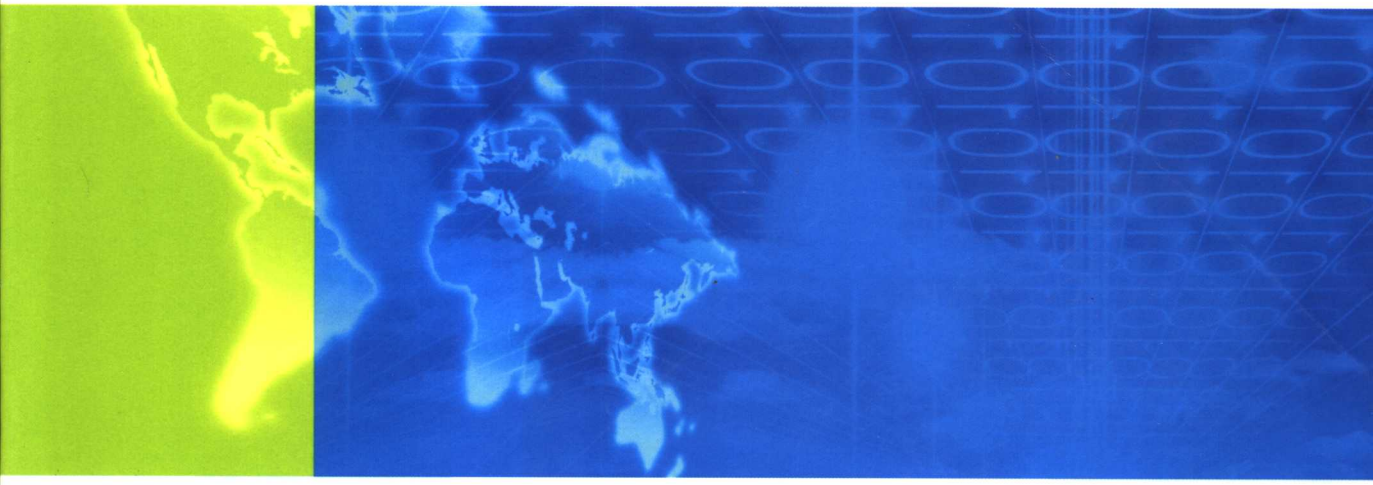
北方联合电力
North United Power

火力发电厂热工自动化系统
安全技术指南



北方联合电力有限责任公司　编

中国电力出版社
www.cepp.com.cn

火力发电厂热工自动化系统安全技术指南

北方联合电力有限责任公司　编

中国电力出版社
www.cepp.com.cn

内 容 提 要

本书规定了火力发电厂热工自动化系统在技术方面提高其安全性的指导性要求。包括提高输入/输出信号可信度措施，分散控制系统设计和配置，汽包水位测量、控制和保护系统的配置和安装，热工自动化系统事故预防和对策等内容。

本书适用于装设单机容量125MW及以上机组的新建和改建热工自动化系统，装设单机容量小于125MW机组的火电厂也可作参考。

图书在版编目（CIP）数据

火力发电厂热工自动化系统安全技术指南/北方联合电力有限责任公司编. —北京：中国电力出版社，2007.4

ISBN 978-7-5083-5248-0

Ⅰ.火… Ⅱ.北… Ⅲ.火电厂-热力系统:自动化系统-安全技术-指南 Ⅳ.TM621.4-62

中国版本图书馆CIP数据核字（2007）第025668号

中国电力出版社出版、发行

（北京三里河路6号 100044 http://www.cepp.com.cn）

航远印刷有限公司印刷

各地新华书店经售

*

2007年4月第一版 2007年4月北京第一次印刷

787毫米×1092毫米 16开本 3.75印张 64千字

印数0001—3000册 定价**10.00**元

前　言

根据《中共中央关于国有企业改革和发展若干重大问题的决定》中关于“坚持预防为主，落实安全措施，确保安全生产”的要求，原国家电力公司于2000年9月28日以国电发［2000］589号文颁发了《防止电力生产重大事故的二十五项重点要求》，对防止电力生产重大事故、保证电厂安全经济运行发挥了重要作用。华能发电集团公司根据最新技术的发展和经验也制定了《防止电力生产重大事故的重点要求》。

