核电厂安全重要仪表和控制功能分类（GB/T 15474—2010）

1范围

本标准规定了核电厂安全重要仪表和控制功能及实施该功能的系统和设备的分类方法，并确定了各个类别在功能度、可靠性、性能、环境耐久性和抗震性能等方面的技术要求和质量保证要求。

本标准适用于新建核电厂所有安全重要仪表和控制系统(包括安全系统和安全有关仪控系统)的设计。

注：有参考电厂和已开展设计的新核电厂根据实际情况，可有条件地执行本标准。

2规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 12727核电厂安全系统电气设备质量鉴定(GB/T 12727-2002，IEC 60780：1998，MOD)

GB/T 13625核电厂安全系统电气设备抗震鉴定(GB 13625—1992，eqv IEC 60980；1988)

GB/T 13626单一故障准则应用于核电厂安全系统(GB/T 13626-2008，IEEE 379-2000，MOD)

GB/T 13630核电厂控制室的设计(GB/T 13630--1992，eqv IEC 60964)

EJ/T 1143核电厂控制室设计功能分析与分配(IEC 61839，MOD)

HAF 003核电厂质量保证安全规定

HAD 102/14核电厂安全有关仪表和控制系统

3术语和定义

下列术语和定义适用于本标准。

3.1

预计运行事件anticipated operational occurrences

在核电厂运行寿期内预计可能出现一次或数次的偏离正常运行的各种运行过程；由于设计中已采取相应措施，这类事件不致于引起安全重要物项的严重损坏，也不致导致事故工况。

3.2

设计基准事故design basis accident；DBA

核电厂按确定的设计准则在设计中采取了针对性措施的那些事故工况。

3.3

设计基准事件design basis event；DBE

为确定设备、系统和构筑物的性能要求，而在设计中采用的假想异常事件。

3.4

仪控功能I＆C function

对确定工艺过程实施的控制、操作和/或监视。

3.5

功能度functionality

规定将输入信息转变为输出信息的功能属性。

3.6

安全重要仪控系统l&C systems important for safety

其故障或误动作可能导致厂区人员或公众经受过量放射性照射的仪控系统，以及防止预计运行事件导致不可接受后果的那些仪控系统，包括安全系统和安全有关仪控系统。

3.7

安全系统safety systems

安全上重要的系统，用于保证反应堆安全停堆、从堆芯排出余热或限制预计运行事件和设计基准事故后果。

3.8

安全有关仪控系统safety related I&C systems

安全上重要但不属于安全系统的仪控系统。

3.9

假设始发事件postulated initiating events；PIE

设计期间确定的可能导致预计运行事件或事故工况的事件。

3.10

不可接受的后果unacceptable consequenees

一种运行状态或一个假设始发事件导致厂址周围环境放射性物质释放量超出规定限值的后果。

4分类原则和方法

核电厂纵深防御的基本原则要求设置多层次的仪表和控制功能，用于核电厂的安全运行、防止出现不安全的工况或缓解不安全工况的后果。

IAEA核电厂安全设计标准要求所有仪表和控制系统、设备，包括计算机软件应依据其实施功能的安全重要性进行分类，并对不同类别的功能、系统和设备确立它们的技术要求和质量要求，使得其设计、建造和运行的质量和可靠性与它们的类别相符。

实施不同程度的安全重要功能的仪表和控制系统，其每项功能的安全重要性是依据其达到并保持核电厂的安全状态所起的作用、当要求实施功能时其故障的潜在后果和产生这些后果的概率的综合分析来确定。因此，在仪表和控制功能分类之前应当完成核电厂的初步安全分析(包括功能度、性能和可靠性)。

核安全导则HAD 102/14已依据功能的安全重要性将核电厂安全重要仪表和控制系统分为“安全系统”和“安全有关系统”。本标准将核电厂安全重要仪表和控制功能分成A类、B类和c类三类，属于安全系统范围内的功能属于A类或B类，安全有关系统范围内的功能属于B类或c类。核电厂安全重

要仪表和控制典型功能与系统参见附录c。

5功能类别说明

5.1 A类

A类功能，是指对于达到或维持核电厂安全以防止DBE导致不可接受的后果起主要作用的功能。

当瞬态初始阶段不能采取其他替代动作时，即使隐患能够被探测，这个作用也是必需的。这些功能使瞬态过渡到受控的稳定状态，使得反应堆处于次临界状态，热量排出得以保证并且使放射性物质释放受到限制。如果为达到受控状态提供了特定手动操作，那么需要考虑下列因素，诸如冗余的、经确认的信息源的可用性、足够的时间供操纵员对替代信息进行评估，以及是否仅仅手动操作就能够减轻事故后果以维持电厂安全等。

