ICS 29.020
K 09
备案号：44814-2014

DL

# 中华人民共和国电力行业标准

DL / T 1340 — 2014

# 火力发电厂分散控制系统故障应急处理导则

**Emergency handling guidance for distributed control system in fossil fuel power plant**

2014-03-18发布　　2014-08-01实施

国家能源局　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由电力行业热工自动化与信息标准化技术委员会技术归口。

本标准起草单位：中国大唐集团公司、国网浙江省电力公司电力科学研究院、国网河南省电力公司电力科学研究院、浙江大唐乌沙山发电有限责任公司、浙江省电力学会、浙江浙能乐清发电有限责任公司、大唐国际盘山发电有限责任公司、上海明华电力技术工程有限公司、内蒙古电力科学研究院、国网湖南省电力公司电力科学研究院、国网安徽省电力公司电力科学研究院、神华国华（北京）电力研究院有限公司、浙江省电力建设有限公司、江苏国信淮安燃气发电有限责任公司、浙江浙能中煤舟山煤电有限责任公司、大唐湘潭发电有限责任公司。

本标准主要起草人：孙长生、罗兴宇、崔猛、华国钧、朱北恒、段南、张启亚、沈丛奇、尹峰、张国斌、叶国满、朱晓星、陈胜利、岳建华、卢伟国、丁俊宏、张学军、吴侃侃、胡昊。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

# 引　言

本标准根据国家能源局《关于 2012 年第二批能源领域行业标准制 （修）订计划的通知》（国能科技〔2012〕326 号，电力行业部分能源 20120494 项）安排制订。

分散控制系统在运行中的故障时有发生，如电源失电、操作员站“黑屏”或“死机”、冗余控制器切换异常、通信中断及模件损坏等，如果处理不当会导致故障扩大，造成机组跳闸甚至主设备损坏事故。为建立分散控制系统故障应急处理和长效管理机制，确保故障发生时能够迅速、准确地组织故障处理，最大限度地降低故障造成的影响，在收集、总结各分散控制系统故障时的应急处理经验教训、深入研究分散控制系统故障应急处理方法和管理经验的基础上，制订了本标准。本标准规定了火力发电厂机组分散控制系统故障应急处理准备、现场应急处置原则和操作处理过程，以及应急处理预案的编制程序及格式，为火力发电厂进行分散控制系统故障应急处理，编制或完善适应本单位的《分散控制系统故障应急处理预案》提供统一的技术依据和指导。

各火力发电厂应依据本标准的编制格式和内容，结合本单位的生产规模和控制系统配置等特点，编制适合单元机组控制系统的故障应急处理预案，作为火力发电厂突发事件总体应急处理预案中的专项预案，并定期组织对运行、维护人员进行故障应急处理方法的培训和演练，提高控制系统故障时的应急处理能力，以保证机组的安全运行。

# 火力发电厂分散控制系统故障应急处理导则

## 1 范围

本标准规定了火力发电厂机组分散控制系统（DCS）故障应急处理准备、现场应急处置原则和操作处理过程，以及应急处理预案的编制程序及格式。

本标准适用于火力发电机组分散控制系统、数字电液控制系统（DEH）、汽轮机紧急跳闸系统（ETS）等设备故障时的应急处理和故障应急处理预案的编制指导。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 18218 重大危险源辨识

GB 50660 大中型火力发电厂设计规范

DL/T 261—2012 火力发电厂热工自动化系统可靠性评估技术导则

## 3 术语和定义

下列术语和定义适用于本标准。

3.1

**应急处理预案 emergency treatment pre-arranged planning**

针对潜在或可能发生的突发事件，为迅速、有序地开展应急行动而预先制订的应急处置措施。

3.2

**应急响应 emergency response**

分散控制系统发生故障后，工作人员按照工作程序，对故障做出判断并确定故障响应级别的过程。

3.3

**应急启动 emergency start**

按确定的故障应急响应级别启动故障应急处理程序，通知故障应急处置人员到位，开通通信网络，调配应急资源的过程。

3.4

**应急行动 emergency action**

在分散控制系统故障应急响应过程中，为消除和减少故障影响，防止故障范围扩大，最大限度地降低故障造成的危害而采取的处理措施或行动。

3.5

**应急恢复 emergency recovery**

分散控制系统故障应急行动结束后，为使生产尽快恢复到正常状态而采取的措施或行动，包括现场清理、人员撤离、善后处理、故障调查等。

3.6

**A 类控制系统 A class control system**

机组从启动、并网、正常运行至停运的整个过程中，涉及安全、经济、环保等且应连续投入运行的控制系统。

3.7

**B 类控制系统　B class control system**

机组在连续运行过程中，可根据控制对象要求，做间断式（间断时间不超过 12h）连续运行的控制系统。

3.8

**C 类控制系统　C class control system**

未列入 A、B 类的控制系统，当该系统故障时，通过手动能完成其相应的功能，不影响机组的安全运行。

3.9

**A 类输入/输出（I/O）模件　A class input/output（I/O）unit**

该类模件故障时，将对控制系统（以及所包含的重要设备）的安全运行构成严重威胁，可能导致控制系统控制对象失控、机组中断运行、环境保护监控功能失去或环境严重污染，影响机组运行的安全性和经济性。

3.10

**B 类输入/输出（I/O）模件　B class input/output（I/O）unit**

该类模件故障时，将导致控制系统部分功能失控，短时间内不会有直接影响，但处理不当会间接影响控制对象连续运行，导致控制对象出力下降、控制范围内主要辅助设备跳闸、控制范围内主要自动系统无法正常投自动、主要设备连锁无法投入或控制范围内的热工自动化设备失去主要监视信号。

3.11

**控制系统一级故障　first level fault of control system**

指故障发生后，将会直接导致系统不能完成规定功能，造成机组跳闸、系统重要设备不可控或损坏、环境保护监控功能失去或其他不可容忍的后果。

3.12

**控制系统二级故障　second level fault of control system**

指故障发生后，如不及时处理或处理不当，可能发展为一级故障。

3.13

**控制系统三级故障　third level fault of control system**

指故障发生后，对设备和系统完成规定功能有一定影响，虽暂时不影响机组继续运行，但有可能发展为二级故障。

3.14

**故障自动辨识报警　automatic fault identification & alarm**

根据信息自动识别判断出现故障的类型和可能的故障源，并发出报警信号。

3.15

**关联信号　relevance signal**

不同控制部件之间相互有联系的信号，包括硬接线信号、系统通信信号等。

3.16

**物理隔离　physical isolation**

指控制系统的网络不直接或间接地与其他设备、部件、公共网络相连接，目的是保护路由器、工作站、网络服务器等硬件实体和通信链路，免受自然灾害、人为破坏和搭线窃听攻击等带来的可能不良后果。

