

目 录

目 录

第一部分 降额设计规范	1
0、概述.....	1
1、降额总则.....	1
2、电阻降额.....	2
2.1、定值电阻	2
2.2、电位器	3
2.3、热敏电阻	3
3、电容降额.....	3
3.1、固定电容器	3
3.2、电解电容器	4
3.3、可调电容器	4
4、集成电路降额.....	4
4.1、放大器	4
4.2、比较器	5
4.3、电压调整器	5
4.4、模拟开关	5
4.5、双极性数字 IC	6
4.6、MOS 型数字电路.....	6
4.7、混合集成电路	6
4.8、大规模集成电路.....	7
5、分立半导体元件降额	7
5.1、晶体管	7
5.2、微波晶体管	7
5.3、二极管	8
5.4、可控硅	8
5.5、半导体光电器件.....	9
6、电感降额.....	9

目 录

7、继电器降额.....	9
8、开关降额.....	10
9、光纤器件降额.....	11
10、连接器降额.....	11
11、导线与电缆降额.....	12
12、保险丝降额.....	13
13、晶体降额.....	13
14、电机降额.....	13
15、灯泡降额.....	13
16、断路器降额.....	14
17、附录 1：根据功率-温度特性曲线计算降额曲线实例	14
18、附录 2：补充规范	14
第二部分 电子工艺设计规范.....	16
0、概述.....	16
1、PCB 板	16
1.1、PCB 尺寸与形状	16
1.2、PCB 基材	17
1.3、镀层.....	17
1.4、板层数.....	17
1.5、可生产性设计	18
2、焊盘、过孔.....	18
2.1、焊盘.....	18

目 录

2.2、导通孔	19
2.3、安装螺钉孔	19
3、布局规则.....	19
3.1、器件方向	19
3.2、器件布局	20
4、布线规则.....	21
4.1、PCB 布线镀层	21
4.2、布线规则	22
4.3、插座引脚走线	23
5、标识.....	23
5.1、标识类型	23
5.2、标识要求	24
6、可测试性设计	24
7、线缆.....	25
8、板级接地措施.....	25
第三部分 电气设备安全通用要求设计规范.....	27
0、概述.....	27
1、标记的要求.....	27
1.1、外部标记	27
1.1.1、外部标记要求.....	27
1.1.2、外部标记种类.....	27
1.2、内部标记	28
1.2.1、内部标记要求.....	28
1.2.2、内部标记种类.....	28
1.3、控制器件及仪表标记	29
1.3.1、控制器件及仪表标记要求.....	29
1.3.2、控制器件及仪表标记种类.....	29
1.4、导线	29
1.4.1、导线绝缘颜色.....	29

目 录

1.4.2、导线电流与导线规格的要求.....	30
1.5、气瓶、气体.....	30
1.5.1、气瓶或通气管内气体识别.....	30
1.5.2、气瓶连接点的标记.....	30
1.6、指示灯的颜色.....	30
1.7、不带灯按钮的颜色.....	31
1.8、符号.....	31
2、随机文件的要求.....	31
2.1、使用说明书的要求.....	31
2.2、技术说明书.....	32
3、环境条件.....	32
3.1、安全类型.....	32
3.2、环境条件.....	32
4、对电击危险的防护.....	33
4.1、剩余电压.....	33
4.2、剩余能量.....	33
4.3、外壳封闭性.....	33
4.4、不用工具就可以打开罩盖和门的安全性.....	34
4.5、灯泡的安全性.....	34
4.6、顶盖的安全性.....	34
4.7、控制器件的导体部件的电阻.....	34
4.8、带电部件的防护和标记.....	34
4.9、整机外壳安全性.....	35
4.10、调节孔安全性.....	35
4.11、应用部分的隔离.....	35
4.12、软轴的隔离.....	35
4.13、可触及部件的隔离.....	35
4.14、接地.....	36
4.14.1、电位均衡导线连接装置.....	36
4.14.2、保护接地阻抗.....	36
4.14.3、功能接地端子.....	36
4.14.4、功能接地线的标记.....	36
4.15、正常温度后的连续漏电流.....	37
4.16、电介质强度.....	37

目 录

4.16.1、正常温度后的电介质强度	37
4.16.2、潮湿预处理后的电介质强度	37
4.17、电气间隙和爬电距离要求	38
5、对机械危险的防护	39
5.1、外壳及零部件刚度	39
5.2、外壳及零部件强度	39
5.3、提拎装置承载能力	39
5.4、支承件承载能力	39
5.5、抗坠落性	39
5.6、抗搬运应力	40
5.7、运动部件的防护	40
5.8、传动部件的安全性	40
5.9、运动部件的可控性	40
5.10、易磨损部件的可查性	40
5.11、电控机械运动安全性	40
5.12、紧急装置可靠性	40
5.13、面、角和边	41
5.14、设备稳定性	41
5.15、可搬运性	41
5.16、防飞溅物能力	41
5.17、有安全装置的悬挂系统	41
5.18、无安全装置的金属悬挂系统	42
5.19、外壳结构	42
6、对气体危险的防护	43
6.1、位置要求	43
6.2、APG 和 AP 型设备标记	43
6.3、AP 和 APG 型设备随机文件	43
6.4、外壳结构	43
6.5、AP 型设备性能要求	44
7、电气连接	45
8、静电防护	45
9、电晕	45