为了配合热工自动化专业的各项反事故措施的顺利实施，提高热工自动化系统的可靠性，北方联合电力公司根据发电企业自身特点，并在充分分析了国内多个事故案例的基础上，组织编写了《火力发电厂热工自动化安全技术指南》，全书共有六部分并编写了编制说明。本书的特点是按照故障类型进行分类分析，从热工自动化专业最关键的几部分内容入手，结合原国家电力公司《防止电力生产重大事故的二十五项重点要求》、华能发电集团公司《防止电力生产重大事故的重点要求》的内容，提出具有普遍意义的对策和日常维护中的有效方法，突出了实用性和可操作性，对提高热工自动化系统安全性有普遍的指导意义。北方联合电力公司所属发电企业应按照《火力发电厂热工自动化安全技术指南》要求，认真指导本企业的热工自动化工作，其他单位可参考。

鉴于编者水平所限，书中难免有疏漏、不妥之处，请读者指正。

北方联合电力公司　总工程师

李国宝

编　委　会

目　次

1 适 用 范 围

本指南规定了火力发电厂热工自动化系统在技术方面提高其安全性的指导性要求。

本指南适用于装设单机容量125MW及以上机组的新建和改建热工自动化系统。对于已建火电厂，应根据本指南的精神和本厂具体情况逐步进行改造，以消除隐患，在未改造前应采取必要的对策。

对于装设单机容量小于125MW机组的火电厂也应参照执行。

2 引 用 标 准

为防止火电厂发生重大生产事故，火电厂热工自动化系统设计、安装、调试和运行应认真贯彻执行下列有关技术规程和行政文件。

GB/T 17626.1—1998	电磁兼容　试验和测量技术
DL/T 655—2006	火力发电厂锅炉炉膛安全监控系统验收测试规程
DL/T 656—2006	火力发电厂汽轮机控制系统验收测试规程
DL/T 657—2006	火力发电厂模拟量控制系统验收测试规程
DL/T 658—2006	火力发电厂顺序控制系统验收测试规程
DL/T 659—2006	火力发电厂分散控制系统验收测试规程
DL/T 608—1996	200MW 级汽轮机运行导则
DL/T 609—1996	300MW 级汽轮机运行导则
DL/T 610—1996	200MW 级锅炉运行导则
DL/T 611—1996	300MW 级锅炉运行导则
DL/T 641—2005	电站阀门电动执行机构
DL/T 838—2003	发电企业设备检修导则
DL/T 774—2004	火力发电厂热工自动化系统检修运行维护规程
DL/T 924—2005	火力发电厂厂级监控信息系统技术条件
DL/T 1012—2006	火力发电厂汽轮机监视和控制系统验收测试规程
DL 5000—2000	火力发电厂设计技术规程
DL/T 5190.5—2004	电力建设施工及验收技术规范　第5部分：热工自动化
电规发［1996］214号	单元机组分散控制系统设计若干技术问题规定
国电安运［1998］483号	火力发电厂热工仪表及控制装置技术监督规定
国家电网生［2003］409号	火力发电厂安全性评价

