# BMS functional safety功能安全

## IEC 60730-1, 附录H

Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.

# IEC 62619的功能安全的要求

- Clause 8: Battery system safety (considering functional safety)

Reliance on electric, electronic and software controls and systems for critical safety shall be subjected to analysis for functional safety.

IEC 61508 (all parts), Annex H of IEC 60730-1:2013 or other suitable functional safety  standard for the application may be used as references.

A process hazard, risk assessment and mitigation of the battery system shall be done by the battery system manufacturers. (e.g. FTA, FMEA)。

# IEC 62619的要求

- Clause 8: Battery system safety (considering functional safety)

The procedure is as follows:

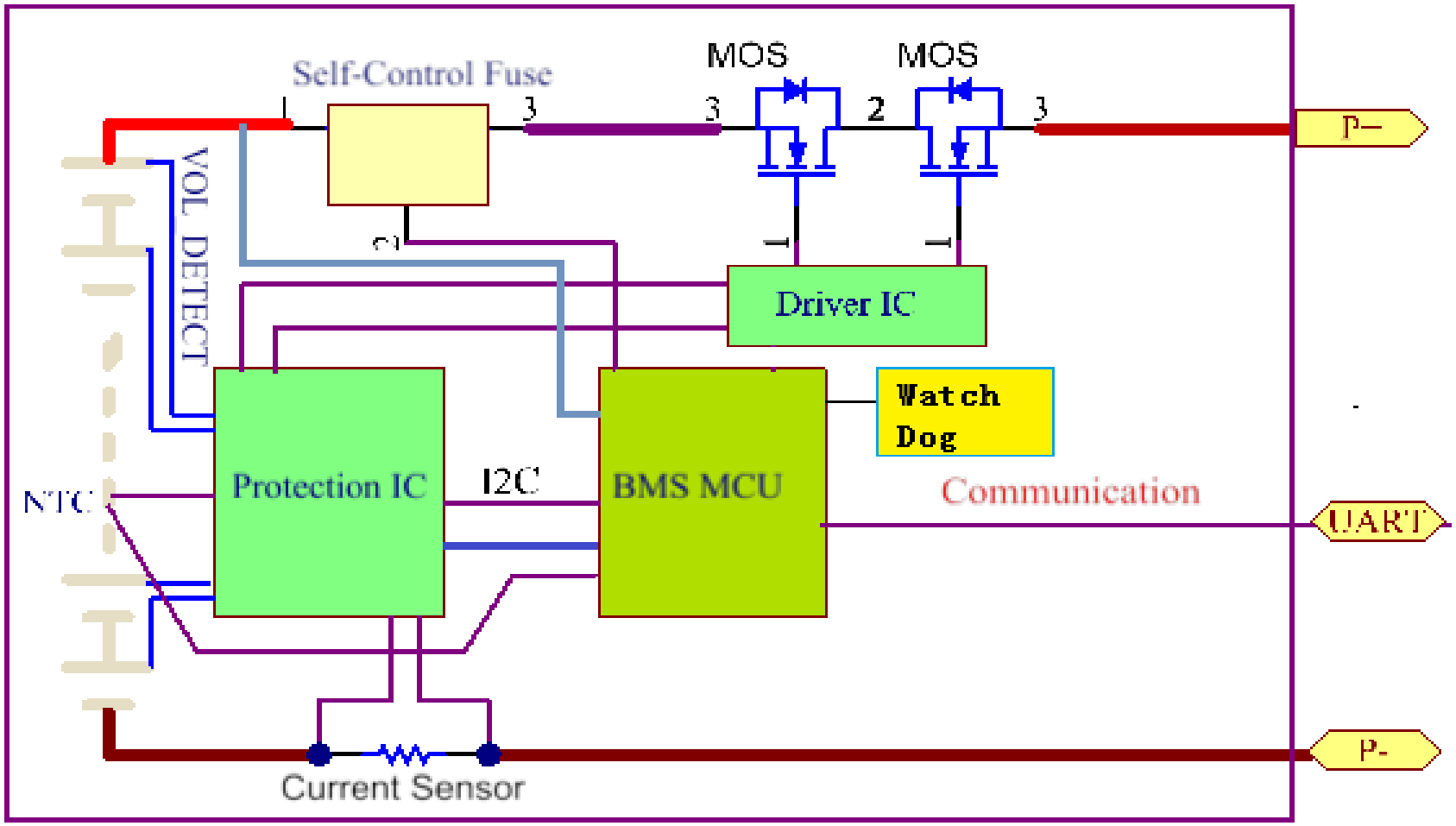
# IEC 62619的要求

➢ Clause 8: Battery system safety (considering functional safety)