目 录

10、超温与防火.....	45
10、溢流.....	45
11、液体泼洒.....	46
12、泄漏.....	46
13、受潮.....	46
14、进液.....	46
15、清洗、消毒和灭菌.....	46
16、压力释放装置.....	47
17、自动复位装置 的选择.....	47
18、电源中断后的复位.....	47
19、电源中断后机械压的解除.....	47
20、危险输出的防止.....	47
20.1、有意地超过安全极限.....	47
20.2、有关安全参数的指示.....	48
20.3、意外地选成过量的输出.....	48
21、必须考虑的安全方面要危险.....	48
22、单一故障的要求.....	48
23、元器件的要求.....	49
23.1、元器件的标记.....	49
23.2、元器件的固定.....	49
24、连接的要求.....	49
24.1、电线的固定.....	49
24.2、连接器的构造.....	49

目 录

24.3、部件之间的连接.....	49
24.4、电容器的连接	50
25、保护装置.....	50
26、温度和过载控制	50
27、电池.....	50
28、指示灯.....	51
29、控制器的操作部件	51
30、有电线连接的手持式和脚踏式控制装置	51
31、与供电网的分断	52
32、辅助网电源输出插座	52
33、电源软电线.....	52
34、电源软电线的连接	53
35、网电源.....	53
35.1、网电源接线端子和布线	53
35.2、网电源熔断器和过电流释放器.....	54
35.3、网电源部分的布线.....	54
35.4、电源变压器	54
36、保护接地端子和连接	55
37、内部布线.....	55
38、绝缘.....	56
39、过电流和过电压保护	56
第四部分 嵌入式软件可靠性设计规范	57

目 录

0、概述	57
1、定义	57
1.1、定义.....	57
1.2、说明.....	57
2、计算机系统设计	58
2.1、一般要求.....	58
2.2、硬件与软件功能的分配原则	58
2.3、硬件与软件可靠性指标的分配原则.....	58
2.4、安全关键功能的人工确认.....	59
2.5、安全性内核.....	59
2.6、自动记录系统故障	59
2.7、禁止回避检测出的不安全状态	59
2.8、保密性设计	59
2.9、容错设计.....	60
2.10、安全关键软件的标识原则.....	60
3、硬件设计	60
3.1、硬件选用.....	60
3.2、总线检测.....	60
3.3、加电检测.....	60
3.4、电源失效的安全措施.....	61
3.5、主控计算机失效的安全措施.....	61
3.6、反馈回路传感器失效的防护措施	61
3.7、电磁干扰的防护措施.....	61
3.8、维修互锁措施	61
4、软件需求分析	61
5、软件风险分析	62
6、安全关键功能的设计	62
7、冗余设计	62
7.1、指令冗余设计	62

目 录

7.2、软件陷阱与软件拦截技术	63
7.3、软件冗余	65
8、接口设计	66
8.1、硬件接口要求	66
8.2、硬件接口的软件设计	66
8.3、人机界面设计	66
8.4、报警设计	67
8.5、软件接口设计	67
9、软件健壮性设计	68
9.1、电源失效防护	68
9.2、加电检测	68
9.3、电磁干扰	68
9.4、系统不稳定	68
9.5、接口故障	68
9.6、干扰信号	69
9.7、错误操作	69
9.8、监控定时器的设计	69
9.9、异常保护设计	69
10、简化设计	69
10.1、单入和单出	69
10.2、模块的独立性	70
10.3、模块的扇入扇出	70
10.4、模块耦合方式	70
10.5、模块内聚顺方式	70
10.6、其他特殊考虑	71
11、余量设计	71
11.1、资源分配及余量要求	71
11.2、时序安排的余量要求	71
12、数据要求	71
12.1、数据需求	71
12.2、属性控制	72

