指导性文件
GUIDANCE NOTES
GD16-2017

中 国 船 级 社

故障模式和影响分析应用指南

2017

生效日期：2017 年 9 月 1 日
北京

目 录

第1章　通 则

1.1 一般要求

1.1.1 本指南对故障模式和影响分析（Failure Mode & Effects Analysis，简称 FMEA）的一般方法进行了规定，提出了 FMEA 在高速船、动力定位系统、双燃料发动机、柴油机电控系统等方面的技术要求，并给出了动力定位系统 FMEA 应用示例，旨在为实施本社规范及国际海事组织（IMO）强制性文件所要求的 FMEA 提供指导。

1.1.2 FMEA 是一种对系统进行分析，以识别潜在故障模式、故障原因及其对系统性能（包括部件、系统或过程的性能）影响的系统化程序。

1.1.3 FMEA 应尽可能在开发周期的早期阶段开始进行，并将 FMEA 报告作为图纸资料的一部分提交本社批准或备查，且 FMEA 试验应纳入船厂试验计划。

1.2 分析目的和目标

1.2.1 进行 FMEA 的目的包括：

（1）识别对系统工作产生有害影响的故障，如系统运行终止、系统运行显著退化、影响船舶航行安全或人员安全等；

（2）提高系统的可靠性和安全性（如：通过设计修正或质量保证行动）；

（3）提高系统的维修性（通过关注有风险的区域或与可维护性不相符的地方）；

（4）协助挑选具有高可靠性的替代性设计方案。

1.2.2 FMEA 的目标包括：

（1）在系统各功能级别上，全面识别和评估由任何原因引起的故障模式及其带来的不期望的影响和事件序列；

（2）确定与系统正常功能或性能有关的每一故障模式的危害度，定位/减轻每一故障模式的优先顺序及其对相关过程的影响；

（3）找出消除或减少每个故障模式的风险控制措施，包括设计改进计划和维护计划；

（4）确定必要的试验和测试以证明相关结论；

（5）信息提供给操作和维护人员，让他们了解系统能力和局限性以实现最佳性能。

1.3 术语和定义

1.3.1 下述定义适用于本指南：

（1）**产品**（Item）：任何能完成预定功能并被单独考虑的部件、装置、功能单元、设备、子系统或系统。能完成预定功能的过程也能被定义为产品，并可进行过程 FMEA。通常，硬

件的 FMEA 不考虑人以及他们与硬件/软件的相互作用，而过程 FMEA 通常包括人的行为。

（2）**部件**（Component）：系指系统组成的基本元件或产品，如传感器、处理器、电磁阀等。

（3）**系统**（System）：相关或相互影响要素的集合。在 FMEA 范畴里，一个系统具有：

.1 根据所需功能确定的目标；

.2 规定的工作使用条件；

.3 确定的边界；

.4 分级的系统结构。

（4）**故障**（Failure）：产品执行规定功能能力的终止。

（5）**故障原因**（Failure Cause）：在设计、制造或使用过程中导致故障的情况。

（6）**故障影响**（Failure Effect）：故障模式对产品运行、功能或状态导致的后果。

（7）**故障模式**（Failure Mode）：产品故障的表现形式。

（8）**故障率**（Failure Rate）：单位时间内故障发生的次数。

（9）**故障概率**（Failure Probability）：故障发生的置信度，衡量标准为从 0 至 1。概率为 0 的事件系指相信该故障不可能发生；概率为 1 的事件系指相信故障肯定发生。

（10）**故障严重度**（Failure Severity）：故障模式对产品工作、环境和操作者影响的严重程度；故障模式影响严重度与分析所定义的系统边界有关。

（11）**故障危害度**（Failure Criticality）：故障严重度与故障率或其他属性的综合，作为处理和减缓故障影响的必要性尺度。

（12）**隐性故障**（Hidden Failure）：操作和维护人员不能立即发现的故障。

（13）**功能**（Function）：是指系统或设备产品按照设计所能做的。每个功能应被记录为包含一个用于描述功能的动词，功能目标和性能标准的功能说明。

（14）**设计目的**（Design Intent）：系指由设计者确定的想法、理念、衡准的详细描述，一般包括系统要求、设计条件、系统限制。

（15）**重要服务**（Essential Services ）：系指对设计目的和柴油机安全运行必要的设备和系统，如燃油供应、气缸润滑、废气门控制等。

（16）**冗余**（Redundancy）：为增加系统的可靠性，而采取两套或两套以上关键部件或功能的设计。

（17）**可靠性**（Reliability）：在特定条件下和一段时间内，产品按规定功能运行的能力。可靠性=1-故障率。

（18）**共因失效**（Common Cause Failure，CCF）：因单一条件导致多个部件，子系统或系统同时故障的故障模式。

（19）**系统边界**（System Boundary）：系统边界构成了系统与环境两者之间的物理和功能界面，包括与该系统相互影响的其他系统。为分析而定义的系统边界应与系统设计和维修

所定义的边界相对应，该原则应应用于系统的任何层次。应当明确处于界限之外的系统和/或元部件，以便分析时排除。

（20）**接口**（Interface）：系指独立系统或部件相互作用或通信的点。

第2章　FMEA 一般方法

2.1 一般要求

2.1.1 一般而言，FMEA 有多种实施方法和表达形式，通常通过识别故障模式、相关的故障原因以及故障的直接和最终影响实现。分析结果用工作表来表示，这张工作表的核心内容包括整个系统的基本信息和详细资料。该表给出系统可能发生潜在故障的途径、部件及其可能导致系统故障的故障模式和每种故障模式的发生原因。

2.1.2 开展 FMEA 时，包括以下 4 个主要阶段，详细流程见图 2.1.2 所示：

（1）开展 FMEA 的准备：确定 FMEA 的基本原则，制定 FMEA 计划，准备分析所需数据和相关信息，以及保证分析有足够的时间和专业技术；

（2）开展 FMEA：选用合适的工作表实施 FMEA，或者采用其他方法，例如逻辑图或故障树；

（3）对分析进行总结并编写报告，包括所有的结论及建议；

（4）随着设计工作的深入及相关试验和测试情况，必要时可根据设计上的更改进一步更新 FMEA。

2.1.3 系统设计如在船舶寿命周期内发生变更，则应依据原 FMEA 对这种变更进行分析，记录分析结果并作为 FMEA 的附件。

2.2 制定分析计划

2.2.1 FMEA 及其后续活动、步骤、与其他可靠性活动之间的关系、纠正措施的实施、闭环过程和时间节点，都应纳入整个程序计划。

2.2.2 确定所使用的 FMEA 方法和标准，作概要性阐述即可。

2.2.3 该计划应包含以下要点：

（1）明确定义分析的目的和预期结果；

（2）与客户/船东讨论确定 FMEA 的范围；

（3）阐述当前分析是如何支持整个项目的可信性；

（4）组建包括设计专家在内的分析团队；

（5）明确项目进度的关键时间节点，确保分析及时进行；

（6）减轻已识别故障模式的过程中采取的所有措施，明确其闭环方式。

2.2.4 计划书应反映多数参与者的意见，并得到项目管理者的认可。

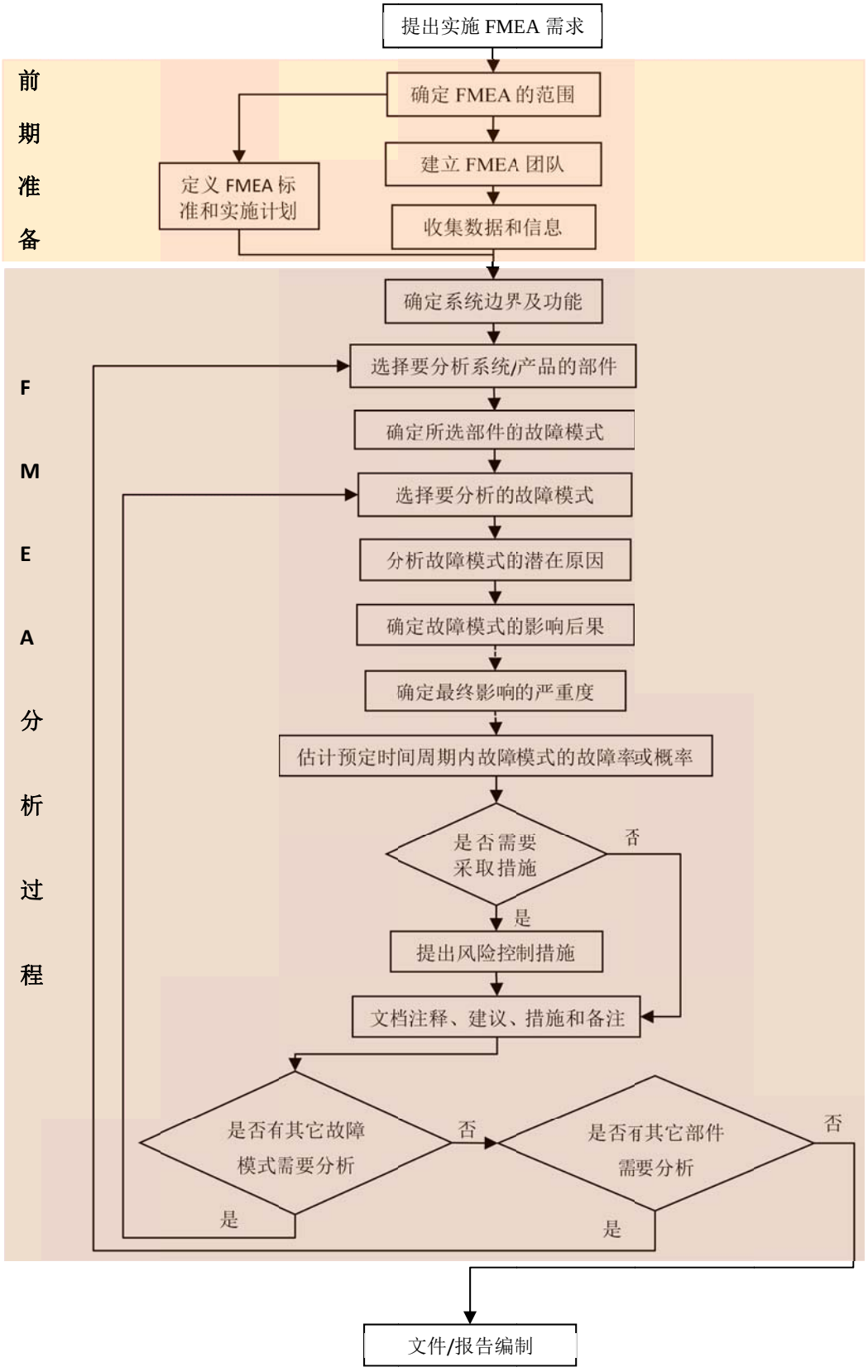

提出实施 FMEA 需求
前期准备
确定 FMEA 的范围
建立 FMEA 团队
定义 FMEA 标准和实施计划
收集数据和信息
FMEA分析过程
确定系统边界及功能
选择要分析系统/产品的部件
确定所选部件的故障模式
选择要分析的故障模式
分析故障模式的潜在原因
确定故障模式的影响后果
确定最终影响的严重度
估计预定时间周期内故障模式的故障率或概率
是否需要采取措施
否
是
提出风险控制措施
文档注释、建议、措施和备注
是否有其它故障模式需要分析
否
是否有其它部件需要分析
否
是
文件/报告编制

图 2.1.2 分析流程图

2.3 数据和相关信息的准备

2.3.1 FMEA 需要有关系统、部件足够详细的数据和信息，以便对各部件出现故障的方式进行有意义的分析。

2.3.2 数据和信息可能包括：

（1）正在分析的系统及系统部件的图形，或者过程步骤的流程图；

（2）了解过程中每一步或系统组成部分的功能；

（3）可能影响运行的过程及环境参数的详细信息；

（4）对特定故障结果的了解；

（5）有关故障的历史信息，包括现有的故障率数据。

2.4 FMEA 过程

2.4.1 明确系统边界（包括物理边界和操作边界）及系统功能的定义，将系统分成部件或步骤，并绘制功能框图；

2.4.2 对于列出的各部件或步骤，确认：

（1）定义故障的判定标准；

（2）分析故障模式，即故障的表现形式：各部分出现明显故障的方式是什么？

通用的故障模式示例　　表 2.4.2

序号	故障模式
1	运行中故障
2	在规定的时刻，无法运行
3	在规定的时刻，无法停止运行
4	提前运行

注：这只是例子，不同类型的系统需要不同的清单。

（3）分析故障原因：造成这些故障模式的具体机制？

（4）分析故障影响：即故障导致的各种后果，包括对部件自身的局部影响、对系统的影响、对总体（船舶）的影响；

（5）探寻故障探测方法：故障如何探测？

2.4.3 一旦确定故障模式和机制，就可以提出可能的预防改进措施，包括：

（1）一个或多个单元故障时，能使系统继续正常运行的冗余产品；

（2）备选的运行方式；

（3）监控或报警装置；

（4）允许有效运行或限制损害的其他手段。

2.4.4 系统 FMEA 一般应按自上而下方式进行，分析时从总系统层开始，然后进行到下一层或子系统，再到设备或部件层。但是，如分析表明，在总系统层和部件层之间的某一水

平上，故障对整个系统没有进一步的影响，那么就没有必要继续下一层分析。

2.5 危害性分析

2.5.1 若需要，且在分析成本、时间和资源条件允许情况下，FMEA 可以进一步扩展，开展危害性分析，目的是确定每一种故障影响的相对大小，为决策提供帮助。可综合故障模式的严重度和故障概率，确定减轻或消除特定故障影响采取措施的优先顺序。这种分析通常是定性或半定量的，最常用的方法是风险等级。

