ICS 25.040.40
CCS N 19

中华人民共和国国家标准化指导性技术文件

GB/Z 42023.2—2022/IEC TR 63164-2:2020

工业自动化设备和系统可靠性 第2部分:系统可靠性

Reliability of industrial automation devices and systems—Part 2:System reliability

(IEC TR 63164-2:2020,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。

本文件是GB/Z 42023《工业自动化设备和系统可靠性》的第2部分。GB/Z 42023已经发布了以下部分：

——第2部分：系统可靠性。

本文件等同采用IEC TR 63164-2:2020《工业自动化设备和系统可靠性　第2部分：系统可靠性》。文件类型由IEC的技术报告调整为我国的国家标准化指导性技术文件。

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。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、沈阳工业大学、中国科学院沈阳自动化研究所、卡奥斯工业智能研究院(青岛)有限公司、北京航空航天大学、重庆川仪自动化股份有限公司、浙江中控技术股份有限公司、上海仪器仪表自控系统检验测试所有限公司、辽宁大学、北京市科学技术研究院城市安全与环境科学研究所、北京角动力技术有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、苏州拓康自动化技术有限公司、西门子(中国)有限公司、北京赛伯产业信息技术研究院有限公司。

本文件主要起草人：丁露、王成城、张晓玲、徐皑冬、唐春娥、宋岩、孙博、黄云彪、任涛林、乔靖玉、谢亚莲、冯强、靳江红、陈宇、郭永振、张庆军、李佳、王姗姗。

引　言

在智能制造的背景下，基于互联工厂的大规模定制等新的生产模式需要实时互联、频繁切换和跨层次集成。因此，可靠性是工厂自动化系统的重要要求。自动化系统的可靠性数据是维护计划的基础，例如生产线备件的库存。一个自动化系统通常由多个不同的设备或机器串联、并联或混联组成。GB/Z 42023《工业自动化设备和系统可靠性》为系统集成商评估整个系统可靠性提供指导，拟由两部分构成。

——第1部分：自动化设备可靠性数据及其来源规范的保证。目的在于规范自动化设备可靠性数据。

——第2部分：系统可靠性。目的在于规范系统可靠性计算方法。

本文件着重于根据系统结构的单个设备的失效率或可靠性指标计算系统的失效率或可靠性指标。这有助于系统集成商或设计者根据单个设备的可靠性指标计算整个系统的可靠性。

工业自动化设备和系统可靠性
第2部分:系统可靠性

1 范围

本文件基于单个设备和/或子系统的可靠性数据以及数据的表示形式,提供了可以简化为串联、并联或混联的自动化系统的可靠性数据计算指南。

注:本过程仅针对自动化系统的可靠性,而非嵌入了自动化系统的系统,如流程工厂。

可靠性包含在可信性中,本文件主要研究影响可靠性的随机硬件失效。可信性是一个与时间有关的质量特性的总称,除可靠性外还包括可用性、可恢复性、可维修性、维修支持性能,以及在某些情况下的其他特性,如耐久性、功能安全和网络安全,但这些不在本文件的范围内。

2 规范性引用文件

本文件没有规范性引用文件。

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

自动化系统 automation system

在过程工业中用于监视和控制生产设备、基于DCS或PLC的系统,包括采用了现场总线技术的控制系统。

注:本文件中提及"系统"时,表示"自动化系统",DCS为集散控制系统,PLC为可编程控制系统。

[来源:GB/T 25928—2010,2.1,有修改,增加了注]

3.1.2

B_{10}阈值 B_{10} threshold

10%的部件出现故障的时间。

注1:适用的时间间隔取决于资产的性质和用途,可以是运行时间、运行小时数、周期数等。

注2:在本文件中,平均失效率通过10%除以B_{10}阈值(单位为小时)获得。忽略早期失效的影响,通常认为失效率仅在B_{10}之后才显著增加。

注3:一旦达到B_{10}阈值,则认为气动和机电部件的失效率不可接受。

3.1.3

可信性 dependability

需要时按要求执行的能力。

注1:可信性包括可用性(192-01-23)、可靠性(192-01-24)、恢复性(192-01-25)、维修性(192-01-27)和维修保障性(192-01-29),以及在某些情况下,诸如耐久性(192-01-21)、功能安全和网络安全等其他特性。

注2:可信性是用于产品与时间相关质量特性的集合性术语。

[来源:GB/T 2900.99—2016,192-01-22,有修改,安全性和安保修改为功能安全和网络安全]

