



火力发电厂分散控制系统 典型故障应急处理预案

国电智深EDPF-NT Plus系统

电力行业热工自动化技术委员会



中国电力出版社
CHINA ELECTRIC POWER PRESS



火力发电厂分散控制系统 典型故障应急处理预案

国电智深EDPF-NT Plus系统

电力行业热工自动化技术委员会



中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

为贯彻落实“坚持预防为主，落实安全措施，确保安全生产”的方针，确保机组在运行过程中发生控制系统故障时，运行和维护人员能够迅速、准确地组织故障处理，最大限度地降低故障造成的影响，电力行业热工自动化技术委员会组织全国 8 家电力科学（试验）研究院、14 家火力发电厂、11 家分散控制系统生产厂家的技术人员，在收集、总结各控制系统故障时的应急处理经验、教训，消化吸收了各分散控制系统技术管理经验、深入研究了各控制系统故障时应急处理方法的基础上，编制了系列《火力发电厂分散控制系统典型故障应急处理预案》丛书，全套书共 11 分册。

本预案介绍了国电智深 EDPF-NT Plus 分散控制系统的结构特点，对其可能发生的故障危险源进行了定义和分类，提出了国电智深 EDPF-NT Plus 分散控制系统故障应急处理预案的编制程序、结构、故障应急处理的通用要求、必须遵循的基本原则和故障时的整个处理流程。在现场故障处置预案中，详细介绍了各类故障时现象、故障原因、故障可能造成的后果以及运行处理操作和维护处理操作方法。

本书可作为火电厂深化热控专业管理、制订和完善各企业分散控制系统故障应急处理预案时的重要参考，也可以作为普通高等院校和电厂热控专业学习、培训的教材。

图书在版编目（CIP）数据

火力发电厂分散控制系统典型故障应急处理预案. 国电智深 EDPF-NT Plus 系统 / 电力行业热工自动化技术委员会编. —北京：中国电力出版社，2012.2

ISBN 978-7-5123-2653-8

I. ①火… II. ①电… III. ①火电厂—分散控制系统—故障修复 IV. ①TM621.6

中国版本图书馆 CIP 数据核字（2012）第 017089 号

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>）

北京丰源印刷厂印刷

各地新华书店经售

*

2012 年 6 月第一版 2012 年 6 月北京第一次印刷

787 毫米×1092 毫米 16 开本 6.5 印张 149 千字

印数 0001—3000 册 定价 23.00 元



敬告读者

本书封面贴有防伪标签，加热后中心图案消失

本书如有印装质量问题，我社发行部负责退换

版权专有 翻印必究

《火力发电厂分散控制系统典型故障应急处理预案》

研究与编制完成单位

丛书主编单位

中国电力企业联合会科技发展服务中心、浙江省电力试验研究院。

丛书各分册完成研究与编制单位（按完成编写时间排序）

1. 《福克斯波罗 I/A 系统》分册，由浙江省电力试验研究院、浙江大唐乌沙山发电有限责任公司和上海福克斯波罗有限公司联合编制。
2. 《ABB Symphony 系统》分册，由湖南省电力公司科学研究院、大唐湘潭发电有限责任公司、浙能乐清发电有限责任公司和北京 ABB 贝利工程有限公司联合编制。
3. 《艾默生 Ovation 系统》分册，由华东电力试验研究院有限公司、上海上电漕泾发电有限公司、浙江华能玉环发电厂和艾默生过程控制有限公司联合编制。
4. 《日立 HIACS-5000M 系统》分册，由河南电力试验研究院、大唐三门峡华阳发电有限责任公司和北京日立控制系统有限公司联合编制。
5. 《国电智深 EDPF-NT Plus 系统》分册，由神华国华（北京）电力研究院有限公司、神华国华徐州发电有限责任公司和北京国电智深控制技术有限公司联合编制。
6. 《和利时 MACSV6 系统》分册，由神华国华（北京）电力研究院有限公司、神华内蒙古国华呼伦贝尔发电有限责任公司和杭州和利时自动化有限公司联合编制。
7. 《GE 新华 XDPS-400 系统》分册，由内蒙古电力科学研究院、北方联合电力有限公司、内蒙古京达发电有限责任公司、新华控制工程有限公司联合编制。
8. 《西门子 T3000 和 TXP 系统》分册，由神华国华（北京）电力研究院有限公司、神华浙江国华浙能发电有限公司、神华广东国华粤电台山发电有限公司、浙江省电力试验研究院、浙能乐清发电有限责任公司和西门子电站自动化有限公司联合编制。
9. 《上海新华 XDC800 系统》分册，由安徽省电力科学研究院、大唐淮南洛河发电厂和上海新华控制技术（集团）有限公司联合编制。
10. 《国电南自 TCS3000 系统》分册，由中国华电集团公司电气及热控技术研究中心、黑龙江华电佳木斯发电有限责任公司和国电南京自动化股份有限公司联合编制。
11. 《南京科远 NT6000 系统》分册，由浙江省电力试验研究院、神华国华（舟山）发电有限责任公司、南京科远自动化集团股份有限公司联合编制。

