第5章

控制系统可靠性分析

教学目标

采用现场总线控制系统实现过程控制与常规控制系统一样，要求控制系统必须具有很高的可靠性，这样才能保证产生工艺的安全和经济运行。为了实现控制系统的高可靠性，在控制系统中必须采用许多提高可靠性的技术。可靠性技术主要包括可靠性设计、可靠性分析、可靠性实验以及可靠性管理等。可靠性设计是指按照一定的技术要求，设计和制造出可靠性高且不易损坏的产品；可靠性分析是指通过对有关数据的收集、分析和处理，得出一些关于可靠性问题的评价与结果；可靠性实验是验证系统是否达到规定指标的手段，通过实验可暴露系统设计中可能存在的问题；可靠性管理是指通过管理提高系统的可靠性。本章主要介绍提高控制系统可靠性的相关内容，包括可靠性分析方法和提高可靠性的有关措施等。通过对本章内容的学习，读者能够：

- 了解控制系统可靠性的主要指标；
- 了解控制系统进行可靠性分析的基本方法；
- 了解进行系统可靠性测试的基本原理和基本方法；
- 了解提高控制系统可靠性的基本方法与措施。

5.1 可靠性指标

要从理论上分析系统的可靠性，必须采用一些能够表征系统可靠性的技术指标。这些指标主要有：可靠度、故障率、平均故障间隔时间、平均故障修复时间、维修率与可用率等。

1. 可靠度

采用概率来表示可靠性时也称为可靠度(Reliability)。可靠度即指产品在规定的时间内，在规定的使用条件下，完成规定功能的概率。

可靠度一般用 $R(t)$ 来表示，它是时间的函数，其取值域为[0,1]。设 T 为产品寿命的随机函数，则：

$$R(t) = P(T > t) \tag{5-1}$$

式(5-1)表示产品寿命 T 超过规定时间 t 的概率，也即产品的可靠度。

系统可靠性有如下几个特性：

- $R(0)=1$，这表示产品在开始时是良好的
- $R(\infty)=0$，这表示产品在长时间使用后其可靠度的值趋于零
- $0 \leqslant R(t) \leqslant 1$，这表示在任何时刻可靠度的值处于 0 和 1 之间
- $R(t)$ 是时间的单调递减函数

2. 不可靠度

不可靠度(Unreliability)是在规定的时间内，在规定的使用条件下，发生故障的概率。不可靠度一般用 $F(t)$ 来表示，则：

$$F(t) = P(T \leqslant t) = 1 - P(T > t) = 1 - R(t) \tag{5-2}$$

3. 故障密度函数

故障密度函数(Failure Density Function)是不可靠度对时间的变化率,记为 $f(t)$,它表示产品在单位时间内失效的概率,其数学表达为:

$$f(t) = \frac{\mathrm{d}F(t)}{\mathrm{d}t} = -\frac{\mathrm{d}R(t)}{\mathrm{d}t} \tag{5-3}$$

系统不同,其失效的密度也不同。对于电子系统,其失效密度一般符合指数规律,即

$$f(t) = \begin{cases} \lambda \mathrm{e}^{-\lambda t} & (t \geqslant 0, \lambda > 0) \\ 0 & (t < 0, \lambda > 0) \end{cases} \tag{5-4}$$

例 5-1　某电子元件的寿命服从指数分布,设 $\lambda = 1/1000$,计算元件在 50h、100h、1000h 的工作时间内的可靠度。

解:由式(5-2)和式(5-4)有电子元件的可靠度函数为

$$R(t) = 1 - F(t) = 1 - \int_0^t f(x)\mathrm{d}x = 1 - \int_0^t \lambda \mathrm{e}^{-\lambda x}\mathrm{d}x = \exp(-\lambda x) = \exp\left(-\frac{t}{1000}\right)$$

所以

$$R(50) = \exp\left(-\frac{50}{1000}\right) = 0.951$$

$$R(100) = \exp\left(-\frac{100}{1000}\right) = 0.905$$

$$R(1000) = \exp\left(-\frac{1000}{1000}\right) = 0.368$$

---

4. 故障率

故障率(Failure Rate)是工作到某一时刻 t 尚未失效的产品,在该时刻 t 后单位时间内失效的概率,一般记为 $\lambda(t)$。也可以说产品的故障总数与寿命单位总数之比叫故障率。换句话说,失效率是时刻 t 尚未失效的产品,在 $t+\Delta t$ 单位时间内失效的条件概率,即

$$\lambda(t) = \lim_{t \to 0} \frac{1}{\Delta t} = P(t < T \leqslant t + \Delta t \mid T > t)$$

由条件概率:

$$P(t < T \leqslant t + \Delta t \mid T > t) = \frac{P(t < T < t + \Delta t)}{P(T > t)}$$

所以

$$\lambda(t) = \lim_{t \to 0} \frac{1}{\Delta t} = \frac{P(t < T < t + \Delta t)}{P(T > t)\Delta t} = \frac{F(t + \Delta t) - F(t)}{P(T > t)\Delta t}$$

$$= \frac{\mathrm{d}F(t)}{\mathrm{d}t} \cdot \frac{1}{R(t)} = -\frac{R'(t)}{R(t)} \tag{5-5}$$

由大量元器件构成的电子设备,其典型的故障率曲线如图 5-1 所示。曲线分为三个区,第一个区为早期故障区,在这一阶段由于设备中元器件质量不稳定和生产工艺不够成熟等原因,故障率比较高,在早期故障区的设备“新不如旧”。随着工作时间的增加,故障率逐渐下降,进入偶发故障区。随着工作时间的进一步增加,设备中的元器件逐渐老化,特性参数发生变化,故障率会上升,这就是晚期故障区,这个时期的设备“旧不如新”。由于故障率曲线的形状酷似浴盆,因此,故障率曲线也称为浴盆曲线。

