Journal of Electrical Engineering 电气工程, 2020, 8(1), 1-7
Published Online March 2020 in Hans. http://www.hanspub.org/journal/jee
https://doi.org/10.12677/jee.2020.81001

Hans汉斯

The Basic Analysis on Function Safety of Offshore Crane Electrical System

Yanwen Yu, Fangwei Qin

Shanghai Zhenhua Heavy Industries Co., Ltd., Shanghai
Email: yuyanwen@zpmc.com

Received: Jan. 17th, 2020; accepted: Jan. 30th, 2020; published: Feb. 5th, 2020

Abstract

In order to fulfill the related requirement of offshore crane export to Europe, the crane electrical system design must satisfy the safety regulation of EU laws, especially the function safety requirement in offshore crane standard. The action of electrical system model selection must be taken, including the controller, safety related sensors and limit switches. The next step is to evaluate the performance level of the crane control system by using SISTEMA software, and verify the calculation result, and finally provide a simple design navigation for offshore crane electrical designers.

Keywords

Function Safety, Offshore Crane, Performance Level

海事起重机电气系统的功能安全评估浅析

俞燕雯，秦方玮

上海振华重工(集团)股份有限公司，上海
Email: yuyanwen@zpmc.com

收稿日期：2020年1月17日；录用日期：2020年1月30日；发布日期：2020年2月5日

摘　要

为了实现国产海事起重机符合出口到欧洲的相关条件，需要满足欧盟法律中对于安全规范的要求，特别是海事起重机标准中对于功能安全的要求，对此进行海事起重机电气控制系统选型，包括控制器、安全相关的传感器和限位等设备，然后使用SISTEMA软件对电气系统的功能安全进行分析评价，并进行结果验证，为海事起重机电气设计人员提供一种简便的设计指南。

文章引用: 俞燕雯, 秦方玮. 海事起重机电气系统的功能安全评估浅析[J]. 电气工程, 2020, 8(1): 1-7.
DOI: 10.12677/jee.2020.81001

关键词

功能安全，海事起重机，性能等级

1. 引言

海事起重机指的是安装在船舶或者海上设施上的起重机，其设计和建造的标准主要为船级社的起重设备标准，如中国船级社的《船舶与海上设施起重设备规范》，在欧洲不仅需要满足当地船级社的规范还需要满足欧洲 ISO 13852-1:2013《通用海事起重机》标准的要求，其中提出了不少安全相关的要求，例如满足 ISO-13849《机械安全－控制系统安全相关功能》对于起重机的性能等级要求。为了设计满足能够在欧洲市场销售和使用的海事起重机，对海事起重机电气系统设计进行研究，并分析论证能否满足当地的标准。而目前在国内针对海事起重机控制系统领域，功能安全的简易评价和分析方法在公开渠道并无太多资料，作者通过自己的日常工作总结分析了一套可用的方法。

2. 欧洲海事起重机标准和功能安全标准

2.1. 欧洲海事起重机标准

欧洲海事起重机标准 ISO 13852-1:2013《通用海事起重机》是在欧盟境内生效的法律，适用于欧盟区域内的海事起重机需要满足其要求。在规范的 5.3.1 节中指出电气技术设备需要满足 EN61508《电气/电子/可编程电子安全系统的功能安全》和 EN ISO 13849-1:2008 的要求，在 5.9.1“过载和过力矩保护”以及 5.10“载人提升”中又一次提出需要满足 EN ISO 13849-1:2008 的要求，且在该规范表 1 中明确了详细要求。

Table 1. Offshore crane risk analysis and performance class requirements [4]
表 1. 海事起重机风险分析和性能等级要求表[4]

风险	严重性	频率	避免风险的可能性	PLr(所需的性能等级)
臂架下坠	S2	F2	P1	d
货物下坠	S2	F1	P1	c
不受控的回转	S2	F1	P1	c
不受控的伸缩	S2	F1	P1	c
不受控的起重	S2	F1	P1	c
不受控的变幅	S2	F1	P1	c