《火力发电厂分散控制系统典型故障应急处理预案》

丛 书 审 委 会

主 任 金耀华
副 主 任 江宇峰 吴茂林 侯子良 金 丰
委 员 段 南 王利国 仝 声 李劲柏 骆 意 颜渝坪
郑慧莉 盛建华 马永真 胡文斌 陈世和

丛 书 编 委 会

主 编 孙长生 尹 淦
副 主 编 朱北恒 孙 耘 李建国
编 委 王建强 刘武林 沈丛奇 岳建华 张秋生 张国斌
崔 猛 蔡 兵 陈五年 项 谨 尹 峰 黄 勃
刘玉成 杨震力

《国电智深 EDPF-NT Plus 系统》分册编审人员

主 编 张秋生
副 主 编 于修林 范永胜 柯 炎
参编人员 吴 伟 韩 冬 梁 华 胡晓花 甘 泉
黄 勃 黄 亚 田雨聪 陈 峰 郑志刚
唐 伟
主 审 沈丛奇

随着发电机组容量和规模的成倍增长,分散控制系统的可靠性水平,已成为确保发电机组以及电网系统安全、稳定、高效运行和满足国家节能环保要求的关键。但分散控制系统品种繁多、技术涉及面广、元部件离散性大,运行过程中发生各种各样的故障难以避免,这就对从事控制系统运行、维护的专业人员提出了一个新课题,就是如何进行故障的有效预防,以及故障发生后如何通过迅速、正确的处理,将故障的影响降到最小。

有那么一批具有高度事业心、勇于探索实践、勤于钻研积累的热控专家和现场专业人员,他们在电力行业热工自动化技术委员会的组织与浙江省电力试验研究院的牵头下,基于上述课题展开了深入的专业研究,取得了丰硕成果——完成《火力发电厂分散控制系统典型故障应急处理预案》丛书编写,并将自己长年用汗水、心血换来的学习、工作、研究中积累的宝贵经验,通过这套丛书的出版,无私地奉献给了全国发电企业和广大读者。

这套丛书着重于电厂规程编写、故障分析查找及处理过程的示范,突出实用性、完整性、先进性和可操作性,因此有别于一般专业规程,也不同于一般的技术交流和经验总结性资料。相信它不仅对各发电企业编写或完善适合本企业的分散控制系统故障应急处理预案具有很好的指导作用,而且各发电企业可通过故障应急处理演练,有效提升运行、维护人员迅速、准确组织故障处理的能力。这套丛书将成为热控及相关专业教学、培训和自学的优秀教材,为从事或有志于从事该项工作的广大读者带来经验、启迪、思考和收益。

希望这套丛书的出版,能促进全国发电企业热控系统故障应急处理预案编制工作的不断完善并建立长效管理机制。通过各企业预案的编写或完善、培训与演练,提高运行、检修人员的故障处理能力,为机组安全、稳定、经济、节能环保运行作出贡献。

中国大唐集团公司副总经理
电力行业热工自动化技术委员会主任委员



二〇一二年三月二十日

前言

电力行业热工自动化技术委员会
Thermodynamic automation technical committee

目前国内大中型发电机组热力系统的监控,都采用了分散控制系统(DCS),电气系统的部分控制也正逐渐纳入其中。由于各厂家产品质量不一,控制系统的各种故障,如电源失电、操作员站“黑屏”或“死机”、主从控制器切换异常、通信中断、模件损坏等事件仍时有发生。有些由于运行或维修人员在控制系统故障时处理不当,导致故障扩大,机组非计划停运,甚至发生锅炉、汽轮机等主设备损坏事故。虽然多年来,根据《防止电力生产重大事故的二十五项重点要求》,电力行业管理部门和各发电集团公司都要求发电企业制订《分散控制系统故障应急处理预案》(以下简称《预案》),并组织运行和检修人员进行反事故演练。但到目前为止,由于《预案》编制无参照依据,大部分发电企业没有进行该工作;有的虽然进行了编写,但编制内容与范围不完整,不能满足控制系统故障时的处理需求,多数情况下还是凭运行和检修人员的经验来处理,结果导致故障扩大或一些本可避免的机组跳闸事件发生。根据“电厂热工自动化网站”已有的机组跳闸事件的归类统计,有30%以上事件是与运行或检修人员处理不当有关。