2.5.2 故障模式的风险等级由故障严重度与故障概率的组合获得。此方法适用于不同故障模式的不同后果，并且能够应用于设备、系统或过程。

风险 = 故障概率×严重度

log(风险) = log (概率) + log (后果)

风险指数（RI）= 概率指数（PI）+ 严重度指数（SI）

危害性可以用风险矩阵表征，如图 2.5.2 所示。将故障发生概率和严重度分为几个等级，随后将概率和严重度置于一个矩阵中，该矩阵即为风险矩阵。该矩阵一般可分为三个区域：高风险区域，低风险区域，以及两者之间的临界区域。应注意的是：危害性并没有统一的定义，但分析人员应对其定义，并得到项目或程序管理者的认可。

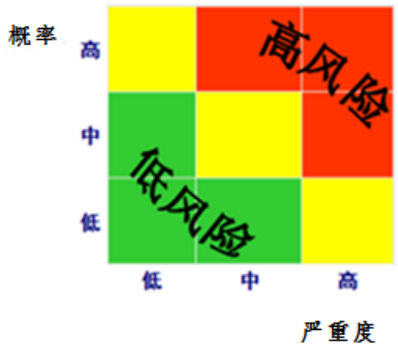


图 2.5.2 风险矩阵

2.5.3 下面示例说明故障模式的发生概率、严重度及风险的定义和等级划分。表 2.5.3.1 至表 2.5.3.3 只是个例子，在具体应用中，可能用不同的等级划分来表示故障模式的危害性。

概率等级划分示例　　表 2.5.3.1

PI	概率	定义
5	10^{-1}	经常发生
4	10^{-2}	有时发生-在产品周期内可能发生几次
3	10^{-3}	偶尔发生-在产品周期的某一时间可能发生
2	10^{-4}	很少发生-不太可能发生但有可能性
1	10^{-5}	极少发生-完全不太可能发生

严重度等级划分示例 **表 2.5.3.2**

SI	严重度	定义
4	灾难	导致整个系统破坏、人身伤亡或严重污染
3	严重	系统严重破坏，人员严重伤害和轻微污染
2	临界	对系统性能、污染不会产生严重破坏，或对人员不会产生严重伤害
1	轻微	系统或过程的局部功能故障，对人员安全、系统性能或污染产生的影响较低

故障风险等级划分示例 **表 2.5.3.3**

	PI	1	2	3	4	5
SI		极少	很少	偶尔	有时	经常
4	灾难	5	6	7	8	9
3	严重	4	5	6	7	8
2	临界	3	4	5	6	7
1	轻微	2	3	4	5	6

2.5.4 故障可探测度等级。在一些 FMEA 应用中，还对探测到的故障可能性进行评估。也就是，设计特性/辅助工具或验证过程能够及时探测潜在故障模式的可能性，防止系统级故障发生。在过程应用中，可探测度指在故障传递到下道工序或最终产品输出前，一整套的现场过程控制能探测到故障并将其隔离的可能性。

2.5.5 风险可接受衡准的评估。在得到由各种故障模式的风险指数所构成的风险矩阵后，还需要定义风险可接受衡准，即故障模式在何种风险指数下可接受、可容忍或不可接受。风险可接受衡准可定性定义，并受专业水平和财务决策影响，在不同的应用领域中也不同。一般需要考虑：

（1）相关的船级社规范和法规要求；

（2）系统或设备制造商提供的系统运行衡准；

（3）对于发动机，可参考 IACS UR M44 附录 3“设计”，例如，单推进发动机装置应比多个发动机推进装置具有更严格的可接受衡准，例如更高冗余容错要求和设计，这意味着系统可以在一定数量和某些类型故障模式下能保持安全运行。

2.6 FMEA 试验

2.6.1 FMEA 时所作的一些假定及分析得出的结论，应通过相关试验予以验证和确认，证明所识别的风险及其后果已经消除或有效控制，或者为控制风险影响而采取的措施有效。

2.6.2 试验是 FMEA 过程中的一部分，两者不能相互孤立。FMEA 将在最后分析中使用试验结果，并将试验测试表纳入到 FMEA 报告中。

2.6.3 FMEA 试验的设计应反映出整个系统在故障模式下的性能，同时应确保试验彻底和完整，以最大可能在试验期间发现不可接受的故障。

2.6.4 FMEA 试验程序应包括试验目的，试验中船舶和设备的安装程序，如何引发或模拟设备故障，以及故障导致的可能后果。

2.7 编制 FMEA 报告

2.7.1 通过 FMEA，列出识别的故障模式，及其原因和可能的影响，列出进一步分析的建议。典型的 FMEA 工作表如下：

FMEA 工作表 **表 2.7.1**

时间：_____ 页数：_____ of _____

船舶：_____ 系统：_____

参考文献：_____ 团队成员：_____

序号	设备	功能	故障模式	故障原因	故障影响		危害性分析（如适用）			故障探测方法	建议采取的行动	备注/试验
					局部	全局	故障严重度	故障概率	故障风险			

2.7.2 FMEA 报告可以包含在一个很大的研究项目中，也可以独立出来。无论何种情况，报告内容应该包括详细的分析记录和总结，以及定义系统结构的功能图和框图。故障模式报告记录的内容包括：

（1）执行概要。

（2）介绍：

.1 FMEA 介绍；

.2 评估范围；

.3 FMEA 程序或方法论；

.4 船舶申请方及详情；

.5 分析中的假设，例如分析时船舶的操作模式等；

.6 相关文件。

（3）分析方法：

.1 框图；

.2 FMEA 工作表；

.3 如开展危害性分析，危害度（风险指数）以及界定危害性的方法；

.4 FMEA 改进工作报告。

（4）分析系统的详细说明，例如：

.1 DP 控制系统；

.2 电气系统；

.3 轮机系统；

.4 安全系统。

详细列出所有重大故障模式的信息及其 FMEA 建议。

（5）建议，有关进一步分析、设计变更或者计划纳入测试计划的特征等方面的建议，以及采取的措施。

（6）结论。

（7）附件，例如：

.1 工作表；

.2 试验测试表；

.3 问答清单；

.4 FMEA 报告表；

.5 船厂和设备供应商清单。

2.8 FMEA 的更新

2.8.1 FMEA 是一个随设计深入而反复更新的过程，设计上的更改要求对 FMEA 的相应部分进行评审和更新。因此在完成上述分析之后，如合适需通过另一轮 FMEA 重新评估系统。

2.9 输出结果

2.9.1 FMEA 的主要输出结果是故障模式，故障机制及其对各部件或者系统或过程步骤影响的清单（可能包括故障可能性的信息），也能提供有关故障原因及其对整个系统影响方面的信息。

2.9.2 危害性分析的输出包括：故障模式危害性的排序，基于系统故障可能性、故障模式的风险水平，或者风险水平和故障模式的“可探测性”的组合等。如果有合适的故障率资料和定量后果，危害性分析可以输出定量结果。

2.10 FMEA 在风险评估中的应用

2.10.1 根据评估对象的不同，FMEA 可用于以下几种应用：

（1）用于部件和产品的设计（或产品）FMEA；

（2）用于系统的系统 FMEA；

（3）用于制造和组装过程的过程 FMEA；

（4）服务 FMEA；

（5）软件 FMEA。

2.10.2 FMEA 可以单独使用。作为一种系统性地归纳方法，FMEA 也常用于其他分析方法的补充，尤其是那些演绎性分析方法，如故障树分析（FTA）等。

2.10.3 风险评估包括了风险识别、风险分析和风险评价的全过程。FMEA 作为一种风险评估的工具和技术，非常适用于风险评估中的风险识别。

2.10.4 在考虑风险评估选用何种分析方法时，主要依据项目的特定要求，不仅是关于技术方面的要求，也包括时间、成本、效率和结果用途等方面的要求。以下是一些总的指导原则：

（1）需要对部件的故障特征全面了解时，适宜采用 FMEA；

（2）FMEA 更适用于小型系统、模块或部件；

（3）在研究开发或设计阶段，需要识别不期望的故障影响并寻求解决方法时，FMEA 是一种基本的分析工具；

（4）对那些采用了新设计、并且无法从以前的使用经验中获得故障特征的部件，进行 FMEA 是必要的；

（5）当系统有大量以串联故障逻辑相连的元部件时，采用 FMEA 往往就更适合；

（6）FTA 通常更适用于分析多重故障模式以及含有复杂故障逻辑和冗余的故障相关性。在早期设计阶段，FTA 可用于系统结构中的较高层次分析，这有助于确定在详细设计阶段对较低层次进行 FMEA 的必要性。

第3章　高速船 FMEA 应用

3.1 一般要求

3.1.1 每艘高速船在投入营运之前，应对船舶的方向控制系统、机械系统及其控制装置、电力系统和稳定系统完成 FMEA。

3.1.2 对设计相同并具有相同设备的船舶，只需对首制船进行一次 FMEA，但每艘船应进行相同 FMEA 结论的试验。

3.1.3 对高速船，FMEA 是建立在单个故障概念基础上的，据此在系统功能体系的各个状态的每一个系统，在任一时刻，假定其他可能由于一个原因发生的故障。该假定故障的影响按期严重性进行分析和分类。这些影响可以包括在其他程度上的次级故障（或多重故障）。任何可能引起船舶灾难性后果的故障模式应通过系统或设备冗余加以防范，除非这种故障的概率为极不可能。对于引起危险后果的故障模式，可以接受纠正措施来代替。应制定试验程序以确认 FMEA 的结论。

3.1.4 高速船的 FMEA 程序、基本方法和要求按本指南第 2 章和 2000 年国际高速船安全规则（HSC 2000）附录 4 执行。

3.1.5 本章规定的高速船 FMEA 的系统（装置），并不意味必须按照规定的系统（装置）进行独立的分析，可根据船舶实际情况确定 FMEA 的系统，特别是由同一系统（装置）完成不同的功能，例如：方向控制和推进为同一系统。

3.2 系统 FMEA

3.2.1 在对系统部件故障关于系统功能输出所产生的影响进行详细的 FMEA 之前，必须先对船舶重要系统进行故障分析，这样，仅对那些功能故障分析失败的系统需通过更详细的 FMEA 进行分析（设备故障模式与影响分析）。

3.2.2 当实施系统 FMEA 时，应考虑以下船舶正常设计环境条件中的典型操作模式：

（1）正常情况下全速航行；

（2）拥挤水域中最大允许操作航速；

（3）靠离码头。

3.2.3 为使故障影响易于被理解，这些系统的功能相互关系还应以框图加以说明或以叙述方式说明。所要分析的每个系统应尽可能假定在以下故障模式下失效：

（1）完全失去功能；

（2）迅速改为最大或最小输出；

（3）输出不受控制或改变输出；

（4）过早操作；

（5）在规定时间不能操作；和

（6）在规定时间不能停止运转。

根据所考虑的系统，其他故障模式也可计及。

3.2.4 如果系统故障不会造成危险性后果或灾难性后果，就不必将详细的 FMEA 引进系统结构。对那些个别故障能造成危险性后果或灾难性后果的系统，且无备用系统，则应进行更详细 FMEA。系统功能故障分析的结果应通过按分析所拟定的实际试验程序来说明和证实。

3.2.5 如果一个可能因其故障而造成危险性后果或灾难性后果的系统配有一个备用系统，就可不要求详细的 FMEA，但其前提是：

3.2.5.1 备用系统能在 3.2.2 所述的典型操作模式的时间限制内，投入运转或接替故障的系统而不危及船舶；

3.2.5.2 备用系统完全独立于该系统，并且不共用会导致该系统和备用系统都会发生故障的公共系统部件。如果故障概率符合规定的概率衡准（参见 HSC 2000 附录 4/13）要求，则公共系统部件可予以接受；和

3.2.5.3 备用系统可以与该系统共用同一动力源，在这种情况下，备用动力源应能按本条 3.2.5.1 的要求迅速投入运行。

3.2.5.4 还应考虑操作者失误，引进备用系统的可能性和后果。

3.3 设备 FMEA

3.3.1 要在这方面作更详细 FMEA 研究的系统应包括所有那些系统 FMEA 已经失败的系统，并且可以包括对船舶及其乘员的安全性有非常重要影响的系统，以及包括要求作较系统功能故障分析更深一层的系统。这些系统常常专门为船舶设计或采用的，例如船舶的电力和液压系统。

3.4 各系统（装置）的 FMEA 要求

3.4.1 方向控制系统

3.4.1.1 方向控制系统包括任何操舵装置或装置组群、任何机械联动装置和所有动力或人力装置、控制器和驱动系统。

3.4.1.2 方向控制系统应按 3.2 和 3.3 规定完成 FMEA，并应考虑 3.2.2 规定的船舶正常设计环境条件中的典型操作模式。

3.4.1.3 方向控制系统的 FMEA 结果（并经试验验证）应满足‘除诸如搁浅、碰撞或重大火灾的紧急情况外，船舶在正常运行时，所有方向控制系统完全故障的可能性应极小’的规定要求。

3.4.1.4 FMEA 应对方向控制系统的构造进行分析，若适用，应使一个驱动装置或系统内

出现的单一故障不会导致任何一个其他装置或系统不能工作或不能使船舶处于安全状态。主管机关可以允许有短暂时间用于连接辅助控制装置，只要船舶的设计使主管机关认为这种延迟不致危及船舶安全。