3.17

**主保护　main protection**

指锅炉总燃料跳闸（MFT）保护和汽轮机紧急跳闸保护。

## 4 总则

4.1 火力发电机组应从设计和基建开始，按附录 A 的规定，检查确认分散控制系统的可靠性。

4.2 为减少运行人员的故障判断时间，控制系统宜逐步配置一、二级故障自动辨识报警功能。

4.3 发电厂应建立控制系统故障应急处理组织体系，参照附录 B 成立分散控制系统故障应急处理领导机构及现场应急处置组，负责组织故障应急处置。

4.4 火力发电厂应根据本标准要求，制订适合单元机组的分散控制系统故障应急处理预案。

4.5 应在发电厂技术领导的主持下，组织热控、锅炉、汽轮机、电气和运行相关专业人员，在控制系统危险预测、预防的基础上，共同完成分散控制系统故障应急处理预案的编制，达到保障人身和电网安全、设备可控、不污染环境的目标。

4.6 火力发电厂应根据本单位批准发布的预案，定期组织对运行、检修、维护等相关人员的培训和故障应急处理演习，建立长效管理机制。

## 5 应急处理准备

### 5.1 故障源辨识

5.1.1 根据 GB 18218 的规定，按照可能发生的设备重大故障源以及可能造成的后果，对控制系统的设备重大故障源划分为三级，即一、二、三级故障。

5.1.2 根据本标准 3.11～3.13 的定义，分散控制系统设备重大故障源分级见表 1。

**表 1 分散控制系统设备重大故障源分级**

| 序号 | 故障类型 | 故障描述 | | 故障级别 |
|---|---|---|---|---|
| A1 | 电源故障 | 分散控制系统电源失去 | 分散控制系统电源全部失去 | 一级 |
| A2 | | | 分散控制系统电源单路失去 | 二级 |
| A3 | | A 类控制系统电源失去 | 电源全部失去（见控制器故障） | 一级 |
| A4 | | | 任一路电源失去冗余 | 二级 |
| B1 | 网络故障 | 分散控制系统网络全部瘫痪（包括数据通信服务器全部故障） | | 一级 |
| B2 | | A 类控制系统任一网络失去冗余（包括数据通信服务器单个故障） | | 二级 |
| C1 | 控制器故障 | 冗余控制器全部故障（包括电源失去） | 锅炉/汽轮机主保护控制器、数字电液控制系统基本功能控制器全部故障或 A 类控制系统任一对冗余控制器全部故障且涉及安全的参数无必要后备监视手段 | 一级 |
| C2 | | | 除一级故障外，A 类控制系统控制器全部故障，没有误发指令，但有必要的后备监视手段 | 二级 |
| C3 | | 冗余控制器单个故障 | A 类控制系统（炉膛安全监控系统、汽轮机紧急跳闸系统、数字电液控制系统基本功能等）控制器失去冗余 | 二级 |
| C4 | | | 非 A 类控制系统控制器失去冗余 | 三级 |
| D1 | 操作员站故障 | 全部操作员站失去监控 | | 一级 |
| D2 | | 部分操作员站失去监控 | | 二级 |
| E | I/O 模件故障 | A 类 I/O 模件故障 | | 二级 |

### 5.2 故障应急处理准备

5.2.1 按 4.3 的要求，应建立分散控制系统故障应急处理体系。

5.2.2 应根据机组实际情况，建立分散控制系统备品库（或建立统一配送机制，根据发电厂分布情况建

立合理的区域分散控制系统备品库），并应列出控制系统备品清单并及时更新，完善备品管理制度，做好故障应急处理的物质保障。

5.2.3 应建立必要的外部应急资源库（含采用同类控制系统的发电厂和设有热线联系方式的设备制造厂商），应确保外部应急资源需求能及时顺畅地响应。

5.2.4 应对控制系统可靠性结果进行确认，达不到 GB 50660 和 DL/T 261 的规定和 4.1 的要求时，应及时落实处理和预防措施。

5.2.5 应根据各机组控制系统的实际组态情况，编制各控制器主要控制对象列表。

5.2.6 应按 5.1 的设备故障源辨识原则和机组分散控制系统的实际配置，结合机组运行规程和事故预防要求，参照附录 C 编制至少包括下列内容的分散控制系统故障应急处理预案：

a） 分散控制系统故障应急启动流程。

b） 分散控制系统故障快速查找表和诊断与处理流程。

c） 分散控制系统故障处理操作卡。

d） 分散控制系统一、二级故障现场处置方案应包括下列内容：

1） 故障现象（运行检查故障现象、热控检查故障现象）；

2） 故障原因；

3） 故障后果；

4） 故障处理（分别给出运行部分和热控部分的处理操作步骤）；

5） 故障关联信号列表。

5.2.7 编制完成的所有控制系统故障应急处理预案，应利用机组检修机会进行验证，保证预案能够在满足运行规程和反事故要求的前提下，直接用于指导故障快速查找定位和应急处理。

## 6 故障应急处理

### 6.1 应急处理响应

#### 6.1.1 报警

发现设备故障应立即报警，运行值班人员应进行故障确认，并参照附录 C 中图 C.1 所示应急响应与处理流程进行响应。如故障为一级故障且设备的参数、状态达到停机保护动作值或规程规定的动作值时，应按规定停机，并汇报值长；如未达到紧急停机条件，应及时将设备故障现象、发生地点、发现时间告知当班值长，通知热控人员到场，协助分析判断和进行故障处理准备。

#### 6.1.2 应急分级

值长接到报警后，应立刻进行设备故障核实，根据发生的故障现象判断故障的可控性、严重程度和影响范围，按控制系统一级、二级、三级故障的定义确定故障级别。

#### 6.1.3 应急启动

一级故障应由值长启动一级故障应急处理预案，同时通知应急处理领导小组；二级故障应由值长启动二级故障现场应急处置方案，通知现场应急处置组成员赶赴现场，在现场应急处理组的组织协调下，根据职责分工开展应急处理工作。

