和下载更多详细信息请访问网址：

www.dguv.de/bgia/en/pra/softwa/sistema

在该出版物即将打印时，它有德语和英语两个版本，其他语种的版本将在日后发布。该工具并不是商业生产。SISTEMA的开发者BGIA是一家位于德国的，备受尊敬的研究与实验机构。依照德国的法定事故保险与保护准则，该机构特别擅长处理与安全相关的科学与技术难题。它与全球超过二十多家的职业健康与安全机构有合作关系。BGIA的专家与他们的BG同事一起重点参与起草了EN ISO 13849-1标准和IEC/EN 62061标准。

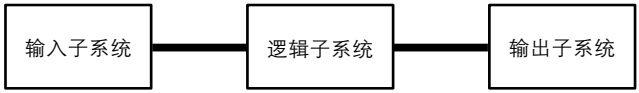
Rockwell Automation®带SISTEMA使用的数据

罗克韦尔安全设备的“library”(文献库)是可用的带有SISTEMA性能等级计算工具。为获得该文献请登陆到：

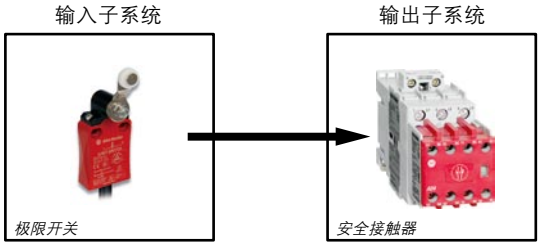
www.discoverrockwellautomation.com/safety

无论是PL以何种方式完成，从正确的基础开始是非常重要的。我们需要以标准允许我们开始的相同方式浏览系统。

系统结构

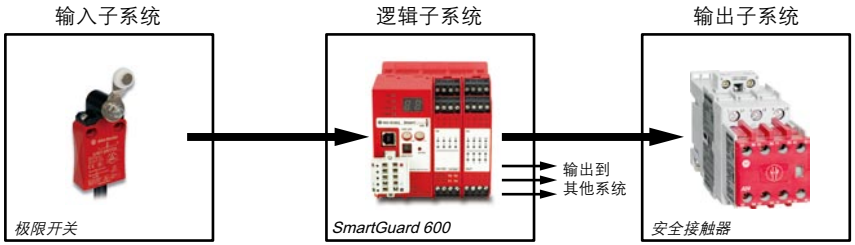


任何一个系统都可以被分为基础系统部件或者称为“子系统”。每个子系统都拥有它自己的离散功能。大多数系统可被分成三个基础功能：输入、逻辑求解和激活[有些简单的系统可能没有逻辑求解功能]。实施这些功能的部件组称为子系统。



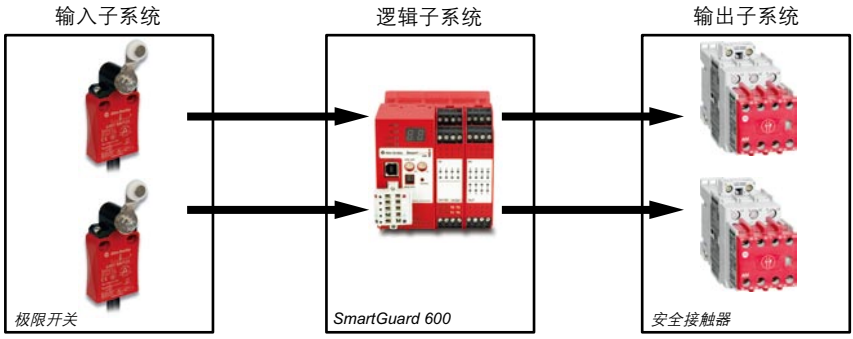
互锁开关与安全接触器

一个简单的单通道电气系统示例如上图所示。它只包括输入和输出子系统。



互锁开关、安全控制器与安全接触器

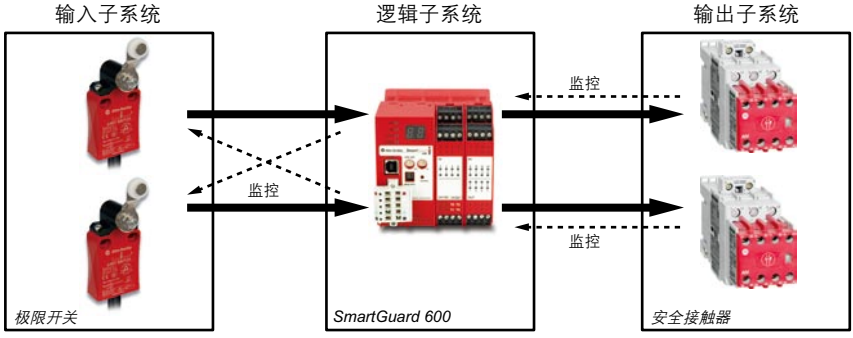
系统稍微复杂一些，因此也需要一些逻辑。安全控制器内部将会产生容错(即双通道)，但整体系统依然限制在单通道状态，这是由于单一限位开关和单接触器的缘故。