3.1.4

失效率　failure rate

λ

设在时间区间$(0,t)$内未发生失效，不可修复产品在时间区间$(t,t+\Delta t)$内出现失效的条件概率与区间长度Δt之比，当Δt趋于0时的极限(如果存在)。

注：更详细的描述，见IEC 61703。

[来源：GB/T 2900.99—2016，192-05-06，有修改，删除瞬时失效率、公式和注2]

3.1.5

平均失效间隔工作时间　mean operating time between failures；MTBF

失效间隔运行持续时间的期望值。

注：平均失效间隔时间仅适用于可修复产品。对不可修复产品，见平均失效前工作时间(3.1.6)。

[来源：GB/T 2900.99—2016，192-05-13，有修改，删除MOTBF术语]

3.1.6

平均失效前工作时间　mean operating time to failure；MTTF

失效前工作时间的期望值。

注：对于失效前工作时间服从指数分布(即恒定失效率)的不可修复产品，MTTF在数值上等于其失效率的倒数。对于可修复产品，如果恢复后被认为是“修复如新”，这个结论也是对的。

[来源：GB/T 2900.99—2016，192-05-11，有修改，删除注2]

3.1.7

平均恢复时间　mean time to restoration；MTTR

恢复时间的期望值。

注：GB/T 2900.13—2008定义的术语“平均恢复时间”是一个英文同义词，但“修复”和“恢复”不是同义词。

[来源：GB/T 2900.99—2016，192-07-23]

3.1.8

任务时间　mission time

T_M

预定使用的时间段。

注：对于有部件维护的复杂系统，系统的任务时间可以比系统单个部件的任务时间长。

[来源：GB/T 16855.1—2018，3.1.28，有修改，删除SRP/CS，增加了注]

3.1.9

随机硬件失效　random hardware failure

在硬件中，由一种或几种可能的退化机制而产生的，在随机时间出现的失效。

[来源：GB/T 20438.4—2017，3.6.5，有修改，删除了注]

3.1.10

可靠性　reliability

在给定的条件下，在给定的时间区间，能无失效地执行要求的能力。

注1：持续时间区间可用产品与有关的适合的计量单位表示，例如日历时间、工作周期、行程等，这些计量单位宜清晰的阐述。

注2：给定的条件包括影响可靠性的各个方面，如：运行模式、应力水平、环境条件和维修。

[来源：GB/T 2900.99—2016，192-01-24，有修改，删除了注3]

3.1.11

系统性失效　systemic failure

原因确定的失效，只有对设计或制造过程、操作规程、文档或其他相关因素进行修改后，才有可能消除这种失效。

注 1：仅修正性维护而不加修改，通常无法消除失效原因。

注 2：通过模拟失效原因可以引出系统性失效。

注 3：系统性失效的原因可包括以下情况中的人为错误：

——安全要求规范；

——硬件的设计、制造、安装、运行；

——软件的设计和实现等。

注 4：在本文件中，安全相关系统的失效被分为随机硬件失效(见 3.1.9)和系统性失效。

[来源：GB/T 20438.4—2017，3.6.6]

3.1.12

使用寿命 useful lifetime

产品从首次使用直到由于运行和维修的经济性或废弃，不再满足用户要求的时间区间。

注：在本定义，“首次使用”不包括先前产品移交给最终用户的测试活动。

[来源：GB/T 2900.99—2016，192-02-27，有修改，有用寿命改为使用寿命]

3.2 缩略语

下列缩略语适用于本文件。

FIT：以时间表示的失效(Failures in time)

FMEA：故障模式及影响分析(Fault modes and effects analysis)

FTA：故障树分析(Fault tree analysis)

METBF：平均失效间隔经过时间(Mean elapsed time between failures)

MTBF：平均失效间隔工作时间(Mean operating time between failures)

MTTF：平均失效前工作时间(Mean time to failure)

PoF：失效物理学(Physics of failure)

RBD：可靠性框图(Reliability block diagrams)

T_M：任务时间(Mission time)

4 系统可靠性

通常自动化系统由几种不同类型的子系统、自动化设备和配件组成，并且要求自动化系统和自动化设备的可靠性数据具有一致性。

系统的可靠性需要考虑硬件的可靠性，包括接口、通信等。除硬件可靠性外，还可以考虑其他因素，如软件、人为因素、网络安全(见附录 A)。

注：本文件中的通信是指用于通信的硬件，如线缆、路由器。

5 系统可靠性计算

5.1 概述

本文件提供了基于可靠性框图的简单系统结构的系统可靠性计算指南，这些结构的元件具有恒定的失效率。对于这些和其他类型的系统结构，例如 n 中取 k 结构，见 GB/T 37981—2019。有关系统其他计算方法的更多信息，请参见 IEC 60300-3-1。

