

# 《了解符合 IEC 62380 和 SN 29500 的功能安全时基故障基本故障率估算》



Bharat Rajaram, Senior Member, Technical Staff, and Director, Functional Safety, C2000™ Microcontrollers, Texas Instruments

## 摘要

诸如国际电工委员会 (IEC) 61508<sup>1</sup> 和国际标准化组织 (ISO) 26262<sup>2</sup> 之类的功能安全标准要求半导体器件制造商同时解决系统性和随机硬件故障。通过采用下面的严格开发流程，可管理和减少系统故障。为了满足硬件安全完整性等级 (SIL) 或汽车 SIL (ASIL) 要求，随机硬件故障必须遵循特定的量化指标。因此，在计算随机硬件故障指标时会排除系统故障。

## 内容

1 引言.....	2
2 故障类型和随机硬件故障的量化指标.....	2
3 产品寿命内的随机故障和 BFR 的估算.....	3
4 BFR 估算方法.....	4
5 Siemens SN 29500 FIT 模型.....	5
6 IEC TR 62380.....	5
7 BFR 计算的假设.....	7
8 瞬态故障的特殊注意事项.....	7
9 IEC TR 62380 和 SN 29500 之间的 BFR 差异 (封装引起).....	7
10 通电时间对 BFR 的影响.....	8
11 适用于 TI 产品的资源.....	8
12 总结.....	8
13 参考文献.....	9

## 商标

所有商标均为其各自所有者的财产。

## 1 引言

基本故障率 (BFR) 量化了半导体元件在 *正常* 环境条件下工作时的固有安全性。BFR 乘以温度、电压和工作小时数等参数，通常得到一个可衡量元件 *质量* 的度量。

BFR 是用于计算随机硬件指标 (按功能安全标准的要求) 的主要输入之一，可通过多种方法进行估算。BFR 估算方法依赖于失效模式的假设；因此，这些基本假设的差异将导致 BFR 估算的差异。

本白皮书重点介绍了两种普遍用于估算半导体元件 BFR 的方法，即分别按照 IEC 技术报告 62380<sup>3</sup> 和 SN 29500<sup>4</sup> 进行估算。BFR 估算是计算定量随机硬件指标的基础，其中包括：

- 安全失效分数 (SFF)
- 高需求模式下的每小时失效概率 (PFH)；或低需求模式下的每日失效概率 (PFD)
- 单点故障度量 (SPFM)
- 潜在故障度量 (LFM)
- 硬件随机失效度量指标 (PMHF)

本文还概述了影响 BFR 的因素，并比较了各种估算方法。

## 2 故障类型和随机硬件故障的量化指标

硬件故障本质上可以是系统故障，也可以是随机故障，如图 2-1 中所示。系统故障是由设计、开发或制造流程中存在的某种不足引起的，并且通常源于开发流程中的缺陷。器件错误是系统故障，因为它在开发过程中的设计验证阶段能够检测到。例如，设计的汽车具有方形车轮将视为系统故障，因为汽车使用该形状的车轮将无法正常使用。遵循严格的开发流程，以通过不断改进流程来管理和缓解系统故障，甚至可将这些故障完全消除。

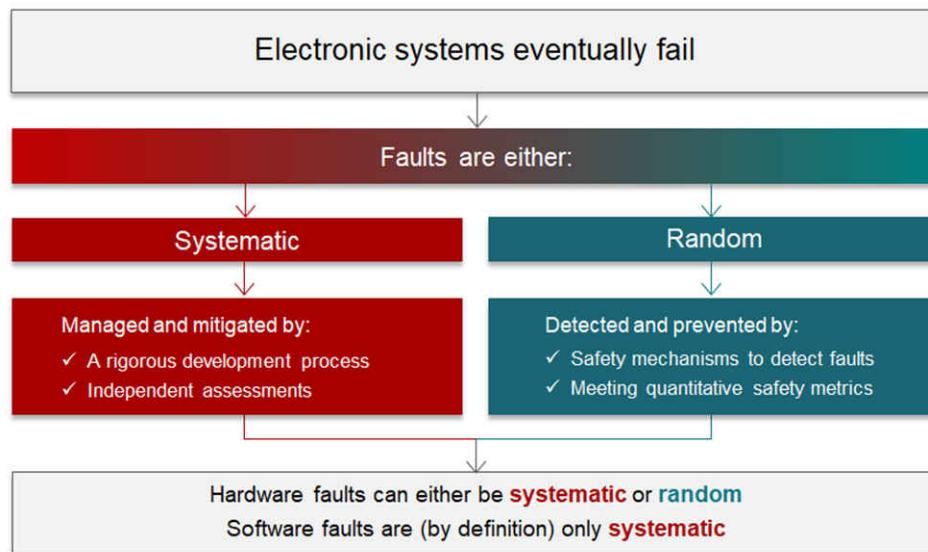


图 2-1. 系统和随机故障概述

另一方面，随机硬件故障是无法消除的，因为所有电子系统最终都会失效。因此，解决随机硬件故障的能力仅限于检测和尽可能防止它们的发生。对于汽车类电气、电子和可编程电子系统，向驾驶员发出问题警报可降低随机硬件故障产生的影响。