双通道安全系统

拿起以前图画中的基础架构，也有其他需要考虑的地方。首先，系统一共有多少个“通道”？如果它的子系统失效，单通道系统将会失效。双通道系统[也称冗余系统]需要拥有两处故障，在系统失效之前每个通道中有一处。因为它有两个通道，它能容忍一个单独的故障，并且依然继续工作。上面的图中展示了一个双通道系统。

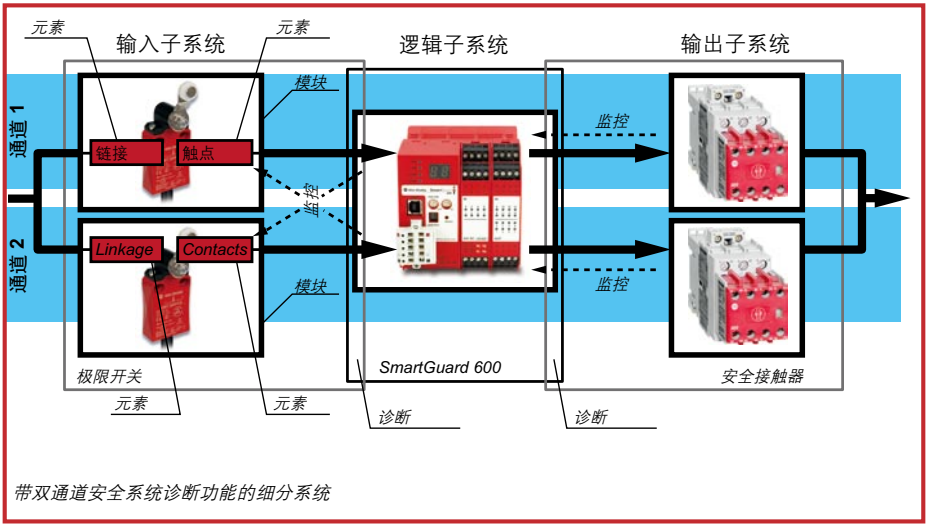
很明显，对于危险条件下时，双通道系统更不容易发生失效，不是单通道系统。如果我们包括故障检测的诊断措施，我们可以让它变得更加可靠[在它的安全功能方面]。当然，检测故障的同时，我们也需要理解它，并将系统转换为安全状态。下图显示包括通过监控技术实现的诊断措施



带双通道安全系统的诊断

通常[但并不总是这样]在所有的子系统中，系统由两个通道组成。因此我们可以看到，在这种情况下，子系统有两个“子通道”。标准中将它们描述为“模块”。双通道子系统会有一个最小的双模块，且单通道子系统会有一个最小的单模块。有可能一些系统是由双通道和单通道模块一起组成的。

如果我们想要更加深入地调查系统，我们需要观看一下模块的部件零件。SISTEMA工具使用“元素”这个术语描述这些部件零件。



带双通道安全系统诊断功能的细分系统

限位开关子系统显示细分成了元素等级。输出接触器子系统被细分成了模块等级，且逻辑子系统根本未被细分。两个限位开关的监控功能和接触器用逻辑控制器执行。因此，盒子代表限位开关，且接触器子系统与逻辑子系统盒体拥有小部分的重叠。

系统细分的原则可在标准EN ISO 13849-1和SISTEMA工具的基础系统结构原则指定的方法辨别出来。然而，注意有一些细微差别是十分重要的。该标准并不限制具体方法，但为了简化方法将预估结果确定为PL，通常的第一步是打破系统结构，闯入每个通道中的通道和模块。带有SISTEMA工具，系统通常首先被划分为子系统。标准并未明确描述出子系统概念，但它在SISTEMA中的用法更易理解和更有直觉方法的特点。当然，这对最终计算没有影响。SISTEMA和标准都使用相同的原则和规则。有趣的是注意子系统方

法也用于标准EN/IEC 62061中。

我们一直在使用作为示例的系统只是标准指定的系统架构中五种基础类型之一。对类别系统熟悉的人会辨别出表示类别3或者4的示例。

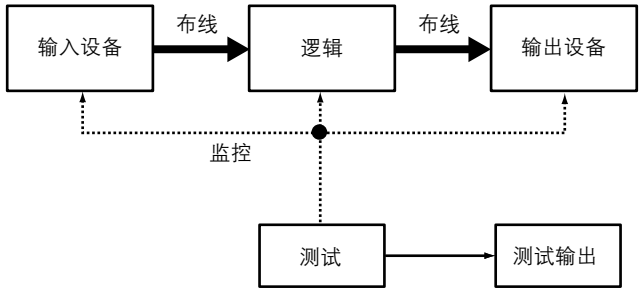
标准使用原来的EN 954-1类别作为它指定系统架构的五种基础类型。它将它们称为指定架构类别。对类别的要求几乎都是相同的[但不完全是]，在标准EN 954-1中指定。指定架构类别是通过下面图画表示的。注意它们能应用于一个完全的系统或者一个子系统，这是十分重要的。这些框图不应被纯粹视为物理结构，它们更多用于概念需求的图形表示。