本文件不涉及现场设备观察和实验室试验的可靠性数据，但可参考 IEC TS 63164-1:2020。

系统的每个元件都需要有可靠性数据，如 MTTF、MTBF、$\lambda(t)$ 或 B_{10}。要计算整个系统的可靠性，所有的元件需要相同类型的可靠性数据。

在一定的条件下，可靠性数据可通过如下方式获得，见 IEC 61703。

示例：

MTTF=1/λ(对于恒定失效率)

λ=0.1×C/B_{10}(假设失效率恒定)，其中 C 等于每小时的操作数，B_{10} 以周期数形式表示，见 IEC 62061。

在自动化系统中，除了随机硬件失效外，系统性失效也很常见。本文件主要的计算方法侧重于随机失效，避免或减少系统性失效也能提高系统的可靠性(见附录 B)。

5.2 可靠性数据的格式

一般来说，可靠性数据可以从以下几个方面考虑。更多详情见 IEC TS 63164-1:2020。

可靠性数据：常见可靠性数据，如 MTBF、MTTF 或 $\lambda(t)$。

参考条件：有关计算系统可靠性的部署条件的信息，如工作时间、暴露时间、工作电压、工作电流、占空比。

参考环境条件：假定为系统环境的参考环境条件的信息，如温度、湿度、压力、腐蚀、振动。

事件：有关自动化系统在其生命周期内发生的任何可能影响可靠性的信息，如维护信息。

5.3 结构和计算

5.3.1 基本公式

在本条中，给出了一些与可靠性有关的基本公式，这些公式也可以在 IEC 61703 中找到。

对于不可修复的对象或系统，常用的可靠性函数 $R(t)=R(0,t)$，其中 $R(0)=1$。$R(t)$可由式(1)计算：

$$R(t)=\exp\left(-\int_0^t\lambda(u)\mathrm{d}u\right) \quad \cdots\cdots(1)$$

其中 $\lambda(u)$是对象或系统的失效率。换言之，可靠性函数表示系统无失效运行到时间 t 的概率。对于恒定失效率 λ(即指数分布的失效时间)，上述公式简化为式(2)：

$$R(t)=\mathrm{e}^{-\lambda t} \quad \cdots\cdots(2)$$

对于不可修复的对象或系统，MTTF 可由公式(3)计算：

$$M_{\mathrm{TTF}}=\int_0^\infty R(t)\mathrm{d}t \quad \cdots\cdots(3)$$

其中，在失效时间服从指数分布的情况下，MTTF 简化为公式(4)：

$$M_{\mathrm{TTF}}=\frac{1}{\lambda} \quad \cdots\cdots(4)$$

虽然 MTTF 的值可以针对几乎任何具有相应恒定或非恒定失效率的失效时间分布进行计算，但对于从 MTTF 反向计算恒定失效率，宜确保失效率确实是恒定的。特别是，对于由不可修复部件组成的冗余系统，情况并非如此，因为冗余系统的失效率不是恒定的。然而，有时为了简化分析，可以计算在一定时间段内的平均恒定失效率，并以合理的精度进一步使用。

对于可修复对象或系统，宜使用 MTBF，而不是 MTTF。但是，如果修复后的对象或系统“完好如新”，这两种表述基本相同。

注 1：对于恢复时间可忽略不计的可修复对象或系统，MTBF 约等于 METBF。

注 2：计算 MTTF 时，假定非工作状态下的失效率为 0。

5.3.2 串联结构

如果系统的每一个元件都是系统的整体功能所必需的，那么这些元件将被视为串联，如图 1 所示。

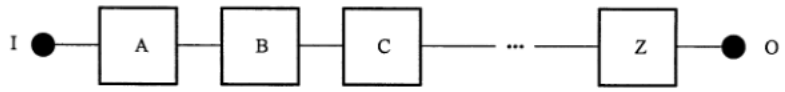

图 1　串联系统可靠性框图

对于串联系统，系统的可靠性函数由式(5)计算：

$$R_S(t)=\prod_{i=A}^{n}R_i(t) \quad \cdots\cdots(5)$$

如果单个元件具有指数分布的失效时间，那么：

$$R_i(t)=e^{-\lambda_i t} \quad \cdots\cdots(6)$$

并且：

$$R_S(t)=e^{-\lambda_S t} \quad \cdots\cdots(7)$$

$$\lambda_S=\lambda_A+\lambda_B+\lambda_C+\cdots+\lambda_Z \quad \cdots\cdots(8)$$