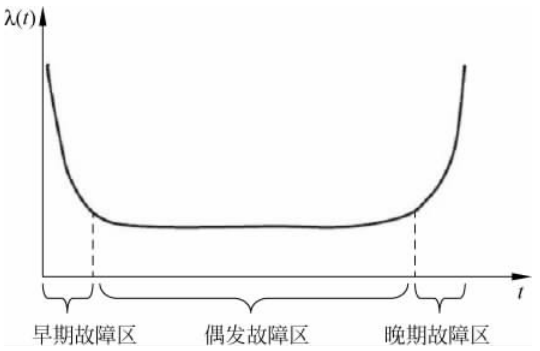

图 5-1　故障率曲线图

制造商提供的控制系统在出厂前，设备中的元器件都已经过了严格的老化处理和出厂检验，目的就是让系统或设备在实际使用时能尽量的工作在偶发故障区。这样系统或设备在整个工作期间其故障率可以视为常数，即：

$$\lambda(t) = \lambda$$

表 5-1 给出了一些常用设备的故障率。

表 5-1　部分常用设备的故障率表

设　　备	故障率 $\lambda/(10^{-6} \cdot h^{-1})$	设　　备	故障率 $\lambda/(10^{-6} \cdot h^{-1})$
传感器	50～100	小型计算机	125～200
变送器	100～200	微型计算机	50～200
调节器	40～200	打印机	1000～2000
执行器	40～100	磁带机	400～1200
数字显示仪表	100～400	集成电路	2000

概括地说，产品故障少就意味着产品可靠性高。

5. 平均故障间隔时间

平均故障间隔时间(Mean Time Between Failure，MTBF)，又称平均无故障时间，是指可修复产品两次相邻故障之间的平均时间，也称平均寿命，单位为小时。

设有一个可修复的产品在使用过程中，共计发生过 n 次故障，每次故障后经过修复又和新的一样继续投入使用，其工作时间分别为 $T_1, T_2, \cdots, T_n$，那么产品的平均故障间隔时间，也就是平均寿命 Q 为：

$$Q = \text{MTBF} = \frac{1}{n}\sum_{i=1}^{n} T_i \tag{5-6}$$

设备的工作时间也即完成规定功能的时间，是系统可靠时间。对于连续系统，上述关系被表达为：

$$\text{MTBF} = \int_0^{\infty} R(t)\,\mathrm{d}t$$

若对式(5-4)两边同时积分有：

$$R(t) = \mathrm{e}^{-\int_0^t \lambda(t)\,\mathrm{d}t} \tag{5-7}$$

所以

$$\mathrm{MTBF}=\int_0^{\infty}R(t)\mathrm{d}t=\int_0^{\infty}\mathrm{e}^{-\int_0^t\lambda(t)\mathrm{d}t}\mathrm{d}t \tag{5-8}$$

当 $\lambda(t)=\lambda$ 时，有

$$\mathrm{MTBF}=\frac{1}{\lambda} \tag{5-9}$$

例如，一款可用于服务器的硬盘，MTBF 高达 120 万小时，保修 5 年。120 万小时约为 137 年，并不是说该种硬盘每只均能工作 137 年不出故障。由 $\mathrm{MTBF}=1/\lambda$ 可知 $\lambda=1/\mathrm{MTBF}=1/137$ 年，即该硬盘的平均年故障率约为 0.7%，一年内，平均 1000 只硬盘有 7 只会出故障。当产品的寿命服从指数分布时，其故障率的倒数就称为平均故障间隔时间。

平均故障间隔时间 MTBF 指标在系统运行中的作用可体现在如下几个方面：

- 可借鉴于 MTBF 针对高频率故障零件制定相应的对策；
- 进行零件寿命周期的推算，以制订最佳维修计划；
- 针对重点项目和对象合理安排点检；
- 设定备品备件基准。各种零件的储备项目及基本库存数量，应根据 MTBF 的记录分析来判断，使其库存水平达到合理的状况；
- 可对设备对象设定预估运行时间标准，以确保设备运行可靠；
- 可作为设备维修计划预估时间基准，以合理进行维护作业的安排；
- 提供设备的可靠性、可维修性设计的技术资料。

6. 平均故障恢复时间

平均恢复时间(Mean Time to Restoration，MTTR)，源自于 IEC 61508 中的平均维护时间(Mean Time to Repair)，它包括确认失效发生所必需的时间，以及维护所需要的时间。MTTR 也必须包含获得配件的时间，维修团队的响应时间，记录所有任务的时间，还有将设备重新投入使用的时间。可以这么说，平均恢复时间是系统运行中总维修时间与总维修次数之比，即

$$\mathrm{MTTR}=\frac{1}{n}\sum_{i=1}^{n}t_i \tag{5-10}$$

式中：t_i 为第 i 次维修所用的时间；

n 为总维修次数。

平均恢复时间的倒数是设备的维修率，通常用 μ 表达，这样

$$\mu=\frac{1}{\mathrm{MTTR}} \tag{5-11}$$

7. 平均失效时间

平均失效时间(Mean Time to Failure，MTTF)，是目前使用较为广泛的一个衡量可靠性的参数。它被定义为随机变量、出错时间等的期望值。MTTF 的长短，通常与使用周期中的产品有关，其中不包括老化失效。

对于一个简单的可维护的元件，MTBF= MTTF + MTTR。因为 MTTR 通常远小于 MTTF，所以 MTBF 近似等于 MTTF，通常由 MTTF 替代。MTBF 用于可维护性和不可维护的系统。