### 6.2 现场应急处置原则

#### 6.2.1 故障应急处理一般原则

6.2.1.1 控制系统一级故障应急响应后，值长应立即汇报调度，并下令停止所有不必要的操作和检修维护工作，按对应的一级故障应急处理预案，协调现场故障应急处置组，展开故障的应急处理；二级故障应急响应后，值长应在现场应急处置组的协调下，按照对应的现场故障应急处置预案进行故障应急处理。

6.2.1.2 当失灵系统涉及主汽轮机或给水泵汽轮机的润滑油系统、主机控制油系统、发电机密封油系统、发电机氢气系统、锅炉炉前燃油系统、锅炉制粉系统等时，应及时做好相关消防措施。

6.2.1.3 运行人员应按照控制系统故障应急处理预案要求进行相应操作，加强对失去监控系统的上、下

游工艺流程参数的监视、分析，判断失控系统的运行状态。若发现相关运行设备跳闸，应核查确认其关联设备动作正常，必要时应安排运行人员就地操作；若运行参数发生大幅波动，应按运行规程要求采取相应措施维持参数稳定；同时安排巡检员进入现场，对失去监控的就地设备和机组主设备运行状态、参数进行检查、监视和操作，过程中应保持通信畅通。

6.2.1.4 热控人员应及时准确地掌握现场情况，了解设备故障前后的机组运行状况及操作和检修情况，按照应急处理预案中的快速查找表、典型故障诊断流程和现场应急处置方案，进行故障的分析、查找和处理。

6.2.1.5 控制系统故障应急处理过程中，应做好模件的防静电措施，并确保处理过程中的人身、设备安全，防止故障影响范围扩大。

6.2.2 一级故障应急处理原则

6.2.2.1 故障触发停炉、停机后应按下列原则处理：

a） 集控室运行人员，应按故障影响最小原则的顺序和紧急停机事故处理预案，正确操作后备手操装置及相关设备的启/停开关置于安全位置，并通过后备监视手段检查确认所有重要保护、连锁对象，在整个停炉、停机过程中动作正确，所有涉及安全的关键参数在允许范围内。

b） 运行巡检人员应按照紧急停机事故处理预案步骤，检查、确认、操作相关现场设备，确保设备处于安全状态。

c） 热控人员应按照紧急停机事故处理预案步骤，检查控制系统及设备状态，确认重要保护、连锁系统动作正确。如发现控制系统发出了错误指令，应迅速通知运行人员采取相应措施。

6.2.2.2 分散控制系统电源全部失去时应按下列原则处理：

a） 发生分散控制系统电源全部失去时，应通过后备监控手段，发出停炉、停机指令，并按 6.2.2.1 执行。

b） 处理重点是确保机组安全停机，防止恢复来电时，油、粉、汽系统不安全状况的发生。

6.2.2.3 分散控制系统网络全部瘫痪时应按下列原则处理：

a） 当网络故障致使分散控制系统无法显示且无后备监视手段，无法判断重要辅机状态和监视重要运行参数时，应立即启动紧急停机事故处理预案进行停炉停机操作。

b） 网络故障致使分散控制系统无法显示但有后备监视手段，能判别重要辅机状态，提供机组重要运行参数监测，且人员配置能保证故障时的现场监控，并确保机组安全运行的情况下，可等待专业人员进行故障处理，但应启动故障应急处理预案，做好紧急停炉停机的准备工作；如故障在规定时间内无法排除，或机组主要参数不能保证稳定，应立即启动紧急停机事故预案进行停炉停机操作。

c） 公用网络故障时，应立即判断循环水出水压力和真空状态，如真空或循环水压力下降，应立即进行降负荷或停机操作。

6.2.2.4 操作员站监控全部失去时应按下列原则处理：

a） 判断故障是由于分散控制系统全部电源失去引起时，应按 6.2.2.2 的要求进行处理。

b） 判断故障是由于其他原因引起时，应按 6.2.2.3 的要求进行处理。

6.2.2.5 主保护冗余控制器同时故障（包括电源失去）时应按下列原则处理：

a） 当机组已经跳闸停机时，应按 6.2.2.1 的要求进行处理。

b） 当冗余控制器电源消失而机组还在运行时，应通过后备控制手段发出停炉、停机指令，并按 6.2.2.1 的要求进行处理。

c） 当控制器本身故障而机组还在运行时，运行人员应通过后备监控手段和其他控制器稳定负荷，维持机组参数稳定，同时密切关注主保护相关的各项参数。如有参数超限，应按运行规程处理并做好紧急停机准备，热控人员应迅速检查控制器状态，进行故障排除。在处理过程中，热控人员应做好防止控制器初始化过程中信号误发的措施，同时通知值长按照紧急停机事故预案做

好准备措施。

6.2.2.6 数字电液控制系统基本功能（完成转速、功率、主蒸汽压力控制等基本功能）冗余控制器同时故障（包括电源失去）时应按下列原则处理：

a） 当机组已经跳闸停机时，应按 6.2.2.1 的要求进行处理。

b） 机组没有跳闸时，运行人员应在操作盘上手动按下汽轮机跳闸按钮，并按照紧急停机事故预案进行设备的检查和停运。

6.2.2.7 其他重要控制系统一对冗余控制器同时故障（包括同时失去监控画面）时应按下列原则处理：

a） 当机组已经跳闸停机时，应按 6.2.2.1 的要求进行处理。

b） 当涉及安全的 A 类控制系统冗余控制器（6.2.2.5 和 6.2.2.6 中提到的情况除外）同时故障，而机组仍在正常运行时，运行人员应确认该控制器的控制范围，减少对该控制器内设备不必要的操作，同时应通过后备监视手段和其他控制器，加强对故障控制器系统重要参数的监控；热控人员应迅速检查故障控制器，进行故障排除。

c） 在处理过程中，热控人员应做好防止误操作和控制器初始化过程信号误发的措施，同时通知值长做好各项预防措施，防止处理过程中紧急情况的发生。

### 6.2.3 二级故障应急处理原则

6.2.3.1 二级故障处理前，应做好防止误操作措施和故障随时升级的应急处理准备工作。

6.2.3.2 发生二级故障时，运行人员应加强参数监视，维持负荷稳定，减少对故障涉及范围内的设备不必要的操作。热控人员应检查对应故障的系统状态，按故障诊断与处理流程、典型故障快速查找表，进行故障原因查找和故障影响范围确认。