指定架构类别B

指定架构类别B必须为基础安全原则[参见EN ISO 13849-2标准附录]。在发生单一故障时，系统或子系统会失效。参见EN ISO 13849-1标准的全部要求。

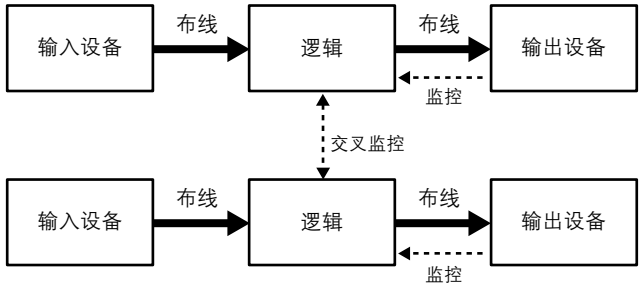
指定架构类别1

指定架构类别1有着与类别B相同的结构，在发生单一故障时同样会失效。但是因为它也必须使用久经验证的安全原则[参见EN ISO 13849-2标准附录]，它比类别B更不容易失效。参见EN ISO 13849-1标准的全部要求。



指定架构类别2

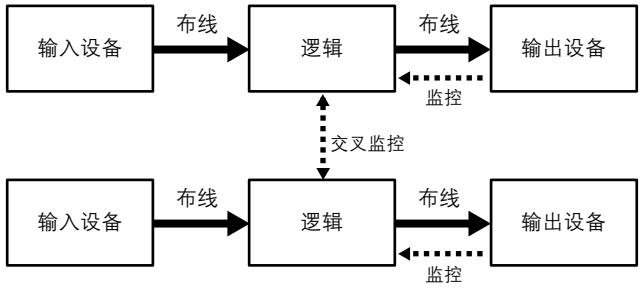
指定架构类别2必须为基础安全原则[参见EN ISO 13849-2标准附录]。同样也必须通过系统或者子系统的功能测试进行诊断监控。这必须在启动时发生，然后周期性带频率，对安全功能的每次需求它等同于至少一百次测试。如果单一故障发生在功能测试期间，系统或子系统依然会失效，但这通常比类别1更不易发生。参见EN ISO 13849-1标准的全部要求。



指定架构类别3

指定架构类别3必须为基础安全原则[参见EN ISO 13849-2标准附录]。也会有发生单一故障时，系统/子系统不能失效的要求。这意味着系统需要与安全功能相关的单一故障容错功能。实现这个要求最常用的方法是部署一个双通道架构，如上图所示。除此之外，它也需要，无论在哪里都可用的功能，即单一故障应能检测到。这个要求与标准EN 954-1的类别3的原始要求是相同的。在短语“无论在哪里都可用”在文中的含义证明其有些问题。它表示类别3可以覆盖来自带有冗余的系统的一切，但对于检测单一故障地方的

冗余系统，没有检测到故障[通常用描述性且适合的术语称为“糟糕的冗余”]。这个问题在标准EN ISO 13849-1中有所讨论，通过需要预估诊断覆盖率[DC]的质量。我们可以观察到系统的可靠性[MTTFd]越大，我们所需的DC就会越少。然而，很显然DC需要类别3架构的至少60%。



指定架构类别4

指定架构类别4必须为基础安全原则[参见EN ISO 13849-2标准附录]。有关类别3拥有一个相似的要求图，它需要的监控能力越大，即诊断覆盖率越高。这是通过重虚线表示监控功能。大体上说，类别3和类别4之间差别是：类别3必须能检测到大多数情况下的故障，类别4必须检测到所有单一故障。DC需要至少99%。即便是故障组合，也不能导致危险故障。

可靠性数据

EN ISO 13849-1标准使用可量化的可靠性数据作为PL计算的一部分，由控制系统的安全零件实现的。这明显违反了EN 954-1标准。引起的第一个问题便是“我们从哪里获得数据？” 有可能使用来自识别可靠性手册的数据，但标准更为清楚地表明优先的资源就是制造商。为此目的，罗克韦尔自动化在SISTEMA数据文献库的表格中获得了相关信息。在适当的时候，它将会以其他形式出版这数据。在我们进行下一步之前，我们应该考虑什么类型的数据是需要的，同时也能明白它是如何产生的。

所需数据的最终形式作为标准的PL目的地[以及SISTEMA]为PFH[每小时危险失效概率]。这是通过PFHd缩写，用于IEC/EN 62061标准的相同数据。

PL (性能等级)	PFH_D (每小时危险故障的可能性)	SIL (安全完整性等级)
A	$\geq 10^{-5}$ to $<10^{-4}$	无
B	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
C	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ to $<10^{-6}$	2
E	$\geq 10^{-8}$ to $<10^{-7}$	3

上面的图表表明了PFH与PL与SIL之间的关系情况。对于有些子系统来说，PFH或许来自制造商。这使计算的生命周期更加容易。制造商通常必须执行一些相对复杂的计算，和/或测试他们的子系统。一旦不适用的话，EN ISO13849-1标准就会给我们一个以单通道的MTTFd[危险失效的平均时间]为基础的备用简单方法。系统或子系统的PL[还有PFH]可以利用标准中的方法和规则计算出来。甚至使用SISTEMA可以更为方便地完成。