8. 可用率

可用率也称有效率(Availability)，常用 A 表示，它是可靠度与维修度的综合指标，用于

反应系统的运行效率。可用率按如下计算公式计算：

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \tag{5-12}$$

由式(5-12)可知，为了提高可用率，应该设法增加系统的 MTBF，同时也应该减少系统的 MTTR。

5.2　可靠性分析

根据系统中每台设备的可靠性指标求出整个系统的可靠性指标，这就是进行系统可靠性分析。要对由若干台设备组成的系统进行可靠性分析，必须建立系统的可靠性分析模型。

系统的可靠性分析模型有串联模型、并联模型、关系矩阵模型、组合模型以及马尔科夫链模型等，最常用的是串联模型与并联模型。

1. 串联系统及其模型

串联系统模型的结构如图 5-2(a)所示。在由设备串联构成的系统中，只要其中一台设备发生故障，系统将会丧失预定的功能。

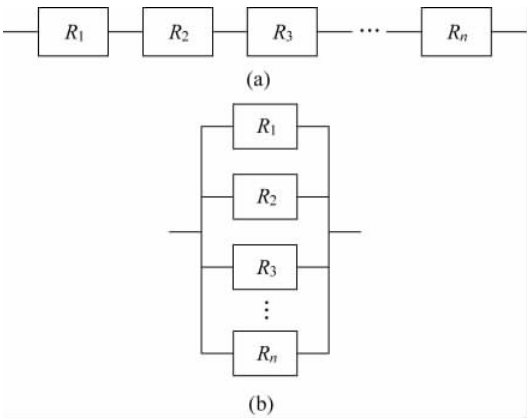

图 5-2　串联与并联可靠性分析模型图

在串联系统中，若用 $R_1, R_2, \cdots, R_n$ 分别表示各台设备的可靠性，则串联系统的可靠性 R_s 为

$$R_s(t) = R_1(t)R_2(t)\cdots R_n(t) \tag{5-13}$$

由式(5-7)，串联系统的可靠性可表达为

$$R_s(t) = \mathrm{e}^{-\int_0^t [\lambda_1(t)+\lambda_2(t)+\cdots+\lambda_n(t)]\mathrm{d}t} = \mathrm{e}^{-\int_0^t \lambda_s(t)\mathrm{d}t} \tag{5-14}$$

当系统处于正常运行阶段(即偶然故障区)，则 $\lambda_1(t) = \lambda_1, \lambda_2(t) = \lambda_2, \cdots, \lambda_n(t) = \lambda_n$，这时系统的故障率为

$$\lambda_s(t) = \sum_{i=1}^{n} \lambda_i = \lambda_s \tag{5-15}$$

由式(5-8)、式(5-14)和式(5-15)，串联系统的平均故障间隔时间为

$$\text{MTBF}_s = \int_0^{\infty} R_s(t)\mathrm{d}t = \frac{1}{\lambda_s} \tag{5-16}$$

式(5-16)也说明串联的元器件越多，系统的可靠性越低。

2. 并联系统及其模型

并联系统模型的结构如图 5-2(b)所示。在并联结构系统中，只有当每台设备全部发生故障时，系统才丧失预定功能。在并联系统中，若用 $R_1, R_2, \cdots, R_n$ 分别表示各台设备的可靠性，则并联系统的可靠性 R_p 为

$$R_p(t) = 1 - [1 - R_1(t)][1 - R_2(t)]\cdots[1 - R_n(t)] \tag{5-17}$$

式(5-17)中，$[1-R_i(t)]$为各台设备的不可靠度。

当 $R_1 = R_2 = \cdots = R_n$ 时，则

$$R_1(t) = R_2(t) = \cdots = R_n(t) = \mathrm{e}^{-\int_0^t \lambda(t)\,\mathrm{d}t} \tag{5-18}$$

同时

$$R_p(t) = 1 - [1 - R(t)]^n \tag{5-19}$$

当系统处于正常运行阶段(即偶然故障区)，如果 $\lambda_1(t) = \lambda_2(t) = \cdots = \lambda_n(t) = \lambda$，由式(5-7)和式(5-8)得，并联系统的平均故障间隔时间为

$$\begin{aligned} \mathrm{MTBF}_p &= \int_0^\infty R_s(t)\,\mathrm{d}t = \int_0^\infty [1 - (1 - \mathrm{e}^{-\int_0^t \lambda(t)\,\mathrm{d}t})^n]\,\mathrm{d}t \\ &= \frac{1}{\lambda}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) = \frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i} \end{aligned} \tag{5-20}$$

注意到式(5-9)有

$$\mathrm{MTBF}_p = \mathrm{MTBF}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) \tag{5-21}$$

由式(5-21)可见，采用并联设备构成的系统，其平均故障间隔时间大于单个设备的均故障间隔时间，并联设备越多，系统可靠性越高。当 $n=2$ 时，MTBF_p 提高了 50%。在这个基础上每增加一台设备，MTBF_p 可提高 $1/n$。当 $n>3$ 时，再增加设备对提高系统可靠性的作用就不大了。在实际应用时，常取 $n=2$ 或 $n=3$。

例 5-2　有某多功能电路板，板上的元器件数量和器件的故障率情况如表 5-2 所示。求该电路板的可靠性和平均寿命。

表 5-2　例 5-2 中元器件数量与故障率表

元　器　件	数　　量	故障率/h
大规模集成电路	2	40×10^{-8}
小规模集成电路	5	5×10^{-8}
线驱动/接收器	5	20×10^{-8}
LED 指示器	1	2×10^{-8}
钽电容	30	5×10^{-8}
96 针连接器	1	0.1×10^{-8}
焊点	500	0.02×10^{-8}

解：为简单起见，电路板上的元器件按照串联情形考虑，则总故障率为

$$\begin{aligned} \lambda_s(t) &= \sum_{i=1}^{n}\lambda_i \\ &= [2\times40 + 5\times5 + 5\times20 + 1\times2 + 30\times5 + 96\times0.1 + 500\times0.02]\times10^{-8}/\mathrm{h} \\ &= 376.6\times10^{-8}/\mathrm{h} \end{aligned}$$

该电路板的可靠度函数为

$$R_s(t) = e^{-376.6\times10^{-8}t}$$

该电路板的平均寿命为

$$MTBF_s = \frac{1}{\lambda_s} = \frac{1}{376.6\times10^{-8}} \approx 265533h \approx 30\text{ 年}$$

例 5-3　对如图 5-3 所示的串联-并联混合系统，求其可靠度。

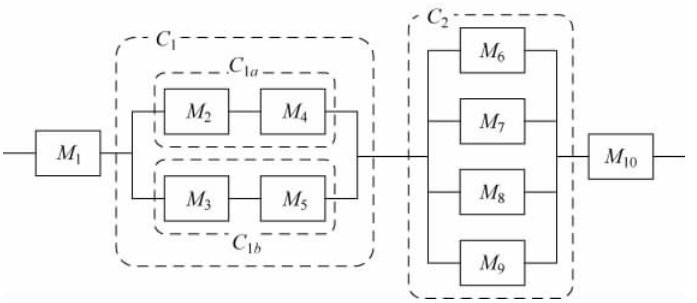

图 5-3　例 5-3 图

解：由图 5-3 可见，系统 M_2 和 M_4 为串联(即 C_{1a})，系统 M_3 和 M_5 为串联(即 C_{1b})，而 C_{1a} 和 C_{1b} 为并联(即 C_1)。系统 C_1 的可靠性为

$$\begin{aligned} R(C_1) &= 1-[1-R(C_{1a})][1-R(C_{1b})] \\ &= 1-[1-R(M_2)R(M_4)][1-R(M_3)R(M_5)] \end{aligned}$$