目 录

12.3、数值运算范围控制	72
12.4、合理性检查	72
13、防错程序设计	72
13.1、参数化.....	72
13.2、公用数据和公共变量.....	72
13.3、标志.....	72
13.4、文件.....	73
13.5、非授权存取的限制	73
13.6、无意指令跳转的处理.....	73
13.7、程序检测点的设置	73
13.8、寻址模式的选用	74
13.9、数据区隔离	74
13.10、安全关键信息的要求.....	74
13.11、信息存储要求	74
13.12、算法选择要求	74
14、编程要求.....	75
14.1、语言要求	75
14.2、汇编语言编程限制	75
14.3、高级语言的编程限制.....	75
14.4、圈复杂度指数（MCCABE）	75
14.5、软件单元的规模	76
14.6、命名要求.....	76
14.7、程序格式要求.....	76
14.8、程序注释要求与方法.....	77
14.8.1、注释的一般要求.....	77
14.8.2、模块头注释要求.....	77
14.8.3、模块内注释要求.....	77
14.8.4、安全关键内容注释要求.....	78
14.9 程序设计风格	78
14.9.1、通用类.....	78
14.9.2、结构类.....	79
14.9.3、说明类.....	79
14.9.4、输入输出类.....	79
14.9.5、语言类.....	80

目 录

15、多余物的处理	80
15.1、文档中未记载特征的清除.....	80
15.2、程序多余物的清除.....	80
15.3、未使用内存的处理.....	80
15.4、覆盖的处理.....	81
16、软件更改要求	81
17、嵌入式软件测试	82
17.1、需求遗漏或不明确.....	82
17.2、配置保存的生效.....	82
17.3、缺省配置的影响.....	82
17.4、报警和清除.....	82
17.5、菜单选项测试.....	82
17.6、缺省配置测试.....	83
17.7、系统测试注意事项.....	83
附录 1：推荐的软件安全关键程度分级	83
附录 2：软件开发各阶段的适用准则和要求	84
第五部分 EMC 设计规范	85
0、概述	85
1、机械结构	85
1.1、材料.....	85
1.2、机壳喷涂工艺及接缝.....	85
1.3、机壳开口.....	87
2、整机外部接口	87
2.1、按键面膜.....	87
2.2、电源接口.....	88
2.3、显示窗口.....	89
2.4、信号接口.....	89

目 录

3、接地	89
4、电路板	90
4.1、电路原理图设计	90
4.1.1、面膜电路.....	90
4.1.2、复位电路.....	92
4.1.3、片选输入口.....	92
4.1.4、敏感电路.....	92
4.1.5、电路板接口.....	92
4.1.6、总线信号质量控制.....	93
4.1.7、退耦电容.....	93
4.1.8、晶振电路.....	94
4.1.9、显示电路.....	95
4.1.10、供电与驱动电路.....	95
4.2、布线.....	95
4.2.1、PCB 布线	95
4.2.2、线缆布线.....	97
4.3、元器件布局.....	97
4.4、安装固定.....	98
4.4.1、绝缘安装.....	98
4.4.2、电气间隙.....	98
4.4.3、爬电距离.....	98
4.5、EMC 元器件选型.....	99
4.5.1、EMC 防护器件选型注意事项	99
4.5.2、其他器件选型注意事项.....	100
5、接插件和电缆分类	102
5.1、接插件的选型	102
5.2、接插件信号线的排布.....	103
5.3、接插件的安装	103
5.4、电缆设计与安装	103
第六部分 电气开发流程设计活动规范	105
0、概述	105
1、立项	105

目 录

1.1、立项.....	105
1.2、调研.....	106
2、策划.....	106
3、方案阶段.....	108
3.1、方案设计	108
3.1.1、输入输出内容.....	108
3.1.2、技术信息收集.....	108
3.1.3、总体设计.....	109
3.1.4、配附件要求.....	109
3.2、方案评审	110
3.2.1、输入输出内容.....	110
3.2.2、方案评审的内容.....	110
4、样机阶段.....	111
4.1、样机设计	111
4.1.1、输入输出内容.....	111
4.1.2、输入确认.....	111
4.1.3、结构沟通.....	112
4.1.4、电气设计.....	112
4.1.5、软件设计.....	113
4.1.6、配附件.....	113
4.1.7、随机文档.....	114
4.2、样机测评	114
4.2.1、输入输出内容.....	114
4.2.2、测评过程活动.....	114
4.3、样机评审	115
4.3.1、输入输出内容.....	115
4.3.2、评审内容.....	115
5、中试阶段.....	116
5.1、中试图纸提交	116
5.1.1、物料编码申请.....	116
5.1.2、中试图纸提交.....	116
5.1.3、输入输出.....	117
5.2、工艺文件	117
5.2.1、设计输入输出内容.....	117
5.2.2、工艺文件.....	117
5.3、中试实施	117

目 录

5.3.1、输入输出内容.....	117
5.3.2、中试过程活动.....	118
5.4、工艺评审.....	118
5.4.1、工艺评审的输入输出.....	118
5.4.2、工艺评审内容.....	119
6、结项.....	119
6.1、图纸修改归档.....	119
6.1.1、归档的输入输出.....	119
6.1.2、归档文件内容.....	119
6.2、项目评审.....	121
6.2.1、项目评审的输入要素.....	121
6.2.2、项目评审的内容和过程活动.....	121
6.2.3、项目评审的输出.....	121