MTTFd

它表示在发生失效之前，导致安全功能失效之前的平均时间。它以年为单位表示。它是每个通道的模块的MTTFd的平均值，可以应用于系统或子系统。标准会运行下列公式用于计算单通道或子系统中每个元素的所有MTTFd的平均值。

在这个阶段，SISTEMA值非常明显。自从这些任务由软件执行以来，用户是在业余时间用于表格的咨询和公式的计算。最终结果可以多种页面报告的形式打印出来。

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}} \quad (D.1)$$

这里

$MTTF_d$

代表全部通道；

$MTTF_{di}$, $MTTF_{dj}$

每个元素的MTTFd，对安全功能起到了很大作用。

第一个和超过了每个单独的部件，第二个和是等数，简单地来自于所有相同MTTFdi被分在同一个组里的相同部件。

在大多数双通道系统中，两种通道是相同的，因此公式的结果可以代表任何一种通道。如果系统/子系统通道不同，标准提供公式去满足它。

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right] \quad (D.2)$$

在这里$MTTF_{dC1}$和$MTTF_{dC2}$是两种不同冗余通道的数值。

实际上，这就是两个平均值的平均值。为了简化，它也允许使用最差情况的通道值。

标准将MTTFd分为三个范围的组，如下所示：

3到<10年 = 低

10到<30年 = 中

30到100年 = 高

正如我们将会看到的，MTTFd平均值的范围结合了指定架构类别和诊断覆盖率[DC]，以提供预备PL等级。这个“预备”的术语用在这里，是因为包括系统化完整和反对通用失效的措施等其他要求必须在相关位置给予满足。

数据确定的方法

我们现在需要深入探究一个阶段，讨论制造商如何确定PFHd或者MTTFd的数据。当处理制造商数据时，理解这些知识是必要的。部件可以分成三个基本类型：

- 机械学(电子机械、机械、气动、液动等等)
- 电子(即固态)
- 软件

在这三种技术类型的通用破坏机理之间是有基本差别的。在基本格式中，它可以被归纳为以下这些：

机械学技术

故障与固有可靠性与使用率成正比。使用率越大，部件零件越有可能降级和出现故障。请注意这不是出现故障的唯一原因，除非我们限制在运行时间/周期内，它将是主要原因之一。很明显的证明是每十秒进行一次开关转换的接触器，它的运行比每天进行一次开关转换的接触器时间更短，所以更为可靠。机械学技术设备通常是由单个部件用于各自具体用途的部件组成的。部件进行成型、模块化、铸模和加工等过程。它们通过连接、弹簧、磁铁、电子绕组等步骤形成一个机械结构。因为部件零件通常上没有其他应用的使用历史，我们不能找到它它们预先的可靠性数据。机械结构的PFHd或MTTFd的估计值通常都是基于测试进行的。EN/IEC 62061标准和EN ISO 13849-1标准都主张进行一个名为B10d测试的测试过程。

在B10d测试中，许多机器样品[通常至少为十个]在适合的典型条件下进行测试。操作周期的平均数目达到危险条件样品故障的10%之前被称为B10d值。在实操中，通常会有全部样品在安全状态中全部故障的情况发生，很明显标准B10d[危险]值是B10[安全]值的2倍。

电子技术 -

有些运动零件没有有形耗损。在指定的操作环境与相应电子电路的特定电气、温度[etc]特性、主要故障与它所构成部件[或者没有]的固有可靠性成正比例关系. 出现单独的部件故障可能会有许多原因；生产期间的错误引进、过多的电压浪涌、机器连接等

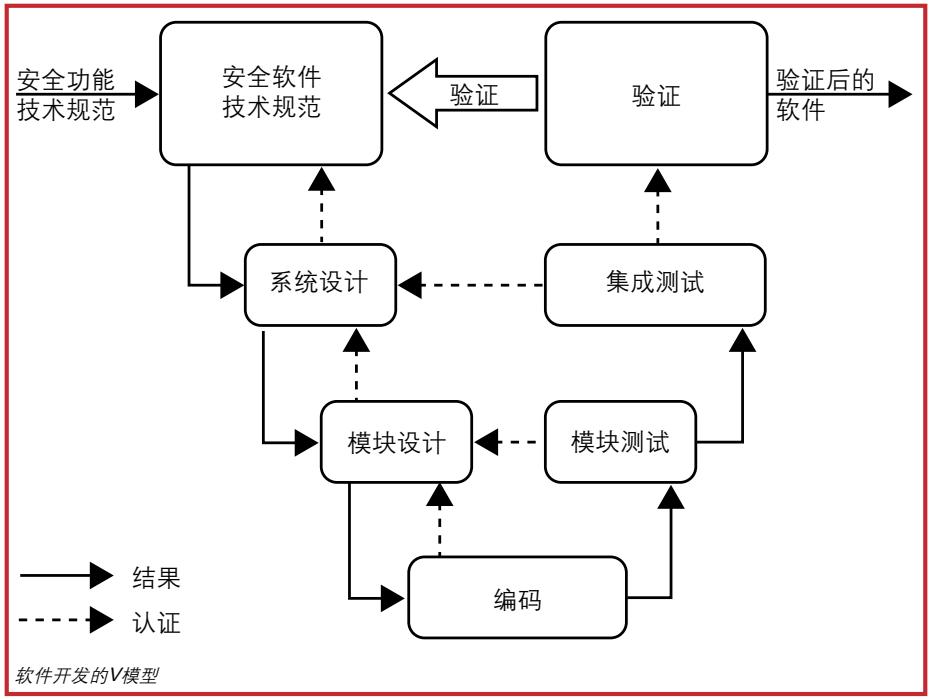
等。通常，电子部件中的故障很难通过分析而预测出来，它们似乎都是随机产生的。因此在测试实验室条件下电子设备的测试不一定发现典型的长期故障型态。