系统 M_6、M_7、M_8 和 M_9 为并联(即 C_2)。系统 C_2 的可靠性为

$$R(C_2) = 1-[1-R(M_6)][1-R(M_7)][1-R(M_8)][1-R(M_9)]$$

因此，由 M_1、C_1 和 C_2 构成的整个系统 M 可靠性可表达为

$$R(M) = R(M_1)R(C_1)R(C_2)R(M_{10})$$

3. 关系矩阵型系统模型

假设采用多个控制器来控制多个子系统，即可构成关系矩阵模型的结构，如图 5-4 所示。

为了描述这个复杂系统的可靠性，首先要描述系统中各部分之间的连接关系，这就需要采用连接矩阵：

$$\boldsymbol{R} = \begin{matrix} U_1 & \cdots & U_n \\ \end{matrix} \quad \begin{matrix} \\ \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix} \end{matrix} \quad \begin{matrix} S_1 \\ \vdots \\ S_m \end{matrix} \tag{5-22}$$

矩阵的每一行对应一个子系统 $\boldsymbol{S}_i$，每一列对应一个子系统 $\boldsymbol{U}_j$。矩阵 $\boldsymbol{R}$ 的元素取值方法是

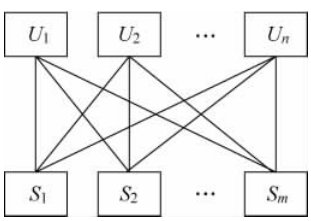

图 5-4　关系矩阵模型图

$$r_{ij}=\begin{cases}1, & \text{子系统 } \boldsymbol{S}_i \text{ 与控制器 } \boldsymbol{U}_j \text{ 相连}\\ 0, & \text{子系统 } \boldsymbol{S}_i \text{ 与控制器 } \boldsymbol{U}_j \text{ 不相连}\end{cases}$$

假设被控对象本身(一般为机械设备)的可靠性比控制器(一般为电子设备)的可靠性高得多,研究可靠度时可以只考虑控制器本身和控制器的输出通道装置的失效率情况。如果用 $\lambda_{U1},\lambda_{U2},\cdots,\lambda_{Un}$ 表示控制器的失效率,用 $\lambda_{O1},\lambda_{O2},\cdots,\lambda_{On}$ 表示控制器输出通道装置的失效率,并假定它们全为常数时,用向量对其进行表达有

$$\boldsymbol{\Lambda}_U=\begin{bmatrix}\lambda_{U1}\\ \lambda_{U2}\\ \vdots\\ \lambda_{Un}\end{bmatrix}$$

$$\boldsymbol{\Lambda}_O=\begin{bmatrix}\lambda_{O1}\\ \lambda_{O2}\\ \vdots\\ \lambda_{On}\end{bmatrix}$$

考虑到控制器和控制器的输出通道装置为串联模型,注意到式(5-15)有

$$\boldsymbol{\Lambda}_s=\boldsymbol{\Lambda}_O+\boldsymbol{R}\boldsymbol{\Lambda}_U=\begin{bmatrix}\lambda_{O1}+r_{11}\lambda_{U1}+r_{12}\lambda_{U2}+\cdots+r_{1n}\lambda_{Un}\\ \lambda_{O2}+r_{21}\lambda_{U1}+r_{22}\lambda_{U2}+\cdots+r_{2n}\lambda_{Un}\\ \vdots\\ \lambda_{Om}+r_{m1}\lambda_{U1}+r_{m2}\lambda_{U2}+\cdots+r_{mn}\lambda_{Un}\end{bmatrix} \tag{5-23}$$

式(5-23)中的每一行表示一个子系统和与它相连的控制器的故障率。Λ_s 称为系统故障率矩阵。

对于关系矩阵型、组合型以及马尔科夫链型等复杂系统的可靠性分析一般都要借助于一些数学理论与工具,本书不做讨论,有兴趣的读者可查阅相关书籍或资料。

5.3　系统可靠性测试

获取系统的可靠性数据,或者说获取设备故障率数据,方法一般有两种,其一是直接采集现场数据,其二是在实验室中测试生存周期来得到其数据。直接采集现场数据更加真实,因为它可代表正常操作条件下设备的故障率,但这一般需要的时间较长。在实验室中测试生存周期是当设备新投入运行且不存在现场数据时的唯一选择。

在实验室中进行可靠性测试或试验依据其试验的目的又分为可靠性增长试验、可靠性验证试验、元件筛选试验和质量验收试验等。而按照试验性质则分为环境试验、性能试验和寿命试验等。

可靠性增长试验用于暴露产品在设计、工艺和元器件等方面的缺陷,发现薄弱环节以便后续改进,同时也可使产品进入可靠性比较稳定的偶然故障区。

可靠性验证试验用于检验系统设计和制造是否达到了预期的可靠性指标。

筛选试验用于将不符合规范要求的元器件或产品剔除。常用的筛选试验方法有振动法、加速度法、机械冲击法、温度循环法和热冲击法等。

质量验收试验主要用于经验产品的可靠性是否符合规定的要求。质量验收试验包括在

生产厂家进行的产品验收试验和交货后在工业现场进行的现场验收试验。

由于检测与控制系统的使用寿命一般都比较长，不可能等到被测设备或系统完全报废才得出结论，实际上是需要在一个相对比较短而又能说明问题的时间内得出试验结论。解决这个问题的方法有两种，一种是截尾试验，另一种是加速试验。

截尾试验又分为定故障次数（定数）截尾试验和定试验时间（定时）截尾试验。定数截尾试验就是试验到预订的故障次数时停止试验，这里故障次数是确定的，停止试验的时间是随机的。定时截尾试验则是试验到预订的时间停止试验，这里停止试验的时间是确定的，故障次数是随机的。对基于计算机的控制系统定时截尾试验的截尾时间一般选用 180 天（约 4320h）。