3 提高输入/输出信号可信度措施

3.1 一般要求

3.1.1 取样装置和管路应满足下列要求：

1）含有粉尘或悬浮物介质（炉膛压力、一次风压、开式循环水压力等）的取样装置和管路应有防堵和吹扫（洗）措施。

2）敷设在气温较低处的取样装置和管路应有防冻或防介质过稠导致传压迟缓的措施。重要保护信号的管路宜采用较为可靠的电伴热装置。

测量油压的取样管路（包括从取样点到表计），以及用于保护的气动阀门（如给水泵气动再循环阀）的控制气源管的通径均应不小于10mm。

3）取样管路在满足被测介质冷却、压力抖动不过大的前提下，应尽可能短，以减少测量管路过长带来的积水、积气、迟延甚至堵塞等各种问题。

4）敷设测量管路时，不应与其他设备相摩擦；穿越结构物时应加装保护套，以免振动摩擦而导致取样管爆裂。

5）炉膛压力取样点应远离人孔、看火孔和吹灰器，以免造成信号误发，其取样短管内径不应小于50mm。

6）测量蒸汽或液体介质的压力和差压的变送器以及开关量仪表应放置在环境条件较好的低于测点的地方，当测量压力时，还应考虑高差对示值的影响和修正；测量真空或风压的变送器应放置在高于测点的地方。

管路敷设坡度应满足《电力建设施工及验收技术规范 第5部分：热工自动化》的要求，不允许出现可能引起积气（测量蒸汽或液体介质时）或积水（测量气体介质时）的弯曲，并为此而装设排气、排水装置。

3.1.2 一次测量元件和线路应满足下列要求：

1）一次测量元件应在工艺设备上安装牢固，并有防止振动和含粉尘被测介质冲刷、磨损而造成损坏的措施。

2）一次元件引线应有防止振动摩擦而断线或过热而破坏绝缘的措施；接线应牢固，防止因振动而松脱开路。

3.1.3 汽包水位、炉膛负压、一次风压、润滑油压、真空、转速等重要保护信号应采取三取中（模拟量信号）或三取二（开关量信号）冗余配置。对于因测点原因无法冗余的重要保护信号，应采用其他相关信号进行逻辑判断以提高该保护信号的可信度。

3.1.4 冗余信号的取样点、取样装置（测量喷嘴除外）、取样阀门和管路以及一次元件和线缆应互相独立分开设置。

3.1.5 制氢站内的接线盒、电气仪表应采用符合相应等级要求的防爆设备。

3.2 开关量信号

3.2.1 除下列情况外，进入DCS的用于机组和主要辅机跳闸保护的输入信号不宜取自没有被测参数监视的开关量仪表：

1）响应速度不能满足保护要求；

2）输入信号必须直接以开关量信号进入继电器逻辑回路。

对于采用开关量仪表输入信号直接接入机组继电器跳闸回路时，应三重冗余配置且应定期进行动态试验；不允许使用死区和磁滞区大、设定装置不可靠的开关量仪表，以及普通的电接点压力表作为保护信号仪表。

3.2.2 用于机组保护的发电机和电动机的断合状态信号应直接取自断路器的辅助触点。

3.2.3 阀门行程开关是保护系统中可靠性较差的发讯装置，在有条件时，应采用其他确能反映阀门状态的工艺参数代替或辅助判断，以最大限度防止保护拒动或误动。

3.2.4 开关量信号的查询电压应有电源监视，当电源消失或电压降至不允许值时，应立即发出报警，当采用触点断开动作的信号时还应将相应的触发保护的开关量信号闭锁。

3.2.5 控制辅机电动机的DCS输出指令应采用短脉冲，并在每个电动机强电控制回路中设置自保持。

给粉机或给煤机（直吹式制粉系统）以及重要辅机油泵等的自保持回路应防止厂用电切换时误跳闸；对于前者，还应防止厂用电失去后恢复时间超过一定值时再重新启动，以免灭火后重启造成炉膛爆燃事故。

要仔细检查随工艺设备供应的电动机控制回路，并使其达到上述规定要求。

3.2.6 输出控制电磁阀的指令型式应根据下列情况确定：

1）汽机紧急跳闸电磁阀、抽汽止回阀（逆止阀）的电磁阀、汽机紧急疏水电磁阀以及锅炉燃油关断电磁阀等具有故障安全要求的电磁阀必须采用失电时使工艺系统处于安全状态的单线圈电磁阀，控制指令采用持续长信号（4.4.3条另有规定时除外）。