A类功能还包括其故障如果没有其他A类功能缓解可能直接导致事故工况的那些功能。由于A类功能要求高可靠性，应限制其功能度和复杂程度。

5.2 B类

B类功能，是指对于达到或维持核电厂安全起补充A类功能的作用，尤其是在达到受控状态后运行所需要的功能，以防止DBE导致不可接受后果或者缓解DBE的后果。B类功能的实施可以避免启动A类功能。B类功能在减轻DBE的后果上可以补充或改善A类功能的执行，这样电厂或设备损坏或者放射性释放可以避免或者减至最少。

B类也包括其故障可能引起DBE或者恶化DBE的那些功能。由于A类功能可以最终防止或减轻DBE的后果，因此B类功能的安全要求不必达到A类功能的高度。如果需要，允许B类功能在对一个需求动作的探测方法上或其后续动作上的功能度高于A类功能。

5.3 C类

C类功能，是指对于达到或维持核电厂安全起辅助或间接作用的功能，包括那些有一定安全重要性但不属于A类或B类的功能。C类功能可以是应对整个DBA的一部分(但不直接参与缓解事故的后果)，或者是超设计基准事故所必需的功能。

5.4分类准则

下列准则用于安全重要仪表和控制功能类别的划分。如果某一系统实施多个功能，其功能类别应取其最重要功能的相应类别。确定的功能类别可以结合6.2给出的原则用概率论法进行调整。