式中：

$R_S(t)$——系统的可靠性函数；

$R_i(t)$——不同元件的可靠性函数；

λ_S——系统的恒定失效率；

λ_i——不同元件的恒定失效率；

i——A,B,C,…,Z。

或者

$$\frac{1}{M_{TBFS}}=\frac{1}{M_{TBFA}}+\frac{1}{M_{TBFB}}+\frac{1}{M_{TBFC}}+\cdots+\frac{1}{M_{TBFZ}} \quad \cdots\cdots(9)$$

式中：

M_{TBFS}——系统的 MTBF；

M_{TBF_i}——不同元件的 MTBF。

注 1：如果失效率用 FIT 表示，则 MTBF 的结果以小时(h)表示。

注 2：FIT 是指以时间表示的失效率，表示 10 亿(10^9)个设备工时内的失效次数。

5.3.3　并联结构

如果一个系统的多个元件需要以冗余方式实现系统的整体功能，则这些元件被认为是并联的，如图 2 所示。

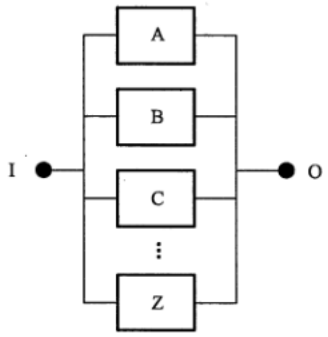

图 2　并联系统可靠性框图

对于含有不可修复元件的系统，使用式(10)：

$$R_S(t)=1-\prod_{i=A}^{n}[1-R_i(t)] \quad \cdots\cdots(10)$$

如果单独的元件符合指数分布，则

$$R_i(t) = e^{-\lambda_i t} \quad \cdots\cdots(11)$$

$$M_{TTFSys} = \int_0^{\infty} \left[1 - \prod_{i=A}^{n} (1 - e^{-\lambda_i t})\right] dt \quad \cdots\cdots(12)$$

式中：

$R_S(t)$ ——系统的可靠性函数；

$R_i(t)$ ——不同元件的可靠性函数；

M_{TTFSys} ——系统的 MTTF；

λ_i ——不同部件的失效率；

i ——A,B,C,…,Z。

注 1：如果失效率 λ_i 用 FIT 表示，则 M_{TTFSys} 的结果用小时(h)表示。

注 2：对于含有不可修复元件的上述并联系统，系统失效率非恒定。

如果系统修复后可以认为和新的一样，那么系统的 MTTF 等于 MTBF。

对于具有可修复元件的系统，如果相比于 MTBF 修复时间可忽略，那么使用以下近似公式(13)：

$$M_{TBFSys} = \left(\prod_{i=A}^{Z} \frac{\lambda_i}{\mu_i} \sum_{i=A}^{Z} \mu_i\right)^{-1}, \text{当 } \lambda_i \ll \mu_i \quad \cdots\cdots(13)$$