为建立热控系统故障应急处理和长效管理机制,确保机组在运行过程中发生控制系统故障时,能够迅速、准确地组织处理故障,最大限度地降低故障造成的影响,浙江省电力试验研究院于2008年开始,在浙江省范围内开展了火力发电厂《预案》的研究编制工作,初步完成了火力发电厂《预案》编制模板,并在浙江省浙能兰溪发电有限公司600MW机组上进行了控制系统故障演习,取得了第一手资料,修改完善后编入已出版的《火电厂热控系统可靠性配置与事故预控》一书中。

2010年10月,电力行业热工自动化技术委员会组织了全国8家电力科学(试验)研究院、14家火力发电公司(厂)、11家控制系统生产厂家,针对目前火力发电厂在线运行的主流控制系统和后起的国产控制系统,成立了11个《火力发电厂分散控制系统典型故障应急处理预案》(以下简称《典型预案》)编制组,在浙江省电力试验研究院前期研究工作经验和《火电厂热控系统可靠性配置与事故预控》提供的预案编制模板的基础上,通过进一步收集、总结各分散控制系统故障时的应急处理经验教训,消化吸收各参编单位技术及管理经验,联合进行分散控制系统故障应急处理方法的研究后,确定了统一的编写格式和编制程序的结构,制定了分散控制系统故障时应急处理的通用要求,规范了分散控制系统故障时的应急处理必须遵循的基本原则和操作过程。经过各编制组近一年的辛勤劳动,并在一些发电企业实际应用检验和修改后,完成了11册《典型预案》的编制。电力行业热工自动化技术委员会两次组织全国性的电厂专业人员进行讨论和广泛征求意见,并于2011年8月23日在北京召开专家审查会,国家电力监管委员会安全局发电处、中国电力企业联合会标准化中心火电处领导参加了会议,大唐、国电、华能、中电投等集团,中国电力工程顾问集团公司,西安热工研究院,华北电力科学研究院等单位的领导和专家组成的专家组,对《典型预案》的主要原则进行了审查,各编写组根据审查意见对各分册《典型预案》进行了完善。

本套《典型预案》均按规程格式要求,基于编制组所在的电厂机组配置和系统进行编写,仅作为指导性文件,为使用这11种控制系统的机组,编制或完善适应各发电企业的火力发电

厂《预案》时提供参考标准和模板。各发电企业可依据这些《典型预案》的编制格式和内容，结合本企业的具体组织结构、管理模式、风险种类、生产规模、控制系统配置等特点进行相应的调整，编制适合本企业的《预案》。通过完善故障时应急处理方法和定期反事故演习，提高运行维护人员在控制系统故障时的应急处理能力，消除因人员操作处理不当而导致分散控制系统故障范围扩大的隐患。

本套《典型预案》编写过程中，得到了国家电力监管委员会安全局、各发电集团公司及全国 30 余家单位领导的大力支持，控制系统厂家提供了宝贵的技术资料，近 70 位技术和运行人员参加编制，贡献了长期积累的宝贵经验，金耀华主任委员主审了丛书，侯子良、金丰、段南等众多专家给予了热情指导，审查委员会专家们认真审查并提出了宝贵的修改意见，使编制组受益良多，在此一并表示感谢。

最后，感谢浙江省电力试验研究院在组织编写中给予的全力支持与配合，使得本套《典型预案》得以顺利出版，让整个电力行业受益。

《火力发电厂分散控制系统典型故障应急处理预案》丛书编委会

二〇一二年三月十日

编者的话

电力行业热工自动化技术委员会
Thermodynamic automation technical committee

国华陈家港发电公司 2×660MW 超超临界机组和徐州 2×1000MW 超超临界机组采用国电智深公司的 EDPF-NT Plus 分散控制系统。为了提前进行风险预控，在电力行业热工自动化技术委员会的组织下，神华国华电力研究院有限公司、国华徐州和陈家港发电有限公司和北京国电智深控制技术有限公司一起，在充分调研、试验、分析、讨论、总结火电机组 DCS 出现各种可能的故障情况下的安全可靠性和故障现象和故障处理方法的基础上，联合编写了本册《火力发电厂分散控制系统典型故障应急处理预案 国电智深 EDPF-NT Plus 系统》。编写过程中几易其稿，并做了比较全面的模拟试验，充分综合了 4 家单位的技术特长和经验积累，凝聚了许多专业人员的心血。