3.4.1.5 对于利用船舶的可变几何形状或船舶的垫升系统部件的方向控制系统，应经FMEA验证其驱动联动装置或驱动系统的任何故障不会严重危及船舶安全。

3.4.2 机械系统及其控制装置

3.4.2.1 机械系统及其控制装置应按3.2和3.3规定完成FMEA。

3.4.2.2 FMEA应对单一的主要推进部件的可靠性予以特别考虑。对设有分离的推进动力源，FMEA应分析其冗余性。

3.4.2.3 应对船舶主要辅机（系统）进行FMEA，以证明即使主要辅机之一不能工作时，也能使推进机械的正常运行得以维持或恢复。应对下列装置的故障予以特别考虑：

（1）主发电机；

（2）发动机燃油供应系统；

（3）润滑油压力源；

（4）水压力源；

（5）起动或控制用空气压缩机和空气瓶；

（6）控制推进主机包括调距桨所用的液压、气动或电动装置。

3.4.3 电力系统

3.4.3.1 电力系统应按3.2和3.3规定完成FMEA。

3.4.3.2 若设备有可能会产生在常规检查中未能发现的故障时，FMEA 应考虑故障同时或连续发生的可能性。

3.4.3.3 电力系统的FMEA应验证电力系统的设计和安装使船舶在营运中因电力故障而发生危险的可能性降至最低。

3.4.3.4 若电力供应的故障会严重危害船舶安全，则应设有纠正措施如在规定时间内启动备用电源等，以消除或减轻故障的后果。

3.4.3.5 特定的重要设备若缺损会严重危害船舶安全，则该设备应至少由两条独立线路供电，以消除或减轻故障的后果。

3.4.4 稳定系统

3.4.4.1 稳定控制系统系指以稳定船舶状态主要参数（横倾、纵倾、航向、高度）及控制船舶运动（横摇、纵摇、首摇、升降）的一种系统，主要包括：执行机构、驱动执行机构的动力机械以及搜集和处理数据并作出判断、发出指令的稳定设备。

3.4.4.2 设有自动稳定控制系统或自动稳定控制系统及手控辅助相结合的联合系统的，应按3.2和3.3规定完成FMEA，并应考虑3.2.2规定的船舶正常设计环境条件中的典型操作模式。

3.4.4.3 稳定系统的 FMEA 结果（包括限制措施，并经试验验证）应满足‘当任一自动设备或稳定装置或其动力驱动故障时，船舶的运动参数仍应保持在安全极限内’的规定。

3.4.4.4 装有侧向与高度控制系统的，还应考虑 HSC 2000 附录 3 第 2.4 节给出的安全值以及与该特定船舶及其用途相适应的安全运动值。

3.5 FMEA 报告及其示例

3.5.1 FMEA 报告应是一份完备的文件，其应对船舶、船舶的系统及其功能、建议的操作和故障模式、原因及后果和环境条件进行充分的阐述，且均不必借助于不在该报告之内的其他图纸和文件而能够被理解。如需要，该文件应包括分析的假设和系统框图，报告应包含结论的摘要，以及系统故障分析和设备故障分析中的每一个分析系统的说明。如需要，还应列出所有可能的故障及其故障概率，在每一种所分析操作模式中对每一个系统的纠正措施或操作限制。该报告应包含有试验程序、所参考的所有其他试验报告和 FMEA 试验。

3.5.2 基于 3.5.1 的要求，报告中应包含以下内容：

（1)图纸资料，包括船舶基本概况以及包含下列有关系统及其功能要求的叙述说明等：系统操作和结构的一般说明、系统部件之间的功能关系、在每一种典型的运行模式中系统及其组成部件的可接受的功能限制以及系统约束；

（2）分析的假设和系统框图、分析说明、结论摘要；

（3）如需要，还应列出所有可能的故障及其故障概率，在每一种所分析操作模式中对每一个系统的纠正措施或操作限制。

（4）试验程序、所参考的所有其他试验报告和 FMEA 试验；

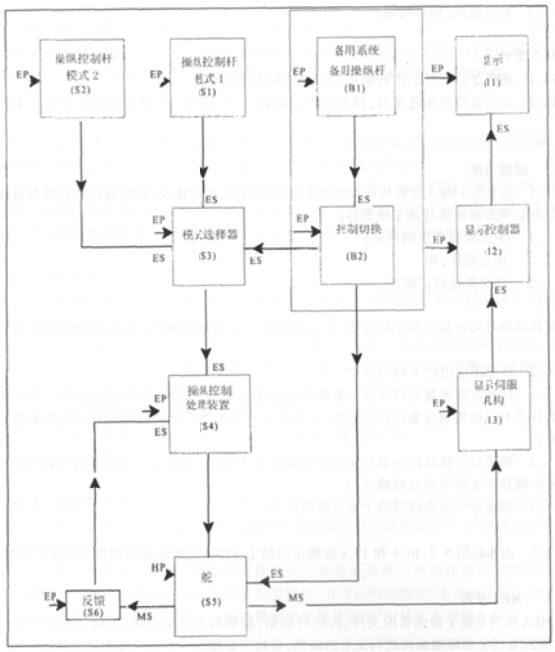
（5）工作表格。

3.5.3 报告示例

3.5.3.1 系统框图

操舵控制系统　　日期：_____

分析者：_____



其中：EP-电力；HP-液压力；ES-电信号；MS-机械信号

3.5.3.2 FMEA 工作表

FMEA 工作表 **表 3.5.3.2**

系统名称：_____ 参考：_____

操作模式：_____ 系统框图：_____

工作单编号：_____ 日期：_____

分析者：_____ 图纸：_____

设备名称或编号	功能	标识号	故障模式	故障原因	故障后果		故障探测	纠正措施	故障后果的严重程度	故障概率（如适用）	附注
					局部	末端					

第4章　动力定位系统 FMEA 应用

4.1 一般要求

4.1.1 对于申请 DP-2 和 DP-3 附加标志的船舶，均应对整个动力定位系统进行 FMEA。动力定位系统 FMEA 的目的在于说明动力定位系统有关设备的不同故障模式。分析时应特别注意，系统中的某一设备可能有多种故障模式，从而对动力定位系统产生多种不同影响。

4.1.2 动力定位系统的 FMEA 程序、基本方法、要求和衡准可以按照本指南第 2 章和 IMO MSC/Circ.645 通函执行。

4.2 动力定位 FMEA 报告

4.2.1 船舶动力定位系统 FMEA 应提供船舶的基本概况（例如：主要参数、设计方、船厂、船东、船名和标识、船舶类型、主要目的、船级符号、主要设备供应商、FMEA 供应商和其他相关信息）和接受衡准。

4.2.2 动力定位系统的 FMEA 应包括船舶所有的 DP 工况（例如：铺管、钻井、ROV 等），并对每种工况下船舶的整个技术状况进行描述。

4.2.3 FMEA 应尽可能详细地包括所有系统及所有系统的主要部件，一般应包括但不局限于下列内容：

（1）所有推进器系统（推进器控制系统、推进器液压系统、推进器冷却系统、控制模式选择装置、控制和辅助泵的供电）；

（2）电力系统（高压配电系统、低压配电系统、应急配电系统、蓄电池和 UPS 系统及配电）；

（3）轮机系统（柴油原动机/发电机、燃油系统、滑油系统、海水/淡水冷却系统、压缩空气系统、机舱通风）；

（4）DP 控制系统（DP 控制计算机系统、联合操纵杆系统、船舶和位置参照系统、模式选择、DP UPS 电源系统、传感器系统）；

（5）综合自动化系统、功率管理系统、发电机电压调节器、柴油原动机调速器；

（6）应急停止/切断设置；

（7）防火和浸水隔离布置（DP-3）；

（8）其他相关系统（消防系统、通风系统、ESD 系统、计算机房间冷却系统等）；

（9）结论/发现项/建议（如适用）；

（10）试验程序。

4.2.4 在编制 FMEA 报告时，应包括所有系统主要部件的描述以及表示他们互相之间作用的功能框图、冗余分组情况、所有严重故障模式、每一故障模式的主要可预测原因、每一故障对船位的瞬态影响、探测故障的方法、故障对系统能力的影响、对可能的公共故障模式的分析等。

4.3 动力定位系统冗余及其他要求

4.3.1 冗余要求

4.3.1.1 冗余系指当发生单个故障时，单元或系统保持或恢复其功能的能力，可通过设置多重单元、系统或其他实现同一功能的装置来实现。冗余单元或系统应能立即投入运行，向冗余单元或系统的操作转换应尽实际可能自动进行，并将操作者的干预减到最小*，转换应平稳，其变化应在可接受的操作范围内。

4.3.1.2 动力定位系统部件的冗余要求如下：

（1）对于 DP-2 附加标志，所有活动部件（发电机、推进器、配电板、通讯网络、遥控阀等）应冗余；

（2）对于 DP-3 附加标志，所有部件包括电缆布线和管路应冗余，并进行“A-60”物理隔离。在低失火危险处所若采用两道“A-0”物理分隔也可以接受。

4.3.1.3 应对所有技术功能的独立性进行考虑，当认为系统的某些部件无需冗余或无法进行冗余时，要进一步考虑这些部件的可靠性和机械保护，如果这些部件的可靠性足够高或故障的影响低，可以接受相应的布置。

4.3.1.4 实现同一功能的冗余单元或系统存在以下三种情况：

（1）所有冗余单元或系统完全独立；

（2）所有冗余单元或系统交叉连接，具有交叉部件或子系统；

（3）所有冗余单元或系统通过一个共用单元或系统连接。

4.3.1.5 冗余系统的以下四种故障模式不能被接受：

（1）某一共因故障会影响所有冗余单元/系统和共用单元/系统；（2）当实现同一功能的冗余单元或系统交叉连接时，交叉部件或子系统故障会影响所有冗余单元或系统；

（3）当实现同一功能的冗余单元或系统通过一个共用单元或系统相连时，共用单元或系统的故障会影响所有冗余单元或系统；

（4）当实现同一功能的冗余单元或系统通过一个共用单元或系统相连时，其中一个冗余单元或系统的一次故障会传播至另一个冗余单元或系统（例如短路）。

*若单一故障发生后不会立即影响船舶保持位置和首向的能力，采取适当的人为干预可以避免船舶失位，且经过 FMEA 分析和试验验证，该干预可以接受。

当上述情况无法避免时，应采取补偿措施例如故障探测、保护功能、备用启动、重启和转换等，FMEA 应对这些补偿措施进行详细描述和分析。

4.3.1.6 FMEA 报告中应以图、表、框图和文字对每个冗余分组进行描述，应明确实现同一功能的冗余单元或系统是否完全独立，是否交叉连接，是否通过共用单元或系统连接。FMEA 报告中还需对冗余单元或系统之一故障时，从一个单元或系统转换到另一个单元或系统的时间（包括切换时间和恢复时间等）、可能产生的影响作出说明。

4.3.2 其他要求

4.3.2.1 对于不直接属于动力定位系统，但其发生故障会导致动力定位系统故障的系统，如普通灭火系统、发动机通风系统、停车系统等，也应进行 FMEA。

4.3.2.2 如果单元或系统中存在隐性故障，且系统没有提醒操作人员，那么可能会发生对船舶定位产生重大影响的进一步故障，从而造成不能在规定的环境条件下，在规定的作业范围内自动保持船舶的位置和首向，则这种情况应作为单一故障考虑。需对上述隐性故障采取监测和报警（例如声光报警设备、自动传感器设备等）、或其他措施来减轻或避免隐性故障带来的影响，并在 FMEA 报告中体现出来。

4.3.2.3 对于操作者无意疏忽的行为可能造成的影响，如果合理且极可能发生的，应在 FMEA 中考虑。

4.4 船舶各系统 FMEA 报告及示例[†]

4.4.1 推进器系统

4.4.1.1 推进器系统包括了推进器控制系统、推进器液压系统、推进器冷却系统、控制模式选择装置、控制和辅助泵的供电等。需在 FMEA 报告中详细说明上述系统的配置及冗余情况并进行相应的分析。

4.4.1.2 下图例和表格描述了某条配置 4 台推进器的船舶：

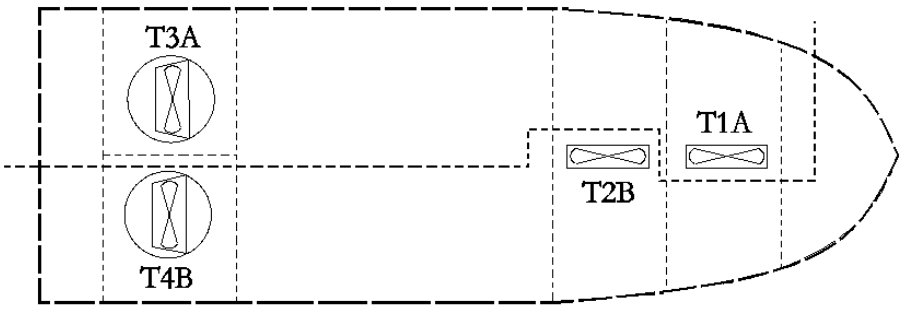


图 4.4.1.2 某配备了 4 台推进装置的船舶

[†] 4.4 中所提供的示例仅供参考，不作为 FMEA 分析的要求，具体项目需具体分析。

推进装置冗余分组设计 **表 4.4.1.2**

情况	保持船舶位置和首向	冗余型式/描述
正常 DP 工况	分组 A（T1A 和 T3A）和分组 B（T2B 和 T4B）	热冗余，没有飘走，没有任何推进器导致驾离‡
单一故障后	分组 A（T1A 和 T3A）或分组 B（T2B 和 T4B）	