6.2.3.3 二级故障处理，应按现场故障处置方案和下列要求，参照附录 C 中控制系统典型故障处理操作卡进行：

a） 当任一网络失去冗余时，处理前应核对该节点下所连接的控制器被其他节点引用的通信点状态，将所属调节设备切除自动，目的地址参数人工临时置值，再进行网络故障排除。

b） 当 A 类控制系统任一对冗余控制器失去冗余时，处理前应做好防止恢复过程中，控制器初始化时信号误发，导致系统设备误动的措施。

c） 当非 A 类控制系统的任一对控制器全部故障、A 类 I/O 模件故障等情况发生时，若关键性参数超过保护定值或无法通过后备手段监视，则故障升级为一级故障，并按对应的一级故障处理预案进行操作处理。

d） 当部分操作员站失去监控时，热控人员应检查确认剩余的运行操作员站为系统独立节点或引自独立的系统服务器；当少于 2 台操作员站运行时，应打开服务器和工程师站操作权限（有此功能时），用于运行人员后备操作；然后进行故障操作员站恢复或故障处理。

e） 当 A 类控制系统 I/O 模件故障时，热控人员应通知运行人员切除所属系统或设备的自动和联动功能，将设备置于就地运行位置（就地应安排专人操作）；并根据实际状态，强制控制器相关信号后进行故障处理。处理过程中，应有防止 I/O 模件初始化时信号误发导致就地控制对象误动的措施。I/O 模件恢复正常后，应核对强制值与实时值的偏差，通过人工减小偏差后，再取消控制器内强制数据；恢复设备远方控制和自动及连锁功能，确认系统恢复正常。

f） 当单台给水泵汽轮机控制系统（MEH）系统全部电源失去时，如机组仍正常运行，运行人员应在操作盘上手动按下给水泵汽轮机控制系统跳闸按钮，机组控制系统应按给水泵故障快速减负荷（RB）情况处理。热控人员应迅速检查电源系统，进行故障排除；在处理过程中，热控人员应做好防止误操作措施，防止恢复过程中控制器初始化时信号误发，导致系统设备误动。

g） 进行非 A 类控制系统控制器冗余故障处理时，应做好故障影响扩大的预防措施，同时启动相应控制器全部故障应急处理预案的准备工作。替换下来的设备在分散控制系统热备柜或其他非重要机柜进行故障检测和试验、确认故障原因。

6.2.4 故障处理需要更换模件前，应确认替换模件的型号版本正确。

6.2.5 故障应急处理完成且系统恢复运行后，应全面检查系统运行状况，确认无任何隐患。

### 6.3 故障应急处理结束

6.3.1 故障应急处理作业结束后，生产管理部门与运行部门应对应急处理后的设备进行试验，确认设备故障已消除。设备运行恢复正常后，由应急处理领导小组召集会议，在充分评估应急工作的基础上宣布应急行动结束，应急处理人员撤离现场。

6.3.2 在控制系统故障应急处理作业过程中，如果故障发展已超出本标准规定的处理工作范围，应由应急处理领导小组下令应急处理预案终止执行。

### 6.4 故障应急处理后期处置

6.4.1 故障应急处理作业结束后，生产管理部门应妥善保存相关数据，并协助安全管理部门按事故调查程序调查故障、评估损失，提出防范类似故障发生的措施。

6.4.2 组织对故障应急处理预案实施全过程进行总结，消除预案存在的缺陷，不断完善故障应急处理预案。

6.4.3 对控制系统故障应急处理过程的资料，应建立专项档案，可溯源。

## 7 故障应急处理长效管理

### 7.1 故障应急处理培训

7.1.1 建立分散控制系统故障的应急处理培训制度，通过事前培训，树立相关工作人员的故障应急处理意识。相关工作人员应熟悉相关的法律、法规，熟悉故障应急处理流程和控制器所涉及的控制对象，掌握故障应急处理过程中所需要的专业知识。

7.1.2 控制系统故障应急处理相关工作人员，其相关知识培训应每年进行一次，并经考核合格后方能参与控制系统故障应急处理工作。

### 7.2 故障应急处理演习

7.2.1 应采用事故模拟演习的形式，培养运行、维护人员在故障应急处理作业过程中的实际操作能力，以及相关部门在应急处理作业过程中的组织协调及物资保障能力。演习结束后应全面评估应急处理预案的预防及处理效果，并及时改进与完善。

7.2.2 分散控制系统故障应急处理预案演习应每年进行一次，演习穿插在全厂的反事故处理演习过程中进行。

### 7.3 故障应急处理预案管理

7.3.1 应急处理预案应由安全生产管理部门备案。

7.3.2 应急处理预案的制订与解释，应由生产技术管理部门负责。

7.3.3 应急处理预案的修改和更新，应由生产技术管理部门负责。

7.3.4 应急处理预案应于发布日起开始实施。

# 附 录 A
（规范性附录）
分散控制系统可靠性确认

## A.1 分散控制系统可靠性确认的一般原则

A.1.1 控制系统配置可靠性，应符合相关设计标准，并满足 DL/T 261—2012 中 6.2 的要求。

A.1.2 控制系统在设备选型、硬件配置、控制逻辑设计、安装等方面，应充分考虑系统故障时的维护要求，并方便应急处理。

## A.2 分散控制系统接地可靠性确认

A.2.1 控制系统接入厂级接地网的接地点，应保持与大功率电气设备接地点的距离大于 5m，且在该点范围内不得有高电压强电流设备的安全接地和保护接地点。

A.2.2 采用现场单独专用接地网的接地铜板面积，应符合设计要求［通常为 900mm×（900mm～1200mm）×1200mm］，与其他接地极的距离应大于 10m，且专用接地网应与电气地网连接。

A.2.3 当厂区电气系统接地网接地电阻值小于 4Ω时，控制系统可直接接入厂级接地网；当厂区电气系统接地网接地电阻值较大或控制系统制造厂有特殊要求时，应独立设置接地系统且接地电阻应小于 4Ω（或按仪表制造厂要求确定）。基建机组与 A 级检修机组的控制系统，接地电阻测试记录应建立档案并可溯源。

## A.3 分散控制系统供电电源及电源装置可靠性确认

A.3.1 分散控制系统电源系统的冗余配置和电源间切换时间，应满足 DL/T 261—2012 中 6.5 的要求。

A.3.2 分散控制系统供电电源应配置电源柜，两路电源应物理隔离；分散控制系统用电设备应设置分路电源开关，任一设备短路或过载时，只跳闸对应的电源开关。

A.3.3 分散控制系统的每个控制单元，必须配置冗余的电源装置；任一路交流电源失去或任一电源装置故障时，应不影响系统的正常工作。

A.3.4 分散控制系统电源系统应具有可靠的状态和故障诊断、显示与报警功能。机组供电电源失电报警信号，应进入故障录波装置和相邻机组的分散控制系统监视（或独立于该分散控制系统电源的报警装置）。当外部或内部的任一路供电电源故障时，应能在人机界面显示故障诊断信息，大屏发出声光报警。