本书由神华国华（北京）电力研究院有限公司张秋生主编，总体统筹协调参编单位的编写任务，确定全书框架和各现场应急处置预案内容，负责正文、G2 部分的编写和全书统稿，国华徐州发电公司的于修林、国华电力研究院的范永胜和国华徐州发电有限公司柯炎任副主编。附录编写由柯炎负责，吴伟、韩冬、黄亚和国华电力研究院的梁华、胡晓花、甘泉参加编写，陈家港发电公司的郑志刚、唐伟对应急预案进行了现场的验证与确认工作，北京国电智深控制技术有限公司的田雨聪参与了本书附录部分章节的编写，并和陈峰一起对本书中涉及国电智深 EDPF-NT Plus 分散控制系统故障现象及处理方法进行了技术指导与把关。浙江省电力试验研究院黄勃参与了正文的修改，对全书进行了最后核对。

本书由沈丛奇担任主审。

衷心感谢电力行业热工自动化技术委员会所做的努力，联合 8 家电力科学研究（试验）院、14 家火力发电公司（厂）、11 家控制系统生产厂家专业人员通力合作，利用繁忙的工作之余在较短时间内完成本套系列丛书的研究、编制和验证，使得 DCS 故障处理预案得以规范化、公开化出版，让整个电力行业受益。书稿编写过程中，各参编单位领导给予大量支持、沈丛奇高级工程师在主审书稿中提出了许多宝贵的意见和建议。国华徐州和陈家港发电公司热控、运行人员参与相关试验和讨论，国电智深自动化有限公司有关人员积极配合、提供资料、参与编写，浙江省电力试验研究院给予大量协助与最终样稿的校对，在此一并表示衷心感谢！

限于编写人员的实践、水平、时间以及模拟试验条件的不足，本预案中难免会有不当之处，尚祈读者批评和指教。

《国电智深 EDPF-NT Plus 系统》编写组

二〇一二年三月十日

序	
前言	
编者的话	
1 范围	1
2 编制依据和参考资料	1
3 术语、定义和缩略语	1
4 EDPF-NT Plus 分散控制系统综述	3
4.1 EDPF-NT Plus 分散控制系统技术特点	3
4.2 EDPF-NT Plus 分散控制系统结构	4
4.3 系统接地	5
5 应急处理预案的总体要求	6
5.1 总则	6
5.2 设备重大故障源风险辨识	7
5.3 应急处理预案编制	8
5.4 故障应急处理准备	10
5.5 组织机构及职责	14
6 故障应急处理过程控制	16
6.1 应急处理响应	16
6.2 现场应急处置	16
6.3 应急处理结束	17
6.4 应急处理后处置	17
6.5 应急处理培训与演习	18
6.6 应急处理预案的管理	18
附录 A 控制系统故障现场应急处理预案流程	19
附录 B 控制系统故障诊断的处理	20
B.1 DCS 故障诊断和处理流程	20
B.2 DCS 控制器故障诊断和处理流程	21
B.3 网络交换机故障处理流程	22
B.4 EDPF-NT Plus 分散控制系统故障快速查找表	22
附录 C EDPF-NT Plus 分散控制系统维护应用操作卡	26
附录 D 一级故障现场应急处置预案	39
D.1 DCS 电源全部失去应急处置预案	39
D.2 DCS 冗余网络全部瘫痪应急处置预案	39
D.3 DCS 全部操作员站功能丧失应急处置预案	40
D.4 DCS 锅炉保护控制器故障应急处置预案	41

D.5	DCS 重要顺控系统控制器全部故障应急处置预案	43
D.6	DCS 重要模拟量系统控制器全部故障应急处置预案	44
D.7	DCS 冗余网络部分瘫痪应急处置预案	45
D.8	DPU01/61 控制站严重故障应急处置预案	47
附录 E	二级故障现场应急处置预案	50
E.1	DCS 单路电源失去应急处置预案	50
E.2	机柜 I/O 分支电源失去应急处置预案	50
E.3	DCS 网络失去冗余故障应急处置预案	51
E.4	DCS 交换机通信负荷率高应急处置预案	52
E.5	DCS 控制柜重要 I/O 模块故障应急处置预案	53
E.6	DPU03/63 控制站严重故障应急处置预案	54
E.7	DPU04/64 控制站严重故障应急处置预案	58
E.8	DPU05/65 控制站严重故障应急处置预案	62
E.9	DPU06/66 控制站严重故障应急处置预案	65
E.10	DPU07/67 控制站严重故障应急处置预案	69
E.11	DPU08/68 控制站严重故障应急处置预案	72
附录 F	三级故障现场处置预案及其他	77
F.1	DCS 某控制柜电源单路失去应急处置预案	77
F.2	DCS 部分操作员站失去监控应急处置预案	78
F.3	锅炉保护控制器失去冗余应急处置预案	78
F.4	重要顺控系统控制器失去冗余应急处置预案	79
F.5	重要模拟量系统控制器失去冗余应急处置预案	80
F.6	DPU19/79 控制站严重故障应急处置预案	80
附录 G	EDPF-NT Plus 控制系统维护方法	82
G.1	控制系统检修与维护技术措施	82
G.2	控制系统可靠性确认	88