为了确定电子设备的可靠性，它通常用于分析和计算。我们可以找到可靠性数据手册中单个部件的良好数据。我们可以利用分析确定部件哪种故障模式是危险的。部件故障模式达到50%安全和50%危险这样的平衡是可接受和普通的。这通常会造成相对而言较为保守的数据。

IEC 61508标准提供了公式用来计算设备子系统的危险故障[PFH或者PFD]的整体概率。这个公式相当复杂，将[适用位置]部件可靠性，潜在的故障原因[贝塔因数]，诊断覆盖率[DC]，功能测试间隔和验证测试间隔等等因素全部考虑了进去。好消息是这种复杂的计算通常是由设备制造商来完成的。EN/IEC 62061标准和EN ISO 13849-1标准接受子系统在IEC 61508标准的方式下进行计算。PFHd结果可直接用于EN ISO 13849-1标准附录K或者ISTEMA计算工具。

软件 -

软件故障在性质上通常系统固有的。通过设计、写入或者编辑的方式都可能导致故障。因此全部故障是由系统生产的方式导致的，而不是使用。因此为了控制故障，我们必须控制系统。IEC 61508标准和EN ISO 13849-1标准可提供这方面的要求与方法。我们不需要在此逐一细说，除了说明一下他们使用是经典的V模型。



软件开发的V模型

嵌入式软件对设备的设计者是一个重要问题。常用方法是开发嵌入式软件，与在IEC 61508标准中第3部分布局的形式化方法相符合。当提到应用代码时，用户进行接口的软件，大部分的可编程安全设备都经过认证的功能模块或例程。这简化了应用代码的验证任务，但它必须记住完整的应用程序需要验证。模块链接与参数处理的方式必须证明对指定任务是有效的。EN ISO 13849-1标准和IEC/EN 62061标准都提供这个过程的指导准则。

诊断覆盖率

当我们考虑到类别架构 类别2、3和4的时候，我们已经接触了这个话题。“诊断覆盖率”这个术语[通常缩写为DC]用于描述测试的有效性。一定要认识到DC不仅仅是部件发生危险故障的数目，它还是占总危险故障率的百分比。λ这个符号用于表示“故障率”。DC代表两种类型的危险故障发生率之间的关系；

危险检测故障[λdd] 即这些故障会导致或者可能导致安全功能的丢失，但会被检测到。在检测到故障之后，故障反应功能会令设备或系统进入安全状态。

危险故障[λd]即所有这些故障可能会潜在导致，或者导致安全功能的丢失。这包括已检测到的故障和未检测到的故障。当然真正危险的故障就是那些未被检测到的故障[术语λdu]

DC用公式表示为，

DC = λdd/λd表示为一个百分数。

这个术语DC的含义对于标准EN ISO 13849-1很普通，且对于EN/IEC 62061标准也一样。然而它的来源方式却是不同的。后者的标准是在故障模式分析的基础上进行计算的，但标准EN ISO 13849-1提供了检查表形式的简化方法。各种不同的诊断技术都与实现其用途的DC百分数一起列在表中。有些情况下，仍然需要进行理性判断，例如有些实现DC的技术与执行测试的时间长度是成正比例关系的。时常有人认为这个方法太过笼统。然而估计DC值取决许多不同的变量，与其所使用的技术，结果也只能尽量描述出大概的情况。

EN ISO 13849-1标准中的表格是通过BGIA进行广泛调查的基础上，由知名的实际诊断技术在真实应用情况下进行的，理解这一点是十分重要的。考虑到简化的原则，标准将DC分成了四个基础范围。

<60% = 无

60% to <90% = 低

90% to <99% = 中

≥99% = 高

以范围的方式处理而不是对待单个的百分数，也能以切实可行的精度更为现实地进行考虑。SISTEMA工具使用与该标准相同的检查表。由电子设备的使用越来越复杂，DC成为了一个更为重要的因素。很可能在该标准的未来版本中会进一步澄清这个问题。同时，利用工程判断与利用常识也是足以正确选择DC范围的。