A.3.5 单元机组电源故障应急处理预案中，应列出单元机组控制系统不同等级电源指标并建立测试记录台账，以便溯源比较，及时发现电源模块的性能变化趋势。

## A.4 控制器可靠性确认

A.4.1 机组分散控制系统的控制器应冗余配置，其对数应严格遵循机组重要保护和控制分开的独立性原则配置，并满足分散度要求，一对控制器配置常规 I/O 宜不大于 400 点。

A.4.2 任一冗余控制器中的单一控制器故障（包括控制器故障、软件出错、通信故障及失去电源等），应不影响对应的控制回路正常工作。

A.4.3 应在控制软件完成后进行控制器冗余能力的测试，控制器切换时，硬件 I/O、通信和控制块的数据、参数和状态应无扰动。

A.4.4 对于两侧布置的风烟系统（两侧的送风机、引风机、一次风机、密封风机及空气预热器），宜按介质流程的纵向组合，各自分配在一对冗余控制器中。

A.4.5 对于配备多台给水泵的机组，每台给水泵控制（包括汽轮机给水泵的给水泵汽轮机和对应的给

水泵）应分配在不同的冗余控制器中。

A.4.6　凝结水泵、真空泵、开式和闭式冷却水泵、重要油泵和循环水泵等多台组合或主/备运行的重要辅机，同一类型设备不应分配在同一对控制器中。

A.4.7　厂用电系统不同母线段，应分配在不同的控制器中。

A.4.8　300MW 及以上机组的每套制粉系统及其油枪等点火装置，应按工艺流程要求纵向组合，分配在同一对冗余控制器中，并宜独立配置控制器。

A.4.9　控制器的故障诊断报警、离线下载和在线下载功能，应验证可靠。

## A.5　通信网络设备配置的可靠性确认

A.5.1　通信网络冗余与容错配置的性能和可靠性，应满足 DL/T 261—2012 中 6.2.2.1～6.2.2.3 的要求。

A.5.2　分散控制系统的通信系统应采取冗余设置。除一对互为冗余的通信设备同时故障外，分散控制系统的通信部件故障应不影响系统正常运行。

A.5.3　对于多对通信设备（如交换机），即使任一对通信设备同时故障，操作员站通信也不应全部失去。操作员站应分散布置在不同的交换机上。

A.5.4　通信设备的供电，应经试验确认冗余可靠。一路交流电源故障时，应不影响通信设备正常运行。

A.5.5　互为冗余的通信设备必须保证完全物理隔离，不应共用一个通信光缆（电缆）、插头和通信模件。

## A.6　操作员站可靠性确认

A.6.1　数字电液控制系统与分散控制系统非一体化的机组，数字电液控制系统操作员站应不少于 2 台。

A.6.2　操作员站应分为两组，分别由不同路电源供电；通过电源切换装置供电时，应经试验验证一路供电电源失去时，操作员站的正常运行不受影响。

A.6.3　操作员站通信应冗余，且连接在不同通信装置上，一对互为冗余的通信装置同时故障，不应造成全部操作员站失效。

A.6.4　任一操作员站故障应不影响其他操作员站的运行。

## A.7　输入/输出信号配置的可靠性确认

A.7.1　应按照风险分散、配置冗余的原则，进行 I/O 通道配置，并符合 DL/T 261—2012 中 6.2.3.1 的要求。

A.7.2　机组各主要控制系统的重要 I/O 信号配置，应符合 DL/T 261—2012 中 6.2.3.2 的要求。

A.7.3　根据控制器的控制任务确定每个 I/O 信号的分配。任一信号的测量元件、I/O 模件通道故障不应造成保护误动和拒动。

A.7.4　锅炉总燃料跳闸、汽轮机紧急跳闸系统、单列布置及主辅机的保护信号，应按三重化冗余原则配置并保证可靠的全程冗余（即同一物理参数的测量，采用三个相互独立的一次测量元件和电源，由三根相互独立的电缆接入三块不同的输入处理模件）。

A.7.5　三重化冗余保护的输出控制指令，应通过独立的输出处理模件（或扩展部件），在控制对象侧通过三选二或三选中逻辑（模拟信号做保护时）进行信号判断。

A.7.6　应保证重要监控信号在控制器故障时不会失去监视；汽包水位（直流机组除外）、主蒸汽压力、主蒸汽温度、再热蒸汽温度、炉膛压力等重要的冗余安全监视参数，应配置在不同的控制器中（配置硬接线后备监控设备的除外）。

## A.8　保护连锁和报警功能配置可靠性确认

A.8.1　机组的保护、连锁功能应安全可靠，确保控制系统局部单一故障不会造成保护拒动和误动。

A.8.2　应利用分散控制系统的自诊断功能，将控制器、电源、各个层次通信网络等关键设备的故障报警信号设计为最高级报警信号。

A.8.3 用于主要设备保护的信号在逻辑图上应有取源标注，组态图上应有取源超链接，控制器间的通信信号应能方便地找到，便于控制器故障处理。

## A.9 控制设备故障和应急处理试验

A.9.1 在分散控制系统出厂前和调试期间，应对系统的电源、网络、控制器、I/O 模件、测量设备、执行设备等控制系统装置的故障进行分析和试验，预测各种故障可能造成的后果，并根据故障对机组安全运行的影响进行分类。

A.9.2 测试分散控制系统的自诊断功能、故障报告和原因显示等功能，确认能够对故障原因快速定位、准确诊断。

## A.10 其他

A.10.1 电源、网络、控制器等冗余设备故障应及时处理；处理时应避免造成相关冗余设备同时故障，并按照一对冗余设备同时故障的情况做好预案。

A.10.2 控制系统在设备选型、分散控制系统硬件配置、控制逻辑设计、安装等方面，应充分考虑控制系统故障时的维护要求，便于应急处理。

A.10.3 气动和电动执行机构应根据工艺系统安全要求，具有三断保护功能，以及后备就地手动操作，在分散控制系统控制器或 I/O 模件发生故障时，仍可对重要设备进行干预。