表 2-1 和表 2-2 根据 ISO 26262 和 IEC 61508 的要求，分别列出了与每个 ASIL 或 SIL 值关联的随机硬件故障指标的允许值。

表 2-1. 基于 ISO 26262-5 的硬件故障指标

ASIL 级别	SPFM	LFM	PMHF (以 FIT 为单位；时基故障)
ASIL B	≥90%	≥60%	≤100FIT

表 2-1. 基于 ISO 26262-5 的硬件故障指标 (continued)

ASIL 级别	SPFM	LFM	PMHF (以 FIT 为单位; 时基故障)
ASIL C	≥97%	≥80%	≤100 FIT
ASIL D	≥99%	≥90%	≤10 FIT

表 2-2. 基于 IEC 61508-3 的硬件故障指标

SIL 级别	SFF	PFH (以 FIT 为单位; 时基故障)
SIL 2	≥90%	≤100FIT
SIL 3	≥99%	≤10FIT

在计算随机硬件指标时，IEC 61508 和 ISO 26262 都排除了系统故障。因此，BFR 仅适用于失效模式分布和随机硬件指标的计算。

### 3 产品寿命内的随机故障和 BFR 的估算

图 3-1 是一条浴盆曲线，以一种典型方式展示了半导体产品寿命内三个关键时期的随机硬件故障。它们是：

- **早期故障率 (或婴儿死亡率)：**此阶段的特点是初始故障率较高，后期会迅速降低。通过执行加速寿命测试 (例如老化或 I<sub>DDQ</sub> 测试)，可进一步减少早期故障率，这些测试作为德州仪器 (TI) 出厂测试中的一部分在工厂内完成。早期故障主要是由于未能有效筛查出制造缺陷而引起的。缺陷始终会存在，开发和持续改进有效的筛选方式势在必行。
- **正常寿命期故障：**这是浴盆曲线中故障率相对较低且恒定的区域。BFR 估算针对的就是半导体组件生命周期的这一部分。该故障率以“时基故障”(FIT) 为单位进行量化 - 这是对产品运行累计十亿小时 (10<sup>9</sup>) 可能发生的故障数量的估算。
- **内在损耗：**这是产品寿命的一个时段，内在损耗占主导地位并且故障数量呈几何级增长。产品有效寿命结束的时间被指定为出现损耗的时间。这些类型的故障是由众所周知的因素引起，例如通道热载离子效应、电迁移、与时间有关的介电击穿和负偏置温度不稳定性。诸如 ISO 26262 和 IEC 61508 等功能安全标准不支持基于非恒定故障率的随机硬件指标计算。因此，使用产品寿命内的恒定 (但悲观) 近似值来估算 BFR。

系统集成商必须在正常使用寿命期间以及出现内在损耗时解决随机硬件故障问题。在此类情况下，系统集成商必须依靠安全机制，该机制可提供一定的诊断范围，并将风险 (由严重性、暴露程度和可控制性而定) 降至允许值。