5.4.1 A类

满足下列任何一条准则的安全重要仪控功能应划分为A类：

a) 为达到受控状态、防止DBE导致不可接受后果或缓解其后果所要求的功能；

b)没有设置其他A类缓解功能，其失效或误动作会导致不可接受后果的功能；

c)为达到受控状态所必需的规定手动操作提供信息和控制能力所要求的功能。

5.4.2 B类

满足下列任何一条准则且没有划为A类的安全重要仪控功能应划分为B类：

a)达到DBE受控状态之后所要求的功能，以防止DBE导致不可接受后果或者缓解其后果；

b)为达到受控状态后所必需的规定手动操作提供信息或控制能力所要求的功能，以防止DBE导致不可接受后果或者缓解其后果；

c)在正常运行期间其失效需要启动A类功能以防止事故出现的功能；

d)为显著降低安全分析中确定的DBE发生频度所要求的功能；

e)将主要工艺变量维持在安全分析假定的限值内的电厂过程控制功能，其失效可能直接导致A类功能运行。

注：根据目前国际上核电厂设计情况，部分此类功能可划分为C类。

5.4.3 C类

满足下列任何一条准则且没有划为A或B类的安全重要仪控功能应划分为c类：

a)将主要工艺变量维持在安全分析假定的限值内的电厂过程控制功能，其失效不会直接导致A类功能运行；

b)在核电厂设计基准范围内，防止或减轻放射性少量释放及燃料性能轻微劣化的功能；

c)为控制室操纵员连续监视执行A类或B类功能的系统可用性提供信息的功能；

d) 为达到概率安全目标(包括降低DBE预期频率)所必需的功能；

e) 安全分析中要求减少A类功能需求的功能；

f) 为保证实施A类和B类功能(尤其是其失效引起PIE的那些功能)的系统的可靠性进行试验并记录这些系统状态(适合运行、正在运行、失效或不可运行)所必需的功能；

g)核电厂发生设计基准内部灾害(例如，火灾、水淹)后进行监视并采取缓解动作的功能；

h)伴随或导致核电厂放射性释放或辐照危险的事件期间或之后，警告现场人员或者确保人员安全的功能；

i) 自然灾害(例如地震、飓风)后监视并采取缓解动作的功能；

j) 为超设计基准事故情况下达到并维持安全状态的事故管理决策提供协助的功能；

k)减轻严重事故后果的功能；

1)提供核电厂出入控制的功能。

6分类程序

图1表示核电厂安全重要仪控系统功能分类的方法和程序。

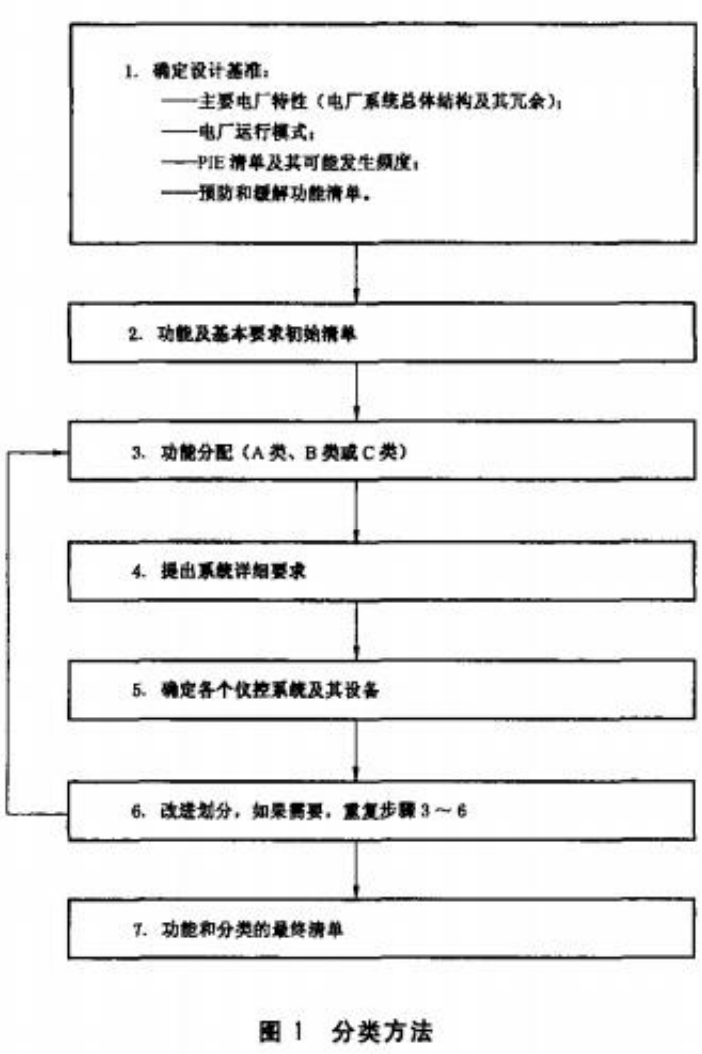

图 1　分类方法

6.1确定设计基准

功能分类过程首先要确定核电厂类型(例如压水堆核电厂或沸水堆核电厂)、与仪表和控制相关的PIE以及机械和电气系统和设备的冗余方面的主要设计准则。其次是确定每个PIE的预防和缓解功能及其支持功能。

评估PIE频度和后果从而确定与电厂设计基准相关的DBE。鉴于运行状态和事故条件的范围和规定的剂量限值将影响核电厂的设计，应研究将各个安全原则集成整体安全原则以确保电厂安全运行。

这些原则可在确定DBE和将辐照限制在允许限值的实体屏障的设计中应用。

6.2功能的确定和分类

核电厂初步设计阶段应确定安全有关功能，并根据GB/T 13630和EJ/T 1143将其分配给自动控制或者操纵员手动控制。功能确定之后应该根据第5章的准则划分每个功能的类别。

功能安全重要性的分类方法应基于确定论的安全分析，并结合概率论分析和工程判断，分类宜考虑下列因素：

a)要实施的安全功能；

b) 在预防或缓解假设始发事件中起的作用；

c)在所有运行模式期间(例如，启动、正常运行、换料等)起的作用；

d)在诸如自然事件(例如，地震、洪水、飓风、闪电)和内部灾害(例如。火灾、内部水淹、飞射物、邻接机组的放射性释放或者其他电厂或工厂的化学物质释放)这样的PIE之后，所起的作用；

e)失效的后果；

f)误动作的影响；

g)需要其实施安全重要功能的概率；

h)在DBE期间或之后要求其运行的时间；

i)维护、修理和试验方案。

初步设计阶段不太可能确定所有功能的细节，因此不能完全确立核电厂的特性。功能确定和分类应在整个设计阶段持续反复地进行。功能分类初次划分不明确的地方，分类中应增加解释性注解。

为了更详细地确定功能的冗余度、多样性及其他技术要求，完成安全分析和操作规程以后应改进并修订分类表，形成最终清单。这个清单应进行存档，以备电厂/仪控设计人员在核电厂寿期内使用。