# 附 录 B
（资料性附录）
分散控制系统故障应急处理组织体系

## B.1 组织机构及职责

B.1.1 发电厂应建立应急组织体系，成立分散控制系统故障应急处理领导机构，由企业主管生产的领导担任组长，运行、维护、生产、设备及后勤物资保证部门相关人员为机构成员，以便统一协调应对故障应急处理。

B.1.2 应急职能部门的职责。

B.1.2.1 应急处理领导小组应有下列职责：

a） 负责控制系统故障应急处理预案的制订，并定期组织演练，监督检查各部门在预案中履行职责的情况。

b） 对发生事件后是否应启动应急处理预案进行决策，全面领导应急处理工作。

c） 组织成立各专业故障现场应急处置组。

d） 故障发生后，根据设备故障报告，按预案规定的程序，组织专业故障现场应急处置组人员赶赴现场，安排故障应急处置人员及应急处理物资及时到位，有效进行设备故障处理。

e） 负责向上级主管部门汇报设备故障情况和处理进展，必要时向地方政府汇报。

f） 根据设备、系统的变化及时对应急处理预案的内容进行相应修改，并及时上报上级主管部门备案。

B.1.2.2 设备管理（检修）部门应有下列职责：

a） 负责备品备件的储备和管理，确保故障涉及的备品处于良好的备用状态。

b） 负责设备故障的应急处理，按照专业分工迅速落实人员到达现场。

c） 检查确定故障原因，并按相应的现场处置方案进行故障处理。

B.1.2.3 技术管理部门应有下列职责：

a） 负责设备故障应急处理过程中的技术支持，必要时负责与相关技术单位（厂家、安装单位、调试单位、技术支持部门）的沟通。

b） 负责协调各方关系，保证故障应急处理工作顺利进行。

c） 负责控制系统故障应急处理预案的编制、完善，演练方案的编写及培训。

B.1.2.4 发电运行部门应有下列职责：

a） 根据设备故障状态，及时有效地进行机组运行参数调整。

b） 设备故障处理期间，根据故障分类对故障设备采取相应的隔离措施，对可能产生的故障影响提出设备故障处理方案；负责与电网调度中心的协调，尽可能减小对电网的影响。

c） 负责设备故障处理后的检查试运。

B.1.2.5 安全管理部门应有下列职责：

a） 发生设备故障后，维持现场秩序、划定警戒区域。

b） 负责处理现场安全隔离措施的检查、落实，督促相关部门执行到位。

c） 负责组织设备故障的调查取证，召开专题分析会，形成处理意见。

d） 设备故障处理结束后，负责向上级相关部门通报设备故障处理情况。

B.1.2.6 后勤物资保障部门应有下列职责：

a） 负责控制系统故障应急处理所需物资，满足故障应急处理的要求。

b） 负责设备故障涉及备品的管理工作，确保设备故障涉及的备品处于良好的备用状态。

## B.2 现场故障应急处置组人员及职责

B.2.1 为保证控制系统故障时现场应急处理工作的有序进行，应成立现场故障应急处置组，由当值值长（检修副总工程师或运行副总工程师）担任组长，热控负责人和机组长担任副组长，组员应包括热控人员和运行当值操作员，负责组织应急处置工作。

B.2.2 现场应急处置组人员及职责。

B.2.2.1 组长应有下列职责：

a） 准确执行应急处理领导小组下达的命令。

b） 组织准确分析在分散控制系统故障处理过程中，机组可能受到的关联影响，落实预防措施，组织故障应急处理。

B.2.2.2 副组长应有下列职责：

a） 准确执行应急处理领导小组下达的命令。

b） 与电网调度中心保持联系，通报生产和电网信息；根据故障情况制订并执行机组运行变更方案，保障机组正常运行。

c） 收集、整理有关设备故障处理信息，向应急处理领导小组提出方案和策略。

d） 热控负责人根据收集到的各种信息，对故障情况进行初步分析，与应急组成员制订初步处理方案，组织专业人员进行应急处理。

B.2.2.3 组员中热控人员应有下列职责：

a） 根据收集到的各种信息，对故障情况进行初步分析，协助应急组成员制订初步处理方案。

b） 执行应急处理指令。

B.2.2.4 组员中运行当值操作员应有下列职责：

a） 准确执行当值值长下达的操作命令。

b） 负责紧急情况下的设备检查巡检及操作。

# 附 录 C
（资料性附录）
分散控制系统应急处理预案编制样本

## C.1 范围

略。

## C.2 编制依据和参考资料

略。

## C.3 术语、定义和缩略语

略。

## C.4 控制系统综述

### C.4.1 网络架构

略。

### C.4.2 电源系统

略。

### C.4.3 接地系统

略。

注：C.4 节至少包含以上内容，重点编制出该控制系统的特点。

## C.5 应急处理总则

见第 4 章。

## C.6 应急处理准备

### C.6.1 重大故障源风险辨识

C.6.1.1 根据 5.1 确定的原则，以控制系统设备的危险预测、预防为基础，辨识可能发生的设备重大故障源风险，并根据可能造成的后果将故障分为三级。

C.6.1.2 分散控制系统重大故障源列表见 5.1.2。

### C.6.2 故障应急处理准备

C.6.2.1 参见附录 B，建立机组分散控制系统故障应急组织体系，其中编制应急处理领导机构成员构成及职责表表头见表 C.1，编制现场应急处置组成员构成及职责表表头见表 C.2。

表 C.1 ×号机组分散控制系统应急处理领导机构成员构成及职责

| 职务 | 姓名 | 部门 | 岗位 | 电话 | 职责 |
|---|---|---|---|---|---|

表 C.2 ×号机组分散控制系统现场应急处置组成员构成及职责

| 职务 | 姓名 | 部门 | 岗位 | 电话 | 职责 |
|---|---|---|---|---|---|

C.6.2.2 根据机组实际情况，建立合理、必要的分散控制系统备品库，列出控制系统备品清单，完善备

品管理制度，做好故障应急处理的物质保障。分散控制系统备品清单列表表头见表 C.3。

**表 C.3 ×号机组分散控制系统备品清单**

| 系统 | 序号 | 备品名称 | 型号 | 数量 | 备品库名称及备品存放位置 |
|---|---|---|---|---|---|

C.6.2.3 根据机组实际情况，建立外部应急资源库，确保分散控制系统发生故障而单位内部应急能力不足以满足故障应急的需求时，外部应急资源请求能及时、顺畅地进行。对外部应急资源的充分利用是热控设备故障应急处理能够顺利进行的重要保证。分散控制系统外部应急资源列表表头见表 C.4。