加速试验也称加速测试，其方法就是为了缩短数据采集的时间，对设备施压，使得设备的故障率由于某个因素而提高。如果可以对加速因子进行估计，就可以基于加速测试的数据推导出正常操作条件下的故障率。最常用的加速因子就是温度。温度越高，器件的故障率越高。加速因子可以由下式给出：

$$R(T) = A\mathrm{e}^{-E_a/kT} \tag{5-24}$$

式中：R 为故障率；

A 为常数；

E_a 为激活能量；

k 为玻尔兹曼常数（0.8625×10^{-4}eV/K）；

T 为温度（K）。

当温度分别为 T_1 和 T_2 时，设备故障率的比值为：

$$\frac{R(T_1)}{R(T_2)} = \mathrm{e}^{-(E_a/k)(1/T_1-1/T_2)} \tag{5-25}$$

如图 5-5 所示为一个 MOS 器件的测试例子。该器件 $E_a\approx0.7$eV，试验以 25℃时的加速因子为基准。由图 5-5 可见，在温度为 100℃时，进行 1h 的测试大约相当于温度在 25℃时进行 250h 的测试。

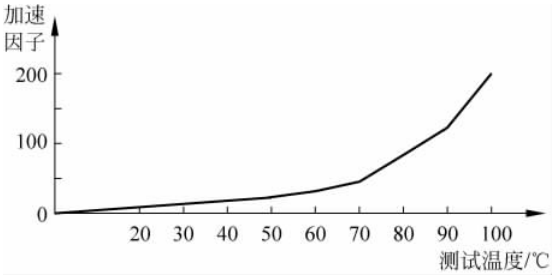

图 5-5　加速因子曲线图

5.4　提高现场总线控制系统与分布式控制系统可靠性的措施

现场总线控制系统与其他控制系统一样，我们希望它具有较高的可靠性。提高自动控制系统的可靠性实际上包括两个方面，一是尽量不发生故障，二则是系统对故障要有一定的容忍度。任何装置或系统不发生故障是不可能的，我们期待的是装置或系统的寿命周期尽

量的长。这可以通过对装置或系统的合理设计、元器件的严格筛选和老化、制造过程的严格把关、以及安装调试过程的严格管理等来实现。另一方面则是在装置或系统发生故障时尽可能减少故障对系统所造成的影响，或者是在出现故障时系统仍然能够继续运行，也即容错。

延长装置或系统寿命周期的措施主要包括以下几个方面。

1. 对元器件进行严格筛选和老化

所谓筛选，就是将不符合使用条件的元器件通过一定的方式予以剔除。所谓老化，就是在元器件投入使用之前将其置于一定的工作条件下，使有可能发生参数漂移的元器件逐步稳定。在控制系统中常用的筛选方法是温度循环法，如图 5-6 所示是温度循环法中的温度变化曲线。将被筛选的元器件置入这样的温度变化环境中，温度的改变重复 8～10 次，则可使元器件产生较大的热应力，有缺陷的元器件会迅速失效，以便将其淘汰。

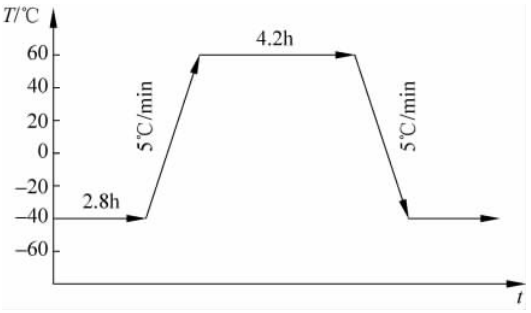

图 5-6　筛选过程中的温度循环曲线图

2. 元器件的降额使用

电子元器件都有一定的使用条件，这些条件是以元器件的某些额定参数值来表示的。当元器件的工作条件低于额定值时，其工作更加稳定，发生故障的机会也会更少。为了提高元器件的可靠性，将元器件降额使用也是一种选择。

3. 充分考虑参数变化的影响

在电路设计时就充分考虑到元器件在使用过程中受参数变化造成的影响，使之在各种不同的工作参数时均能正常工作。

4. 采用低功耗元件

低功耗元件的发热量比较少，其故障率相对比较低。大量采用低功耗元件时也可减轻电源的负担，从而可提高电源的可靠性。

5. 采用噪声抑制技术

在工业控制现场，各种脉冲干扰往往是造成控制系统硬件故障的原因。因此采用噪声抑制技术是提高控制系统可靠性的一种行之有效的办法。

6. 耐环境设计

在控制系统硬件设计上，充分考虑各种环境因素的影响，采用适当的冷却、抗震、防尘、防爆、防腐等技术措施，以提高控制系统抵御外部环境侵袭的能力。

装置或系统要能容忍故障可从两个方面考虑，即限制故障范围和使系统具有后备能力。限制故障范围是指当发现故障时，系统能将故障设备与系统的其他部分隔离开来，使其不至于影响其他设备的正常运行。另一种限制故障范围的做法是固定（也即“冻结”）控制输出，

以免造成输出混乱。在智能系统中还可将输出转为安全模式，如交通信号系统在故障情况下，信号灯全部转为安全模式（全部转为红灯），以免造成交通事故。

控制系统具有后备能力也称系统冗余。系统冗余包括硬件冗余、软件冗余、时间冗余和信息冗余。

硬件冗余就是采用附加的（也即后备的）硬件来弥补发生故障的硬件功能。

软件冗余相对是一个新兴的领域。如果只是对软件进行复制作为冗余，很多时候是不能起到提高可靠性的作用。因为对于相同的输入，所复制的软件可能也会产生同样的错误。这就需要运行不同版本的软件来实现冗余。

时间冗余也称后向错误恢复，最简单的做法就是在出错的地方重试，或者回到前一个检验点重试，再或者整个计算重新开始。

信息冗余的基本思想就是利用比必要的数据多一些的数据来检查错误。换句话说，信息冗余就是采取一种编码方式，使得一些数据位出错时也可以被检测出来或被更正，具有保证系统继续运行的能力。这些编码技术与通信中采用的编码校验技术非常相似，比如重复码、奇偶校验码、循环码和算术码等都是信息冗余中常用的检错与纠错技术。

这里重点介绍提高硬件可靠性的措施。提高分布式控制系统或现场总线控制系统可靠性一般从硬件的冗余结构设计、不易发生故障的硬件设计和能迅速排除故障的硬件设计几个方面考虑。