注释：S1：轻微伤害，S2：严重伤害；F1：极少发生或不频繁发生，F2：持续发生；P1：在某种情况下可能发生，P2：很低可能。

以上表格是根据海事起重机的风险进行分析，然后得出所需的性能能级，举例来说，臂架下坠的风险属于会造成人员和物品严重损坏的情况，而且其发生的概率为持续发生，而能够避免风险发生的可能性为很低，故提出其所需的性能等级为 PLr = d，此分析结论已经由 EN13852 附录 K 进行了规定，可作

为设计的输入依据。从上述要求中可知，对于起重机来说最严重的情况就是臂架下坠的风险，所以如果设计的电气系统能够满足“臂架下坠”要求的性能等级，即能够满足 PLd 的话，则该起重机的电气系统满足欧洲海事起重机标准。

2.2. 欧洲机械安全标准

前述的欧洲海事起重机标准是主要针对海事起重机的各种安全要求的标准，其中提及了性能等级的要求，这方面涉及的内容则需要查看 EN ISO 13849《机械安全 - 控制系统安全相关功能》。里面对于如何评估到达所需的性能等级 PL 进行了说明。

在该规范中使用了 4 种重要的参数来评估是否满足安全等级[1]。

1) Category 类别描述控制系统的基本设计

2) MTTFd 到危险失效的平均时间

3) DC 诊断覆盖率，有多少失效能够被检测

4) CCF 共因失效

性能等级 PL = (类别, MTTFd, DC, CCF)/(软件或系统失效)

以上的分析过程其实非常复杂，如从基本元器件开始分析的话，需要非常多的基础统计数据和复杂的统计公式，对于工程设计来说很困难的。故从工程实际出发，可以采购具有安全评估的元器件，然后基于这些元器件的参数进行某个功能或机器的安全评估，验证是否满足规范的要求。

3. 电气系统设计

3.1. 海事起重机及其电气系统介绍

一般的海事起重机如下图 1 所示，包含起升、变幅、回转这三种机构类型，起升机构用来提升货物使用；变幅机构用来调节起升的最大高度和吊载的幅度，回转机构能在船体的水平方向进行回转，完成货物的水平方向的搬运任务。

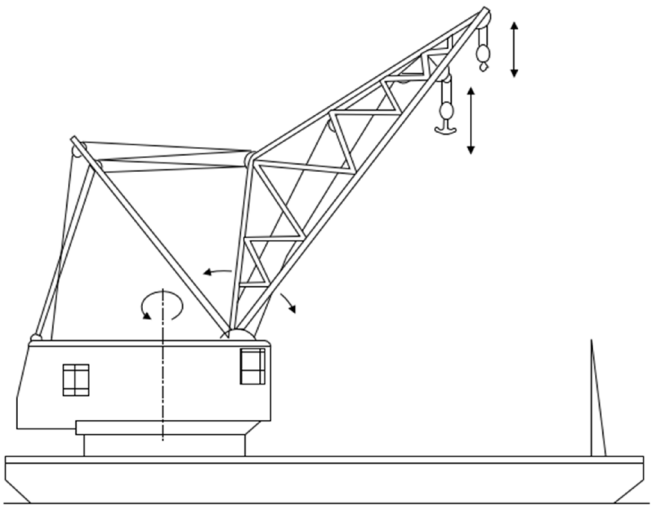

Figure 1. Offshore crane structure diagram
图 1. 海事起重机结构简图

一般的海事起重机电气系统由配电系统、驱动系统、控制系统和辅助系统组成，配电系统实现起重机的主电源和辅助电源的配电、辅助电机的启动和保护管理；驱动系统是驱动上述起升变幅和回转机构

的动力系统、一般分为液压驱动和变频驱动两种类型；控制系统包括控制器、输入输出模块、限位和传感器等元件，实现起重机的正常控制和安全保护，本文主要讨论的就是控制系统。辅助系统则指的是起重机上的照明、通讯、火警、视频监控等辅助设备。

3.2. 机械方案

从 2.1 节可知，起重机中最严重的风险是臂架下坠，故以变幅机构为例进行研究，如变幅机构能够满足安全性能要求，则其他类似的起升机构和回转机构也能轻易满足规范的要求。