Examples of hazards or risks are as follows:

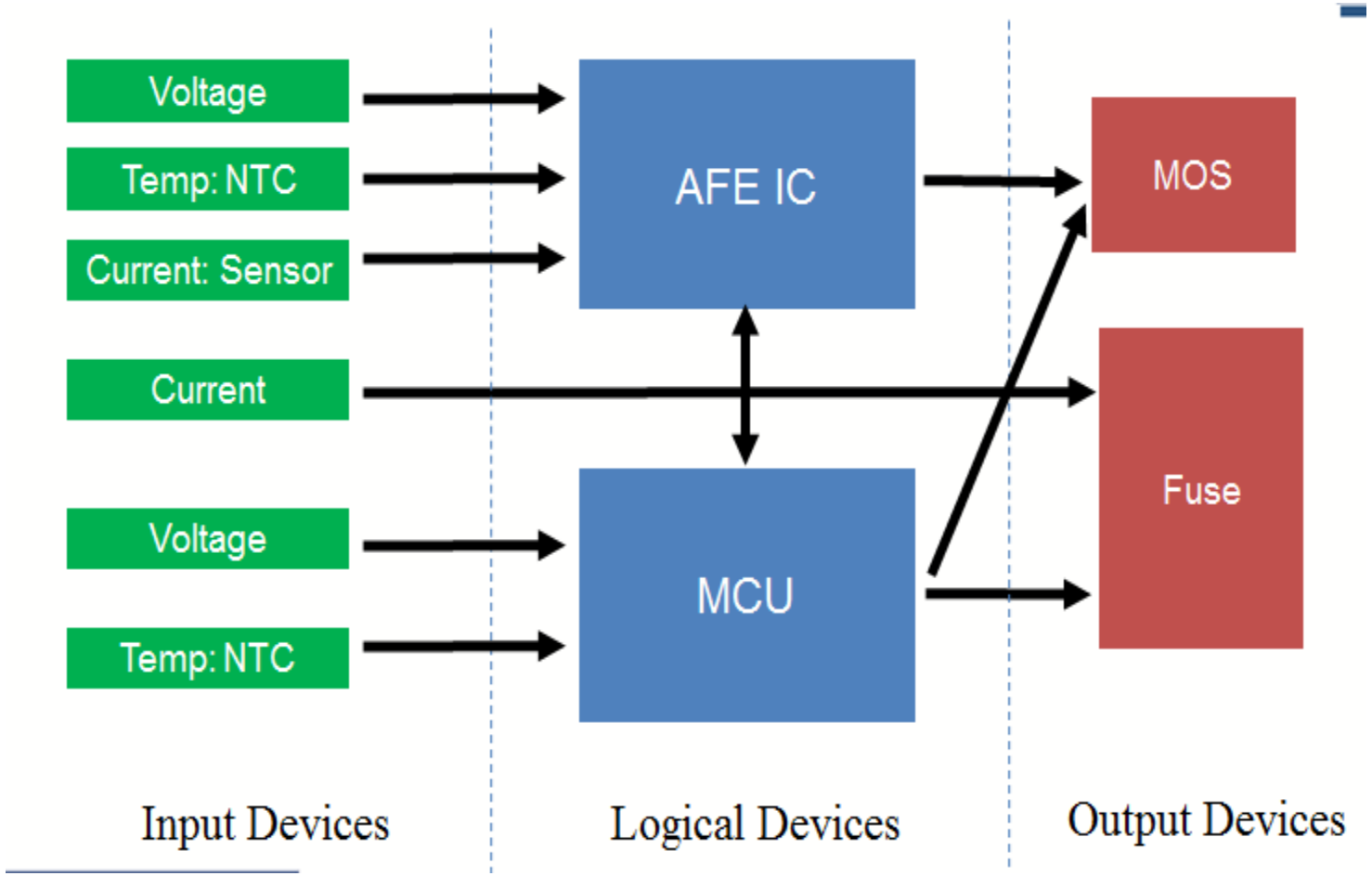
- EMC
- electric shock
- water immersion
- external short-circuit
- internal short-circuit
- overcharge
- overheating
- drop
- crush
- overdischarge
- discharge with overcurrent
- charging after an overdischarge
- electrolyte leakage
- ignition of emission gas
- fire
- earthquake
- seismic sea wave, etc.