4.4.1.3 下图例和表格描述了某条配置 5 台推进器的船舶：

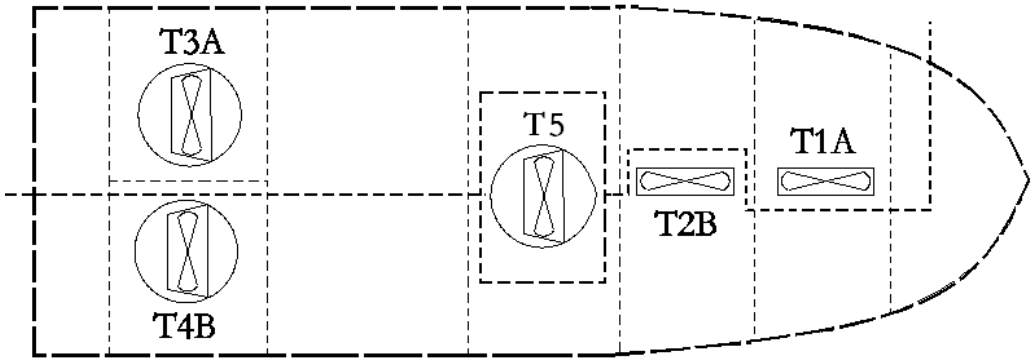


图 4.4.1.3 某配备了 5 台推进装置的船舶

推进装置冗余分组设计 **表 4.4.1.3**

情况		保持船舶位置和首向	冗余型式/描述
运行模式一	正常 DP 工况	分组 A（T1A 和 T3A）和分组 B（T2B、T4B 和 T5）	热冗余，没有飘走，没有任何推进器导致驾离
	单一故障后	分组 A（T1A 和 T3A）或分组 B（T2B、T4B 和 T5）	
运行模式二	正常 DP 工况	分组 A（T1A、T3A 和 T5）和分组 B（T2B 和 T4B）	热冗余，没有飘走，没有任何推进器导致驾离
	单一故障后	分组 A（T1A、T3A 和 T5）或分组 B（T2B 和 T4B）	

4.4.1.4 下图例为某船主推进系统简图，主推进具有独立的供电、控制回路、淡水冷却系统等。下表是对该主推进器系统各单元进行的 FMEA。

‡ 飘走表示综合推力弱于环境力时导致船舶不能保持位置和首向的情况；驾离表示部分推进器未按期望输出推力，而 DP 控制系统未踢出对应推进器，造成综合推力与环境力失衡，导致船舶不能保持位置和首向的情况。

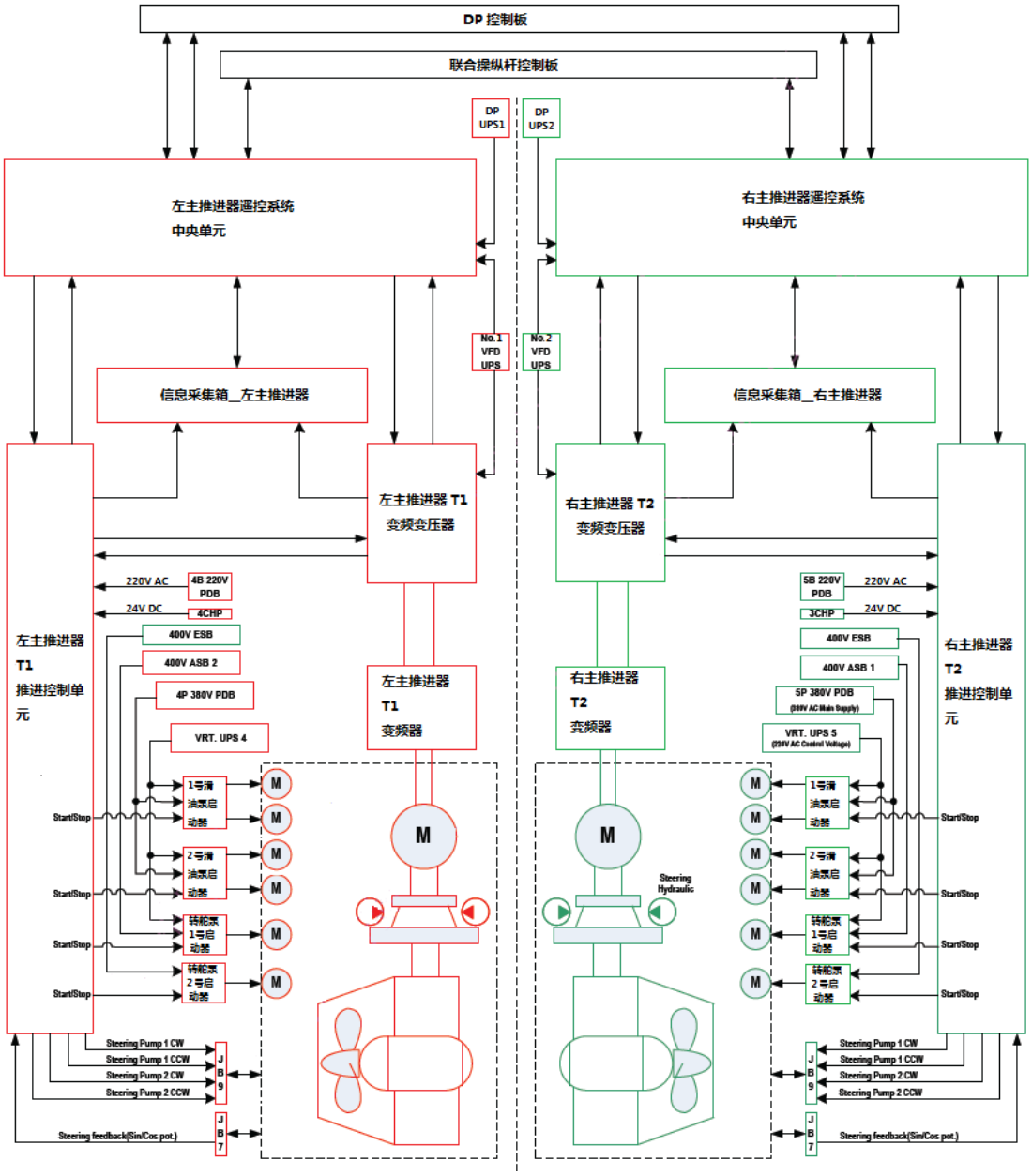


图 4.4.1.4 某船主推进控制系统简图

主推机器系统 FMEA 表格 **表 4.4.1.4**

主推进器驱动单元：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	整流器故障	熔断器故障 内部故障	推进器开关断开	通过监测报警系统报警，另外在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推进器保持船位和首向	小	小	无
2	变频器故障	内部故障	变频器脱扣，推进器停车	通过监测报警系统报警，另外在	丢失相应推进器，由剩余推	小	小	无

				DP 控制显示相应推进器未备机	进器保持船位和首向			
3	CPU 故障	内部故障	变频器脱扣，推进器停车	通过监测报警系统报警，另外在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推进器保持船位和首向	小	小	无
…	…	…	…	…	…	…	…	…
推进器控制单元：								
1	主 AC230V 电源故障	短路，接地故障，过载或线路断开	一路电源丢失，自动转换到备用电源供电	监测报警系统显示电源故障报警	对 DP 没有立即影响，受影响的主推进仍正常工作	小	小	无
2	备用 DC24V 电源故障	短路，接地故障，过载或线路断开	一路电源丢失	监测报警系统显示电源故障报警	对 DP 没有立即影响，受影响的主推进仍正常工作	小	小	无
3	主 PLC 故障	供电故障，内部故障	PLC 失去冗余，转换到备用 PLC	监测报警系统报警	对 DP 没有立即影响，受影响的主推进仍正常工作	小	小	无
4	备用 PLC 故障	供电故障，内部故障	PLC 失去冗余	监测报警系统报警	对 DP 没有立即影响，受影响的主推进仍正常工作	小	小	无
5	舵机泵 1 CW 信号故障	接线断开，部件故障	受影响的主推进器操舵冻结，退出 DP 控制	在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推进器保持船位和首向	小	小	无
6	舵机泵 2 CW 信号故障	接线断开，部件故障	受影响的主推进器操舵冻结，退出 DP 控制	在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推进器保持船位和首向	小	小	无
7	舵机泵 1 CCW 信号故障	接线断开，部件故障	受影响的主推进器操舵冻结，退出 DP 控制	在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推进器保持船位和首向	小	小	无
8	舵机泵 2 CCW 信号	接线断开，部件故障	受影响的主推进器操舵	在 DP 控制显示相应推进器未备机	丢失相应推进器，由剩余推	小	小	无

	故障		冻结，退出 DP 控制		进器保持船位和首向			
10	舵机反馈信号故障	接线断开，部件故障	推进器操舵冻结，但是仍然执行 DP 命令	操舵信号错误报警	对 DP 没有立即影响	小	小	无
…	…	…	…	…	…	…	…	…
主推进器遥控系统/信息采集单元								
…	…	…	…	…	…	…	…	…
推进器辅助系统：								
1	操舵液压电机故障	主部件机械损坏	…	…	对 DP 没有立即影响	小	小	无
2	操舵控制阀故障	机械损坏或电源丢失等	操舵控制丢失，影响相应推进器	监测报警系统报警	对 DP 没有立即影响	小	小	无
3	液压油系统故障	…	…	…	对 DP 没有立即影响	小	小	无
4	滑油系统故障	…	…	…	对 DP 没有立即影响	小	小	无
…	…	…	…	…	…	…	…	…

4.4.2 电力系统

4.4.2.1 电力系统包括轴带发电机（如有时）、柴油发电机、配电板、分电箱、电缆和电缆通道（DP-3）、UPS 和蓄电池、功率管理系统等。

4.4.2.2 下图例和表格描述了某条配置 4 台推进器和 4 台主发电机的船舶：

电力系统冗余分组设计 **表 4.4.2.2**

分系统	冗余分组 A	共同组 X	冗余分组 B
推进器	T1A，T3A		T2B，T4B
柴油发电机	DG1，DG2		DG3，DG4
配电系统	SWBA		SWBB

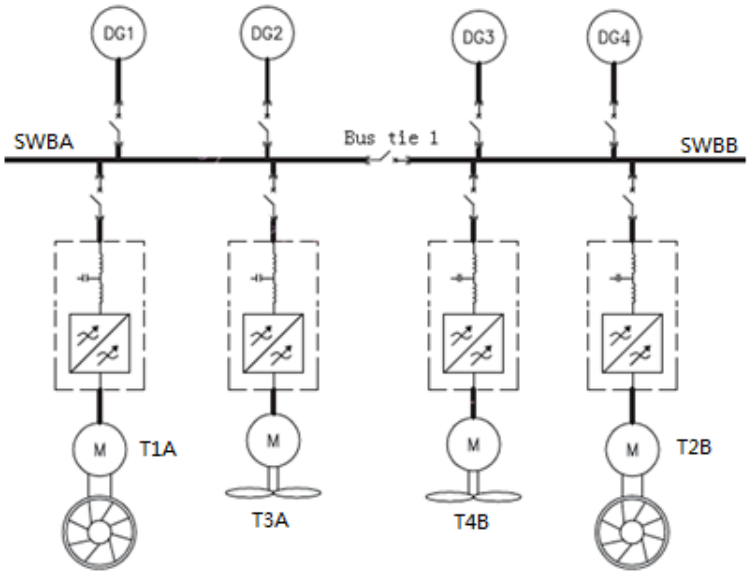


图 4.4.2.2 某配置了 4 台推进器和 4 台发电机的船舶

上述例子在 DP 模式下，Bus tie1 假定为断开状态，冗余分组 A 和冗余分组 B 能做到完全独立。对电力系统的 FMEA 还需考虑很有可能发生的误操作作为一个单一故障，上述例子中汇流排分段开关 Bus tie 在 DP 模式下应保持断开状态，但是若由于误操作造成上述开关闭合则会降低系统冗余，故应采取联锁或其他合适的措施。

若上述例子在 DP 模式下，Bus tie1 为闭合状态，则冗余分组 A 和冗余分组 B 具有共同组 Bus tie1，此种情况需进行特殊考虑（例如实船短路电流试验或其他有效证明文件）。

4.4.2.3 若并联运行的发电机存在电气连接，或发电机的控制和保护系统有一些共同的故障模式，应保证一台发电机故障不能导致并联运行的发电机断电。需将整个电力系统的冗余分组进行列表说明。下图例和表格描述了某条申请 DP-2 附加标志的船舶的整个电力系统图：