变幅机构为钢丝绳臂架变幅方案，变幅卷筒由电动机驱动能够正反转运行，变幅卷筒上缠绕钢丝绳，钢丝绳经过人字架变幅滑轮上到臂架，然后到臂架头部的变幅滑轮，经过多个如此的滑轮组，最后生根固定。变幅卷筒往收绳方向运行则臂架被拉升起来，变幅卷筒往放绳方向运行则臂架被下放，如图 2 所示。

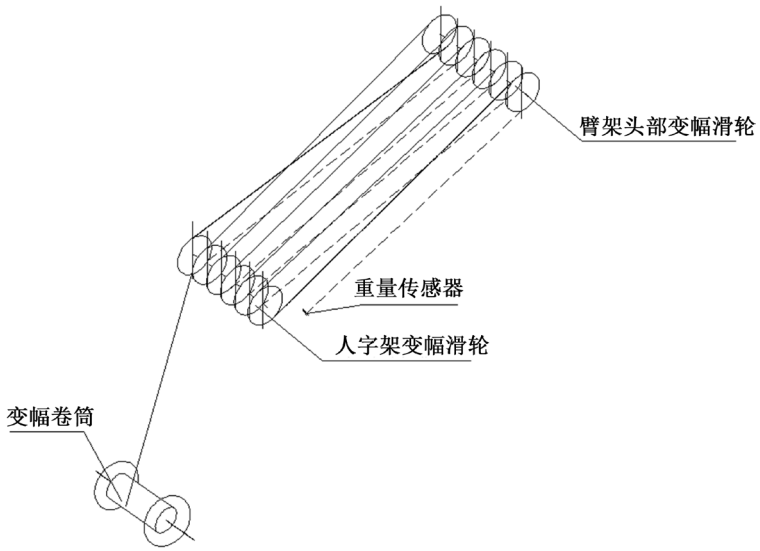

Figure 2. Wire rope scheme diagram of luffing mechanism
图 2. 变幅机构钢丝绳方案图

3.3. 电气保护元件方案

如表 2 所示，以上限位和传感器监测包括了变幅机构可能出现的超行程，过载，过力矩，超速等风险，功能上已经覆盖了这些要求，但是其本身的可靠性也需要满足性能等级要求。

Table 2. List of electrical protection elements for luffing mechanism
表 2. 变幅机构电气保护元件表

限位传感器	作用	型号
臂架上下极限限位	监测变幅上下行程极限	GS711S
臂架重量传感器	监测变幅钢丝绳受力，防止过载荷输出	0201 系列
臂架角度传感器	监测变幅角度，防止变幅过力矩输出	HAT1200
臂架卷筒超速开关	监控卷筒转速，防止下坠超速	FSI
紧停开关	手动紧急停止变幅操作	SMILE10
绝对值编码器	监测卷筒的运行位置	FSI
电机驱动器	驱动电机运转速度和方向	S120（安全集成）

3.4. 电控系统方案

电控系统主要基于西门子的故障安全 PLC 产品，本次以 S7-1513F 为例。该安全 PLC 产品包含 CPU，IO 站以及现场总线 PROFIsafe。故障安全 CPU 包含 2 个内部的处理器，对输入的信号进行计算，只有双方计算的结果相同时才输出，不同时用故障安全值代替输出，保证逻辑判断结果正确的高可靠性。而故障安全 IO 包括安全的数字量输入，数字量输出，模拟量输入模块。故障安全的数字量输入模块一般采用 1oo2 评估的方式，例如一个外部限位包含 2 副常闭触点，只有这 2 副常闭触点均闭合才认为该外部限位处于正常状态，而通过常闭触点也是一种线路安全的考量。此外该安全数字量模块还会对限位进行脉冲测试，测量是否断线，有无短路和断路的情况，通过这些手段确保该外部限位输出正常可信的状态。而安全数字量输出模块外部可以连接指示灯、接触器的执行机构，该模块也会监测执行机构是否有短路、断路的故障。而安全模拟量输入模块则会评估外部传感器 2 路信号是否都存在、有无短路、断路的故障、以及 2 者的偏差是否在一个可接受的范围之内。总之各种 IO 模块都采取了一些措施来检测外部设备的状态，确保故障能够被检测到。