1

范 围

本预案规定了火力发电厂编制国电智深 EDPF-NT Plus 分散控制系统故障应急处理预案的程序、内容和要素等基本要求。各发电企业编制时，应结合本单位的组织结构、管理模式、风险种类、生产规模等特点，进行相应的调整。

本预案适用于火力发电厂采用国电智深 EDPF-NT Plus 分散控制系统的已投产机组，进行控制系统故障应急处理预案的制订和故障时的现场应急处理指导。

2

编制依据和参考资料

编制过程，参考了下列规程、标准、资料的格式、内容和要求：

GB 50660 大中型火力发电厂设计规范

DL/T 774 火力发电厂热控自动化系统检修运行维护规程

AQ/T 9002 生产经营单位生产安全事故应急预案编制导则

Q/LD 208005 危险源辨识与风险评价控制程序

火电厂热控系统可靠性配置与事故预控

3

术语、定义和缩略语

下列术语、定义和缩略语适用于本预案。

3.1

应急预案 emergency pre-arranged planning

是指根据评估分析或经验，对潜在的或可能发生的突发事件的类别和影响程度而事先制订的应急处置预案。

3.2

应急响应 emergency response

分散控制系统故障发生后，有关部门或人员按照工作程序对故障作出判断，确定响应级别。

3.3

应急启动 emergency start

应急响应级别确定后，按确定的响应级别启动应急程序，通知应急人员到位，开通通信网络，调配应急资源。

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、减少故障危害，防止故障影响扩大，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、事故调查等。

3.6

分散控制系统 distributed control system (DCS)

DCS 是指采用计算机、网络通信和屏幕显示技术，实现对生产过程的数据采集、控制和保护等功能，利用通信技术实现数据共享的多计算机监控系统。其主要特点是：功能分散，操作显示集中，数据共享，可靠性高。

3.7

操作员站 operating station (OPR)

操作员站具有完整的人机接口 (MMI) 功能，实时运行状态下，操作员通过操作员站实现对生产过程的实时监控。一个系统中可以有多个操作员站，各站之间相互独立，互不影响。操作员站能够以过程画面、曲线、表格等方式为操作人员提供生产过程的实时数据，借助人机对话功能，可对生产过程进行实时监控。

3.8

工程师站 engineer station (ENG)

工程师站是 EDPF-NT Plus 系统中组态、维护和管理工程的计算机。一个系统中可以配置多台工程师站，安装了工程师软件，具有相应权限的计算机就是工程师站。用户可以在工程师站上管理项目工程，组态、安装 DPU，维护工程的组态数据，维护操作员站、历史站、分布处理单元 (DPU) 等设备管理信息。工程师站是系统管理的核心，但生产过程的控制和运行并不依赖于工程师站。

3.9

高速数据公路 highway

EDPF-NT Plus 数据高速公路采用高速工业以太网协议，扁平化对等型网络结构，无实时数据服务器，以面向功能和对象而实现的“站”为基本单元，采用分布式动态实时数据库技术，管理分布在各站的系统运行所需的全部数据。

3.10

分布式处理单元 (DPU)

分散控制系统过程控制级中最基本的控制单元，内置实时多任务软件操作系统和嵌入式组态控制软件，用以实现对工业生产过程的数据采集和/或直接数字控制等各种实时任务，

DPU 可以独立工作，也可以通过通信总线与其他 DPU 一起组成复杂控制系统。

3.11

I/O 控制总线 I/O bus

I/O 控制总线是现场控制站的内部网络，为冗余双总线结构，实现 DPU 与各个 I/O 模块之间的互连和信息传递，通信速率为 1.5Mbit/s，柜内本地 I/O 通过底座总线传输，远程 I/O 传输介质为屏蔽双绞线或光纤。