常见原因故障

在大多数的双通道中[即单一的容错]系统或者子系统中，诊断原则是以两个通道不会同时出现危险故障为假设前提的。术语“同时”比“在诊断测试间隔时间内”的表达更为准确。如果诊断测试时间间隔相当地短[即小于八小时]，它就会合理假设两个分隔的并无关的故障极不可能在那同一段时间内发生。然而，标准清楚地阐明我们需要谨慎考虑有关故障是分隔和无关的这一可能性。例如，如果在部件中的故障可预测会导致其他部件的故障，然后导致的故障总数被视为单一故障。

也有可能导致一个部件故障的事件或许也会导致其他部件的故障。术语“常见原因故障”通常缩写为CCF。CCF发生的侧向等级通常被描述为贝塔(ß)因素。子系统和系统设计者要留意CCF的可能性，这是非常重要的。有许多类型的CCF，相应也有许多不同的方式去避免它的发生。EN ISO 13849-1标准在极端的复杂性与过于简单性之间作出了一定程序的合理调整。与EN/IEC 62061标准一样，它采用本质上是定性的方法。它提供了一个已知措施的列表，其中列出可以有效避免CCF的方法。这些措施数目充足，必须在

系统或子系统的设计中予以实施。据声称，根据有些证明结果，列表单独使用这些措施不力可能并不能足以防止所有CCF发生的可能性。然而，如果合理考虑列表的意图，使设计者分析CCF的可能性，在技术类型和指定应用的特性的基础上适当实施一些避免措施，就可以使它的要求变得更为清晰。列表的使可加强大多数基础的、有效的技术的注意事项，如多样化的故障代码和设计能力。BGIA SISTEMA工具也需要实施标准CCF检查表，让它们以方便的形式加以使用。

系统性故障

我们已经讨论过用MTTFd的形式和危险故障的可能性将安全可靠性数据定量化。然而，这还不是全部。当我们参考这些术语时，我们真正考虑的是故障似乎是随机发生的。确实，IEC/EN 62061标准具体地引用PFHd缩写的含义是随机硬件故障的可能性。但还有一些类型的故障选择性被称为“系统性故障”，它们的原因可归于设计或制造过程中产生的错误。这个方面的经典例子就是软件代码的错误。标准在标准附录G中列出了一些避免此类错误[因此也是故障]的措施。这些措施包括例如使用适用材料和生产技术、评审、分析以及计算机仿真等等这些条款。也有一些可预测到的事件和特性，除非效应是可控制的，它们就会发生在运行环境中引起故障。标准附录G中也提供相关措施。例如，介面出现掉电的情况是很容易预测到的。因此部件的断电可使系统处于安全状态。这些或许只是一些常识，确实它们也是，但他们是仍然是必要的。标准的所有其他要求没有意义，除非是为了控制和避免系统性故障，可进行必要考虑。有时也会需要相同类型的措施用于控制随机硬件故障[目的是实现所需的PFHd]，例如自动诊断测试和冗余硬件。

罗克韦尔自动化

机器安全问题会以不同的方式对公司造成影响。机械制造商/供应商，典型上被称为OEM(原始设备制造商)需要遵守相关的机器安全法规(例如： 在欧洲要遵守机械规范)，但他们也希望在为客户输送价值的同时，改善机器的吞吐量。他们机器的终端用户希望提高设备综合效率。减少平均维修时间、降低材料浪费以及避免不需要的机器停止可有助于实现以上目标，产生一个更为安全高产的工作场所，同时确保满足安全法规的要求。

通常的共识是法规应确保在安全环境内运行，并且符合如EN ISO 13849-1这样的标准，向相关法规展示其符合性是一个好方法。但实现符合性会出现你无法预料到的挑战.....

- 它真的对你的设备性能有效吗?
  当它不该停止时停止了怎么办? 出现干扰脱扣怎么办?
- 它的成本对你来说是不是太高?
  你是否实施了太多的安全方案?
  你在错误实施的安全解决方案导致的问题
  管理其他安全供应商所需的成本
- 安全方案正限制你的能力：
  是否在高产有效地运行机器?
  执行维护任务是否快速和容易?
  你的客户是否能快速得到机器?
- 你的工厂的意外事件是否有所增加?
  你的安全措施是否正确应用?
  是否有明显的意外保险和残废救济金

这些问题在对机器应用安全方案时，许多都不会考虑到。然而有了EN ISO 13849-1和IEC 62061这样的功能安全标准，在所有的运行模式中(生产、维护、启动、调试等)，安全应用方法正在指导朝着机器的整体运行特性应用，并且应用安全自动化的正确等级，实现了最大的OEE(设备综合效率)。

这会引起关于安全供应商能力的一个问题。从以前的经验中，安全被应用在防护机器上，是通过停止机器，移除危险的方法。这是一种允许制造商实现与法规保持一致性的做法。但是关于产量和效率会怎么样呢?