# 功能框图—示例



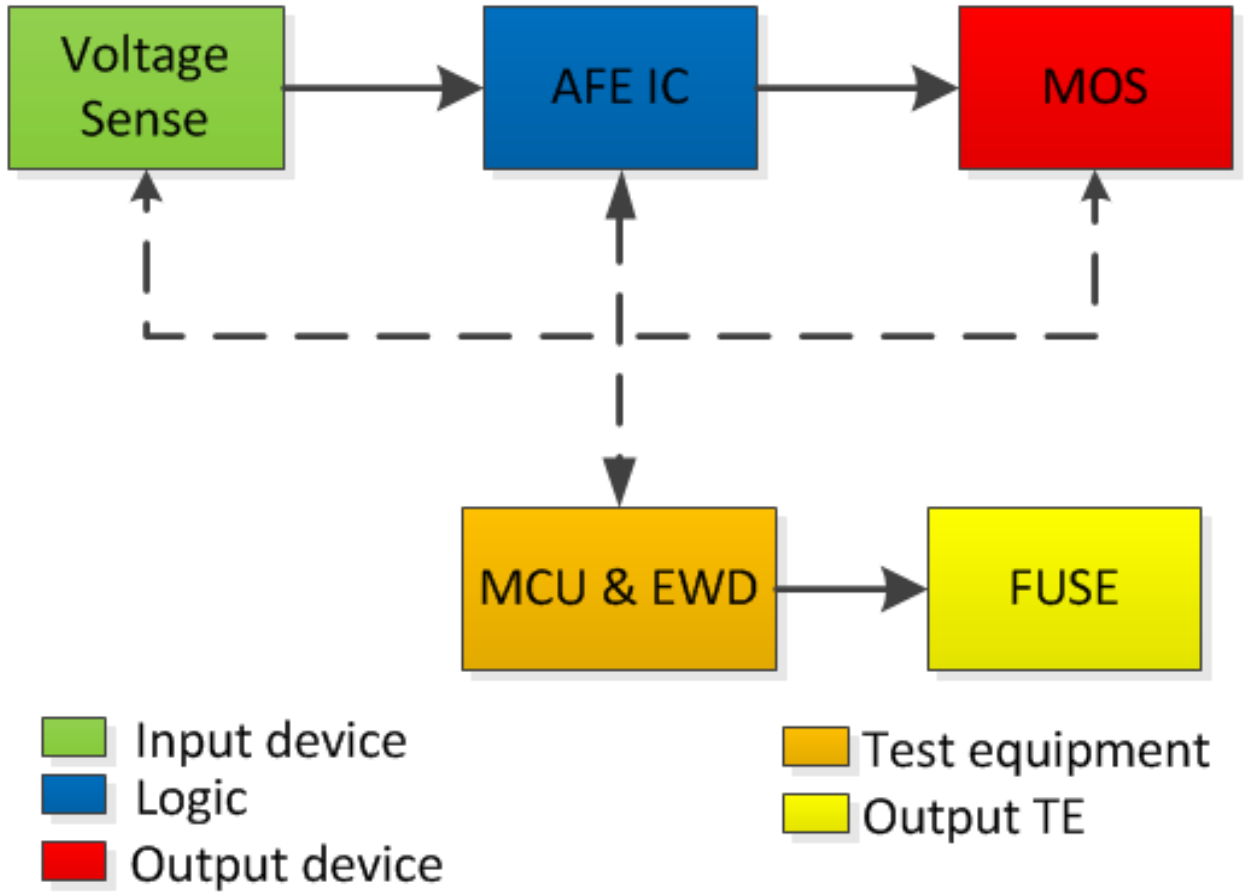

--温度保护
--电压保护
--电流保护

# 功能框图—示例




--温度保护
--电压保护
--电流保护

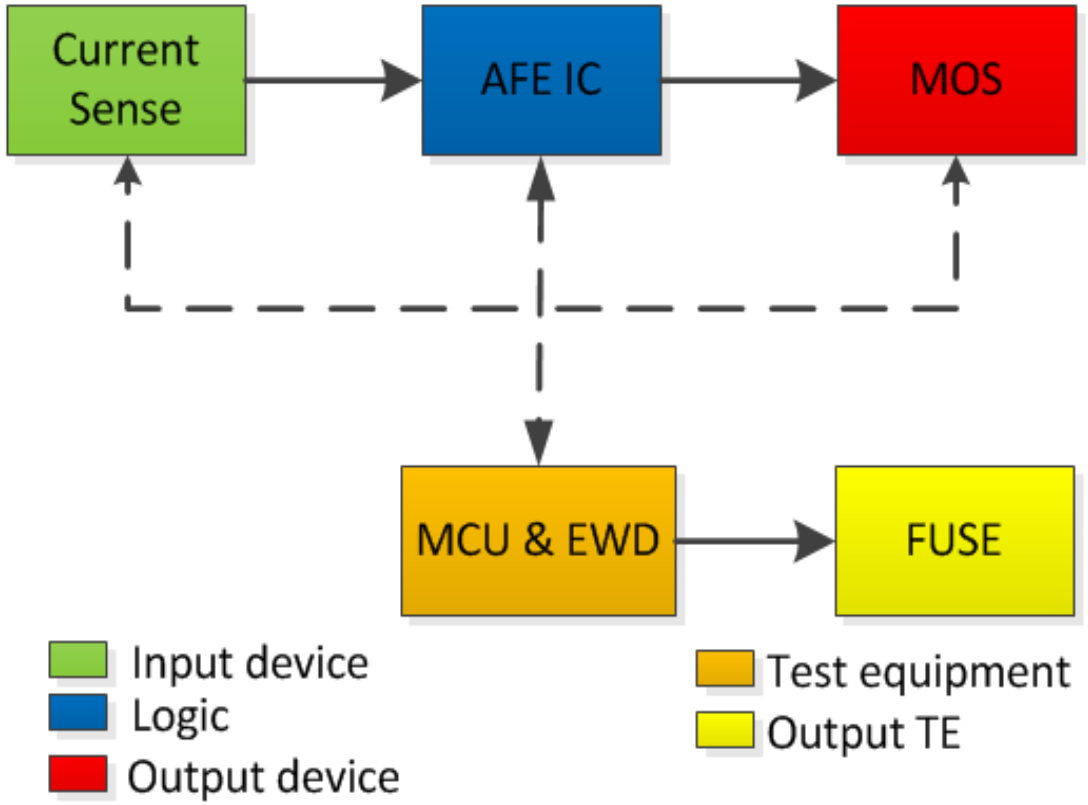
# 功能安全描述—电压保护示例




功能安全的描述要求：

1. 电压采样的电路图，原理和参数；
2. 逻辑处理的电路图，原理和参数；
3. 输出控制的电路图，原理和参数；
4. 采样，逻辑和输出元件失效的诊断原理

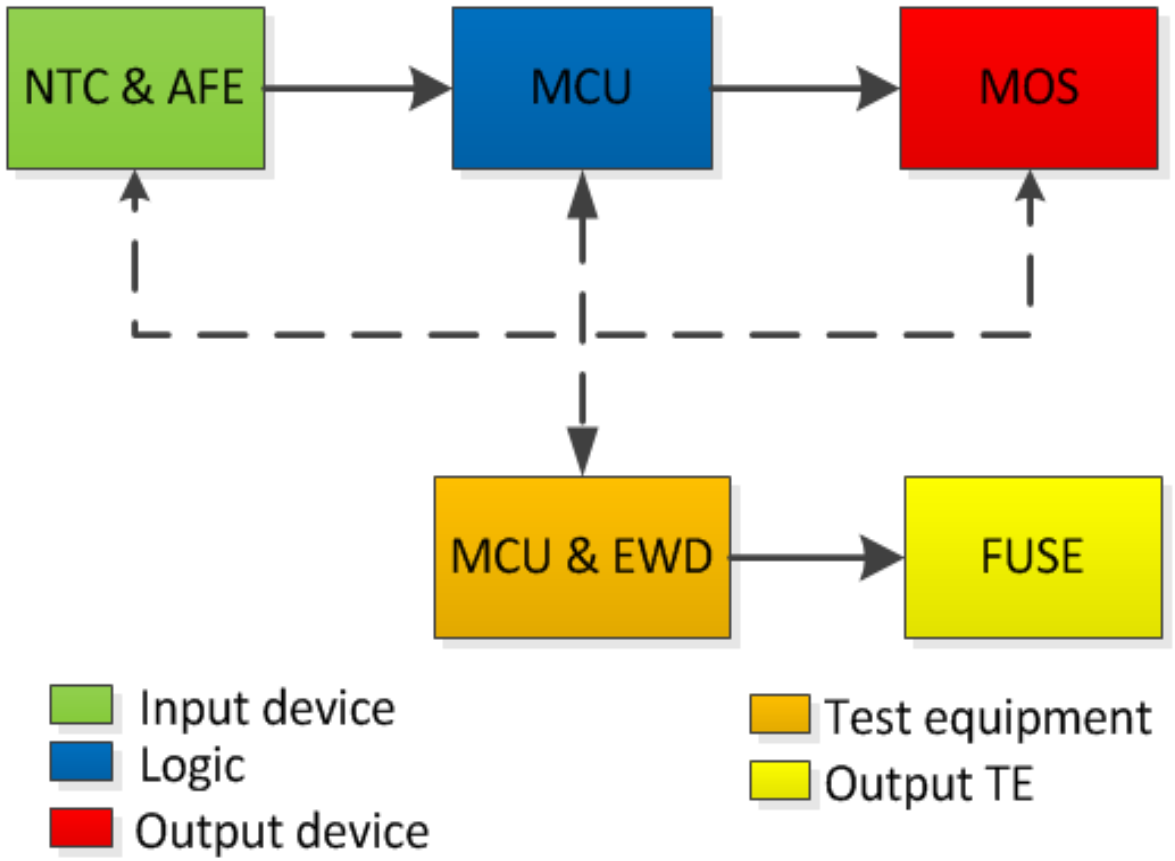
# 功能安全描述—电流保护示例




功能安全的描述要求：

1. 电流采样的电路图，原理和参数；
2. 逻辑处理的电路图，原理和参数；
3. 输出控制的电路图，原理和参数；
4. 采样，逻辑和输出元件失效的诊断原理

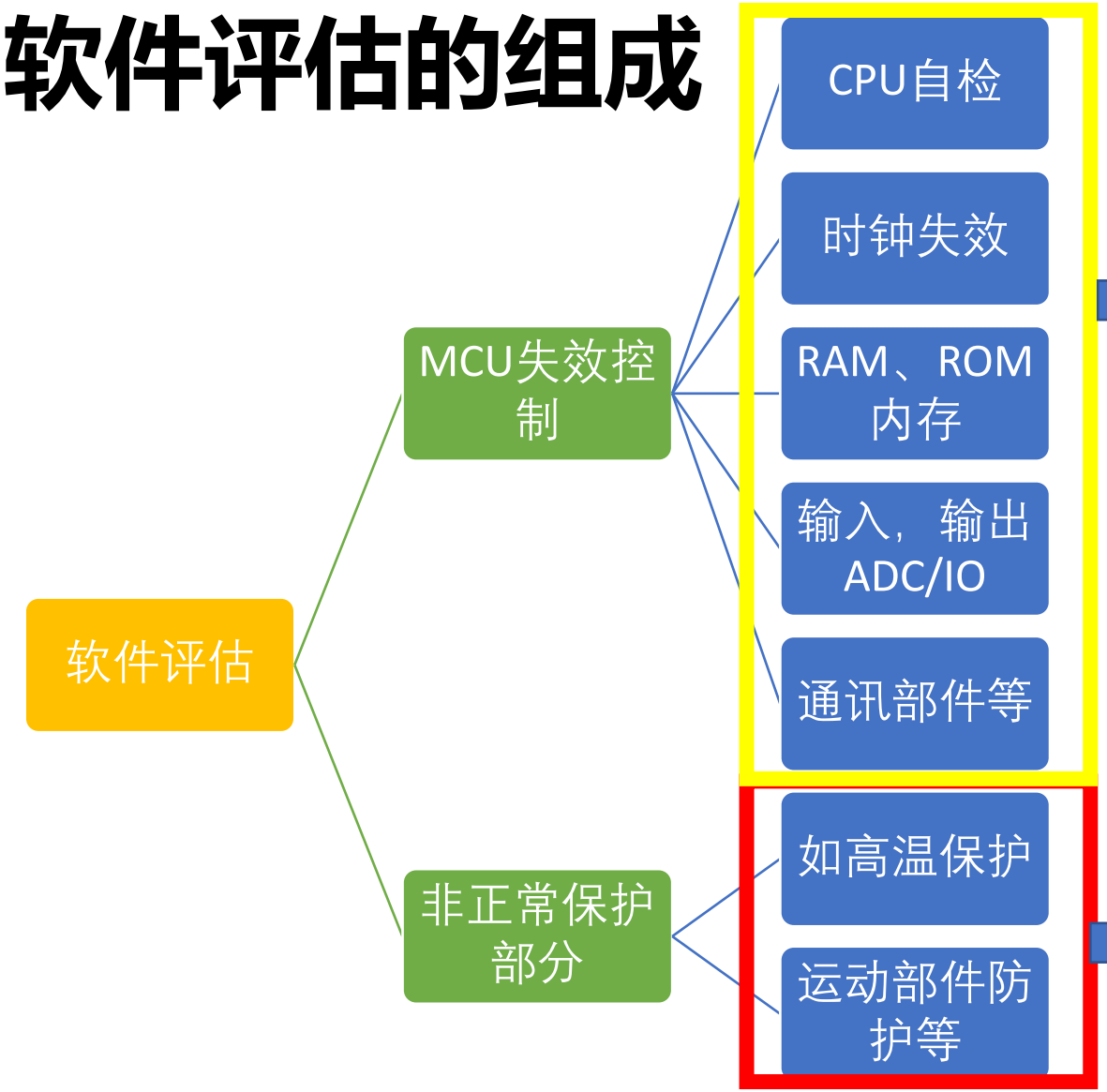
# 功能安全描述—温度保护示例




功能安全的描述要求：

1. 电流采样的电路图，原理和参数；
2. 逻辑处理的电路图，原理和参数；
3. 输出控制的电路图，原理和参数；
4. 采样，逻辑和输出元件失效的诊断原理

# 软件评估的组成




-IEC 60730附录H