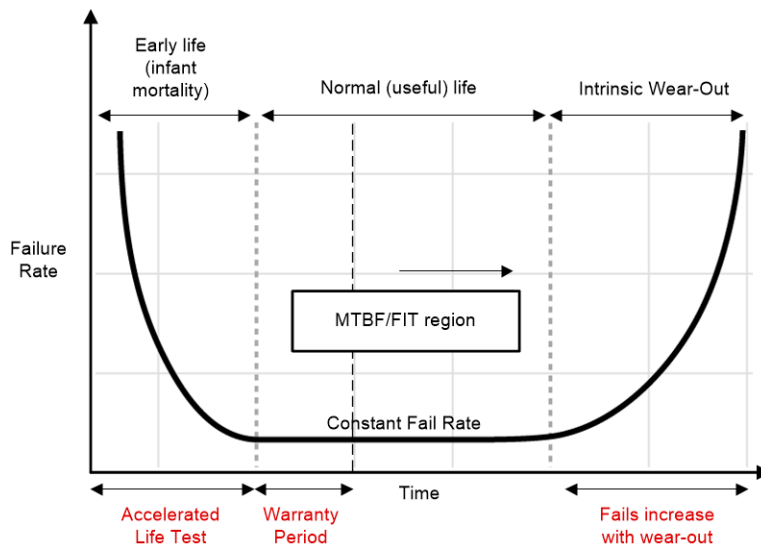


图 3-1. 浴缸曲线是表示随机硬件故障的典型曲线

## 4 BFR 估算方法

有多种估算 BFR 的方法：通过实验、从事件和客户退货/现场故障的实地观察中得出估算值，或基于行业认可的可靠性指南以及一些工程判断的估算值。

这里有一些经验方法的例子。但是，这些示例仅说明了固有（器件）故障，而忽略了器件和封装相互作用的影响。

- 温度偏置运行寿命测试
- 高温运行寿命测试
- 扩展寿命可靠性测试

另一方面，现场观察需要准确和广泛的记录保存，而这在新产品投放市场时无法做到。此外，许多半导体制造商并没有收到所有的客户退货，因此无法满足通过大量的准确记录来估算 BFR 的要求。

可根据以下行业可靠性指南对功能安全分析进行估算：

- IEC 技术报告 (TR) 62380 和 IEC 61709<sup>5</sup>
- SN 29500，用于电子和机电元件可靠性预测的 Siemens AG 标准
- FIDES，例如军事手册或其他来源可靠的文档

本白皮书的其余部分将重点介绍如何使用 IEC TR 62380 和 SN 29500 来估算 BFR。

## 5 Siemens SN 29500 FIT 模型

SN 29500 使用查找表查找各种元件类型的时基故障率参考值和温度值，例如：

- 集成电路 (IC)
- 分立半导体
- 无源器件
- 开关、继电器、灯、连接器等

估算 IC 时基故障率的方法是从表中查找时基故障率参考值和内核温度参考值。这些表分为三种类型：一种适用于集成电路，一种适用于分立半导体，第三种则适用于无源器件。这三个表进一步按 IC/元件类型的子类别划分，然后按 IC 或分立半导体元件中的晶体管数量划分。

在图 5-1 中所示的摘录（来自双极运算放大器的 TI 功能安全时基故障文档）中， $\lambda_{ref}$  时基故障率是 12FIT，内核基准温度为 55°C。该信息源自 SN 29500 标准。

FIT Siemens Norm SN29500 (2)			
Table	Category	Ref FIT $\lambda_{ref}$	Ref Virtual Tj $\theta_{vj,1}$
4	Bipolar Op Amp	12 FIT	55 C

图 5-1. 面向 SN 29500 标准的 TI 标准功能安全时基故障文档

SN 29500 标准介绍了将参考条件下的时基故障率调整为适合实际预期系统运行条件的时基故障率所需的计算过程。只需将预期的温度曲线和参考值代入等式中，然后根据元件在预期应用中的使用情况来计算其时基故障率。

下面列出了适用于所有类型元件的一般方程：

$$\text{应用时基故障率} = \text{时基故障率参考值} \times \text{时间} \times \text{温度因子} \times \text{电压因子} \times \text{电流因子} \times \% \text{时压因子}$$

系统集成商将需要参考 SN 29500 标准中的信息，推导出其应用针对 TI 所提供元件的特定时间基故障率。

## 6 IEC TR 62380

在功能安全分析中估算 BFR 时，也通常使用 IEC 62380 标准。这是一本可靠性数据手册，概述了用于预测电子组件、印刷电路板 (PCB) 和设备可靠性的通用模型。它发布于 2004 年，后来被废除。但是，ISO 26262 标准（现在为第二版，已于 2018 年修订）已将 IEC 62380 标准纳入其新发布的第 11 部分 - 将 ISO 26262 应用于半导体的指南。

可将 IEC TR 62380 IC 故障率建模为内核、封装和电气过应力 (EOS) 相关故障率的总和，其中：

- 与芯片相关的故障率公式包括以下各项的术语：IC 类型和 IC 技术、晶体管数量、热任务曲线、结温以及工作寿命和非工作寿命。
- 与封装有关的故障率公式包括由热膨胀、热循环、热任务曲线、封装类型和封装材料引起的机械应力的相关术语。
- EOS 故障率公式包括具有外部接口和电气环境的特定系统的相关术语。