这就是罗克韦尔自动化在自动与安全领域的经验与其他提供安全解决方案的众多公司产生差异化之处。作为一家领先的自动化供应商，将安全集成到整体的自动化解决方案之中，您就会看到为何客户在帮助他们遵守安全法规，并且帮助他们实现所需要的生产率与灵活性。罗克韦尔的核心理念是供应自动化解决方案，采用功能安全标准确保功能安全。您可以清晰地看到例如EN ISO 13849-1这样的功能安全标准是如何助生产过程一臂之力的。

罗克韦尔自动化是一家理解安全理念的自动化公司。开发出适用于机器控制、运动和过程的一体化解决方案，并将安全集成入这个一体化的控制平台中。

与罗克韦尔自动化共同合作

我们是理解自动化与安全的自动化供应商.....不仅仅只是安全。

- 帮助您好获得需要的 **性能** .....安全可靠
- **成本** – 帮助您从投资获得最大回报
- 法规需求 – 帮助您实现与法规的**一致性**

更加安全的自动化全方位服务与解决方案

- 全面的产品组合(输入/逻辑/执行)
- 同一个网络中的标准与安全(CIP安全)
- 安全服务(评估、验证、培训等等)

将安全功能集成到标准自动化解决方案中

- 驱动器，PLC，I/O，运动，网络，编程软件.....
- 简化架构
- 降低成本
- 提高性能

罗克韦尔自动化，安全解决方案的全球领先公司，如果您想了解更多内容请联系当地办公处。

输入设备

互锁开关

这些设备被设计用来物理互锁防护门和设备，只有当危险处于安全条件下时，才能提供接近潜在危险区域的机会。可用设备包括：带或不带防护锁定的互锁开关，截留钥匙系统和安全限位开关。

压力感应设备

这些设备设计用于检测在危险区域是否有人或物体存在。它们不提供有形屏障，因此在安全条件下频繁接近是理想的应用。可用设备包括：安全光帘、安全激光扫描仪、压力感应安全地毯和安全边。

逻辑

安全继电器

这些设备设计用来监控安全电路的状态，并且提供各种各样的配置。它们可以是单一功能继电器，或者是硬件配置的多功能继电器。

可编程安全控制器

这些设备设计用来监控安全电路的状态，可以进行具体功能的软件配置。它们是专用的安全控制器，为安全电路控制特别设计。

输出设备

安全接触器

安全接触器用来移除执行器的电源。在接触器上添加了特别功能，以提供安全额定值。
机械连接的常闭触点用于对逻辑设备的接触器状态作出反馈，因此要确保安全功能。

PowerFlex®交流变频器，带集成安全功能

PowerFlex交流变频器有可选的集成安全功能，包括安全转矩断开板、安全速度控制和有条件防护闸控制。目前PowerFlex 40P，70，700S和700H提供安全转矩断开板，750系列PowerFlex变频器提供所有以上提及的安全功能。

急停和脱扣设备

这些设备设计用于提供机器的急停开关功能，且用于操作员身体范围内的位置控制。这些设备包括：急停开关按钮，启动绳(电缆)急停开关设备和带有急停开关功能的启用开关。

操作员界面

这些设备是设计用于提供操作员机器控制的安全相互作用，包括如3位置启用开关和双手控制启用设备等设备。

集成安全控制器

这些设备设计用于在一个平台内提供标准自动化控制和安全控制。它们是可编程软件，允许在相同的编程环境中进行标准和安全功能的配置。

安全I/O

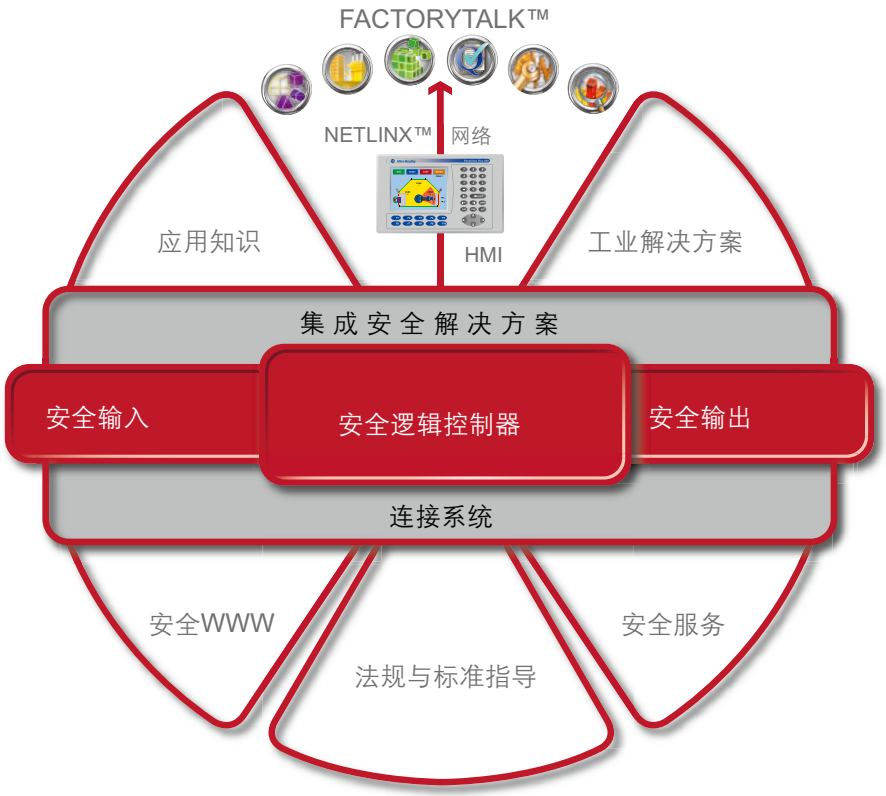
这些设备提供具有应用的灵活性安全等级I/O解决方案。它们在解决方案的范围之内通过DeviceNet网络或者EtherNet/IP网络进行CIP安全通讯。这个家族系列产品包括：CompactBlock Guard I/O, ArmourBlock Guard I/O和POINT Guard I/O。