-有固定失效模式
-有标准的应对措施

-保护参数因产品和标准而已
-应对措施因产品和设计方案而定

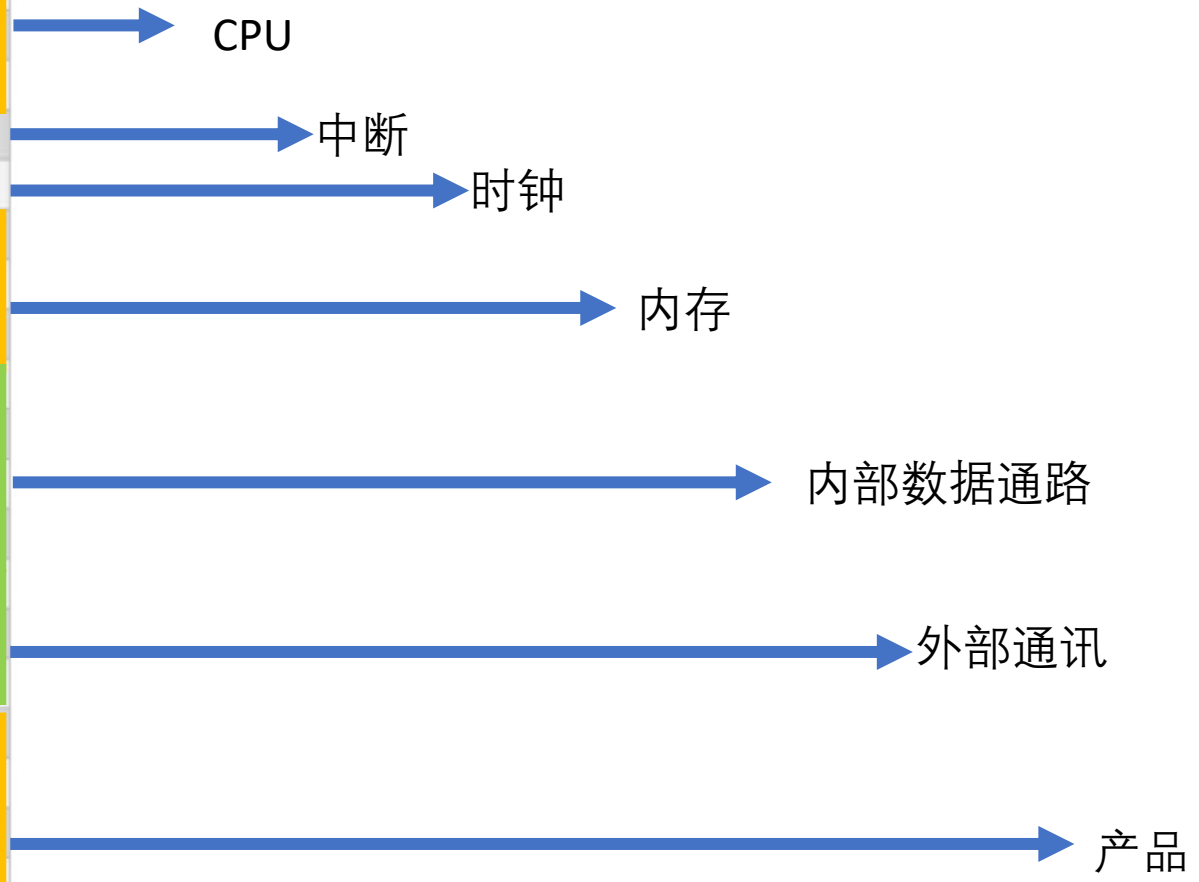
# 软件评估的内容


MCU一般包含的功能模块：

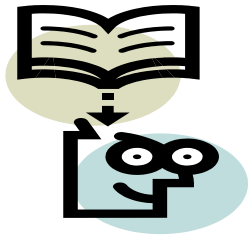
1. CPU （core）
2. 时钟clock
3. 定时器（Timer），看门狗
4. 内存，RAM，ROM
5. ADC
6. 通讯IO

# 软件评估的内容

| Component | Component to Test | Typical Error Detected by Tests |
|---|---|---|
| 1 | CPU | - |
| 1.1 | Registers | Stuck at |
| 1.3 | Program counter | Stuck at |
| 2 | Interrupt handling and execution | No/too frequent interrupts |
| 3 | Clock | Wrong frequency |
| 4 | Memory(1) | - |
| 4.1 | Invariable memory | All single bit faults |