必须选择持续带电能可靠运行的单线圈电磁阀，不允许为改善电磁阀运行条件而随意改用双线圈电磁阀。

2）没有故障安全要求的电磁阀可采用双线圈电磁阀，此时，控制指令应采用短脉冲信号。

要仔细检查随工艺设备供应的电磁阀型式，并使其满足上述规定要求。

3.2.7 具有故障安全要求的气动阀必须按失气安全的原则设计。要仔细检查随工艺设备供应的气动阀型式，并使其满足这一规定要求。

3.3 模拟量信号

3.3.1 用于保护的温度等变化缓慢的模拟量输入信号除应设置量程超限方法对信号进行“质量”判别外，还应设置变化率超限等方法对信号进行“质量”判别。

3.3.2 DCS应设置执行机构控制信号和阀门位置反馈信号间差值过大的故障判别功能，并及时发出明显的报警。当差值过大时（由于超驰控制信号引起时除外），DCS应将控制回路切至手动，并发出报警。

3.3.3 新建大机组工程，重要变送器、执行器及开关柜宜采用具有故障诊断和分析功能的现场总线智能设备，借助设备管理系统及早发现故障。

3.3.4 当DCS模拟量控制系统的输出指令采用4～20mA连续信号时，与安全相关的重要执行机构应具有三断（断电、断气和断信号）保护功能。

3.3.5 热电偶冷端补偿器至少应在每个热电偶输入模件机架内配置一个，不应仅在一个机柜内公用一个补偿器。

3.3.6 为隔离或增加容量等需要而在DCS的I/O回路中加装隔离器时，应采取有效的防止积聚电荷而导致信号失真或漏电流而导致执行器位置漂移等的措施。

4 分散控制系统设计和配置

4.1 总体配置

4.1.1 DCS中的操作员站、控制器、实时数据服务器和通信网络必须采用可靠的冗余配置。

对于锅炉炉膛安全系统（FSS）、汽机数字电液控制系统（DEH）以及汽机紧急跳闸系统（ETS）宜优先采用具有较完善安全措施的控制器。

当DCS采用集中式实时数据服务器时，应采用提高冗余配置等增加系统可靠性的措施。

4.1.2 对于循环水泵、空冷系统的冷却水泵以及仪用空压机等重要公用系统（或扩大单元系统），应按单元或分组纳入单元机组DCS中，以免因公用DCS故障而导致全厂或两台机组同时停止运行。不宜分开的次要公用部分则可配置在公用DCS中。

4.1.3 对于供汽、供热的电厂，当供汽、供热中断会造成用户较大损失和支付较多赔款时，应按一台锅炉和一台汽机为单元配置一套DCS的配置方式将全厂锅炉和汽机分组置于两套及以上DCS中，而不应将其全部集中于一套DCS中。

4.1.4 电气自动同期系统（ASS）、自动电压调节系统（AVR）、厂用电快速切换装置以及电气继电保护装置不应纳入DCS。

当ETS采用独立于DCS的PLC组成时，应采用安全型PLC和安全系统配置，并满足4.2.7条、4.4.2条和4.4.5条的要求，当ETS纳入DCS时，应满足4.1.1条、4.2.7条、4.4.2条和4.4.5条的要求。