3.12

通信网关站 gateway

通信网关站用于向 DCS 外的第三方发送 DCS 中的实时点信息。根据预定义的点列表，按照规定的发送周期定期向数据接收方（一般为 SIS 或 MIS）发送 DCS 中点的实时信息，实时信息包括点的数值和状态。

4

EDPF-NT Plus 分散控制系统综述

4.1 EDPF-NT Plus 分散控制系统技术特点

国电智深 EDPF-NT Plus 分散控制系统是针对大型火电机组开发的一套先进的自动化控制系统面向整个生产过程，适用于各类大型、复杂的工业程控应用，也可构成简单系统，满足小规模、低成本应用的要求，其采用可扩展标记语言（XML）和分布式计算环境（DCE）技术，使得 EDPF-NT Plus 软件可以在多操作系统和硬件平台下运行。工程师站软件包括了一个集成开发环境工程管理器（PO），专门提供用于工程设计、组态、调试、运行、诊断和服务的统一用户接口。系统具有以下的主要技术特点：

a) EDPF-NT Plus 系统的数据高速公路采用高速实时工业以太网协议，对等型网络结构，无网络或实时数据服务器，不会产生网络瓶颈和危险集中，实现了功能分散、危险分散。

b) 采用基于分布式计算环境（DCE）的多域网络结构，新式“域”间隔离技术解决了多套控制系统高性能隔离互连及集中监控难题，为自动控制系统大规模集成运行提供技术基础，满足各行各业的过程控制要求。其系统数据高速公路、过程控制站控制器、电源、I/O 模块、I/O 通道、人机交互工作站等系统重要部分均可冗余配置，提高了系统的实时性、可靠性和容错能力。

c) 控制器通过 I/O 控制总线，可以直接连接 32 个 I/O 模块，通过中继器可最多扩展到 63 个 I/O 模块。互为热备的主备控制器切换时间小于 10ms。双网并发的网络冗余方式避免了网络切换带来的弊端。

d) 以站为基本单位的大容量分布式实时数据库采用了基于聚簇索引技术的数据库引擎核心，解决了 DCS 工程分步投运中易出现的相互干扰问题，提高了系统动态安全性。数据库的局部修改对数据库其他部分无影响，无需整体重新编译和装载。历史数据采用例外报告技术和二进制压缩格式收集生产过程参数或衍生数据。在采集 10 万点的历史数据时，仍然能够快速

响应多用户的并发查询。通过“卷”管理功能，借助外部存储介质，可以保存几年的生产数据。

e) 跨平台的系统软件。控制系统的过程控制站和人机交互设备软件都兼容 Windows 和 Linux 操作系统，以适应不同应用领域对软件环境的要求。

f) 过程控制站算法库动态加载技术。过程控制站算法库与 DPU 支撑软件的主体分开，可以各自独立升级，在线增加或替换算法。方便系统的升级和维护，为用户提供了灵活的定制功能。便于针对不用控制对象、不同过程控制领域开发专用算法库。通过提供 EDPF-NT Plus 增值开发包，支持用户自行编制高级控制算法。

g) 控制系统具有后台分层软硬件深度自诊断功能，可诊断网络、站、I/O 模块直至 I/O 通道。

h) 过程控制站控制器内置 GPS 秒脉冲同步时钟信号接口，控制器与 I/O 模块之间通过同步脉冲电路保持高度时钟同步，使得控制站之间的时间同步达到微秒级，保证跨站 SOE 精度小于 1ms。SOE 模块可以分散安装在任何过程控制站内。

i) 强化的结构设计，所有 I/O 模块采用金属外壳全封闭结构，电路板上涂敷军用三防漆，防尘、防潮、防腐蚀、防静电、抗电磁干扰。内置通道电气隔离装置，所有 I/O 通道采用光电隔离和电源隔离技术实现与外部的电气隔离和路与路的电气隔离。且 I/O 通道设计有 PTC 强电串入保护电路。当误接入强电信号时，通道自动被阻断保护，强电信号撤除后通道恢复正常。

j) 虚拟控制器的运用。借助跨平台软件移植技术，EDPF-NT Plus 系统的虚拟控制器软件与真实控制器软件具有几乎完全相同的功能和特性，实现了控制系统高精度仿真，可以对控制策略进行全面仿真测试，并且支持进一步应用功能扩展。

k) 自主创新的扩展 I/O 接口（EIO）为各类现场总线设备提供了统一、灵活地接入平台。支持各种网络通信协议和多种现场总线标准。

l) 控制系统过程故障安全设计。控制系统过程的故障安全是 EDPF-NT Plus 分散控制系统应用设计的重要准则。在控制系统配置、控制逻辑的设计、紧急跳闸功能的实现、极端情况下的应对措施等方面突出强调故障安全，防止设备拒动，在不增加控制系统成本情况下有效提高了控制系统的安全级别。

m) 全自由格式的 SAMA 图形化控制组态软件。便捷的全图形化 SAMA 图控制组态功能，非常直观，易学易用。设计图纸、组态调试图纸和竣工图纸完全相同，便于维护。

n) 智能化的 I/O 模块。每块 I/O 模块都设计有 CPU 处理器、通信协处理器和冗余网络总线接口。依托智能化 I/O 模块设计生产了大量具有先进控制功能和针对工业各类工作环境的驱动级输出模块。