| 4.2 | Variable memory | DC fault |
| 4.3 | Addressing | Stuck at |
| 5 | Internal data path(1) | - |
| 5.1 | Data | Stuck at |
| 5.2 | Addressing | Wrong address |
| 6 | External communication | - |
| 6.1 | Data | Too long Hamming distance |
| 6.3 | Timing | Wrong point in time |
| 7 | I/O peripherals | - |
| 7.1 | Digital I/O | Fault conditions specified in H.27.1(2) |
| 7.2.1 | A/D- and D/A-converter | Fault conditions specified in H.27.1(2) |
| 7.2.2 | Analog multiplexer | Wrong addressing |
| 9 | Custom chips (ASIC, GAL, Gate array etc.) | Any output outside static and dynamic functional specifications |



# 文件要求




| Hardware Engineer | Document Requirement | Software Engineer |
|---|---|---|
| • Circuit diagram电路图<br>• PCB layout、BOM<br>• FMEA (system+component)<br>• Risk analyses/safety requirement风险分析<br>• Interfaces b/w SW and HW 软件硬件接口<br>• Safety architecture安全架构 | • Software document list<br>• **Hardware specification**<br>• **Software Specification**<br>• **IDE: Integrated Development Environment** | • SRS功能安全需求<br>• Software architecture specification软件架构<br>• Code for safety module<br>• Validation and verification report仿真报告<br>• Code stanard<br>• IDE tools |