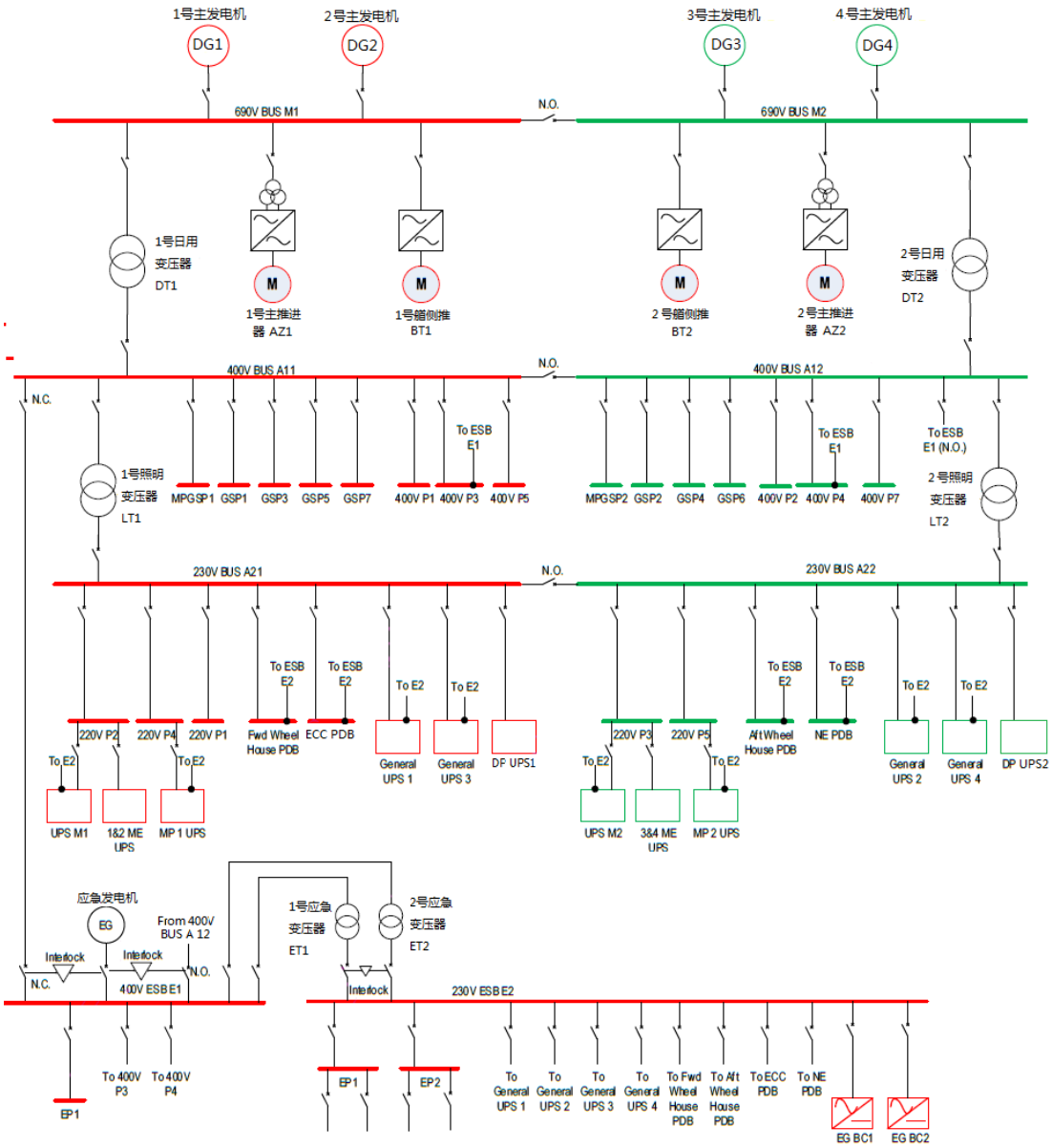


图 4.4.2.3 某申请 DP-2 附加标志的船舶的电力系统

电力系统冗余分组　　表 4.4.2.3.1

分系统	冗余分组 A	共同组 X	冗余分组 B
柴油发电机	DG1，DG2		DG3，DG4
AC690V 系统	690V BUS M1	Bus tie 1	690V BUS M2
AC400V 系统	400V BUS A11、其供电负载、相关分电箱 400V ESB E1	Bus tie 2	400V BUS A12、其供电负载、相关分电箱
AC230V 系统	230V BUS A21、其供电负载、相关分电箱 230V ESB E2	Bus tie 3	230V BUS A22、其供电负载、相关分电箱
DC24V 系统	…	…	…

对于电力分配系统，可以将每一个电压等级的不同故障模式用同一表格进行分析，也分别进行分析。对于存在共同组 X 的元器件或系统应尽可能详细分析。对于应急配电板供电

负载，只要在 DP 模式所用到设备均需列入故障模式分析表格中。

电力系统 FEMA 工作表　　表 4.4.2.3.2

发电机								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	DG1 故障	燃油、滑油、冷却系统或电源故障，低速脱扣，低压脱扣，安全停车，应急停车等	DG1 开关脱扣，但不影响其他发电机和推进器	DG1 脱扣报警	不影响 DP 定位，所有推进器可用	中	小	无
2	DG2 故障	同上	同上	同上	同上	同上	同上	同上
3	DG3 故障	同上	同上	同上	同上	同上	同上	同上
4	DG4 故障	同上	同上	同上	同上	同上	同上	同上
AC690V 配电系统：								
1	690V BUS M1 故障	短路或接地故障	BT1、AZ1 丢失，400V BUS A11、230V BUS A21、400V ESB 和 230V ESB 断电	BT1 和 AZ1 退出 DP 控制 通过监测报警系统发出汇流排断电报警	不影响船舶保持定位和首向，但是损失 DP 冗余功能降低	中	小	提醒 DPO 注意
2	690V BUS M2 故障	短路或接地故障	BT2、AZ2 丢失，400V BUS A12、230V BUS A22 断电	BT2 和 AZ2 退出 DP 控制 通过监测报警系统发出汇流排断电报警	不影响船舶保持定位和首向，但是损失 DP 冗余功能降低	中	小	提醒 DPO 注意
3	1 号日用变压器故障	元器件故障	相关负载丢失	监测报警系统报警	不影响船舶保持定位和首向	中	小	通过试验验证
…	…	…	…	…	…	…	…	…
AC400V 配电系统：								
1	400V BUS A11 故障	短路或接地故障	BT1、AZ1 丢失，400V BUS A11、230V BUS A21、400V	BT1 和 AZ1 退出 DP 控制 通过监测报警系统发出汇流排断电报警	不影响船舶保持定位和首向，但是损失 DP 冗余功能降低	中	小	提醒 DPO 注意

			ESB 和 230V ESB 断电					
2	400V BUS A12 故障	短路或接地故障	BT2、AZ2 丢失，400V BUS A12、230V BUS A22 断电	BT2 和 AZ2 退出 DP 控制 通过监测报警系统发出汇流排断电报警	不影响船舶保持定位和首向，但是损失 DP 冗余功能降低	中	小	提醒 DPO 注意
3	MPGSP1 故障	短路或接地故障	MP1 风机丢失	监测报警系统报警	不影响船舶保持定位和首向	小	小	无
4	GSP1 故障	短路或接地故障	BT1 风机丢失	监测报警系统报警	不影响船舶保持定位和首向	小	小	提醒 DPO 注意
…	…	…	…	…	…	…	…	…
AC230V 配电系统：								
…	…	…	…	…	…	…	…	…
应急配电板：								
…	…	…	…	…	…	…	…	…
DC24V 配电系统：								
…	…	…	…	…	…	…	…	…

4.4.3 功率管理系统

4.4.3.1 FMEA 报告中需对功率管理系统进行分析，可参考 PMS 设备商提供的资料。下图列举了某 DP-2 船舶的 PMS 系统。

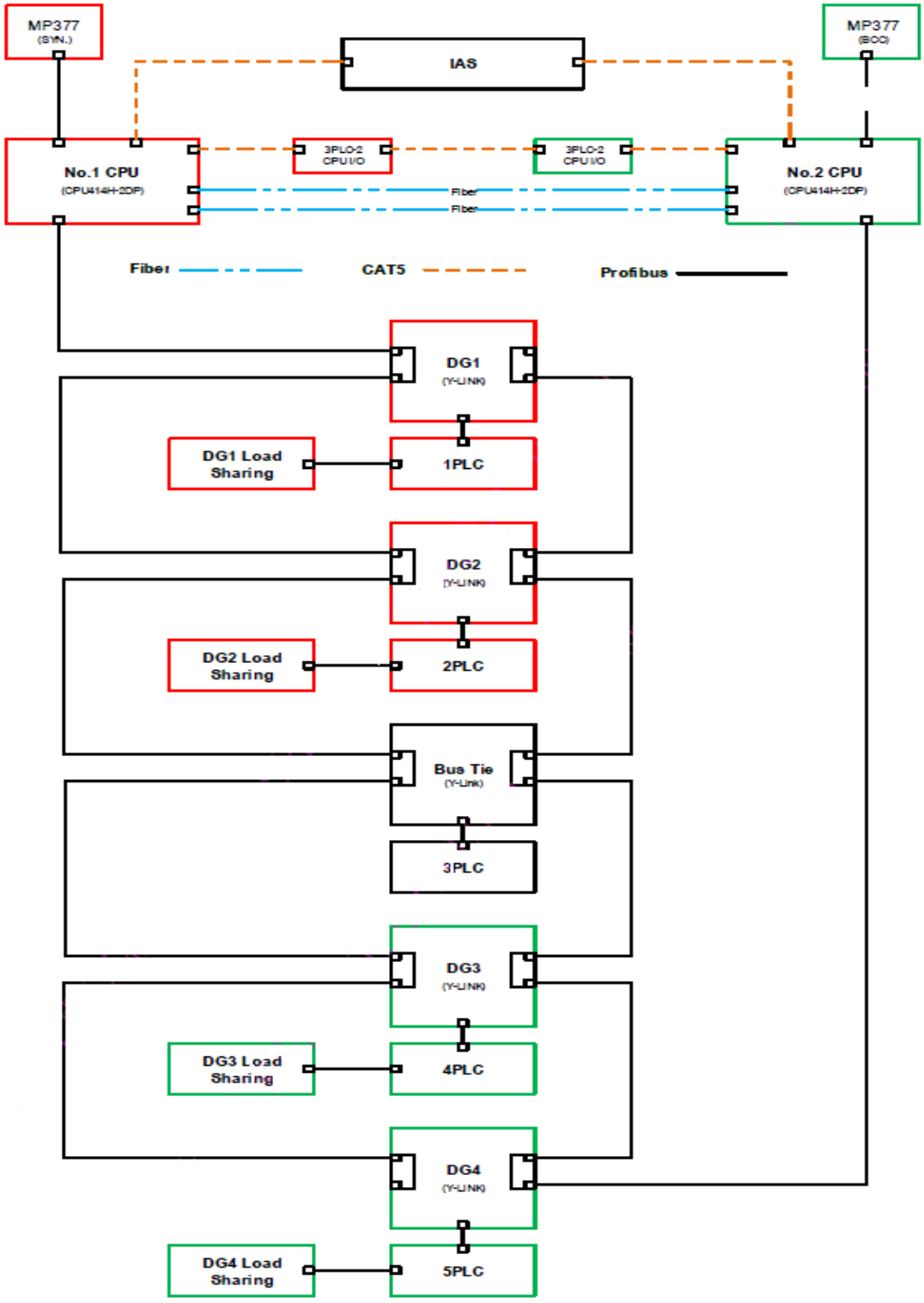


图 4.4.3.1 某船 PMS 系统

PMS 冗余分组 **表 4.4.3.1.1**

分系统	冗余分组 A	共同组 X	冗余分组 B
CPU	No.1 CPU		No.2 CPU
Y-Link	No.1 DG, No.2 DG	Bus tie	No.3 DG, No.4 DG

Load Sharing	No.1 DG, No.2 DG		No.3 DG, No.4 DG
Screen	No.1		No.2

功率管理系统的 FMEA 表格　　表 4.4.3.1.2

序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	CPU 故障	元器件故障	CPU 失去冗余	监测报警系统报警	不影响船舶保持船位和首向	中	小	无
2	PLC 故障	元器件故障	受影响的 PLC 丢失	监测报警系统报警	不影响船舶保持船位和首向	中	小	无
3	PPU 故障	元器件故障	受影响的发电机退出 DP	监测报警系统报警 DP 控制站功率限制报警	不影响船舶保持船位和首向	中	小	无
4	网络故障	元器件故障，接线断开	CPU 之间通讯丢失	监测报警系统报警	不影响船舶保持船位和首向	中	小	无
…	…	…	…	…	…	…	…	…

4.4.4 DP 控制系统

4.4.4.1 对 DP 控制系统的 FMEA 包括 DP 控制计算机系统、联合操纵杆系统、船舶和位置参照系统、模式选择开关、相关供电单元等。DP 控制系统的 FMEA 应对每一硬件模块、网络构架和供电电源进行分析，可以参考相应产品审图批准的 FMEA。