公式 1 是基于 IEC TR 62380 标准的 BFR 公式（根据原始标准演变而来）。系统集成商必须参考 IEC 62380 标准以获得计算 BFR 所需的信息。

$$\lambda = \underbrace{\left\{ \lambda_1 \times N \times e^{-0.35 \times \alpha} + \lambda_2 \right\} \times \left[ \frac{\sum_{i=1}^y (\pi_t)_i \times T_i}{T_{on} + T_{off}} \right]}_{\lambda_{die}} + \underbrace{\left\{ 2.75 \times 10^{-3} \times \pi_\alpha \times \left( \sum_{i=1}^z (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3 \right\}}_{\lambda_{package}} + \underbrace{\left\{ \frac{\pi_1 \times \lambda_{EOS}}{\lambda_{overstress}} \right\}}_{\text{EOS FIT}} \times 10^{-9} / h$$

Total FIT = Die FIT + Package FIT + EOS FIT (1)

公式 2 根据 IEC TR 62380 将裸片时基故障表示为：

$$\lambda_{die} = \left\{ \lambda_1 \times N \times e^{-0.35 \times \alpha} + \lambda_2 \right\} \times \left[ \frac{\sum_{i=1}^y (\pi_t)_i \times T_i}{T_{on} + T_{off}} \right]$$

(2)

- 其中  $N$  是按类型编号的晶体管， $\lambda_1$  是晶体管类型比例因子， $\lambda_2$  是技术基础时基故障率， $\alpha$  是制造商当前年度相关因子。

公式 3 根据 IEC TR 62380 将封装时基故障表示为：

$$\lambda_{package} = \left\{ 2.75 \times 10^{-3} \times \pi_\alpha \times \left( \sum_{i=1}^z (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3 \right\}$$

(3)

- 其中， $\pi_\alpha$  是 IC 的热胀系数与 PCB 的热胀系数之间的差异， $\lambda_3$  是按封装类型和尺寸划分的封装比例因子。

公式 4 根据 IEC TR 62380 将 EOS 时基故障表示为：

$$\lambda_{EOS} = \frac{\pi_1 \times \lambda_{EOS}}{\lambda_{overstress}}$$

(4)

- 其中，默认假设是  $EOS = 0$ 。

如果表中列出了 IC 应用，并且系统在电路板上的 IC 与外部环境之间具有外部连接，则系统集成商可根据需要添加 EOS 值。

表 6-1 是汽车任务剖面表的屏幕截图（根据 IEC TR 62380 得出）。根据此表，汽车电机控制应用的总工作时间约为每年 500 小时，其中包括四次日间启动、两次晚间启动以及一年有 30 天不使用。



表 6-1. IEC TR 62380 中具有代表性应用的任务剖面

任务剖面阶段	温度 1		温度 2		温度 3		比率开/关		2 次晚间启动		4 次日间启动		未使用的车辆	
应用类型	(t <sub>ac</sub> )1 °C	t <sub>1</sub>	(t <sub>ac</sub> )2 °C	t <sub>2</sub>	(t <sub>ac</sub> )3 °C	t <sub>3</sub>	t <sub>on</sub>	t <sub>off</sub>	n1 周期/年	ΔT <sub>1</sub> °C/周期	n2 周期/年	ΔT <sub>2</sub> °C/周期	n <sub>2</sub> 周期/年	ΔT <sub>3</sub> °C/周期
电机控制	32	0.020	60	0.015	85	0.023	0.058	0.942	670	$\frac{\Delta T_j}{3} + 55$	1340	$\frac{\Delta T_j}{3} + 45$	30	10
旅客舱	27	0.006	30	0.046	85	0.006	0.058	0.942	670	$\frac{\Delta T_j}{3} + 30$	1340	$\frac{\Delta T_j}{3} + 20$	30	10

## 7 BFR 计算的假设

- 仅选择并始终使用一种方法。它可以是：
  - 根据经验
  - 基于现场数据
    - 说明可根据现场数据推导故障率的模型（威布尔或指数）
  - 基于可靠性指南。（TI 产品使用根据可靠性指南得出的 BFR。）
- 采用一个使用情况配置文件。下面是一些示例：
  - 工业：全年全天候，直到计划的预防性维护周期开始
  - 汽车电机控制：每天启动 2 到 4 次，每天使用约 4 小时，如 IEC TR 62380 中所述
- 为用于估算的基础统计选择（并陈述）置信区间（75%、80%、90%）
- 清楚地记录已纳入 BFR 估算的任何比例因子或减额
- 考虑非工作时间和基于焊点的故障