硬件的冗余结构设计就是系统除了运行的硬件以外，还需配有后备的硬件能在故障情况下投入。硬件的冗余配置是昂贵的，一般只对系统的关键部件进行硬件冗余配置，如控制器，电源或者通信设施等。对于分布式控制系统（DCS）以及 Profibus-PA 现场总线控制系统，对系统控制器模块进行备份的结构如图 5-7 所示。这种一对一的控制器备份，也称控制器的 1∶1 冗余。

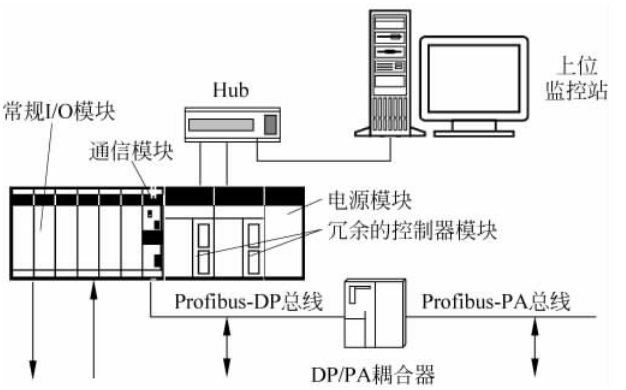

图 5-7　Profibus-PA 现场总线系统控制器冗余的配置图

对于图 5-7 所示的控制器冗余配置，一个控制器处于正常工作状态，设其故障率为 λ_1。另一个控制器处于备用工作状态，设其备用期间故障率为 μ（在备用期间有可能发生故障），工作期间故障率为 λ_2。系统的可靠性为：

$$R(t) = \mathrm{e}^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \mu - \lambda_2}\left[\mathrm{e}^{-\lambda_2 t} - \mathrm{e}^{-(\lambda_2+\mu)t}\right] \tag{5-26}$$

系统的平均故障间隔时间为：

$$\mathrm{MTBF}=\frac{1}{\lambda_1}+\frac{1}{\lambda_2}\frac{\lambda_1}{\lambda_1+\mu} \tag{5-27}$$

如果假设备用控制器在备用期间不会发生故障，同时假设备用控制器与工作控制器的故障率相同，则式(5-27)与式(5-21)表达相同，即并联一台备用控制器，系统可靠性将提高，其平均故障间隔时间大于单台控制器的均故障间隔时间。这时的 MTBF_p 提高了 50%。

为了提高控制系统的可靠性，除了将控制器进行冗余之外，有时还需将通信网络、通信总线、操作站以及系统电源和现场电源进行冗余配置，甚至还要将整个控制室的不间断电源系统(UPS)进行冗余配置。一种典型的控制系统冗余配置结构如图 5-8 所示。

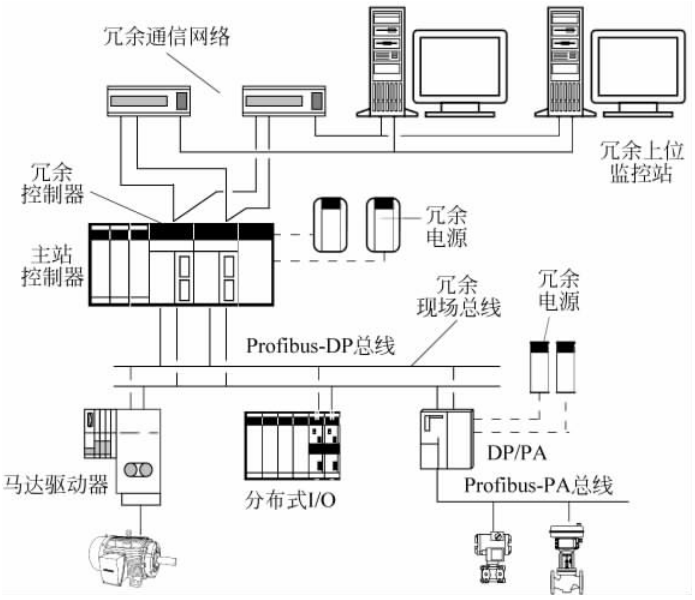

图 5-8　分布式系统冗余的配置图

在图 5-7 和图 5-8 的系统配置中，对 Profibus-PA 现场总线没有进行冗余配置，这是因为 Profibus-PA 总线上的设备是从站设备，其控制功能在中央控制器上实现。如果对 Profibus-PA 总线进行冗余配置，几乎所有总线设施都要做备份，系统造价会过高。通行的做法是多配置一些 DP/PA 耦合器与 Profibus-PA 总线段，每个总线段上不要挂接过多设备，适度提高系统的分散程度。对于基金会现场总线，其情况与 Profibus-PA 现场总线相似，但每台基金会现场总线设备都可用作控制器，其分散程度已经非常高。同样多安排一些总线段，每个总线段上不挂接过多现场设备即可。

在工业控制中，除了上述系统冗余外，还有一个重要的措施是采用手动后备来提高可靠性。尤其对于重要的控制回路，一旦自动控制失灵，可以手动操作生产过程。分布式控制系统可在三个不同层次设置手动操作，如图 5-9 所示。

在运行操作站进行手动操作。这种手动操作要求上位操作站、通信网络、中央控制器等都能正常工作时才能进行。

在专用的手动操作站进行手动操作。对重要回路一般都要配置专用的手动操作站，它可绕开中央控制器对现场设备进行手动操作。专用的手动操作站非常类似(有时就是采用)数字调节仪表。

