doi:10.3969/j.issn.1671-5152.2015.01.003

# 家用燃气具控制功能的安全解析

□ 广东万和新电气股份有限公司（528305）陈必华

**摘　　要：** 本文论述了家用燃气燃烧器和燃气器具控制功能的安全等级的特点及如何通过功能安全的失效分析对安全等级进行分类。

**关 键 词：** 燃气具　功能安全　失效分析　控制功能

# Functionality Safety Analysis for Gas Burners and Gas Burning Appliances

Guangdong Vanward New Electric Co., Ltd　Chen Bihua

**Abstract:** This articles describes the methods of functionality safety classification and classes of control functions is given for automatic electrical controls of gas burners and gas burning appliances.

**Keywords:** gas appliances　functionality safety　failure analysis　control functions

## 1　概述

从国内外燃气具发展的历程看，燃气具控制装置的发展经历了全机械、机械电气、到电气/电子/可编程系统（E/E/PES）控制装置的发展，而功能安全的研究最初是从机械领域开始的，机械的控制装置结构简单，受环境的影响小，失效模式也相对简单，长期的实践应用也证明是安全的，如水气联动阀、温度调节阀等。电气/电子/可编程系统（E/E/PES）的应用扩展了安全方面的功能，实现了许多机械控制无法实现的功能，使得器具显得更为安全，但容易发生的潜在的各种失效模式，如温度湿度电磁干扰等环境影响产生的失效，威胁到功能的可靠性，从而产生安全问题。国外在这方面的应用及规范实施走在前面。

目前，国内中高端燃气具产品控制均采用电气/电子/可编程系统（E/E/PES），如点火、燃气关断、火焰检测、恒温控制、安全时间控制等功能都是通过电子控制系统来实现，这种先进智能化技术应用增加了对燃气具系统安全要求的复杂程度。由于行业内对电子控制系统在安全可靠性设计方面的认识不足，主要表现在对家用燃气具的功能安全的特点及分类不明确，导致了控制系统设计没有采取必要的安全措施，存在许多安全隐患。随着住房和城乡建设部的标准《家用燃气燃烧器具电子控制器》CJ/T421-2013的实施，对家用燃气具的功能安全的特点分析研究表现得更为紧迫和必要。

## 2　燃气具功能安全的定义与分类

简单地说，功能安全是指依赖控制系统执行正确的功能。

GB/T 20438标准的定义是功能安全的含义更为广

义，引入“安全相关系统”的概念，不仅仅是技术上的安全措施，还包括功能安全的管理等，是整体安全的概念。具体可参考参考文献[2]，本文只针对燃气具具体的控制功能安全做分析。

燃气具功能安全主要包括电气安全及控制功能安全，电气安全是燃气具基本的功能安全，本文不做论述。

按照《家用燃气燃烧器具电子控制器》CJ/T421–2013 4.1节的规定。依据失效产生的结果的严重性，控制功能的安全性分为：A类、B类、C类。

### 2.1 A类：控制功能与安全性无关

如：室内温控器，其功能具有开/关机，设置运行温度等功能，如果该控制器的功能失效可能导致没有开关机指令，或不能设置温度，但受控系统安全不会因此降低。

但如果这个室内温控器可以执行锁定功能的解除，是否与安全性有关需要依受控系统设计来判定。（具体可参见3.5节）

### 2.2 B类：控制功能的设计能防止可预见的不安全的运行

如：燃烧系统中的对风压开关的检测，如果检测电路失效并不直接导致CO或火焰外溢产生，但会存在这种风险。在设计时要能判定检测电路失效或通过另外的回路判断，起到预防作用。

### 2.3 C类：控制功能的设计能防止特定的危险状况，诸如火灾、爆炸之类的特别风险

如：燃烧控制及燃气切断功能，如果控制功能失效，将导致燃气泄漏而产生火灾及爆炸，通常在设计中通过增加冗余设计及错误检测来降低这种风险的概率。

## 3 燃气具功能安全分类的解析

燃气具主要的控制功能包括燃气切断功能、燃烧控制功能、温度控制功能、燃烧产物排放功能、系统重置功能等。通常这些功能的实现都离不开电气/电子/可编程系统（E/E/PES），这与传统的对功能安全的要求是不一样的。由于控制器功能的失效可能导致燃气泄漏而产生火灾及爆炸，有毒烟气及过热等危险，功能设计就必须能防止这种危险的发生，在失效分析的基础上来进行控制电路功能及故障保护的设计，从而保证功能安全而不仅仅是实现功能。要达到这种目的，必须先正确分析理解这些功能在安全上的特征及要求。