4.1.5 DCS与SIS（MIS）的接口必须按照《火力发电厂厂级监控信息系统技术条件》的要求，配置可靠的隔离措施，信号的传送应该是从DCS向SIS（MIS）单向的。严禁将DCS与SIS（MIS）以及上级公司的信息网络直接互联。

严禁将全厂煤、灰、水公用控制系统通过网络与DCS互联，并将公用系统信息通过单元机组DCS上传至SIS（MIS）。

严禁将工业电视系统接入DCS网络。

4.1.6 应选择对电源波动不敏感（－15%，＋20%）的操作员站，否则其供电设计应

满足 4.5.1 条和 4.5.4 条的要求。

4.1.7 当 DCS 只有单个时钟发生装置时，应有防止其发生故障而导致 DCS 失去时钟，进而造成操作员站和控制器站脱网事故的措施；当采用主、备时钟时应定期重启一次主、备时钟所在的工作站，以消除时钟累积误差。当 DCS 时钟通过 GPS 自动校准时，应有防止 GPS 故障导致 DCS 时钟混乱而故障的措施。

4.1.8 DCS 响应时间应尽可能短，任何时候任何指令从操作员站发出到 DCS 输出不应大于 1s；从操作员站发出指令到开始执行并返回显示器上反应的总时间不应大于 2s。

4.2 控制器配置

4.2.1 控制器宜按工艺系统功能区配置。重要的多台冗余或组合的辅机（辅助设备）应按下列原则配置，以确保一对控制器故障不会造成机组被迫停止运行：

1）送风机、引风机、一次风机、凝结水泵和循环水泵等两台冗余的重要辅机，以及 A、B 段厂用电应分别配置在不同的控制器中，但允许送风机和引风机等纵向组合在一个控制器中。

2）给水泵、磨煤机和油燃烧器等多台冗余或组合的重要设备应适当分组配置到几个控制器中。

4.2.2 为了减少一对控制器故障对模拟量控制系统失灵造成的影响，重要模拟量控制回路应适当分散配置，影响同一重要参数的控制回路应尽量配置在不同控制器中，例如，主汽一级和二级减温控制系统、再热汽摆动火嘴和喷水控制系统、送风和引风控制系统等不宜配置在同一对控制器中。

4.2.3 控制器的配置必须严格遵循机组重要保护和控制分开配置的独立性原则。

4.2.4 DEH 控制器应按故障安全原则配置，当该控制器失电或故障时应自动停止机组运行。FSS 和 ETS 控制器在满足 4.4.2 条要求的前提下，其跳闸输出可按带电动作的原则配置，否则也必须按故障安全原则配置。

DCS 控制器的组态应确保任何一对冗余控制器或其电源故障和故障后复位时，所有保护和控制信号的输出符合工艺处于安全状态的要求。

4.2.5 除 DEH 控制器外，当任何一对控制器故障时，为确保短时恢复期间机组在稳定负荷能安全运行，除应按照 4.4 条要求配置硬接线后备监控设备外，至少对下列重要安全参数，应在两对控制器中同时予以配置：

1）汽包水位（超临界压力机组除外）；

2）主蒸汽压力；

3）主蒸汽温度；

4）再热蒸汽温度；

5）炉膛压力。

4.2.6 控制器的对数除满足4.2.1～4.2.5条要求外，还应满足控制器在4.2.7条规定的处理周期下处理器的最大负荷率不大于60%的要求。

4.2.7 控制器的处理周期，对于一般模拟量控制回路应不大于250ms，对于一般开关量控制回路应不大于100ms。

DEH控制器的处理周期不应大于50ms，在条件允许的情况下应将处理周期减少到30ms，或另设特殊模件处理其中要求快速响应的转速控制回路。

ETS控制器的处理周期不应大于30ms。

4.2.8 控制器I/O信号的配置必须按下列故障分散原则设计：

1）冗余的I/O信号必须分别配置在不同的I/O模件上。

2）两台互为冗余辅机各自控制回路的I/O信号必须分别配置在不同的I/O模件上，多台组合辅机（如给粉机）各自的I/O信号也必须分组分散配置在几个I/O模件上，使一个I/O模件故障对机组安全稳定运行的影响尽可能小。