只要所有半导体供应商都使用相同的 BFR 估算假设或至少明确陈述其假设，就有可能对两个不同制造商制造的同类型半导体组件的 BFR 进行比较。

## 8 瞬态故障的特殊注意事项

在 BFR 估算中必须考虑到由辐射事件（内部或外部）导致的软错误，这些软错误会导致随机硬件故障。但是，由电磁干扰或串扰引起的软错误不应包括在 BFR 计算中，因为它们被归类为系统故障，可通过遵循良好的设计规范来管理。可通过以下属性来调制瞬态故障：

- 使用的方法
- 故障的影响和适用情形
- 封装中的标准和低阿尔法与超低阿尔法模塑化合物

架构易受损因子 (AVF) 反映的是设计结构中软错误引起的故障概率，可能导致功能的最终输出中出现可见错误。根据 ISO 26262，不应基于 AVF 或诸如错误检测和纠正 (EDAC) 电路等安全机制来降低软错误的 BFR。因此，最好分别为半导体元件中的随机存取存储器和逻辑块计算软错误的 BFR。

## 9 IEC TR 62380 和 SN 29500 之间的 BFR 差异（封装引起）

SN 29500 在考虑器件和封装相互作用造成的故障方面存在缺陷（相对于 IEC TR 62380）。因此，功能安全标准建议：

- 半导体组件制造商估计器件与封装材料以及器件与封装的连接点（引脚）相互作用而导致的故障
- 系统集成商负责半导体组件与电路板（焊接点）之间连接点引起的故障。这些故障通常在元件或系统级别进行分析。
- ISO 26262 将
  - 元件定义为系统、组件（硬件和软件）、硬件部件或软件单位；并
  - 将系统定义为一组元件或子系统，将至少一个传感器、一个控制器和一个致动器关联起来。

IEC TR 62380 既考虑了硅片与引线框架/基板之间的相互作用，也考虑了焊点之间的连接。相比之下，SN 29500 中的封装故障率仅考虑内核与封装之间的相互作用，从而导致在使用 SN 29500 进行 BFR 估算时过于乐观。

## 10 通电时间对 BFR 的影响

ISO 26262 建议应用以下属性，最大限度地减少所计算 BFR 的缩放比例或不合理的降低：

- 准确的任务剖面
- 评估失效模式在操作条件下的适用性（如任务剖面中所指定）
- 确定每单位故障率（按系统运行一小时、一天、一个月或一年的故障率）

IEC TR 62380 中的 BFR 公式会考虑  $\tau_{ON}$  和  $\tau_{OFF}$ ，其中 SN 29500 会考虑  $\tau_W$ 。

## 11 适用于 TI 产品的资源

TI 的功能安全产品有三个类别：功能安全合规型、功能安全质量管理型和功能安全型。有关 TI 功能安全产品的更多信息，请点击[此处](#)。所有 TI 功能安全产品均随附功能安全时基故障率和失效模式分布 (FMD) 文档，旨在提高功能安全系统的适用性。

对于我们的微处理器、微控制器和模拟信号链产品等绝大多数复杂器件，系统集成商将获得全面的失效模式、影响和诊断分析 (FMEDA)，其中包括 FMD（基于根据 IEC TR 62380 估算得出的 BFR）。

对于低压降振荡器、运算放大器和电压监控器等并不复杂的模拟产品，系统集成商将获得采用 TI 标准格式的功能安全时基故障、引脚失效模式分析和 FMD 报告。

下面是概述此信息的示例报告链接：

- 德州仪器 (TI)，[功能安全时基故障率、失效模式分布 TPS7A16A-Q1](#)
- 德州仪器 (TI)，[功能安全时基故障率、失效模式分布 TPS3851-Q1](#)

## 12 总结

借助 TI 的产品、工程专业知识和设计资源，系统集成商能够以更快的速度创建更安全、可靠的设计。此外，通过选择根据 IEC TR 62380 或 SN 29500 估算 BFR 的产品，系统集成商能够满足 ISO 26262 和 IEC 61508 等功能安全标准的严格要求。



### 13 参考文献

1. [IEC 61508: Second edition 2010-04](#): Functional safety of electrical/electronic/programmable electronic safety - related systems.
2. [ISO 26262: Second Edition 2018-12](#): Road Vehicles - Functional Safety, ISO 26262, International Organization for Standardization (2018)
3. [IEC/TR 62380:2004\(E\)](#): Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment
4. SN 29500: Siemens Norm SN 29500/ Edition 2010-09
5. [IEC 61709: Third Edition 2017-02](#): Electric components - Reliability - Reference conditions for failure rates and stress models for conversion

## 重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 [TI 的销售条款](#) 或 [ti.com](#) 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

Copyright © 2022，德州仪器 (TI) 公司