**表 C.4 ×号机组分散控制系统外部应急资源**

| 系统 | 设备制造商（商务联系人/电话） | 设备制造商（技术联系人/电话） | 技术支持单位（联系人/电话） |
|---|---|---|---|

C.6.2.4 根据机组实际情况，编制各控制器主要控制对象列表，通过事前培训，使运行和检修人员掌握控制器所控制的对象，防止故障查找时因考虑不周、强制的关联点不全而出现漏洞，导致故障影响扩大事件的发生。分散控制系统控制器主要控制对象列表表头见表 C.5。

**表 C.5 ×号机组分散控制系统控制器主要控制对象**

| 序号 | 控制器编号 | 机柜号 | 主要控制对象 |
|---|---|---|---|

C.6.2.5 根据 5.1 的设备故障辨识原则和机组分散控制系统的实际配置，结合运行规程和反事故要求，制订控制系统故障应急处理预案启动流程（参见 C.9），各类控制系统典型故障快速查找表与查找流程（参见 C.10）、控制系统典型故障处理操作卡（参见 C.11），一级典型故障现场应急处置方案（参见 C.12），二级典型故障现场应急处置方案（参见 C.13）、控制系统维护方法（参见 C.14）。

## C.7 故障应急处理

C.7.1 应急处理响应，见 6.1。
C.7.2 现场应急处置，见 6.2。
C.7.3 应急处理结束，见 6.3。
C.7.4 应急处理后期处置，见 6.4。

## C.8 故障应急处理管理

C.8.1 故障应急处理培训，见 7.1。
C.8.2 故障应急处理演习，见 7.2。
C.8.3 故障应急处理预案管理，见 7.3。

## C.9 控制系统故障应急处理预案启动流程图

控制系统故障应急处理预案启动流程见图 C.1。

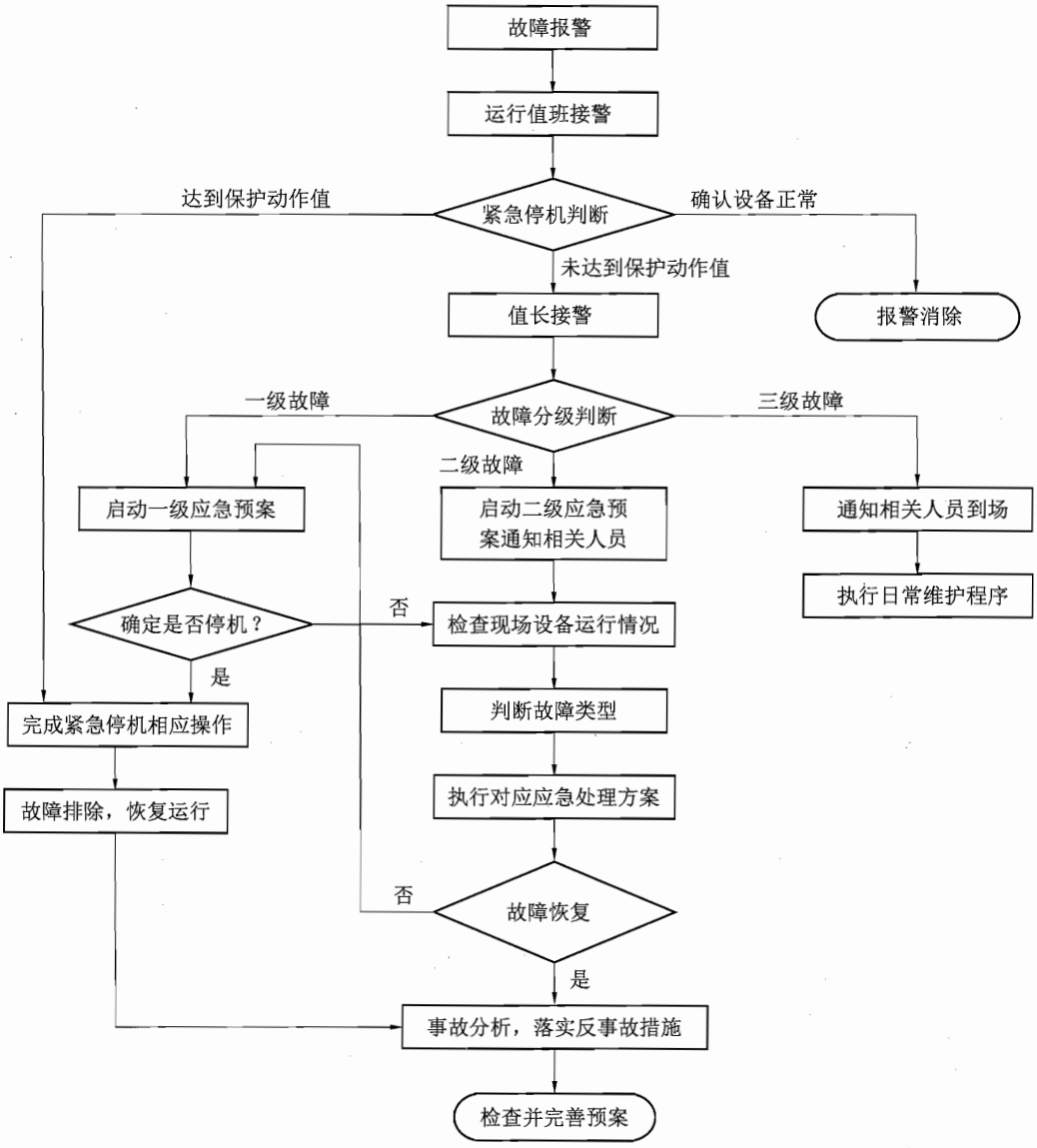


**图 C.1　控制系统故障应急处理预案启动流程图**

## C.10　控制系统故障快速查找表与查找流程图

C.10.1　编制分散控制系统典型故障快速查找表，样张如表 C.6 所示。

**表 C.6　分散控制系统典型故障快速查找表**

| 故障类型 | 故障现象 | 具体检查处理步骤及注意事项 | 应采取的安全措施 | 故障涉及设备及连锁保护 |
|---|---|---|---|---|
| 电源故障 | 部分电源失去 | | | |
| | 全部电源失去 | | | |
| | … | | | |
| 网络故障 | 部分操作员站离线 | | | |
| | 所有操作员站离线 | | | |
| | 部分控制节点离线 | | | |
| | 全部控制节点离线 | | | |
| | … | | | |