### 3.1 燃气切断功能

燃气切断功能的失效会直接导致燃气泄漏，产生着火及爆炸的风险，燃气切断功能要求C级安全。

燃气切断功能必须使用两个截止阀来保证燃气切断，通常阀的连接组合如下：

（1）两个自动截止阀连接

由于自动截止阀通过已验证的机械结构及寿命保证可靠性，不存在电子器件，没有额外补充要求。

（2）一个自动截止阀和一个储能关闭截止阀连接

储能关闭截止阀在结构上的功能保证需要补充一些验证措施，具体可参见参考文献[3]，如果是基于电子元件时（电容、电池），在电源断电后为确保关闭阀门，电路部分的性能应符合标准CJ/T 421 D4.4的内部故障保护试验要求。

（3）一个自动截止阀和一个无储能关闭截止阀连接

无储能关闭截止阀与储能关闭截止阀功能安全的要求相同。但这种组合不能用在连续运行的器具上，也就是说24小时中必须执行关闭重启，并进行故障测试。

（4）两个储能关闭截止阀连接

（5）一个有储能关闭截止阀和一个无储能关闭截止阀连接

（6）两个无储能关闭截止阀连接

这种组合方式在电源断电后不能关闭阀门（如步进电机驱动的阀门），这是不可接受的。

阀的组合符合功能安全要求，但并不意味切断功能符合安全要求，阀的驱动电路的失效会直接导致切断功能失效。燃气泄漏后状况较为复杂，所有的安全措施都是保证不产生泄漏，而不是产生燃气泄漏后再进行保护。由于储能关闭截止阀与无储能关闭截止阀在国内较少使用，本文只分析自动截止阀的切断功能。

第一，两个阀门的控制均符合B类安全要求，但组合是不能达到C安全要求的，如图1。从阀门组合的容错上分析，当其中一个阀门失控（如有杂物或卡死），另一个阀能保持正常即可符合安全要求。例如，自动阀2失控，自动阀1必须保证安全。B类安全

的要求是电子控制1在第一个故障的条件下保证安全状态，但该故障可能不被检测到，当第二个故障仍出现在电子控制1时，电子控制1可能导致自动阀1不受控，这样两个阀都不受控，所以不符合C类安全要求。

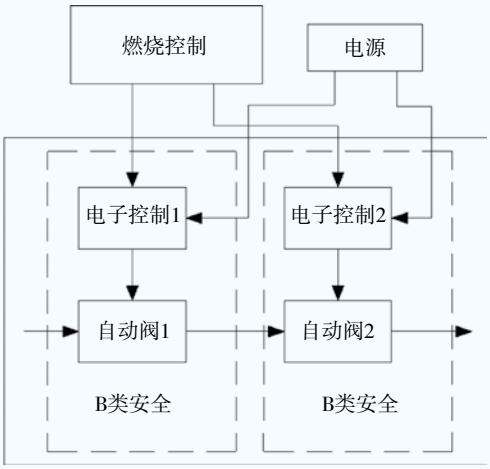


图1 不符合C类要求的燃气切断功能控制

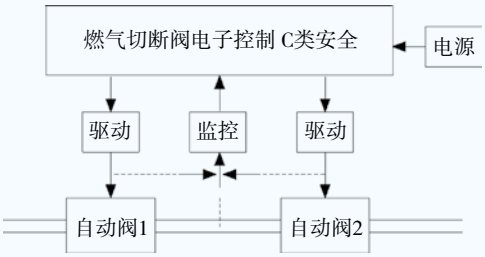


图2 符合C类要求的燃气切断功能控制

第二，两个阀门同时由符合C类安全的电子控制器控制，整体可以达到C安全要求，如图2。当自动阀1失效，如果电子控制器符合C类安全，自动阀2在任意两个故障的条件下均可以保证处于安全状态，所以整体符合C类安全要求。按照这种分析，自动阀1、2是可以同时驱动的（并联）。所以阀的冗余与阀驱动的冗余是安全设计两个方面，都必须要做到。