故障安全 CPU 和故障安全的 IO 站之间可以采用现场总线连接，无需全部硬线接到 CPU 中。利用西门子的 PROFINET 或 PROFIBUS 现场总线，在这上面叠加 PROFIsafe 安全协议，确保 IO 站和 CPU 之间的通讯是可靠的。为了避免网络传输错误，PROFIsafe 采用了故障安全按位编号，带应答的时间监控，用密码标识发送器和接收器，增设 16/32 位循环冗余校验(CRC)等措施以保证数据的安全。此外，PROFIsafe 还采用了 SIL-Monitor 专利技术，SIL 监视器本身不是硬件，而是可实现 PROFIsafe－驱动器软件的一部分。借助 SIL-Monitor，F－系统能够在故障率超过一定限度之前即采取有效的安全保护措施，从而避免系统中出现险情[2]。

如上所述此电控方案使用故障安全 CPU、故障安全 IO 站和安全的现场总线协议，构成一个完整的故障安全控制器系统。并且对于外部的限位传感器采用规范中 CAT.3 架构，对于一个信号采用 2 路输入评估，然后经过故障安全 CPU 的逻辑处理，最后采用 2 路安全输出，把输出的执行器在回路中串联，保证只有 2 路均有安全输出之后才能使执行机构动作，如图 3 所示。

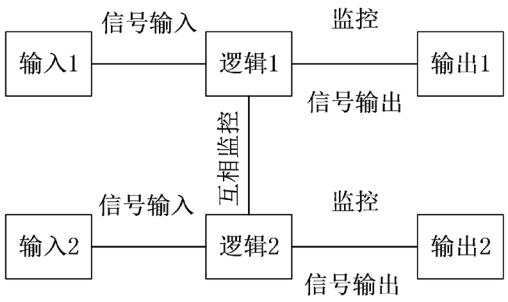

Figure 3. CAT.3 diagram
图 3. CAT.3 架构图

4. 功能安全分析和评估

4.1. SISTEMA 软件

SISTEMA 软件是 IFA (德国社会意外保险的职业安全和健康研究所)推出的一款帮助进行基于 ISO13849-1 功能安全评估分析的软件。这款工具能够建立安全相关控制系统的结构模型，自动计算可靠性数据，包括性能等级 PL [3]。

在 SISTEMA 软件中建立一个项目，然后创建一个臂架的安全功能，在里面添加上述的传感器、限位和安全 PLC 的可靠性数据。然后通过该软件创建一个分析报告。根据规范的要求臂架安全功能要求的性能等级为 PLd，下面根据相关的数据进行计算方案是否满足规范要求，如图 4 所示。