4.4.4.2 下图例和表格描述了某船 DP 控制系统的冗余设置：

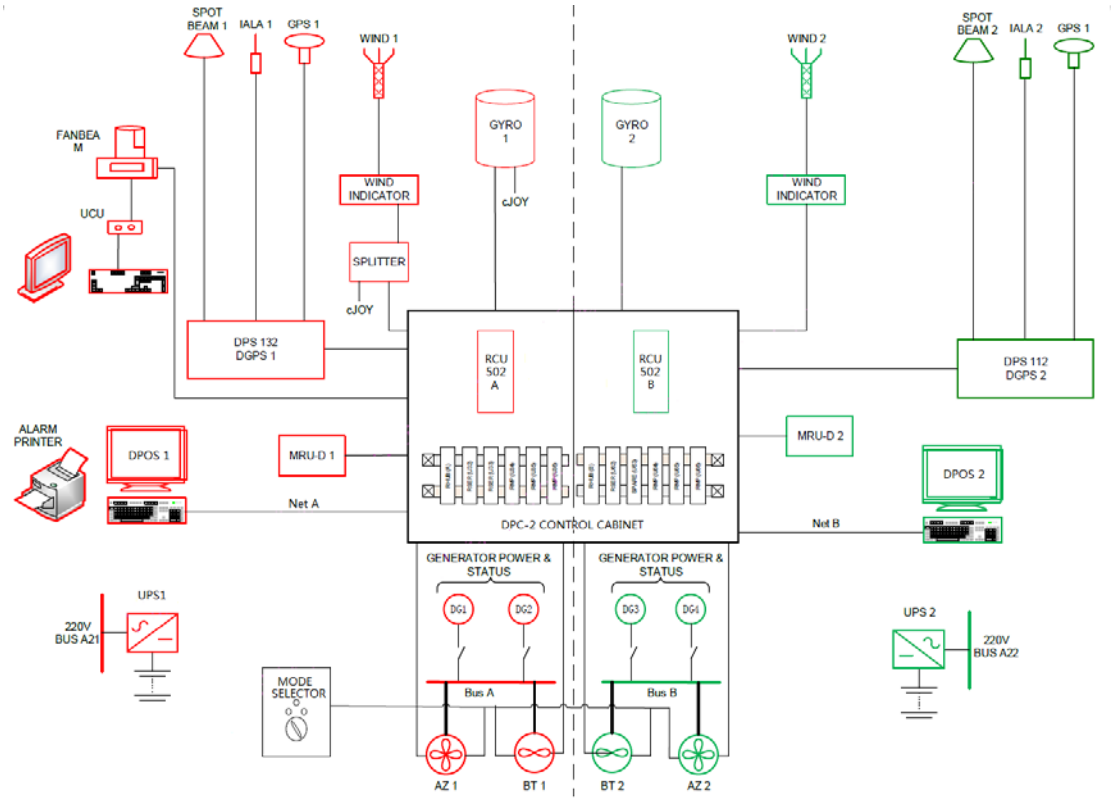


图 4.4.4.2.1 某船 DP 控制系统

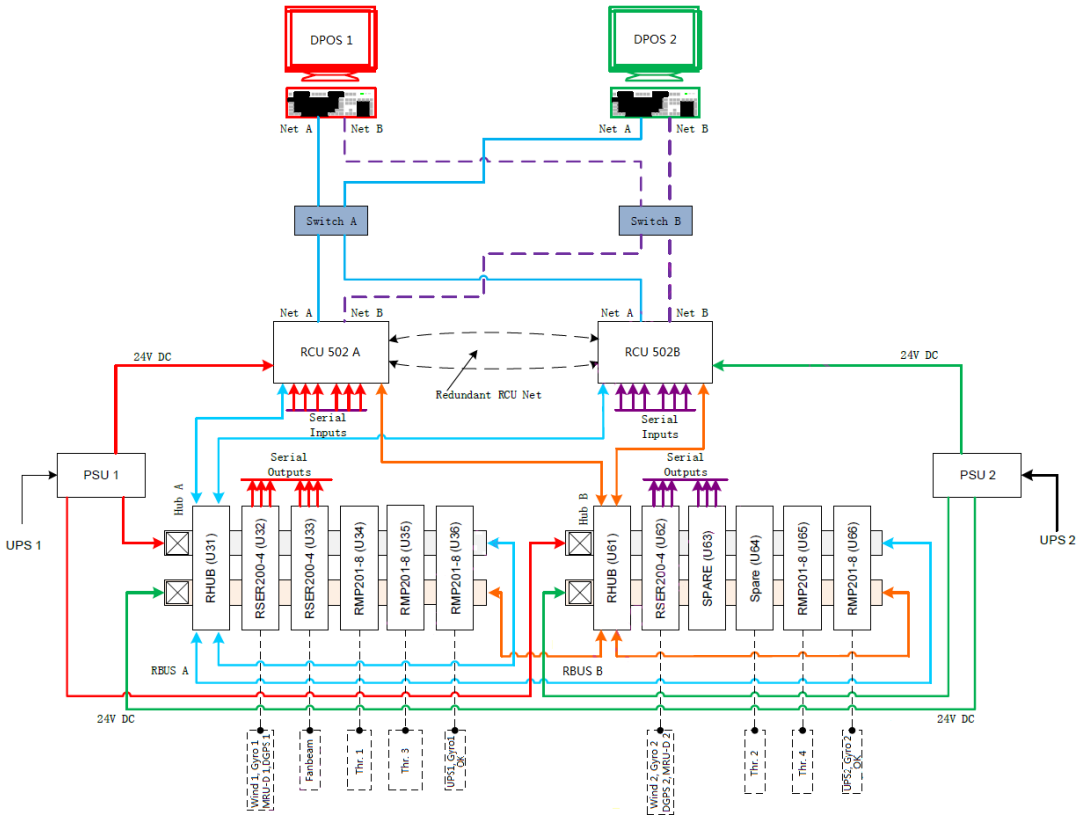


图 4.4.4.2.2 上述船舶 DPC-2 控制箱设置

DP 控制系统冗余分组 **表 4.4.4.2.1**

分系统	冗余分组 A	共同组 X	冗余分组 B
操作站	DPOS1		DPOS2
DP 主控制箱 （DCP-2）	PSU1	DP 控制软件 RCU 501A(主)， RCU502B(备) 模式选择开关 网络通讯线 RMP/RSER/RHUB 模块	PSU2
UPS	DP UPS1		DP UPS2
传感器	Gyro 1, Wind 1, MRU 1 DGPS 1, Fanbeam		Gyro 2, Wind 2, MRU 2 DGPS 2
网络	Switch A	DPOS1 Net A DPOS2 Net B RCU A Net B RCU B Net A	Switch B
推进器	T1，T3		T2，T4

DP 控制系统的 FMEA 表格 **表 4.4.4.2.2**

传感器：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	DGPS 故障	元器件故障	失去相关位置参照	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
2	Fenbeam 故障	元器件故障	失去相关位置参照	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
3	风速传感器故障	元器件故障	失去相关风速传感器	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
4	风速信号不协调	信号障碍	选择使用的风速传感器	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
5	罗经故障	元器件故障	失去相关罗经信号	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
6	MRU 故障	元器件故障	失去相关垂直面参照	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
…	…	…	…	…	…	…	…	…
控制器：								
1	以太网 A 或 B	元器件故障	失去一个通讯网络	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
2	主控制器故障	元器件故障	备用控制器工作	DP 控制站报警	不影响船舶保持船位和首向	小	小	无

3	备用控制器故障	元器件故障	无影响	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
4	DPC-2 电源故障	电源失电	丢失一路电源	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
5	RHUB A 或 B 故障	元器件故障	丢失一路 RBUS 通讯连接	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
6	串行模块故障	元器件故障	…	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
7	I/O 故障	元器件故障	…	DP 控制站报警	不影响船舶保持船位和首向	小	小	无
…	…	…	…	…	…	…	…	…
联合操纵杆系统：								
1	罗经 1 故障	元器件故障	不能使用自动首向功能	DP 控制站报警	对 DP 无影响	小	小	无
2	风速传感器 1 故障	元器件故障	Joy 风速补偿功能不能使用	DP 控制站报警	对 DP 无影响	小	小	无
…	…	…	…	…	…	…	…	…

4.4.5 船舶辅助系统

4.4.5.1 以下例子列举了某船燃油系统配备两路燃油输送系统；左舷侧和右舷侧。每侧有共用燃油供应管路，可以让每个燃油日用油柜向所有主机供油。每台主机都有各自的燃油回油管路返回到自己的燃油日用油柜。回油管路的并联管路上设有隔离阀（FOV71）。这些隔离阀在 DP 2 模式下保持常闭，以使两个系统保持隔离从而保持冗余。每台主机设有一台电动燃油泵，互为备用。

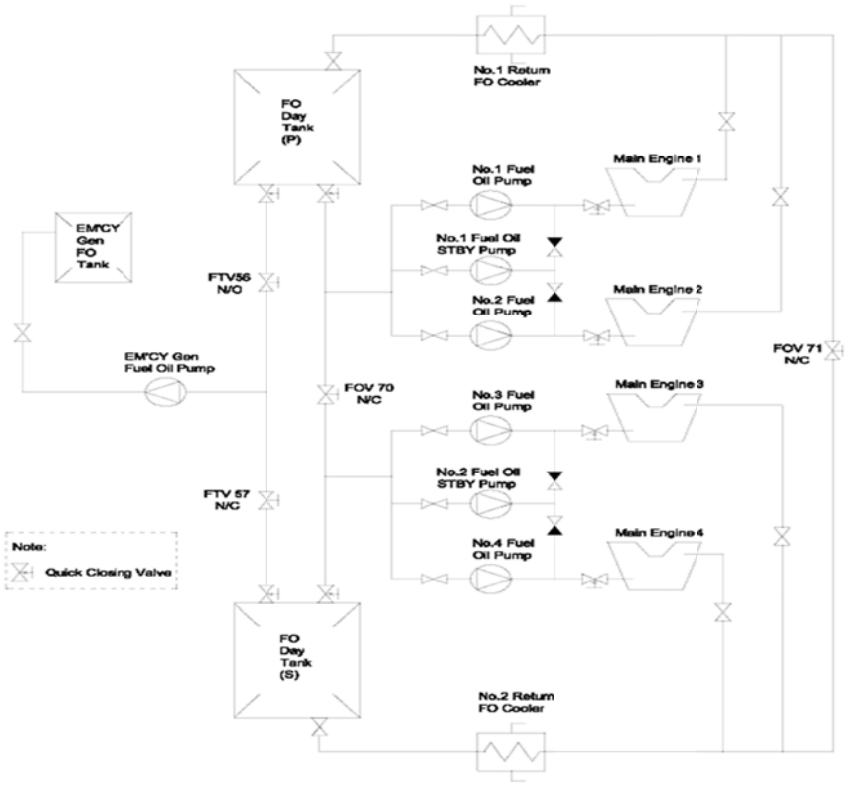


图 4.4.5.1 某船舶燃油输送系统

燃油输送系统的 FMEA 表格 **表 4.4.5.1**

燃油供应系统：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	主燃油泵	燃油泵故障或压力低报警	失去主燃油泵	传感器探测	对船舶定位能力不影响	中	小	备用燃油泵自动起动并持续向主机供油
2	备用燃油泵	隐性故障	失去备用燃油泵	NIL	对船舶定位能力不影响	中	小	备用燃油泵不使用
…	…	…	…	…	…	…	…	…

4.4.5.2 以下例子列举了某船海水冷却系统包括两个通过主海水管路连接的海底门，主海水管路中间设有隔离阀（CSV 10），此隔离阀在 DP 模式运行时保持关闭。第一主冷却器为 1 号和 2 号主机提供冷却，第二主冷却器为 3 号和 4 号主机提供冷却。设有 3 台主海水冷却泵，2 用 1 备。

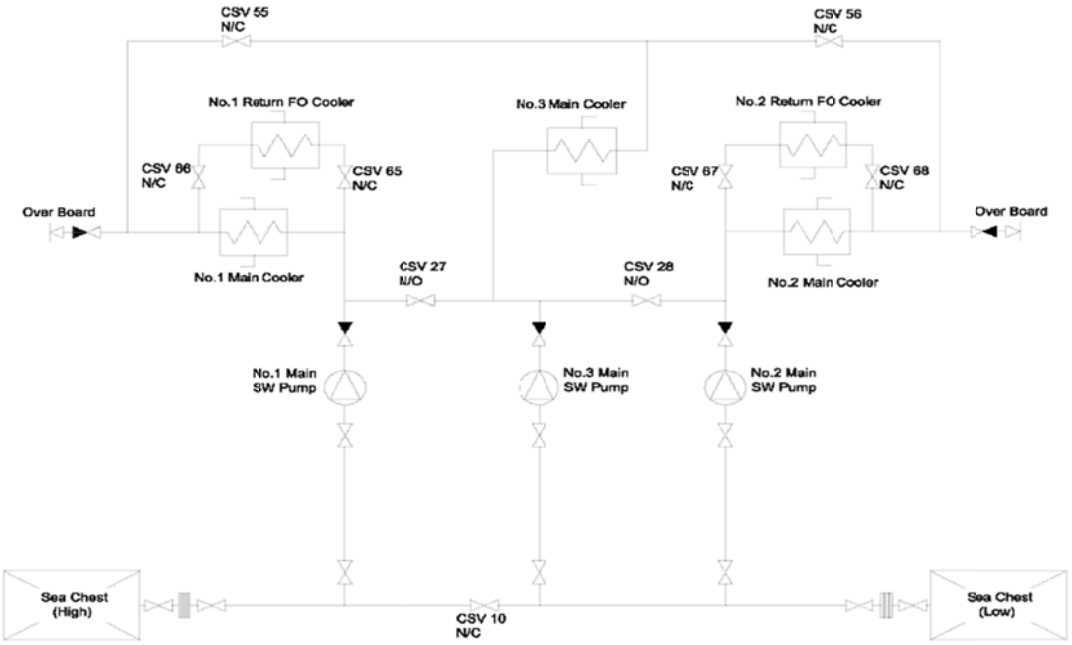


图 4.4.5.2 某船海水冷却系统

海水冷却系统的 FMEA 表格 **表 4.4.5.2**

海水冷却系统：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	主机海水冷却系统	海水泵故障或压力低报警	主机失去海水冷却	传感器探测	对船舶定位能力不影响	中	小	管路上的阀打开后，起动备用泵
2	舵桨装置海水冷却系统	海水泵故障或压力低报警	舵桨失去海水冷却	传感器探测	对船舶定位能力不影响	中	小	管路上的阀打开后，起动备用泵
…	…	…	…	…	…	…	…	…

4.4.5.3 以下列举了某船淡水冷却系统的例子，每台主机配备独立的淡水冷却系统，包括低温淡水冷却管路和高温淡水冷却管路。主机低温淡水管路包括机带低温淡水冷却泵，低温空气冷却器和润滑油冷却器。主机共用主冷却器，高温淡水膨胀水箱和温控阀。高温淡水冷却管路包括机带高温淡水冷却泵、高温空气冷却器和温控阀。此配置确保在任何时间，单一故障的主机淡水冷却系统不会导致其他主机故障。