### 3.2 燃烧控制功能

燃烧控制功能主要包括点火控制、火焰监控、安全时间、故障反应时间、前后清扫时间、锁定时间等时序与逻辑的控制。

火焰监控通常与燃气切断功能关联，所以燃烧控制功能属于C类安全。如果燃烧控制不包括火焰监控功能，仅是一些时序与逻辑的控制，其功能安全可根据失效后果归为B类，具体可参见表1。

表1 燃烧控制功能中的风险与分类

| 失效 | 风险分析 | 安全分类 |
|---|---|---|
| 点火安全时间 | 爆燃或燃气泄漏 | C 类 |
| 点火时序 | 爆燃或燃气泄漏。 | C 类 |
| 风压信号监控 | 有毒或超标烟气排放，或排放不畅 | B 类 |
| 熄火安全时间 | 燃气泄漏 | C 类 |
| 进入故障锁定时间 | 可能发生不正常重启 | B 类 |
| 前后清扫时间 | 未燃烧气体残留 | B 类 |
| 火焰监控 | 燃气泄漏，着火 | C 类 |

单独的火焰监控（独立于时序与逻辑控制之外）装置应是C类安全。因为最直接的风险是熄火后，不能有效地反馈火焰信号，导致燃气关闭延迟或不能关闭。

采用电子系统的火焰监控通常与其他燃烧控制，燃气切断等功能构成一个集成的控制系统，该系统必须符合C类安全无疑，这很容易理解。

### 3.3 温度控制功能（TCF）

燃气具温度控制功能主要实现温度恒定，预防过热，防止燃气燃烧过热导致的着火风险。这类风险如：燃气热水器水温过高产生伤人事故、缺水干烧产生的着火事故。

温度控制功能（TCF）应是C类安全，与燃烧控制功能比较，在功能安全方面的实质是相同的。TCF满足C类安全可以通过完全电子控制器来实现，也可以允许较低安全类的电子控制器与结构的安全措施结合达到TCF整体符合C类安全。

TCF符合C类安全设计的例子如图3、图4、图5。

如图3，这是一个传统的解决方法，使用了机械控温的组合，即由温度控制（温度调节器）和防止温度过热风险（温度限定器）构成，具体要求可参见器具标准（例如EN297、EN483）的内容要求。机械温控结构是由多年实践而产生的并依赖冗余技术作为原理，被认为是安全的，不需要控制器另外采取特别的措施。此处A类温度控制电子电路与低温温控器可以相当于一个机械的温度调节器。