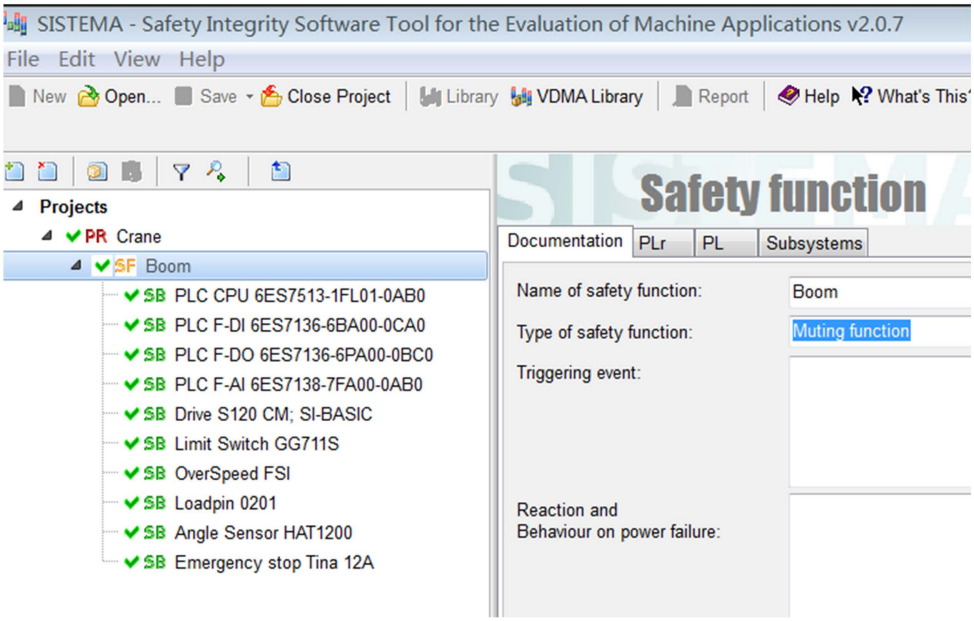

Figure 4. SISTEMA Screenshots
图 4. SISTEMA 软件截图

4.2. 数据

通过搜集厂家的样本信息，整理汇总功能安全所需的数据如下表 3 所示；以及性能等级与每小时危险失效概率之间的对应关系，如下表 4 所示。

Table 3. Summary of electrical component failure safety information
表 3. 电气元件故障安全信息汇总表

名称	型号	性能等级 PL	每小时危险失效概率 PFHD[1/h]
CPU	6ES7513-1FL01-0AB0	e	2.0E−9
安全数字量输入模块	6ES7136-6BA00-0CA0	e	1.0E−9
安全数字量输出模块	6ES7136-6PA00-0BC0	e	1.0E−9
安全模拟量输入模块	6ES7138-7FA00-0AB0	e	1.0E−8
驱动器	S120 CM	e	2.4E−8
感应限位	GG711S	d	1.0E−7
超速开关	FSI	d	1.0E−7
重量传感器	0201	d	3.2E−7
角度传感器	HAT1200	d	3.2E−7
紧停开关	Tina 12A	e	4.5E−9

Table 4. The relationship between performance level and probability of dangerous failure per hour
表 4. 性能等级与每小时危险失效概率之间的对应关系(ISO 13849-1)

性能等级 PL	每小时危险失效概率 PFHD [1/h]
a	10^{-5}~10^{-4}
b	10^{-6}~10^{-5}
c	10^{-6}~10^{-5}
d	10^{-7}~10^{-6}
e	10^{-8}~10^{-7}

4.3. 结果

在 SISTEMA 中点击生成报告，软件会统一计算，并出具计算报表，告知当前方案的性能等级 PL，以及是否满足期望的性能等级。

设每个部件的 PFHD 为 P，$P_{总}=1-(1-P_1)\times(1-P_2)\times(1-P_3)\times(1-P_4)\times(1-P_5)\cdots$

通过以上公式计算以上 10 个零件叠加后的变幅机构的安全相关控制系统的每小时危险失效概率。

此次方案的期望性能等级 PLr = d，而 PL d 所对应的每小时危险失效概率 PFHD[1/h]的范围为 10^{-7}~10^{-6}，软件计算得出每小时危险失效概率 PFHD[1/h] = 8.7E−7(即 8.7×10^{-7})，得出的性能等级 PL = d，故满足设计要求，此方案满足欧洲海事起重机规范要求。此数据说明，安全相关的控制系统的发生危险失效的概率很低，意味着零件即使发生失效但是能够检测到失效从而进行保护；以及零部件本身的无故障工作时间很长，运行可靠性很高，如图 5 所示。

Figure 5. SISTEMA Screenshots
图 5. SISTEMA 软件截图

5. 结束语

本文首先在欧洲海事起重机规范中找到了关于海事起重机风险分析的表格以及对于性能等级的要求，然后初步了解了性能等级分析的关键因素。再从工程实际出发，通过选择已经获得安全认证的电气产品来作为起重机的电气控制方案，查找并整理这些电气产品的性能等级数据，输入到 SISTEMA 软件中，生成了起重机变幅功能的功能安全分析数据，最后结论证明这一套电气控制方案满足欧洲海事起重机规范中的性能等级要求。本文的作用是为进行海事起重机电气设计工作的工程设计人员提供一种简便有效的进行功能安全设计和验证的指南，充实了国内在此细分专业领域相关文献的欠缺。

参考文献

[1] EN ISO 13849-1. (1999) Safety of Machinery Safety-Related Parts of Control Systems Part1: General Principles for Design.

[2] 褚为中. 西门子工业自动化技术丛书: 机械安全技术及应用[M]. 北京: 机械工业出版社, 2014.

[3] SISTEMA 相关描述[EB/OL]. https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

[4] EN 13852-1:2013. (2013) Cranes- Offshore Cranes Part1: General Purpose Offshore Cranes.