式中：

M_{TBFSys} ——系统的 MTBF；

λ_i ——不同元件的恒定失效率；

μ_i ——不同元件的恒定修复率，当每个元件的修复时间符合指数分布时，它等于 MTTR 的倒数；

i ——A,B,C,…,Z。

注 3：如果失效率 λ_i 和修复率 μ_i 用 FIT 表示，则 M_{TTFSys} 和 $M_{TTR,i}$ 的结果用小时(h)表示。

5.3.4 混联结构

通常，一个系统不能仅用简单的串联或并联系统来组成。通常情况可能是一个混联结构，如图 3 所示。

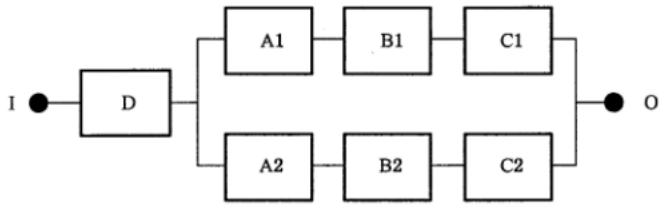

图 3 常见串并联(冗余)可靠性框图

混联结构可以简化为串并联结构，如图 4 所示。

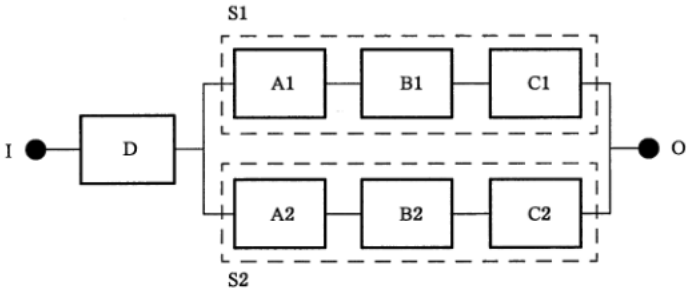

图 4 简化的混联结构

$$\lambda_{S1}=\lambda_{A1}+\lambda_{B1}+\lambda_{C1} \quad \cdots\cdots(14)$$

$$\lambda_{S2}=\lambda_{A2}+\lambda_{B2}+\lambda_{C2} \quad \cdots\cdots(15)$$

$$M_{TTFSys}=\int_0^{\infty}R_S(t)\,dt=\int_0^{\infty}e^{-\lambda_D t}\left[1-(1-e^{-\lambda_{S1}t})(1-e^{-\lambda_{S2}t})\right]dt \quad \cdots\cdots(16)$$

式中：

λ_{S1} ——系统 S1 失效率，S1 包含 A1、B1 和 C1；

λ_{i1} ——设备 A1、B1 或 C1 的失效率，其中 i=A,B,C；

λ_{S2} ——系统 S2 失效率，S2 包含 A2、B2 和 C2；

λ_{i2} ——设备 A2、B2 或 C2 的失效率，其中 i=A,B,C；

λ_D ——设备 D 的失效率；

$R_S(t)$ ——系统的可靠性函数；

M_{TTFSys} ——系统的 MTTF。

注：如果失效率 λ 用 FIT 表示，则 M_{TTFSys} 的结果用小时(h)表示。

5.3.5 小结

系统可靠性相关的常见公式见表 1。

表 1 系统可靠性相关常见公式总结

系统可靠性指标	串联结构	并联结构(热备份)
不可维修对象或系统		
可靠度 $R_S(t)$	$\prod_i R_i(t)$	$1-\prod_i(1-R_i(t))$
可靠度 $R_S(t)$(恒定失效率 λ_i)	$\prod_i \exp(-\lambda_i t)$	$1-\prod_i(1-\exp(-\lambda_i t))$
$MTTF_S$(恒定失效率 λ_i)	$(\sum_i\lambda_i)^{-1}$	$\int_0^{\infty}R_S(t)\,dt$
可维修对象或系统		
$MTBF_S$(恒定失效率 λ_i 和维修率 μ_i)	$(\sum_i\lambda_i)^{-1}$	$\left(\prod_i\frac{\lambda_i}{\mu_i}\sum_i\mu_i\right)^{-1}$，当 $\lambda_i \ll \mu_i$
平均停机时间 MDT_S(恒定失效率 λ_i 和维修率 μ_i)	$\sum_i\frac{\lambda_i}{\mu_i}(\sum_i\lambda_i)^{-}1$，当 $\lambda_i \ll \mu_i$	$(\sum_i\mu_i)^{-1}$

附 录 A
（资料性）
典型自动化系统示例

A.1 概述

自动化系统可利用控制系统和信息技术减少工业生产中的人工劳动和服务。例如，发电、交通管理、水管理、捣浆和纸张处理、印刷、金属处理、炼油厂、化工过程、医药制造或运输船使用的自动化系统。

A.2 给出了一个简化的过程自动化系统串联结构的示例，A.3 给出了一个简化的过程自动化子系统混联结构的示例。

A.2 过程自动化系统串联结构示例

过程自动化或自动化系统(PAS)用于自动控制一个过程，该过程常见于冶金、化工、炼油、造纸和纸浆等行业。PAS 通常使用网络将传感器、控制器、操作终端和执行器互连，如图 A.1 所示。

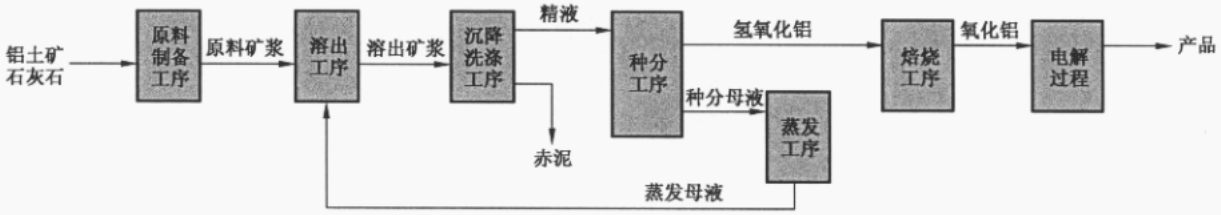

图 A.1 典型的过程自动化系统(铝冶炼)