表 C.6（续）

| 故障类型 | 故障现象 | 具体检查处理步骤及注意事项 | 应采取的安全措施 | 故障涉及设备及连锁保护 |
|---|---|---|---|---|
| 硬件故障 | 单个控制器故障 | | | |
| | 一对冗余控制器同时故障 | | | |
| | 同一控制站内部分 I/O 模件故障 | | | |
| | 同一控制站内全部 I/O 模件故障 | | | |
| | … | | | |
| 软件故障 | 不能记录历史数据 | | | |
| | 工程师站软件故障 | | | |
| | 操作员站软件故障 | | | |
| | … | | | |
| 其他故障 | … | | | |

C.10.2 编制与验证适合机组控制系统的各种典型故障诊断与处理流程图，应至少包括下列流程图：

——控制系统故障诊断与处理流程图；

——控制器故障诊断与处理流程图；

——操作员站失去显示诊断与处理流程图；

——电源系统故障诊断与处理流程图；

——网络故障诊断与处理流程图。

## C.11 控制系统故障典型故障处理操作卡

编制与验证适合机组控制系统的各种典型故障处理操作卡（样张如表 C.7 所示），应至少包括下列操作卡：

——分散控制系统电源模件故障处理操作卡；

——分散控制系统网络及通信模件故障处理操作卡；

——操作员站故障处理操作卡；

——控制器初始化处理操作卡；

——控制器冗余故障和单一故障处理操作卡；

——组态下装操作卡；

——重要 I/O 模件故障处理操作卡。

表 C.7 控制系统故障典型故障处理操作卡

×号机组××故障处理操作卡

操 作 人：_____ 监 护 人：_____

开始时间：_____ 完成时间：_____

| 步骤 | 操作内容 | 注意事项 | 完成确认 |
|---|---|---|---|
| 1 | | | |
| … | | | |
| | | | |

## C.12 一级故障现场应急处置预案

C.12.1 根据重大故障源风险辨识分级结果，编制各一级故障现场应急处置预案。典型的一级故障现场应急处置预案应包括但不限于表 C.8 所列。

表 C.8 一级故障现场应急处置方案目录

| 系统 | 方案编号 | 现场处置方案名称 | 级别 |
|---|---|---|---|
| 分散控制系统 | DCS1-1 | 分散控制系统全部电源失去应急处置方案 | 一级 |
| | DCS1-2 | 分散控制系统全部操作员站失去监控应急处置方案 | 一级 |
| | DCS1-3 | 分散控制系统网络瘫痪应急处置方案 | 一级 |
| | DCS1-4 | 分散控制系统锅炉保护控制器全部故障应急处置方案 | 一级 |
| | DCS1-5 | A 类控制系统[a]任一对冗余控制器同时故障（含电源失去）且涉及安全的参数无必要后备监视手段的故障应急处置方案 | 一级 |
| 数字电液控制系统 | DEH1-1 | 数字电液控制系统基本控制器全部故障应急处置方案 | 一级 |
| 汽轮机紧急跳闸系统 | ETS1-1 | 汽轮机紧急跳闸系统控制器全部故障应急处置方案 | 一级 |
| [a] 除 DCS1-1～DCS1-4 和 DEH1-1 外的 A 类控制系统。 | | | |

C.12.2 每一项现场应急处置预案应至少包括下列内容：

——故障现象（运行人员检查、热控人员检查）；

——故障原因；

——故障后果；

——故障处理（运行人员处理、热控人员处理）；

——列出故障所有关联设备和重要关联 I/O 点，重要关联 I/O 点列表样张如表 C.9 所示。

表 C.9 重要关联 I/O 点列表样张

| 序号 | 设计编号（KKS 码） | 描述 | 信号类型 | 详细位置 |
|---|---|---|---|---|
| 1 | … | … | DO | … |
| 2 | … | … | AI | … |
| … | | | | |

## C.13 二级故障现场应急处置预案

C.13.1 根据重大故障源风险辨识分级结果，编制各二级故障现场应急处置方案。典型的二级故障现场应急处置方案应至少包括表 C.10 所列的内容。

表 C.10 二级故障源现场应急处置方案目录

| 系统 | 方案编号 | 现场处置方案名称 | 级别 |
|---|---|---|---|
| 分散控制系统 | DCS2-1 | 系统电源任一路失去 | 二级 |
| | DCS2-2 | 除一级故障外，有必要后备监视手段的 A 类控制系统控制器全部故障 | 二级 |
| | DCS2-3 | A 类控制系统任一电源失去冗余 | 二级 |
| | DCS2-4 | A 类控制系统任一对冗余控制器失去冗余 | 二级 |

表 C.10（续）

| 系统 | 方案编号 | 现场处置方案名称 | 级别 |
|---|---|---|---|
| 分散控制系统 | DCS2-5 | A 类控制系统任一网络失去冗余 | 二级 |
| | DCS2-6 | A 类系统监控画面失去监控 | 二级 |
| | DCS2-7 | 部分操作员站失去监控 | 二级 |
| | DCS2-8 | 重要 I/O 模件故障 | 二级 |
| MEH（METS） | MEH（METS）2-1 | MEH 全部电源失去 | 二级 |

C.13.2 每一项现场应急处置预案，应包括以下内容：

——故障现象（运行人员检查、热控人员检查）；

——故障原因；

——故障后果；

——故障处理（运行人员处理、热控人员处理）；

——列出故障所有关联设备和重要关联 I/O 点，重要关联 I/O 点见表 C.11。

表 C.11 重要关联 I/O 点列表样张

| 序号 | 设计编号（KKS 码） | 描　述 | 信号类型 | 详细位置 |
|---|---|---|---|---|
| 1 | | | DO | |
| 2 | | | AI | |
| … | | | | |

## C.14 控制系统维护方法

编制三级故障现场处置预案。录入机组分散控制系统常见故障代码、故障含义及维护方法等。

中 华 人 民 共 和 国
电 力 行 业 标 准
火力发电厂分散控制系统故障
应 急 处 理 导 则
DL / T 1340 — 2014
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）
北京九天众诚印刷有限公司印刷
*
2014 年 10 月第一版　　2014 年 10 月北京第一次印刷
880 毫米×1230 毫米　16 开本　1.5 印张　39 千字
印数 0001—3000 册
*
统一书号 155123 • 2114





155123.2114
上架建议：规程规范/
电力工程/火力发电