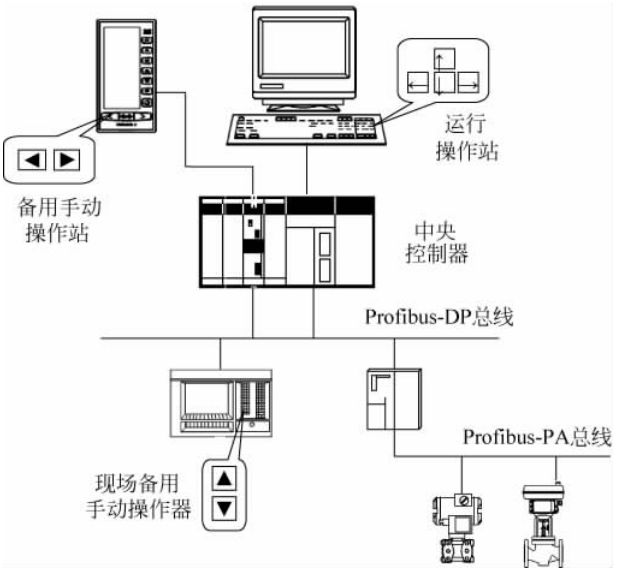

图 5-9　手动备用操作方式的配置图

在现场手动操作站进行手动操作。目前现场总线都可配置总线型现场显示与操作设施，在该设备上即可进行现场手动操作。

在诸如核电或航空航天等领域的控制回路，有时还会用到 1∶2 冗余，即 3 个控制器并联运行，1 台工作 2 台备份。这种冗余是昂贵且奢侈的，只有要求最严格的功能才会用到这么高级的冗余技术。

1∶2 冗余或者 1∶n 冗余有一个优点是它可以消除故障的影响。在 1∶1 的冗余系统中，如果发生故障的控制器仍然有输出，这时系统可以判断已发生故障，但很难判断是哪台控制器发生了故障。在 1∶2 冗余系统中可以采用表决器（也称选举）的方式判断哪台控制器发生了故障。表决器有多种，包括大多数人表决器、一般 k 系数表决器、一般中值表决器等。

（1）大多数人表决器

大多数人表决器按照如下方式工作。如果 x_1 和 x_2 是控制器的输出，当 x_1 和 x_2 的差值满足 $d(x_1,x_2)\leqslant\varepsilon$ 时，则可以认为它们在工程意义上充分相等。要注意的是充分相等不具备真正相等所具有的传递性，也就是说，如果 x_1 和 x_2 充分相等，x_2 和 x_3 充分相等，但并不表示 x_1 和 x_3 充分相等。表决器产生一组输出类 $P_1,\cdots,P_n$，满足

（a）$x,y\in P_i$，并且仅当 $d(x,y)\leqslant\varepsilon$。

（b）P_i 是最大的，即如果 $z\notin P_i$，则必然存在 $w\in P_i$，满足 $d(w,z)<\varepsilon$。

这些类可能共享某些元素，选出最大的 P_i，如果其中含有 $\lceil N/2\rceil$ 个元素，则每个元素（也就是每个控制器的输出）都可以作为表决器的输出。

例 5-4　有一个包含 5 个控制器的系统，令 $\varepsilon=0.001$，5 个控制器的输出分别为 1.0000，1.0010，0.9990，1.0005 和 0.9970。求在采用大多数人表决器时表决器的可选输出值是哪些？

解：对满足条件(a)，即控制器输出差距小于 $\varepsilon=0.001$ 时可产生的输出类有

$$P_1 = \{1.0000, 1.0010, 1.0005\}$$

$$P_2 = \{1.0000, 0.9990\}$$

$$P_3 = \{0.9970\}$$

注意到 P_1 和 P_2 都包含 1.0000，P_1 为最大输出类，并且含有 $3 > \lceil N/2 \rceil$ 个元素，所以 P_1 中的任何一个元素(即控制器输出)都可以作为表决器的输出。

由大多数人表决器可构成 N 模冗余系统。该系统是由 N 个控制器构成，系统对它们的输出进行表决。一般来说 N 为奇数。为了使系统能够容忍最多 m 个控制器发生故障，N 模冗余系统中共需要 $(2m+1)$ 个控制器。最流行的是 3 模冗余系统($m=1$)，它由 3 个控制单元组成，在其中一个发生故障时，系统可以通过大多数人表决器判断出是哪个控制器发生故障，其余 2 个控制器能够正常工作，从而保证系统正常工作。

对于 3 模冗余系统表决器的配置方式也有两种，如图 5-10 所示，一种是表决器与控制器一对一配置，另一种是系统只用一个表决器，显然第二种方式更为简单。

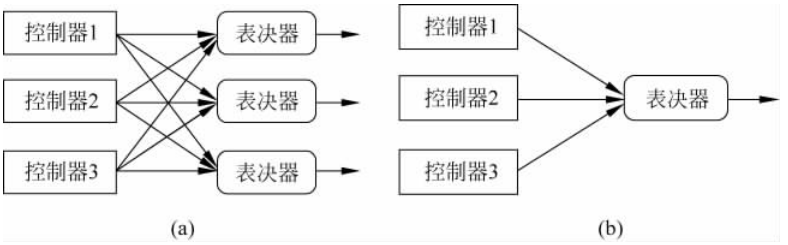

图 5-10　N 模冗余系统表决器的配置图

(2) 一般 k 系数表决器

一般 k 系数表决器按与大多数人表决器基本上相同，只不过是只要至少 k 个元素(k 的值由设计者制定)，就可以选取 P_i 中的任何一个元素(控制器的输出)作为表决器的输出。

(3) 一般中值表决器

一般中值表决器是选取所有输出中的中间值(N 需为奇数时中间值才存在)。表决器不断地剔除距离最大的 2 个输出，直至只剩下一个值，该值即为中间值。计算方法如下，令被表决的输出为 $s=\{x_1, \cdots, x_N\}$，则

① 对于所有的 $x_i, x_j \in S$，并且 $i \neq j$，计算所有的 $d_{ij}=d(x_i, x_j)$。

② 令 d_{kl} 是所有 d_{ij} 中最大的，如果有相等的就选任意一个。令 $S=S-\{x_k-x_l\}$，如果 S 中只包含一个元素，则该元素即为表决器的输出；否则返回步骤(a)。

在 1∶1 的冗余系统中，由于系统很难判断是哪台控制器发生了故障，对有高可靠性要求的应用，一个最简单的方案就是把控制器进行配对，只要一个控制器出现故障，就丢弃这一对控制器。这种配置方案也称之为静态配对，如图 5-11 所示。图 5-11 中这对控制器接受相同的输入并运行相同的软件，系统对其输出进行比较。如果输出相同，则表示控制器工作正常。