图 A.2 描述了铝冶炼的自动化系统配置。铝冶炼自动化系统配置包括以下生产过程：

a) 原料制备工序(A1)；
b) 溶出工序(A2)；
c) 沉降洗涤工序(A3)；
d) 种分工序(A4)；
e) 蒸发工序(A5)；
f) 焙烧工序(A6)；
g) 电解过程(A7)。

图 A.1 可用图 A.2 的框图表示。

图 A.2 铝冶炼自动化系统框图

铝冶炼系统框图为串联结构。A1，A2，…，A7 是铝冶炼自动化系统的子系统，A1，A2，…，A7 是独立的，是铝冶炼系统整体功能所必需的。

铝冶炼自动化系统的 MTBF 值表示为 $M_{TBF,Ai}$($i=1,2,\cdots,7$)。

铝冶炼自动化系统的系统失效率 λ 采用 RBD 计算：

$$\lambda_S=\lambda_{A1}+\lambda_{A2}+\lambda_{A3}+\lambda_{A4}+\lambda_{A5}+\lambda_{A6}+\lambda_{A7} \quad \cdots\cdots(A.1)$$

或者：

$$\frac{1}{M_{TBFSys}}=\frac{1}{M_{TBF,A1}}+\frac{1}{M_{TBF,A2}}+\frac{1}{M_{TBF,A3}}+\frac{1}{M_{TBF,A4}}+\frac{1}{M_{TBF,A5}}+\frac{1}{M_{TBF,A6}}+\frac{1}{M_{TBF,A7}} \quad \cdots(A.2)$$

式中：

λ_S ——系统的失效率；

λ_{Ai} ——不同子系统的失效率(A1 至 A7)；

M_{TBFSys}——系统的 MTBF；

$M_{TBF,Ai}$——不同子系统的 MTBF(A1 至 A7)。

A.3 过程自动化子系统混联结构示例

以铝冶炼自动化系统的沉降洗涤过程为例计算 λ_{A3}。沉降洗涤过程如图 A.3 所示。

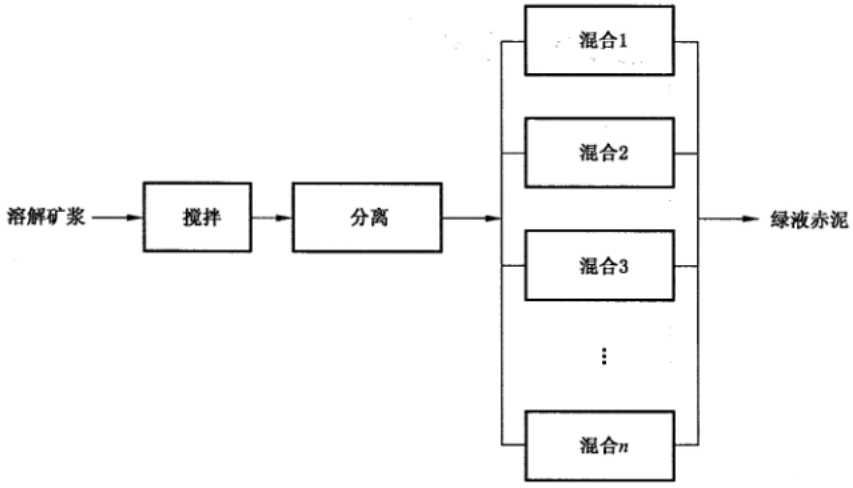

图 A.3 铝冶炼自动化系统的沉降洗涤过程

图 A.3 可用图 A.4 的框图表示。

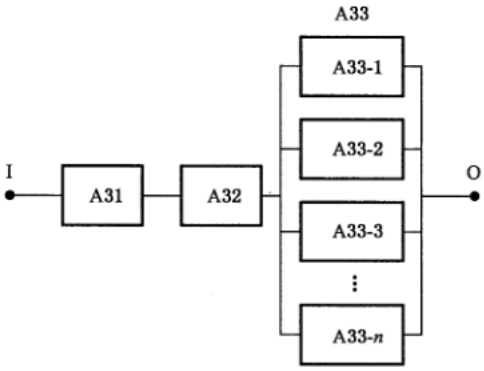

图 A.4 沉淀洗涤过程框图

沉降洗涤过程的框图是一个混联结构。A31，A32 和 A33 表示沉淀洗涤过程的子系统，A33-1，A33-2，…，A33-n 是独立的。A33-1，A33-2，…，A33-n 需要冗余的方式实现沉淀洗涤过程的整体功能。A33-1，A33-2，…，A33-n 是并联的。