# 软件评估的资料要求

## SRS安全需求说明

- 产品介绍：产品架构，连接情况，各个部分模块描述
- 标准和指令：定义产品需要符合的具体标准和指令
- 定义，术语：解释关键的专业术语
- 基本功能：描述产品的所有功能模式，如待机，充电模式，手动，自动，半自动模式等
- 安全功能目标
- 软件功能：通过软件实现的安全功能

## 软件设计规格书

- 基本软件环境
- 软件工具
- 架构
- 模块划分
- 安全功能的实现
- 流程图
- 时序图
- 状态变换图
- 数据流图

## MCU开机自检和周期性自检方案

- 寄存器
- PC
- 中断
- 看门狗
- ROM
- RAM
- 时钟
- 时序
- IO
- ADC
- 通讯等

# 软件评估的资料要求

## 软件规范

- 使用代码标准
- 不使用动态对象和变量
- 中断的有限使用
- 指针的有限使用
- 递归的有限使用
- 在更高级别的程序中没有无条件跳转等

## 产品基本资料

- 型号管理+变更作业指导书：硬件版本，软件版本，软件发布日期，软件校验码
- 产品的电路图，layout，BOM表，图片

## 静态分析报告+仿真报告

- 软件代码是否满足coding standard
- 软件是否在硬件失效的时候能满足标准的要求