7各类别的技术要求

7.1一般要求

本章给出A类、B类和C类功能的技术要求和质量要求。这些要求适用于仪控系统寿期内的技术规格书编写、设计、确认、鉴定、制造、安装、运行和维护。技术要求和质量要求由4部分组成：

a)与功能特性相关的要求，包括技术规格书的编写，功能度、性能和可靠性的确定。

b)与设计特性相关的仪控系统设计要求，例如冗余、多样性、可试验性和隔离。这些特性主要决定了相关功能的可靠性。这些要求也包括人机接口(HMD要求。

c) 与抗震和环境耐久性以及电磁兼容性相关的设备特性要求。

d)与功能、系统和设备的质量保证、验证和维护相关的要求。

多数情况下，这些要求已在相应标准和规范内作了详细规定(不同类别功能的适用标准参见附录A)，本标准不再重复这些标准和规范的详细要求。7.2～7.5给出一些其他要求。

应尽量采用有可靠运行经历(在核或其他工业条件下使用过并有文件证明)的设备。

7.2与功能有关的要求

7.2.1基本要求

保障功能度的基本要求已有一套清晰、完整、明确的功能要求和设计技术规范，在设计、制造、安装和运行期间应根据这些基本要求检查这些功能，并作为在役期间变更的参考文件。

A类、B类、c类任一功能所要求的可靠性应在技术规格书中规定。可靠性分析既可以采用定量的概率评价法，也可以通过定性的工程评价法。应通过适当的分析确定A类、B类或c类功能的性能要求，且在技术规格书内规定。这些分析应按照一组已批准的程序以模块化的方式进行，并形成文件。

尽管不同类别功能的可靠性要求可能相同，但三类功能达到规定可靠性的质保等级却不一样，其中A类为最高。

不同类功能之间应有良好的隔离。

7.2.2特殊要求

7.2.2.1 A类

A类功能的设计应按照适用的法规、导则和标准的要求以确保与A类功能相适应的功能度。设计的目的还在于通过简单的维护使确定的功能度容易得到验证和确认。为此，应力求避免A类系统实施较低类别功能(例如，特殊显示计算和通信协议转换不宜由安全系统软件完成)。

A类仪控功能的可靠性要求应按照7.2.1确定。A类仪控功能的可靠性要求取决于不可接受后果的最低风险度，据此再确定仪控功能应具有的可靠性。

7.2.2.2 B类

B类功能的设计也应遵守适用的法规、导则和标准的要求，或者使用有可靠运行经历(在类似情况下使用过并有文件证明)的系统和设备。

7.2.2.3 C类

C类功能的设计应通过检查或试验，以验证系统和设备在规定运行条件的全范围内(包括需要实施功能的最严酷的运行条件下)能提供规定的功能。

7.3与仪控系统有关的要求

7.3.1基本要求

系统设计应确保功能达到确定的可靠性。保证高可靠性的基本要求涉及恰当的冗余、多样性、可达性、实体分隔和电气隔离，以及有效的人机接口(HMI)。对于所有系统，设计和设计变更期间应考虑故障检测和维修措施。

可靠性和可用性评估应考虑修理周期、试验和维护周期，以及能自检出的或不能自检出的故障的可能。可靠性分析中关于维护、试验和维修周期作出的假设应在运行期间进行验证，如果证实有差异应纠正。

设计过程应包括对人因和HMI的特殊要求。这些要求在设计初期实施的人因工程大纲中给出。

系统设计应允许运行期间在线和/或定期试验，以证明系统性能得到维持。为确保安全重要仪控系统长期可靠性的定期试验和维护活动要求在7.5做了规定。

应尽可能在与主控制室实体分隔和电气隔离的辅助控制点设置足够数量的信息和控制设备，这样当主控制室丧失实施这些功能的能力时，可以使反应堆置于并保持在安全停堆状态，并监视电厂重要变量。

7.3.2特殊要求

7.3.2.1 A类

执行A类功能的仪控系统应遵从单一故障准则(详见GB/T 13626)，系统应设置冗余。冗余序列之间的隔离应使得任一内部危害事件不会使系统的冗余部分丧失功能。单一故障不应导致预定安全功能失效，即使在预防性维修、定期试验、检查或更换期间。

在A类功能必须由操纵员执行的情况下，应设置有关监测和控制系统，这些系统应与其他监测和控制系统隔离，且使操纵员有适度的反应时间。

应按照技术规格书评估和比较执行A类功能的仪控系统的可靠性。如果存在差异应及时解决。

可靠性评估应考虑共因故障的影响，包括硬件失效、软件失效，运行、维修期间的人为错误，以及纠正和更换活动。评估这些影响所使用的技术从纯粹定性工程评估至详细的定量分析，后者可能本身也取决于定性评估。所选取分析技术的类型应与可靠性要求一致，可靠性要求越高，技术要求越严格。