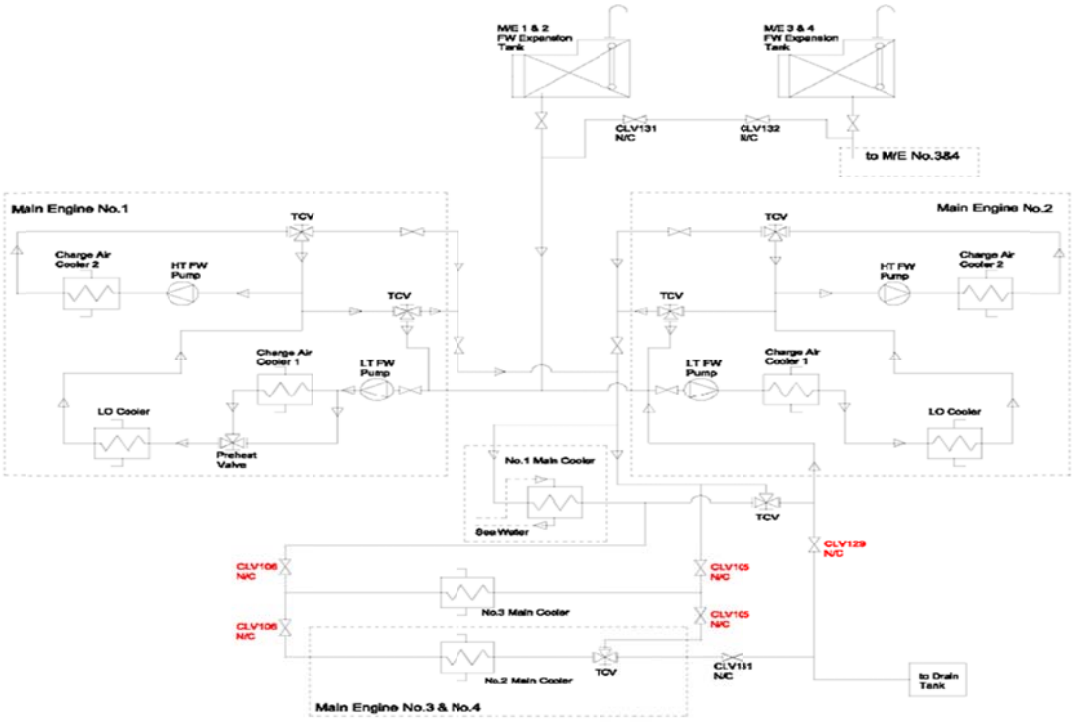


图 4.4.5.3 某船淡水冷却系统

淡水冷却系统的 FMEA 表格 **表 4.4.5.3**

淡水冷却系统：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	主机低温淡水冷却泵(机带泵)	淡水泵故障或压力低报警	主机失去低温淡水冷却泵。失去一台主机、一台发电机导致可用功率降低	传感器探测	船舶在所有推进器作用下保持定位	中	小	
2	主机高温淡水冷却泵(机带泵)	淡水泵故障或压力低报警	主机失去高温淡水冷却泵。失去一台主机、一台发电机导致可用功率降低	传感器探测	船舶在所有推进器作用下保持定位	中	小	
3	主冷却器	冷却器堵塞或泄漏导致高温报警	失去工作冷却器	传感器探测	对船舶定位能力不影响	中	小	管路上的阀打开后，使用备用冷却器
…	…	…	…	…	…	…	…	…

4.4.5.4 以下例子列举了某船控制空气系统的例子，两台主空压机提供压缩空气到两个

起动空气瓶，供四台主机启动空气。并通过减压阀提供控制空气和服务空气。左舷起动空气瓶为主机 1 和 2 提供起动空气，右舷起动空气瓶为主机 3 和 4 提供起动空气。隔离阀在 DP-2 模式下保持常闭。

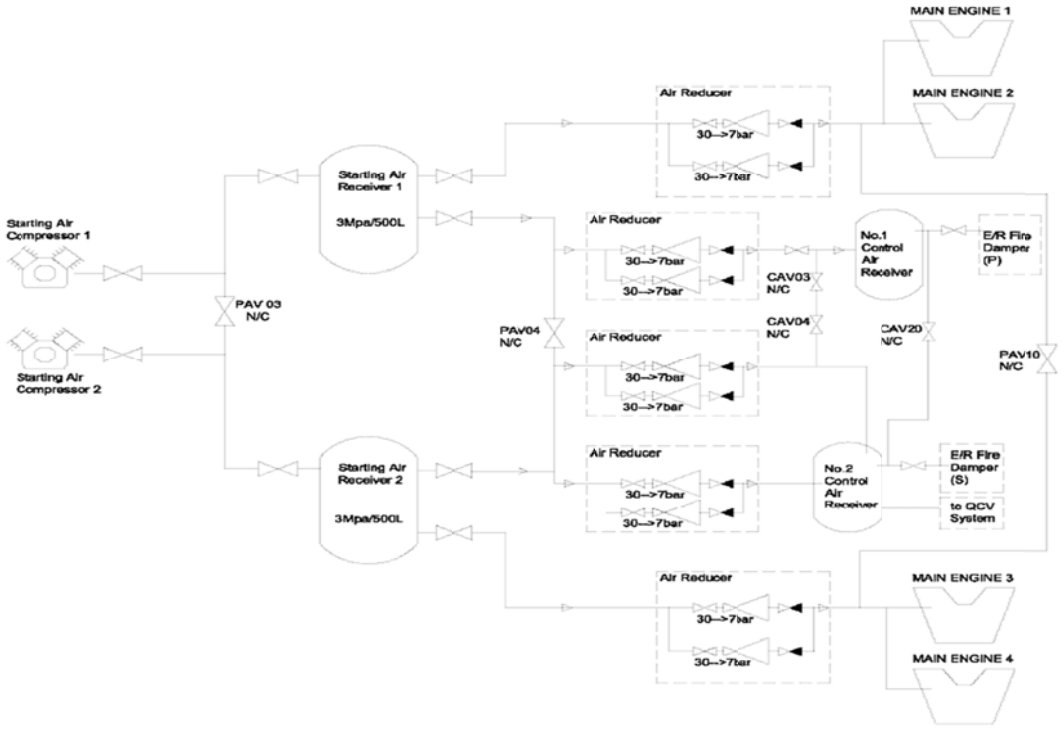


图 4.4.5.4 某船起动空气系统

起动空气系统的 FMEA 表格 **表 4.4.5.4**

起动空气系统：								
序号	部件/故障模式	故障原因	故障影响	故障探测方法	DP 影响	发生概率	危险程度	建议采取的行动或其他
1	1#空压机	空压机故障	失去 1#空压机	传感器探测	对船舶定位能力没有影响	中	小	2#空压机投入使用
2	1#起动空气瓶	泄漏、堵塞、阀故障…	失去 1#起动空气瓶	传感器探测	对船舶定位能力没有影响	中	小	2#起动空气瓶投入使用
3	1#控制空气瓶	泄漏、堵塞、阀故障…	左舷气动防火风闸失去控制空气。左舷防火风闸关闭，机舱动力通风能力降低。	传感器探测	对船舶定位能力没有影响	中	小	
…	…	…	…	…	…	…	…	…

4.4.6 防火和浸水（DP-3 附加标志）

4.4.6.1 申请 DP-3 附加标志的船舶，还需考虑到 DP 控制站失火或进水、配电室失火或进水、共同的电缆通道失火或进水、主/辅机舱失火或进水、集控室失火或进水等可能影响到船舶定位能力的故障。

4.4.6.2 申请 DP-3 附加标志的船舶，在 FMEA 报告中需对电缆敷设、可能浸水舱室设备布置、A60 物理隔离进行详细描述。

4.5 FMEA 试验程序

4.5.1 应对每一种故障模式下的系统冗余度进行试验，冗余度的试验程序应以模拟故障模式为基础，应尽可能在实际情况下进行试验。详细的冗余度试验程序应提交审查。

4.5.2 船上应放置 FMEA 和冗余度试验程序。FMEA、试验程序和试验报告在船舶运营阶段必须一直有效，保持最新状态，若有以下情况发生时，必须及时进行评估：

（1）必须增加附加的 FMEA 时；

（2）试验程序需要更新时；

（3）要求进行功能测试和/或故障试验时；

（4）文件的其他部分需要更新时。

第5章　双燃料发动机 FMEA 应用

5.1 一般要求

5.1.1 我社《钢质海船入级规范》第 3 篇第 9 章、《天然气动力船规范》对气体燃料发动机提出了 FMEA 分析要求。本章规定了气体燃料发动机 FMEA 的范围、方法、程序与过程等方面的要求。

5.1.2 气体燃料发动机一般在成熟的普通燃油发动机基础上研制而成。按柴油机类型的定义，燃油柴油机通过改进设计，增加燃气供给、喷射、监测、控制、安保等系统，为点燃气缸内的天然气，增加了引燃油供应、喷射及控制系统，为保证燃气的使用安全，还可能增加其他安全辅助系统，例如密封油系统、惰气系统等，另外气体燃料发动机不同工作模式下稳定安全工作，还需要专门的控制、监测与安全系统，控制燃气供应、燃气喷射、燃气-空气混合比、气缸内点火等工作过程，因此，气体燃料发动机属于新型发动机，需要重新进行认可、型式试验、检验和发证。

5.1.3 如上所述，气体燃料发动机是在成熟的燃油发动机基础上研制，原有的燃油发动机设计时已经开展过相应的风险分析，并进行了不断的改进设计及营运经验验证，具有足够的可靠性，对气体燃料发动机进行 FMEA 时，不需要对基本发动机进行详细分析，但需要考虑基本发动机及其辅助系统（燃油系统、滑油系统、冷却水系统、空气进气系统、排气系统、液压控制系统、起动空气系统等）因使用气体燃料可能导致的附件潜在风险，比如因气缸点火失败或燃烧不充分，部分可燃气体进入排气系统可能导致的爆炸风险等。

5.1.4 气体燃料发动机有各种设计，比如缸内直喷的高压双燃料发动机、进气道低压喷射双燃料发动机、增压器前预混单气体燃料发动机等，不同的设计理念、不同的工作模式其潜在的风险及危害会有很大差别，需要结合系统设计进行 FMEA。

5.1.5 柴油机在船上的用途不同，故障导致的后果影响也不一样，因此 FMEA 时可接受的安全标准需要区别对待，相应的风险控制措施也会有所差异，比如冗余配置及安全保护要求等。

5.1.6 气体燃料发动机安全与可靠性应不低于普通燃油为燃料的发动机。

5.1.7 气体燃料发动机 FMEA 风险分析应按本指南第 2 章进行。

5.1.8 气体燃料发动机 FMEA 应基于单项故障原则，即同时仅考虑一项故障，不考虑两项或两项以上故障同时发生的可能。对于其他部件的单项故障即可直接导致另一部件故障这种情况也需要考虑。另外，分析时可探测或不可探测的故障都需要考虑。

5.2 FMEA 范围

5.2.1 气体燃料发动机在船上应用，气体燃料使用有关的风险不仅局限于发动机设备本

身，发动机外部系统（如燃料储存、燃料供应系统）故障会需要发动机的控制和监测系统采取附加的安全保护动作。

5.2.2 气体燃料发动机 FMEA 至少应考虑如下范围：

（1）气体模式运行相关的系统或部件失效或故障；

（2）气体燃料供应系统中，气体阀组下游段发生气体泄漏；

（3）气体模式运行时，紧急停机或全船突然失电情况下柴油机的安全；

（4）发动机和气体燃料系统之间的相互关联动作。

5.3 气体燃料发动机系统设计与应用描述

5.3.1 作为 FMEA 的基础和前提，应首先参考图纸资料及设备系统的手册等确定气体燃料发动机系统设计与应用，并以文字及图表形式等对系统设计、操作模式、边界、功能要求进行详细说明。

5.3.2 气体燃料发动机可能的应用进行说明，可能会影响该机型将来的型式认可范围以及证书中的关于产品应用范围的限制，有关发动机用途主要包括：

（1）单主机推进，包括直接驱动定距桨或可调桨等；

（2）多主机推进，包括电力推进、机械推进；

（3）辅助用发动机；

（4）应急用发动机。

5.3.3 气体燃料发动机及其系统的设计特征说明。对于气体燃料发动机系统，气体燃料喷射有各种形式，主要包括：

（1）气缸直接喷射；

（2）气体喷入进气总管、扫气箱、各气缸进气道

（3）增压器前燃气和空气预混。

5.3.4 气体燃料发动机及其系统操作、结构及边界的功能描述，包括：

（1）各种工作模式与设计目标说明；

（2）通过方块图的方式阐述系统各功能元素之间的相互关系，将气体燃料发动机系统分解成子系统及部件，各子系统的输入输出和标识号进行合理编号。图 5.3.4.1 和 5.3.4.2 是以某公司双燃料发动机为例描述的各元素之间的功能框图及方块图。

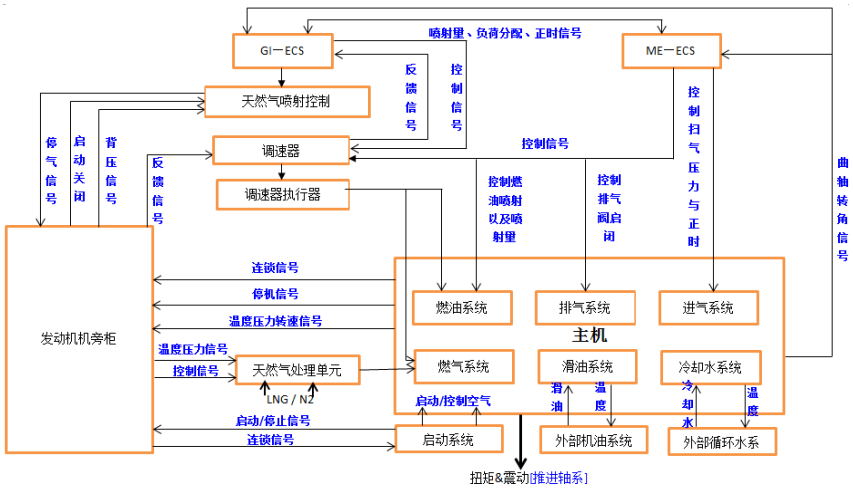


图 5.3.4.1 双燃料发动机功能框图

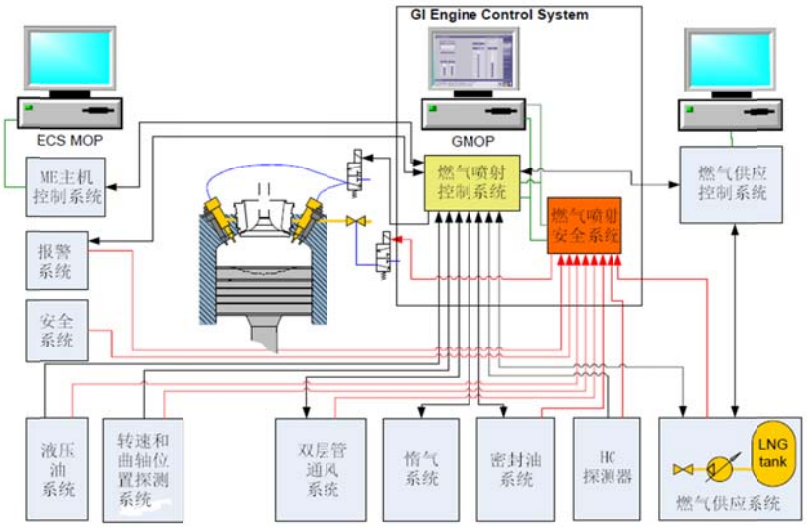


图 5.3.4.2 方块图

5.4 FMEA 程序

5.4.1 FMEA 应按如下程序进行：

5.4.1.1 识别相关设备和系统可能导致如下后果的所有故障：

（1）部件或者位置存在可燃气体（本身设计时不存在可燃气体），或者；

（2）点燃、火灾或爆炸。

5.4.1.2 评估故障所产生的后果；

5.4.1.3 识别故障的探测方法；

5.4.1.4 如风险无法完全消除，需识别相应的纠正措施，比如在系统设计方面，通过冗余配置，或者采取安全装置、监测或报警设施等限制系统的安全运行；在系统运行方面，通过起动冗余设置或者触发替代工作模式。