沉降洗涤过程的子系统 MTBF 值表示为 $M_{TBF,A3i}(i=1,2,3)$。

沉降洗涤过程的系统失效率 λ_{A3} 用 RBD 计算：

$$R_{A33}(t)=1-\prod_{i=1}^{n}[1-R_{A33-i}(t)]=1-\prod_{i=1}^{n}(1-e^{-\lambda_{A33-i}t}) \quad \cdots\cdots(A.3)$$

$$R_S(t)=R_{A31}(t)\cdot R_{A32}(t)\cdot R_{A33}(t)=e^{-(\lambda_{A31}+\lambda_{A32})t}\left[1-\prod_{i=1}^{n}(1-e^{-\lambda_{A33-i}t})\right] \quad \cdots\cdots(A.4)$$

$$M_{TBFSys}=\int_0^{\infty}R_S(t)\,dt=\int_0^{\infty}e^{-(\lambda_{A31}+\lambda_{A32})t}\left[1-\prod_{i=1}^{n}(1-e^{-\lambda_{A33-i}t})\right]dt \quad \cdots\cdots(A.5)$$

式中：

$R_{A33}(t)$ ——系统 A33 的可靠度；

$R_{A33-i}(t)$ ——系统 A33 中设备的可靠度($i=1,2,3$)；

λ_{A33-i} ——系统 A33 中设备的失效率($i=1,2,3$)；

$R_S(t)$ ——系统的可靠度；

$R_{A31}(t)$ ——设备 A31 的可靠度；

$R_{A32}(t)$ ——设备 A32 的可靠度；

λ_{A31} ——设备 A31 的失效率；

λ_{A32} ——设备 A32 的失效率；

M_{TBFSys} ——系统的 MTBF。

附 录 B
（资料性）
提高系统可靠性的方法

B.1 概述

自动化系统的失效将导致系统可靠性的降低。可以通过减少或避免自动化系统的失效来提高自动化系统的可靠性。

自动化系统的失效可分为系统性失效和随机硬件失效。本附录提供了减少系统性失效和随机硬件失效的通用方法。有关提高系统可靠性的附加信息见 IEC 60300-3-15。

B.2 减少系统性失效的方法

B.2.1 概述

系统性失效是人为失效，可以通过改变设计、生产工艺、操作方式等因素来消除。系统性失效可通过以下方法避免和控制。

B.2.2 避免系统性失效的措施

以下避免系统性失效的措施是在生命周期的不同阶段实施的，这些措施适用于硬件和软件，包括：

a) 设计需求规范阶段：项目管理、文件编制、规范结构化、规范检查、计算机辅助规范工具等；

b) 设计和开发阶段：项目管理、文件编制、遵循指南和标准、规范结构化、规范检查、计算机辅助规范工具、半形式化方法、形式化方法等；

c) 系统集成阶段：项目管理、文件编制、功能测试、黑盒测试、现场经验、统计测试；

d) 操作和维护阶段：项目管理、文件编制、操作和维护说明、操作员错误的防护。

注：这些措施可根据开发过程的 V 模型来实施。例如，如何使用 V 模型，参见 GB/T 20438.3—2017 中的软件开发部分。此外，操作或维护阶段的信息可用于未来系统的开发。

B.2.3 控制系统性失效的措施

设计中采用以下方法控制系统性失效，包括：

a) 控制由设备引起的系统性失效的技术和措施：程序顺序监控、在线故障监测、代码保护、硬件多样化、应力筛选、加速寿命试验和基于 PoF 的措施；

注 1：设备包括硬件、软件、接口、网络等。对于网络可信性，可参考 GB/T 34040—2017、IEC 62673 和 IEC 61907。

注 2：PoF 方法可用于可靠性设计和评估，这是为了确定设计的“最薄弱环节”，以确保设计超过所需的设备寿命和可靠性。基于 PoF 的方法包括有限元分析(FEA)建模、失效机理建模、失效概率密度计算和必要的测试。这些方法通常用于处理焊点失效，更多详情参考 IEC 61709:2017 附录 F。