4.2 EDPF-NT Plus 分散控制系统结构

EDPF-NT Plus 分散控制系统以网络通信系统为基础，以面向功能和对象而实现的“站”为基本单元，分布式动态实时数据库用于管理分布在各站的系统运行所需的全部数据。

EDPF-NT Plus 分散控制系统支持面向厂区级应用的基于分布式计算环境（DCE）的多域网络环境。采用“域”管理技术，成功解决多套控制系统隔离互连及集中监控功能要求。每个域是其中一个中小型系统，完成相对独立的数据采集处理和监控功能。各个域通过网络连接在一起，形成一体化大型自动化系统。各域之间相互隔离，合法数据可以在域间共享，杜绝非法信息跨域流动，降低数据规模，提高系统可靠性。系统结构如图 1 所示。

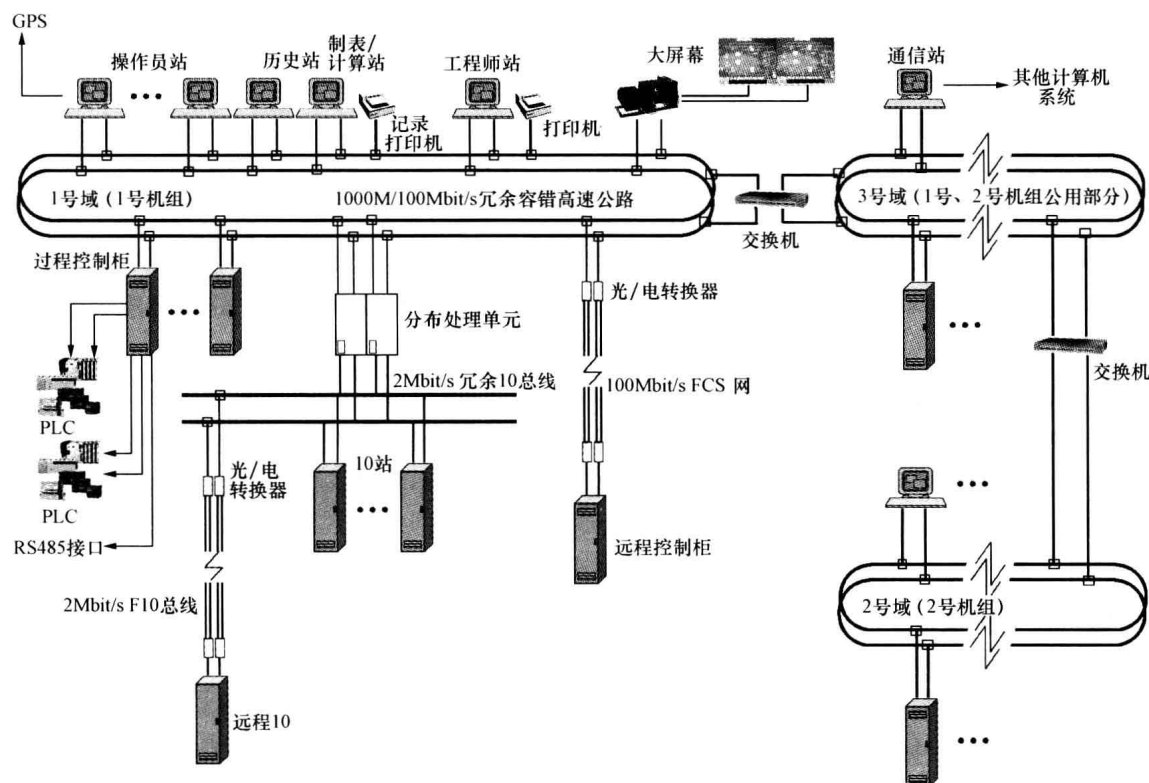


图1 EDPF-NT Plus 分散控制系统结构图

4.2.1 EDPF-NT Plus 分层次的综合在线自诊断

为了提高DCS可靠性，EDPF-NT Plus分散控制系统提供系统软硬件多层次在线自诊断，以便及时发现、报警和处理系统故障。操作员站提供专门的诊断画面显示系统各部分运行状态，并实时刷新。EDPF-NT Plus分散控制系统的综合在线自诊断内容包括：人机交互工作站的在线诊断、网络通信设备的在线诊断、控制器运行状态在线诊断、所有智能I/O模件、I/O通道级的在线诊断、电源系统在线诊断等。