3）几个重要控制回路的I/O信号不应放置在同一个I/O模件上。

4.3 热工保护和报警

4.3.1 单元机组的锅炉、汽机和发电机之间应装设下列跳闸保护：

1）锅炉故障发出总燃料跳闸（MFT）停炉信号时，应立即停止汽轮机运行。

2）汽轮机故障停止运行和故障发电机解列时，在满足下列条件之一时，可以不联动停止锅炉运行，否则也应立即停止锅炉运行：

a）机组具有FCB功能。

b）解列前汽机负荷小于30%～40%（视旁路容量而定），且旁路系统可以快速开启，投入工作。

应采用汽机安全油压低（三取二）表征汽轮机故障停运信号作为触发MFT停炉的信号。

3）汽机故障发出ETS停机信号，应立即关闭汽机主汽门，并应按4.3.2条规定，通过逆功率信号解列发电机。

4）发电机内部故障解列时，应立即停止汽机的运行；发电机外部故障解列时，在满足下列条件之一时，可以不联动停止汽机的运行，否则也应立即停止汽机的运行：

a）机组具有 FCB 功能。

b）解列前汽机负荷小于 30%～40%（视旁路容量而定），且旁路系统可以快速开启，投入工作。

4.3.2 当汽机 ETS 发出跳机指令时，必须采用发电机逆功率信号作为最后判别主汽门确已关闭的依据去解列发电机。

解列发电机逻辑应按下列原则设计：

1）当发电机出现逆功率信号时，经一定延时后解列发电机。

2）当汽机安全油低（二取一或三取二）且发电机出现逆功率信号，不经延时立即解列发电机。

4.3.3 对于汽机振动保护常误动、可靠性差以致该保护不能投入的机组，允许汽机振动大跳机的逻辑修改为：一个轴承振动达到事故值，且相邻轴承任一振动达到报警值，经一定延时后应立即停机。逻辑修改后，当任一轴承振动达到事故值时，应有明显的声光报警，此时，运行人员应及时进行判别，除非明确断定是振动信号误发，否则运行人员应及时手动停机。

4.3.4 当 DCS 总电源消失时，必须直接通过 FSS 和 ETS 继电回路自动发出停炉和停机指令。

4.3.5 用于动作机组和主要辅机跳闸的输入信号必须直接通过相应保护控制器的输入模件接入。

4.3.6 为防止炉膛压力开关取样系统堵塞而导致保护拒动，除在 FSS 控制器中将三个炉膛压力开关信号，三取二发出 MFT 外，还应利用炉膛负压控制器中的 3 个炉膛压力变送器，转换成开关量信号，分别通过各自的 I/O 通道发送到 FSS 控制器中经三取二运算同时发出 MFT 信号。

4.3.7 为防止由于主汽门行程开关信号不可靠导致抽汽逆止门关闭保护拒动或误动，关闭抽汽逆止门条件，对于两侧主汽门时可采用 2×2 方式，对于单侧主汽门时宜以汽机安全油压低（三取二）代替主汽门行程开关信号。

4.3.8 机组必须设置能快速关闭的至除氧器抽汽截止门和抽汽机组的可调整抽汽截止门，以防止抽汽倒流引起超速。

4.3.9 DCS 控制器发出至 MFT、ETS 和发电机跳闸系统（GTS）的执行部分继电回路的机组跳闸指令，应采用三重或 2×2 冗余，通过各自的输出模件发出至继电回路，并按三取二或 2×2 逻辑启动跳闸继电器。

4.3.10 给水泵入口压力低解列给水泵的防止给水泵入口汽化的保护逻辑应为给水泵入

口和除氧器之间的压差小于设定值，并延时一定时间后解列给水泵。

压差值和延时设定值的大小应确保给水泵启动或突然增加给水的动态过程中不致造成保护误动，也不应造成给水泵入口汽化导致泵振动损坏。

4.3.11 四角喷燃锅炉的中速磨煤机跳闸条件应为：A（B/C/D/E）层相邻两角或三角火焰丧失，且相邻层火焰和该层点火能源都丧失。

4.3.12 高压加热器解列应列入机组辅机故障减负荷（RB）的条件。RB应确保不管机组脱硫系统投运与否均能使机组RB时不跳闸。

4.3.13 保护逻辑组态时，应精心配置逻辑页面和正确的保护执行时序。

要注意相关保护间的时间配合，防止由于取样管路、仪表和DCS处理周期引起的延迟以及延迟时间设置不当而导致两个保护动作时序不当。如由于发讯设备和取样管迟延不同，导致风机油压低一值启动备用油泵较慢，以致造成油压低二值动作使风机已经跳闸。