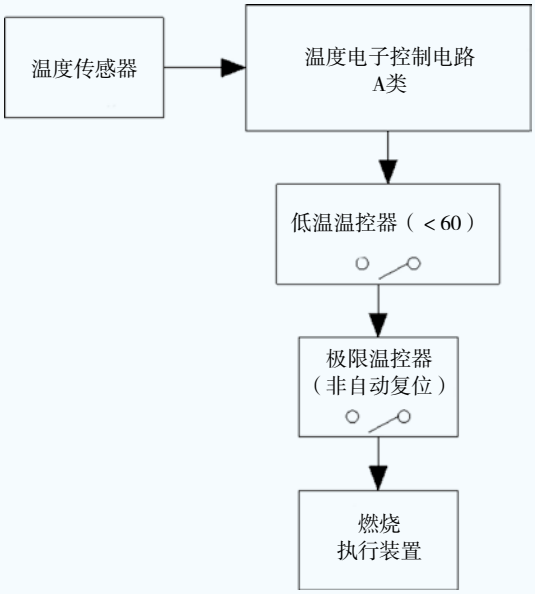


图3 A类温度控制器与机械温控器的组合

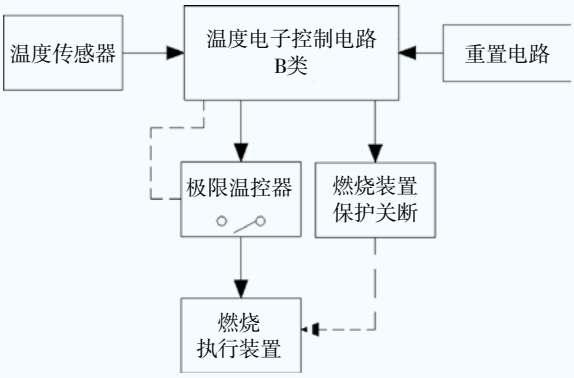


图4 B类温度控制器与极限温控器的组合

如图4，温度传感器（如 NTC）与电子控制电路构成温度调节器的功能，由于采用了电子控制，应基于失效模式做功能安全评价。在出现第一个任意故障（温度传感器或其检测电路失效）时，应能被检测到，所以电子控制电路被要求为B类。极限温控器属于一个“高限制”保护性器件，是独立于电子控制部分的，当出现第二个任意故障时（B类电子控制器功能失效），可以直接断开燃烧执行装置，从而使整体功能符合C类功能安全。

如图5，这种设计没有一个最后的独立保护装置，安全依赖于系统安全完整性（参考文献[2]）的要求保证。其中一个温度传感器设在燃烧器（或热交换器），另一个在输出热水端。当其中一路温度传感器或其检测电路失效，另一路可以被监测并保护。由于采用全电子控制器来实现温度控制功能，该电子控制器必须按照C类电子控制器的要求来设计，软件也必须符合C类软件要求，这样使整体符合C类安全要求。

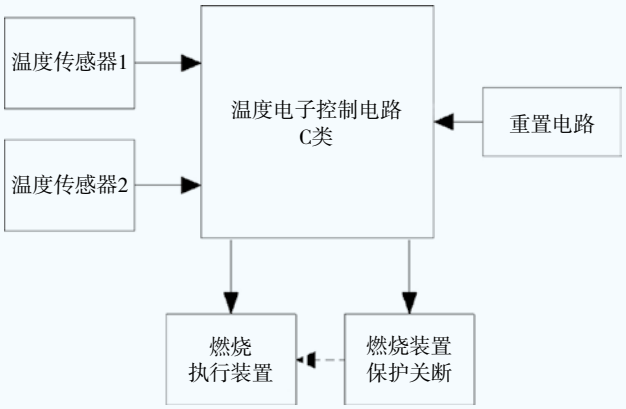


图5 C类温度控制器与电子温度传感器的组合

### 3.4 燃烧产物排放控制功能

燃烧产物排放控制功能通常理解为防止缺氧或是不完全燃烧功能，用于预防在使用环境中毒及窒息的风险，该功能由一个传感器和一个控制器组成。在安装燃具的地方，当燃烧产物溢出进入到环境时，传感元件检测到燃烧产物溢出超过不可接受的某个物理值，燃烧产物排放控制功能应起保护作用。

燃烧产物排放控制功能可以分属于A类、B类或C类安全，这与燃烧结构及燃烧控制等安全相关系统有关。实例如图6、7、8，从中可以看到分类的区别，总的原则是根据该功能失效产生的后果来评估。