Kinetix®运动驱动器，带有集成安全功能

Kinetix 6000运动驱动器具有可选的集成安全功能，包括安全转矩断开板，即将发布的版本也将有安全速度控制和条件防护闸控制。

罗克韦尔自动化

利用产品、知识与全球基础设施的优势，帮助您好实现安全与自动化的需求。



www.discoverrockwellautomation.com/safety

www.rockwellautomation.com

www.rockwellautomation.com.cn

动力、控制与信息解决方案

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1)414 382.2000, Fax: (1)414 382.4444
亚太地区－香港数码港道100号数码港3座F区14楼 电话：(852)28874788 传真：(852)25109436

中国总部－上海市漕河泾开发区虹梅路1801号B区宏业大厦1楼 邮编：200233 电话：(8621)61288888 传真：(8621)61288899
北京－北京市建国门内大街18号恒基中心办公楼1座4层 邮编：100005 电话：(8610)65217888 传真：(8610)65217999
天津－天津市和平区解放北路188号信达广场写字楼3310-3312室 邮编：300042 电话：(8622)58190588 传真：(8622)58190599
青岛－青岛市香港中路40号数码港旗舰大厦2206室 邮编：266071 电话：(86532)86678338 传真：(86532)86678339
济南－济南市历下区泺源大街229号金龙大厦东楼23层东北室 邮编：250012 电话：(86531)81778388 传真：(86531)81778389
西安－西安市高新区科技路33号高新国际商务中心数码大厦1201室 邮编：710075 电话：(8629)88152488 传真：(8629)88152466
乌鲁木齐－乌鲁木齐市友好南路576号凯宾斯基酒店717室 邮编：830000 电话：(86991)6388683 传真：(86991)6388980
郑州－郑州市中原中路220号裕达国际贸易中心A座1216-1218室 邮编：450007 电话：(86371)67803366 传真：(86371)67803388
太原－山西省太原市府西街69号山西国际贸易中心B座8层801室 邮编：030002 电话：(86351)8689580 传真：(86351)8689580
唐山－唐山市路北区东方大厦C座303室 邮编：063000 电话：(86315)3195962/63 传真：(86315)3195951
南京－南京市中山南路49号商茂世纪广场44楼A3-A4座 邮编：210005 电话：(8625)86890445 传真：(8625)86890142
无锡－无锡市解放东路1000号保利广场8号2208室 邮编：214007 电话：(86510)82320076 传真：(86510)82320176
武汉－武汉市建设大道568号新世界国贸大厦I座2202室 邮编：430022 电话：(8627)68850233 传真：(8627)68850232
长沙－长沙市韶山北路159号通程国际大酒店1712室 邮编：410011 电话：(86731)5450233/5456233 传真：(86731)5456233 ext. 608
杭州－杭州市杭大路15号嘉华国际商务中心1203室 邮编：310007 电话：(86571)87260588 传真：(86571)87260599
广州－广州市环市东路362号好世界广场2703-04室 邮编：510060 电话：(8620)83849977 传真：(8620)83849989
深圳－深圳市福田中心区金田路4028号荣超经贸中心4305-06室 邮编：518035 电话：(86755)82583088 传真：(86755)82583099
厦门－厦门市湖里区湖里大道41号联泰大厦4A单元西侧 邮编：361006 电话：(86592)2655888 传真：(86592)2655999
南宁－南宁市青秀区金湖路59号地王国际商会中心31层3117、3118、3119室 邮编：530000 电话：(86771)5594308 传真：(86771)5594338
成都－成都市总府路2号时代广场A座906室 邮编：610016 电话：(8628)86726886 传真：(8628)86726887
重庆－重庆市渝中区邹容路68号大都会商厦3112-13室 邮编：400010 电话：(8623)63702668 传真：(8623)63702558
昆明－昆明市东风西路123号三合商利写字楼13层C座 邮编：650000 电话：(86871)3635448/ 3635458/ 3635468 传真：(86871)3635428
沈阳－沈阳市沈河区青年大街219号华新国际大厦15-F单元 邮编：110015 电话：(8624)23961518 传真：(8624)23963539
大连－大连市西岗区中山路147号森茂大厦2305室 邮编：116011 电话：(86411)83687799 传真：(86411)83679970
哈尔滨－哈尔滨市南岗区红军街15号奥威斯发展大厦26层B座 邮编：150001 电话：(86451)84879066 传真：(86451)84879088
长春－长春市西安大路1688号新润天国际大厦2201室 邮编：130061 电话：(86431)87069871 传真：(86431)87069882

Publication SAFETY-RM004A-ZH-P November 2009