4.3.14 DCS的报警应分级，下列信号应列入一级报警信号：

1）保护动作信号；

2）主辅机事故跳闸信号；

3）保护参数偏差大二值和三值信号；

4）电源和气源丧失信号；

5）保护参数坏质量信号；

6）DCS重要故障信号。

一级报警信号应显示在大屏幕显示器上，或特别指定的一台显示器上，并配置不同的声响。

4.3.15 保护回路中不应设置供运行人员切、投保护的任何操作设备。保护切投应经一定审批后可由热工自动化专业责任人员通过工程师站（对DCS）或机柜内相应设施（对PLC）进行。

4.4 硬接线设计和后备监控设备

4.4.1 硬接线设计和后备监控设备的配置必须满足下列工况下机组的短时安全运行或安全停机：

1）当DCS总电源消失时，凭借后备监视和报警设备，通过硬接线回路，确保机组安全停止运行。

2）当DCS操作员站显示器出现“黑屏”或“死机”现象时，凭借后备监视和报警

设备判别控制器工作状况，当断定控制器工作不正常或无法判别其工作正常与否时，运行人员可以通过后备操作设备，凭借后备监视和报警设备，通过硬接线回路，确保机组安全停止运行。

3）当DCS操作员站显示器出现“黑屏”或“死机”现象时，凭借后备监视和报警设备明确断定涉及安全的主要控制器工作正常时，运行人员可借助后备监控设备能安全地维持机组在稳定负荷下短时运行，以提供迅速修复这类局部故障的机会，减少机组非计划停运所造成的损失。

4）当DCS的任何一对冗余的控制器（DEH控制器除外）故障时，通过该控制器中的重要安全信号在其他控制器中的备份配置（4.2.5条），以及必要的后备监控设备能安全地维持机组在稳定负荷下短时运行，以提供迅速修复这类局部故障的机会，减少机组非计划停运造成的损失。

4.4.2 锅炉总燃料跳闸（MFT）、汽机紧急跳闸系统（ETS）和发电机解列系统（GTS）的执行部分逻辑必须由独立于DCS的继电器逻辑回路组成。

该回路设计必须满足下列基本要求：

1）选用的继电器必须是经实践证明安全可靠的，条件具备时应选用经权威机构认证的安全继电器。

2）必须按故障安全的原则设计，当继电回路的电源消失时，自动停止机组运行（除4.4.3条规定外）。

3）DCS发来的机组保护解列指令信号必须是三重冗余或2×2冗余的，以便在该回路中进行三取二或两路并串联（2×2）判别后发出执行指令。

4.4.3 当MFT、ETS或GTS的执行部分分别采用两套完全独立的继电器逻辑回路，且分别直接由单元机组的两组蓄电池直流总电源柜供电时，主机组跳闸可按带电跳闸的原则设计。

4.4.4 除4.3.6条规定外，所有用于触发跳闸的输入信号不允许通过安全等级较低的其他控制器处理后再通过通信总线或I/O模件送至保护控制器，而必须直接通过输入模件送入相应保护控制器。但在响应时间满足要求的情况下，允许通过通信方式从FSS控制器将上述信号传送到其他控制器。

4.4.5 至少下列触发机组跳闸的信号，必须直接接入MFT、ETS和GTS的执行部分的继电器逻辑回路：

1）MFT：

- FSS发出的MFT指令。