当考虑共因故障的影响后表明冗余系统不能达到可靠性要求时，应采用具有多样性的独立系统。

涉及到的功能可能需要两个或多个子系统，且彼此独立。

试验可能要求抑制输出信号，或者提供旁通设施。如果引入旁通设施应评估其完整性，以证明使用旁通设施不会防碍系统完成其规定安全功能。例如，应采取限制措施，使得任何时刻旁通只能作用到冗余序列的一个序列。

对于一些功能的实现，需要提供额外的冗余为电厂运行期间的常规检查做准备。这非常有必要，例如当一个能动通道不能在功率运行下进行试验，而为了保证必需的功能可靠性必须在电厂运行期间进行试验时。在这种情况下不必对整个系统引入额外的冗余。

动力供应应设有后备动力源。

应对A类系统进行规范的系统故障分析，例如故障模式和影响分析(FMEA)，以确定由设备故障引起的系统易损性，并评估设计方案是否能很好地发现这些故障或减轻其后果。

如果系统具有内置式自检特性(作为功能可靠性分析的一部分)，故障分析应评估这些装置以确定自检范围。如果故障分析表明系统自检装置不能检测某些故障并反馈给操纵员，那么应该进行验证试验来检测这些故障。应根据未发现故障的可能发生频率和功能可靠性要求确定验证试验的时间间隔。

不能获得可靠性数据时，应通过与类似系统比较选取试验时间间隔。功能试验的时间间隔应根据积累的经验重新评估。

7.3.2.2 B类

应按照技术规格书评估和比较执行B类功能的仪控系统的可靠性。B类功能应通过隔离和冗余的方法实现，否则应提供相应的证明。例如，证明系统不通过冗余和隔离达到可靠性目标的能力、功能失效后果的可接受性，或者功能失效时提供替代响应的可用时间。

动力供应应设有后备动力源。

使用的部件应有高质量和高可靠性，且设有确保故障能够快速检测并修理的手段。

对需要在主控室提供信息和控制能力，以便允许实施为减轻DBE后果所必需的手动操作的系统，其功能设计的基本目标是对所有DBE为操纵员提供有关电厂设备和系统状态的正确、完整和及时的信息，并尽量缩小操纵员监视和控制电厂所要求的活动范围。

在线和/或定期性能试验应包括各子系统的功能能力确认，特别是冗余序列的单独试验。

7.3.2.3 C类

除了为达到特定的功能可靠性可能要求之外，实施c类功能的系统一般不需要冗余设置或隔离。

但可能需要承受内部和外部危害。

根据情况，动力供应可能需要后备动力源。

为达到特定可靠性要求冗余设置的c类系统，其冗余宜按照B类功能的要求设置。

冗余设置的c类系统，各个冗余序列或子系统应单独进行定期功能试验，在线试验是满足此要求的一个方法。

7.4与设备有关的要求

7.4.1基本要求

在PIE期间或之后设备可能要承受事故环境条件，为防止其故障应采取必要的措施。可以通过设备鉴定实现。设备鉴定可以通过一种或几种不同方法的组合实现，例如，试验法、分析法或两者结合的方法，或者从运行经验获得的数据。

7.4.2特殊要求

7.4.2.1 A类

为确保A类设备在所有预计运行工况下持续运行，应进行设备鉴定。设备鉴定应遵守GB/T 12727和GB/T 13625的规定。试验结果应记录并在核电厂寿期内保存。鉴定试验期间发生的任何故障都应查明，故障原因和纠正措施应形成文件。

7.4.2.2 B类

B类设备应按A类设备的要求进行鉴定。

7.4.2.3 C类

根据执行的功能，c类设备可能需要进行鉴定。应确定设备运行过程中预期最恶劣的环境条件，并在技术规格书中作出规定，应依据技术规格书系统地检查设备的设计。

对一个新设备或者商用设备(通常不进行抗震和极端环境条件设计)，应制定一组规则来指导设备设计，或者评估既定设计。这些规则应根据从A类设备的特殊设计要求中获得的经验制定。

除非设备有特殊要求(例如地震或防火要求，或者防止c类设备内过电压或电噪声影响A类或B类功能)，其他情况下c类设备一般可以遵从常规商业设计标准。异常环境条件下的运行要求应有文件证明。