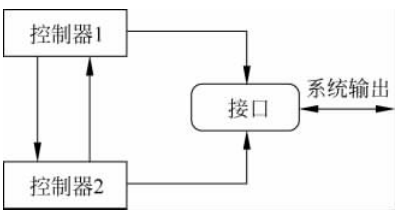

图 5-11　静态配对配置图

如果其中任何一个控制器检测到不同的输出，就表示至少有一个控制器出现了故障，检测到这一差异的控制器就会将它们与系统之间的接口关掉，控制器就与系统隔离开来。

如果分析 N 模冗余系统的可靠性时，若考虑由 k 个或 k 个以上控制器能正常工作，系统就能正常工作，也称该系统为(k,n)表决系统。设每个控制器具有相同的故障率，且服从指数分布，分布函数为 $F(t)$，分布密度为 $f(t)$，则(k,n)表决系统的可靠度 $R(t)$为：

$$R(t) = \sum_{i=k}^{n} C_n^i [1 - F(t)]^i [F(t)]^{n-i} \tag{5-28}$$

由于 $F(t)=1-e^{-\lambda t}$，

对于 $k\geqslant 2$ 有如下递推关系：

$$R(k-1,n) = C_n^{k-1} e^{-\lambda(k-1)t}(1-e^{-\lambda t})^{n-k+1} + R(k,n) \tag{5-29}$$

由此，系统的平均故障间隔时间为：

$$\mathrm{MTBF}(k,n) = \frac{1}{\lambda}\sum_{j=k}^{n}\frac{1}{j} \tag{5-30}$$

对于 $k=2,n=3$ 的系统也称三取二表决系统，这种表决系统在锅炉控制等一些对可靠性要求较高的对象中常用到。三取二表决系统的可靠性与平均故障间隔时间为：

$$R(2,3) = 3e^{-2\lambda t} - 2e^{-3\lambda t} \tag{5-31}$$

$$\mathrm{MTBF}(2,3) = \frac{5}{6}\frac{1}{\lambda} \tag{5-32}$$

式(5-32)表明，三取二表决系统的可靠性比普通系统的可靠性要低 1/6。但要注意式(5-31)的分布关系是如图 5-12 所示。由图 5-12 可以看出，当 $t<0.693\mathrm{MTBF}$ 时，三取二表决系统的可靠性比普通系统的可靠性高。当 $t>0.693\mathrm{MTBF}$ 时，三取二表决系统的可靠性才比普通系统的可靠性低。在实际应用中，系统的工作时间一般远远少于平均故障间隔时间。所以，在大多数情况下，三取二表决系统的可靠性都会比普通系统的可靠性高。

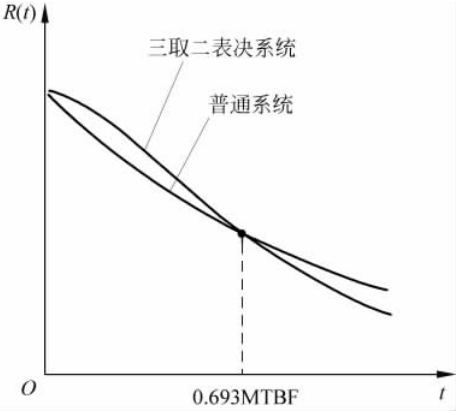

图 5-12　三取二系统与普通系统可靠性曲线比较图

在系统只剩下一台控制器可以工作时，其平均故障间隔时间为：

$$\mathrm{MTBF}(1,n) = \frac{1}{\lambda}\sum_{j=1}^{1}\frac{1}{j} \tag{5-33}$$

有时还将系统的冗余(备份)分为冷备份、温备份和热备份。冷备份是指在工作部件失

效后才通过切换开关启动备用部件投入工作。温备份是指备用部件处于通电状态，但它不带负载，在工作部件失效时通过切换开关将备用部件投入工作。热备份是指备用部件与工作部件处于完全相同的工作条件，带有相同的负载，在工作部件失效时通过切换开关将备用部件投入工作。

5.5　本章小结

本章主要介绍提高控制系统可靠性的相关内容和基本方法，包括可靠性分析方法和提高可靠性的有关措施等。通过本章内容，读者主要学习了如下内容：

- 表征系统可靠性的技术指标主要包括可靠度、故障率、平均故障间隔时间、平均故障修复时间、维修率与可用率等。
- 可靠度既指产品在规定的时间内，在规定的使用条件下，完成规定功能的概率。
- 故障率是产品的故障总数与寿命单位总数之比。
- 平均故障间隔时间(MTBF)，又称平均无故障时间或平均寿命，是指可修复产品两次相邻故障之间的平均时间。
- 系统的可靠性分析模型有串联模型、并联模型、关系矩阵模型、组合模型以及马尔科夫链模型等，其中最常用的是串联模型与并联模型。
- 并联设备构成的系统，其平均故障间隔时间大于单个设备的平均故障间隔时间，并联设备越多，系统可靠性越高。
- 获取系统的可靠性或者说设备故障率数据的方法一般有两种，其一是直接采集现场数据，其二是在实验室中测试生存周期来得到其数据。
- 系统具有后备能力称之为系统冗余。系统冗余包括硬件冗余、软件冗余、时间冗余和信息冗余。
- 提高系统可靠性可以通过对装置或系统的合理设计、元器件的严格筛选和老化、制造过程的严格把关，以及安装调试过程的严格管理等来实现。
- 在 1∶n 冗余系统中可以采用表决器(也称选举)的方式判断哪台控制器发生了故障。
- 表决器有多种，包括大多数人表决器、一般 k 系数表决器、一般中值表决器等。

习题

5.1　什么是可靠度的密度分布函数？

5.2　MTBF 的含义是什么？

5.3　系统冗余有哪几种？

5.4　确定图 5-13 中系统的可靠性？

5.5　1∶n 冗余系统中所使用的表决器主要有哪些？

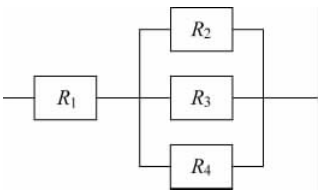

图 5-13　习题 5.4 图

参考文献

[1]　Krishna C M，Shin K G. 实时系统[M]. 北京：清华大学出版社，2004.

[2]　白焰，等. 分散控制系统与现场总线控制系统[M]. 北京：中国电力出版社，2005.

[3]　俞金寿，何衍庆. 集散控制系统原理及应用[M]. 北京：化学工业出版社，1995.

[4]　魏晓东. 分散型控制系统[M]. 上海：上海科学技术文献出版社，1991.