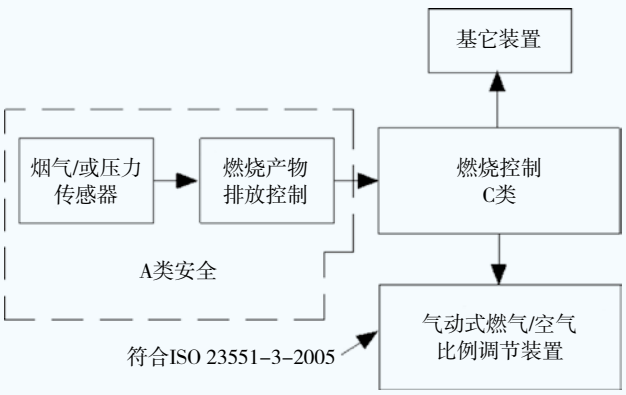


图6 燃烧产物排放—A类安全

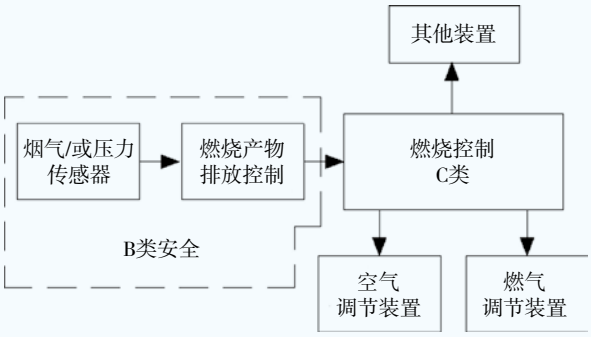


图7 燃烧产物排放—B类安全

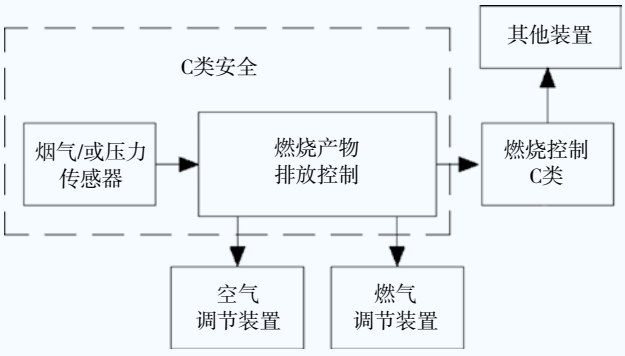


图8 燃烧产物排放—C类安全

### 3.5 系统重置功能

重置功能是指燃气器具在安全锁定状态下重启，要求不能由自动装置产生重启，必须通过手动动作来实现。

燃气具重置功能属于B类安全。重启故障导致的结果可能是：

——在锁定状态下自动重启。

——在锁定状态下可以频繁重启。

——重启元件失效，导致不能进入故障锁定状态。

以上结果，不会直接导致器具产生危险的状况，但存在导致危险状况的风险，如表2。

表2 故障锁定下的重启风险

| 故障锁定 | 非正常重启导致的风险 |
|---|---|
| 过热温控器断开 | 过热保护失效，热聚集或火焰溢出，产生火灾 |
| 连续点火失败 | 爆燃或燃气泄漏。 |
| 风压开关保护 | 有毒或超标烟气排放，或排放不畅 |
| 第一内部故障 | 出现第二内部故障时，燃气切断功能失效 |

所以重置功能的设计应能预防非正常重启导致的风险。重置功能的实现相对简单，可以通过一个开关，器具上的控制面板或遥控器来实现，在电路上除了要满足单个故障的条件下重置功能不失控外，还需要补充一些措施，这些措施要求是整体安全的一部分，如：

——利用可移动装置进行重置时，要求至少由两个手动动作激活重置装置；

——在重置前、后和过程期间的状态和相关信息应是可见的；

——在15min时间内的重置动作最多5次，进一步的重置应被拒绝。

## 4 结束语

本文分析了燃气具功能安全的特点、失效的后果及影响，对于本行业的专业人员在控制系统的安全设计上具有一定的参考意义；只有充分理解了这些功能在安全上的要求，才能首先在具体的设计过程采取有效的措施确保器具的安全。随着燃气具的发展，一些新功能被增加与组合进来，只要按照以上的分析及评估方法，应能准确地做到对新的功能安全的分类。同时也能更好地去理解国内外的相关标准要求，提升燃气行业的安全设计水准。

**参考文献**

1 ICS 91.140 P 45 CJ/T 421–2013. 家用燃气燃烧气具电子控制器 [S].中国标准出版社，2013

2 ICS 25.040 GB/T20483.1 –2006. 电气/电子/可编程电子相关系统的功能安全 第1部分 一般要求[S].中国标准出版社，2007

3 ICS 23.060.40 BS EN 13611–2007. Safety and control devices for gas burners and gas burning appliances — General requirements[S]

4 ICS 91.140.40 BS EN 14459–2007. Control functions in electronic systems for gas burners and gas burning appliances —Methods for classification and assessment[S]