7.5对质量方面的要求

7.5.1基本要求

核电厂安全重要仪表和控制系统、设备在设计、制造、安装、调试和运行期间应遵循有关质量保证(QA)的一些基本要求，以保证系统和设备的合格性能。

QA的目的是配置管理、变更控制和可追溯性。设计应形成足够详细的文件，为核电厂的建造、安装、调试和运行每个阶段进行的验证提供支持。为了后续的设计修改，文件应归档。

对于新设计或改进的核电厂，还应依据新颖性或复杂程度制定相应的特定QA要求和要进行的试验。这些活动应根据功能对安全的重要性形成相应的文件。

QA计划应依据相应的法规或标准制定，这个QA计划应给出性能规格要求和被确定及验证的试验项目。

在制造、组装和现场安装期间都应依据QA大纲对设备、模块、子系统和系统进行性能试验，以表明它们符合功能要求。

应按照制造质量计划要求测试部件、模块和子系统，以确保其功能符合技术规范的要求。现场已安装在机械设备上的仪控系统，应在电厂运行前与机械设备一起进行功能试验。

各类功能的仪控系统，其现场试验的科目尽管相同，但质量控制和要求遵守的文件随着不同类别有所区别，详见7.5.2。

运行期间应进行试验，以证明安全重要仪控系统的硬件设备没有因为故障而劣化。仪控系统应设计成允许足够的试验并可查明设备内的故障。应根据变更控制程序纠正识别的缺陷。应保留这些纠正的记录。对冗余设置的系统应分别核查每个冗余通道的功能度。所选择的试验间隔时间应使得评定的故障率或要求运行时故障的概率满足可靠性分析的要求。

当使用计算机设备时，应执行与功能类别相应的软件生存周期的质量大纲。

7.5.2特殊要求

7.5.2.1 A类

QA要求应遵守HAF 003。形成的文件应能记录各物项的设计、制造和运行方面的历史。这应包括在设计范围内所有设备(包括模块)。配置上必须控制到能追踪的最小元件。批号、材料等的可追溯性应扩大到整个系统的功能模块。

QA文件必须能使审查人员从一个硬件或软件追溯到对其规定要求的技术规格书，也能根据技术规格书的任一要求查到执行该要求的部件。

应进行型式试验，以证明在预计运行环境条件下，核电厂内安装的同类设备能实施设计要求的功能。

部件、模块、子系统乃至整个系统应进行功能试验。试验必须由核电厂业主/采购方或其代表见证。

可以在制造厂或现场进行功能试验。制造厂或现场进行的试验应相互配合以确保试验覆盖了完整的范围。不能用试验提供证明能完成所有规定的功能时，应提供专项证明。

现场试验应尽可能测试已安装设备和系统的所有规定安全功能能达到要求的性能。这些试验应考

虑运行参数的变化。这称为现场验收试验(SAT)，验收试验应由核电厂业主/采购方或其代表见证。

在线或定期试验应证明执行所有要求安全功能的能力没有降低。试验间隔时间应根据自检水平并考虑到仪控设备预期和监测的故障率选定，使得安全重要仪控系统满足可靠性指标要求。

7.5.2.2 B类

OA要求应遵守HAF 003。QA文件应包括各物项的设计、制造和运行方面的历史文件。尽管OA大纲宜一致，但用于B类功能、系统或设备的QA的详细程度可能低于A类。

型式试验应在同类设备上进行，以便使安装在核电厂的设备可由分析表明设备的差异不会导致试验结果无效。

运行之前应完成功能试验，以证明核电厂内安装的使用类似结构设备的系统能够完成规定的功能。

所有这些试验或部分试验可在现场进行。

SAT试验应尽可能证明，已安装的设备应均能完成所有规定的安全功能。控制设备试验应证明对瞬态和要求变化的正确响应能力。显示和报警设备的试验应包括相应输入信号的注入试验，以证明其良好性能。

7.5.2.3 C类

C类系统和设备可接受商业QA水平。

如果制造商的试验足以证明能够达到规定性能，许可证持有人即可接受。这些试验应对同类设备进行。必要时宜进行特定类型的试验和功能试验，但一般情况下不要求。

可以进行SAT试验来证明系统达到了规定的安全有关功能和性能。

对那些不连续运行的功能，定期性能试验可以限制在换料大修阶段，或者类似停堆期间进行。

原文地址：http://www.china-nengyuan.com/tech/79802.html