5.4.2 风险分析的结果应以文件形式予以记录。

5.5 气体燃料相关的系统、设备及操作

5.5.1 气体相关的系统或部件故障，尤其是气体管路及其护罩、气缸气体供应阀等。对于非柴油机上的气体供应系统部件故障，比如互锁阀、气体阀组内的其他部件，可不在气体燃料发动机的 FMEA 中考虑。

5.5.2 点火系统故障，对于双燃料发动机，主要是引燃油喷射相关的故障，对于单气体燃料发动机，主要是指火花塞等点火故障。

5.5.3 空燃比控制系统故障，包括进气旁通阀、气体压力控制阀等。

5.5.4 对于涡轮增压器压缩机上游喷射气体的柴油机，可能形成点火源（热点）的部件故障。

5.5.5 气体燃烧故障或燃烧不正常，如死火、敲缸等。

5.5.6 气体燃料发动机控制、监测和安全系统故障。

5.5.7 发动机部件和与之连接的外部系统漏入可燃气体，发动机辅助系统一般正常情况下不会有可燃气体，采用气体燃料运行时，可能因部件及材料老化、疲劳、应力集中等导致气体燃料泄漏至滑油、冷却水、排气、起动空气、空气进/扫气等系统中。

5.5.8 气体燃料发动机本身的空间存在可燃气体，如曲轴箱、活塞下部空间、扫气箱等。

5.5.9 气体燃料运行相关的操作，如起动、换向、停车（正常或紧急停机）等操作。

5.5.10 双燃料发动机不同工作模式的转换，包括燃油模式、气体燃料模式或其他工作模式之间的相互转换。

5.5.11 活塞下部空间直接与曲轴箱相通的发动机，曲轴箱内气体燃料积聚的潜在风险。

5.6 分析结果的验证

5.6.1 FMEA 时所作的一些假定及分析得出的结论，应通过一系列试验予以验证和支持，证明所识别的风险及其后果已经消除或有效控制，或者为控制风险影响而采取的措施有效。

5.6.2 FMEA 所得出的结论应作为制定气体燃料发动机型式试验程序和工厂试验程序输入和依据。

5.6.3 以某公司双燃料发动机 FMEA 为例，根据分析结果，对该型双燃料发动机型式试验试验项目提出如下建议：

（1）软件版本及参数验证；

（2）燃油燃气转换模拟试验，模拟气体模式不可用，起动中断等状态；

（3）燃气模式紧急停车试验；

（4）燃气压力低模拟试验；

（5）液压油压力低模拟试验；

（6）双壁管气体浓度高、探测器故障模拟；

（7）燃气供气系统切断；

（8）气缸压力、气体喷射阀压力监控；

（9）气体燃料喷射控制阀、 气体燃料调节阀故障；

（10）气缸控制单元、 气体供应安全单元、气缸气体安全单元模块故障；

（11）网络故障；

（12）电源故障；

（13）电控系统信号故障；

（14）主控制面板故障；

（15）关键传感器故障模拟试验，模拟单个传感器数据错误及无信号试验，如转速传感器；

（16）气体管路部件故障模拟试验。

第6章　柴油机电控系统 FMEA 应用

6.1 一般要求

6.1.1 我社《钢质海船入级规范》第 3 篇第 9 章要求提交柴油机电控系统 FMEA 报告。本章规定了柴油机电控系统 FMEA 的方法、过程、报告等方面的要求。

6.1.2 对柴油机电控系统进行 FMEA 的主要目的，是通过全面系统的分析建立故障条件，并根据安全和性能衡准评估其重要性。FMEA 应证明控制系统单项故障不会导致柴油机性能恶化超出可接受衡准，单项故障是指一次仅考虑一个部件故障模式，不考虑多个故障模式的组合，但共因失效的可能性需要考虑。

6.1.3 发动机可接受的性能和安全衡准以及专门针对柴油机用途的衡准（见 6.2.1.1），应在 FMEA 报告中予以说明，所有识别的故障模式应根据相应的性能和安全衡准进行评估。从这个角度来说，本章关于柴油机电控系统的分析方法更像是 FMEA 的扩展分析，即开展了危害性分析，但证明符合接受标准的目标也可以通过本章规定的分析方法实现。

6.1.4 电控柴油机的安全与可靠性应不低于非电控柴油机。

6.1.5 本章主要侧重于柴油机控制系统 FMEA 及相关文件材料要求，有关 FMEA 过程、程序等参考本指南第 2 章的规定。

6.1.6 柴油机控制系统应按系统 FMEA 进行故障模式与影响分析。

6.1.7 系统 FMEA 按自上而下方式进行，分析时从总系统层面开始，然后进行到下一层或子系统，再到设备或部件层。但分析时如果能充分表明某一层面发生故障对总系统不会产生任何影响，就没有必要再进行下一层的分析。这种情况下，没有必要再进行部件层面的分析。

6.1.8 柴油机控制系统 FMEA 应基于单项故障理念，系统功能层次结构中各种层面下的子系统或设备，假定一次只会因一个可能的原因导致故障。分析假定故障的影响并按其严重程度进行分类，对系统影响超出接受衡准的任何故障模式，都应采取措施（如系统或设备冗余）避免或减轻其危害。

6.1.9 应制定一个试验程序对 FMEA 假定条件和分析得出的结论进行验证和确认。

6.2 FMEA 过程

6.2.1 确定并描述系统和柴油机应用。作为 FMEA 的基础，应参考图纸、设备手册等对拟分析的系统进行详细说明，系统的文字说明、工作模式、边界和功能要求应考虑如下方面：

（1）发动机应用说明，主要包括：

.1 单主机推进（应用限制条件，比如仅用于可调浆）；

.2 多机推进（电力推进和柴油机推进）；

.3 辅助发动机；

.4 应急发动机。

（2）系统运行、结构、边界的功能描述，包括：

.1 系统边界描述（物理边界，如柴油机和分析时考虑的控制系统单元，运行边界，如性能参数）：

- I/O 信号技术规格、传感器、执行器；
- 信号接口技术规格；
- 监测系统，包括人机界面；
- 网络接口，如 CAN 总线、以太网；
- 保护，如电隔离；
- 硬件安全电路；
- 供电源布置；
- 与发动机外部系统的接口定义（如船舶报警系统、齿轮箱、可调浆自动化、电力管理、气体探测、排气、通风、滑油供应、燃油供应系统）；
- 受控制系统影响的性能参数限定的定义（温度、压力、功率、转速）。

.2 电控系统的设计目的和操作模式

- 手动操作模式说明；
- 就地/遥控模式说明；
- 报警/警告。

.3 与发动机安全系统的任何接口（如适用）

.4 通过方框图说明系统功能单元之间的关系，方框图应能提供系统及其部件的图示，以便于接下来的分析，对于每个操作模式，可能需要编制相应的方框图。方框图至少包括：

- 把系统分解为主要的子系统或部件；
- 输入输出进行合适的标识，每个子系统分配参考识别号；
- 所有用于保证故障安全措施的冗余、选择性信号通路和其他工程特征。

（3） 系统元件之间的功能关系，包括：

.1 控制系统边界内所有的部件单元和部件清单(部件清单、名称、功能)；

.2 冗余水平以及冗余、隔离、独立性；

.3 从理念/系统架构的角度对多 CPU 运行进行说明；

.4 分布式控制系统架构。

（4） 每种典型系统工作模式下，系统及其组成元件的系统要求与功能（包括可接受的系统性能限值）。

.1 电控系统和不同发动机应用情况下安全系统性能的接受衡准。

（5）系统约束。

6.2.2 建立安全和性能可接受的衡准。可接受性能衡准按 2.5.4 的要求确定，并满足如下要求：

（1）可接受衡准的表达方式应便于每个故障的评估结果与衡准进行比较。建议采用风险矩阵，严重性指数反映了故障模式对安全和发动机性能的影响，概率指数反映了事件发生的概率。

（2） 评估严重程度和发生概率概数时进行的假定应予以文件记录。

（3）故障模式的概率指数、严重度指数及风险指数的定义和取值见 2.5.3。风险矩阵（表 2.5.3.3）可分为三个区域：可接受的风险指标区域（左下指数 2、3 部分）、不可接受的风险指标区域（右上指数 6、7、8、9 部分）、风险指标中间区（指数 4、5 所在的对角线区），依据对事件的进一步描述来觉得接受与否。例如故障探测方法、故障发生后手动操作模式的可能性。该区域应尽可能采取措施降低风险。

6.2.3 识别潜在故障模式和原因。故障模式是故障所观察到的特定影响，结合控制系统框图输入输出性能规格，所有潜在的故障模式都可以识别和描述。

6.2.3.1 每个系统（子系统）应从上至下考虑，从系统的功能性输出开始，一次假定考虑一个可能原因导致的故障。既然故障模式可能有多个原因，每个故障模式潜在的原因都要进行识别。

6.2.3.2 所有潜在的共因失效也要识别。仅考虑随机发生和单个故障是不够的，因单个故障源、环境压力或人为错误，几个系统部件同时故障，就可能发生 CCF，导致系统性能恶化或故障。CCF 违反了 FMEA 时认为故障模式是相互独立的基本假设，CCF 会导致不止一项同时故障，或者具有短时间内同时故障的影响。导致 CCF 的典型因素包括环境影响、电干扰、温度循环、振动以及人为因素（如操作或维护错误等）。

6.2.4 评估故障模式的影响。故障模式对系统或部件的运行、功能或状态产生的后果称为“故障影响”，故障影响应考虑安全和可获得性进行评估局部和总体影响评估，比如局部影响主要考虑对发动机安全系统的影响，总体影响和发动机的应用相关（比如单主推进柴油机或多机推进布置）。

6.2.5 识别故障探测方法。故障探测方法可以是视觉或听觉报警装置、自动感应装置、传感仪器、手动检查或其他专门的指示。每个故障和原因都应识别探测方法。

6.2.6 评估严重程度和发生概率。每个故障影响的严重程度和每个故障模式发生的概率应进行评估（按 2.5.3 规定的指数表）。在确定严重度指数时应考虑对安全和可获得性的局部影响和总体影响。

6.2.7 评估已建立的风险指数。每个故障模式的风险指数都应按 2.5.3 和表 2.5.3.3 的要求进行评估。

6.2.8 识别故障模式纠正措施。为防止或减少系统元件或部件故障模式的影响，在给定系统水平触发的备用设备响应或任何纠正措施（手动或自动）都应进行识别和评估。

6.2.9 文件形式进行分析。FMEA 最好按 2.7.1 所示的工作表进行分析，工作表应从系统最高级开始，然后逐步向下层进行。

6.2.10 试验程序输入的描述。应制定试验程序支持 FMEA 得出的结论，验证分析时的各种假定。FMEA 通常应作为试验项目制定的输入，尤其是型式试验（TAT）和工厂认可试验（FAT）期间的相关试验项目。

6.3 FMEA 报告

6.3.1 柴油机电控系统应按 2.7 的要求编制 FMEA 报告，并至少包含如下方面的内容：

（1）柴油机控制系统的说明；

（2）子系统和功能；

（3）故障模式的工作和环境条件；

（4）原因和影响；

（5）分析假设；

（6）系统方框图；

（7）性能接受衡准；

（8）工作表（2.7.1）；

（9）试验程序和其他试验报告。

6.3.2 报告还应包含 FMEA 主要结论的总结，比如针对接受衡准的评估结果等。

参考文献

[1] IEC 60812-2006: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[2] IEC/ISO 31010-2009: Risk management – Risk assessment techniques

[3] GB/T 7826-2012：系统可靠性分析技术 故障模式和影响分析（FMEA）程序

[4] IACS REC.138: Recommendation for the FMEA process for diesel engine control systems, 2014

[5] The International Marine Contractors Association (IMCA). Guidance on Failure Modes & Effects Analyses (FMEAs), 2002

[6] 国际海事组织. 2000 年国际高速船安全规则. 中国船级社，译，北京：人民交通出版社，2002

[7]国际海事组织. MSC/Circ.645: Guidelines for Vessels with Dynamic Positioning Systems, 1994

[8]中国船级社. 钢质海船入级规范（2015），人民交通出版社股份有限公司，2015