b) 控制由环境条件引起的系统性失效的技术和措施：电磁兼容(EMC)测试、物理环境防护措施、程序顺序监控、强弱电分离、硬件多样化；

c) 控制由操作引起的系统性失效的技术和措施：修改保护、在线故障监测、输入确认、异常断言编程。

B.3 减少随机硬件失效的方法

B.3.1 容错设计

在发生特定失效时，系统或程序可以通过以下措施保持正常运行：

a) 冗余设计:可通过多个功能通道实现功能,保证了在通道故障时能正常工作。冗余设计包括:
——硬件冗余:冗余系统、冗余部件、冗余电路;
——信息冗余:冗余代码、多数据表决;
——时间冗余:程序重新计算。
b) 纠错设计:纠错代码、程序重复执行。
c) 故障处理:错误检测、故障屏蔽、故障隔离、自切换技术。

B.3.2 防错设计

错误信息可用于产品的校正。可通过以下方法在最大限度内避免错误。
a) 环境耐受性技术:热设计、机械应力保护、化学防护、电磁兼容设计。
b) 质量控制要求:对所有材料、工艺和设备实行严格的质量控制标准。
c) 提高组件的集成度:随着集成度的提高,整个系统的失效率降低。
d) 故障诊断技术:通过对异常设备的分析,确定失效位置和失效原因。
e) 错误自检及修正技术:通过设备自检和数据修正避免失效。
f) 预测性维护技术:通过对状态监测等历史数据进行分析和预测,采用的有针对性的维护方法。PoF 是预测性维护技术之一。它利用产品生命周期载荷和失效机制的知识来进行可靠性设计和评估。基于 PoF 的预测允许在实际应用条件下评估产品的可靠性。它将传感器数据与模型相结合,从而能够对产品的健康状态偏离或退化进行原位评估。因此,在产品发生故障之前,可以采取必要的措施,如预测性维护。

B.3.3 系统降额设计

为了使系统部件上的应力低于其额定应力,降低部件的失效率,通常按以下步骤进行降额设计。
a) 降额参数的确定:确定影响部件失效率的系统应力参数,包括电应力、机械应力和热应力。
b) 降额等级的确定:通过综合权衡系统安全性、总成本、重量和尺寸等限制因素,确定降额等级。降额分为三个等级,即:
——一级降额等级:设备失效造成人员伤亡或设备及配套设备严重损坏;
——二级降额等级:设备失效导致设备及配套设备损坏;
——三级降额等级:设备失效不会造成人员伤亡和设备损坏。
c) 系统降额设计:根据 a)和 b),确定相关部件的降额指标,完成部件选型和系统设计。

参 考 文 献

[1] GB/T 2900.13—2008 电工术语 可信性与服务质量(IEC 60050(191):1990+Amd.1:1999+Amd.2:2002,IDT)

[2] GB/T 2900.99—2016 电工术语 可信性(IEC 60050-192:2015,IDT)

[3] GB/T 16855.1—2018 机械安全 控制系统安全相关部件 第1部分:设计通则(ISO 13849-1:2015,IDT)

[4] GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

[5] GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求(IEC 61508-3:2010,IDT)

[6] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语(IEC 61508-4:2010,IDT)

[7] GB/T 25928—2010 过程工业自动化系统 出厂验收测试(FAT)、现场验收测试(SAT)、现场综合测试(SIT)规范(IEC 62381:2006,IDT)

[8] 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(IEC 61784-3:2016,IDT)

[9] GB/T 37981—2019 可信性分析技术 可靠性框图法和布尔代数法(IEC 61078:2006,IDT)

[10] IEC 60300-3-1:2003 Dependability management—Part 3-1:Application guide—Analysis techniques for dependability—Guide on methodology

[11] IEC 60300-3-15:2009 Dependability management—Part 3-15:Application guide—Engineering of system dependability

[12] IEC 61703:2016 Mathematical expressions for reliability,availability,maintainability and maintenance support terms

[13] IEC 61709:2017 Electric components—Reliability—Reference conditions for failure rates and stress models for conversion

[14] IEC 61907:2009 Communication network dependability engineering

[15] IEC 62061 Safety of machinery—Functional safety of safety-related control systems

[16] IEC 62673:2013 Methodology for communication network dependability assessment and assurance

[17] IEC TS 63164-1:2020 Reliability of industrial automation devices and systems—Part 1:Assurance of automation devices reliability data and specification of their source