4.2.2 控制机柜

EDPF-NT Plus系统采用满足IP52/56标准的控制机柜。机柜配有220V AC冗余电源装置为柜内设备供电。柜内设置为控制器及I/O模件提供电源的直流24/48V冗余电源。机柜内安装冗余的程控站控制器和各种智能I/O模件。机柜用隔板分成前后两个部分，前后可独立对称布置，每一面可布置2列I/O模件，最多可安排24块I/O模件。I/O模件安装在预制的总线底座上，信号端子也已经预制在底座的一侧，机柜柜门上或顶部装有风扇用于柜内的散热。

4.2.3 系统电源及配电系统

整套DCS统一由系统配电柜供电。配电柜接受两路220V AC电源，并可配置UPS电源。配电柜为系统内的所有用电单元（控制机柜等用电设备）提供两路交流220V AC电源，包含为用电单元提供保险和独立投切开关。系统提供交流电源快切装置，其切换输出专门为重要交流用电设备可靠供电。

4.3 系统接地

a) DCS系统接地包括以下三种：

1) 机壳保护地(机柜外壳、操作台外壳等)(CG): 将系统中平时不带电的金属部分(机柜外壳、操作台外壳等)与地之间形成良好的导电连接,与大地连接成等电位,以防止漏电或静电积聚造成对设备及人身伤害。

2) 信号屏蔽地(SG): 为了抑制变化的电磁场对信号的干扰而采用的多种屏蔽层、屏蔽体,都必须良好地接地,才能起到良好的屏蔽作用。对于 DCS 系统,各种信号电缆、网络电缆等都要求采用屏蔽电缆,这些电缆的屏蔽层要求在一端单点接地。

3) 逻辑电源地(PG): DCS 系统将外部交流电源被转换成直流电源,分别给控制器、I/O 模块、现场变送器、中间继电器等提供工作电源,保证控制系统电路工作时只有一个统一的基准电位,不致因零电位浮动而引起信号的误差,同时可以提高防止外界电磁场干扰能力。

EDPF-NT Plus 系统所有电路采用浮空设计,直流电源负端不需要接地,电路中对地采用电容连接以达到释放静电和外部干扰,这样设计避免了整个系统对良好接地的依赖性。

b) EDPF-NT Plus 系统的接地要求。

由于 EDPF-NT Plus 系统的过程控制站及 I/O 设备的电路采用浮空设计,所以整个系统主要考虑机壳保护接地(CG)和信号屏蔽接地(SG),从实用性、经济性和可靠性等方面考虑,对系统接地有如下要求。

- 1) CG 与 SG 在机柜内连接,无需相互绝缘。
- 2) 为保证单点接地,机柜要求与现场安装槽钢绝缘,绝缘电阻 $>10\text{M}\Omega$ 。
- 3) 同排机柜或操作台的 CG 串联后从两侧分别引线至汇流铜排。
- 4) 整个系统与电气接地网之间只允许有一个连接点,接地电阻应小于 1Ω 。
- 5) 接地点周围 15m 半径内不允许有 6kV 及以上电气设备,且无避雷针的接地点。
- 6) 远程机柜或操作台可以就近接地,接地电阻及单点接地等要求与上述一致。

5

应急处理预案的总体要求

5.1 总则

5.1.1 为贯彻“安全第一、预防为主,综合治理”的方针,确保控制系统故障时,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,根据 AQ/T 9002 要求了制订分散控制系统典型故障应急处理预案。

5.1.2 为负责组织和统一协调应对控制系统故障时的应急处理,发电企业应建立控制系统故障应急组织体系,成立故障应急处理领导机构和故障现场应急处置组。

5.1.3 单元机组控制系统故障应急处理预案,在进行设备重大故障风险辨识,调研、收集、总结、提炼分散控制系统故障应急处理经验与教训的基础上,以热控设备的危险预测、预防为基础,以保障人身安全、电网安全、设备可控为目标,由热控、运行、机务专业人员联合编制。内容包括典型故障诊断与处理流程图、故障快速查找表、故障处理操作卡和故障现场处置预案。