DOI：10.14056/j.cnki.naoe.2017.02.007

自升式钻井平台安全系统设计

袁飞晖，陈　霖
（上海外高桥造船有限公司，上海 200137）

摘要：自升式钻井平台安全系统（Safety Instrument System，SIS）是一种保护系统，用于平台事故预警、人员和设备保护，并在安全的前提下实现生产效益最大化。介绍自升式钻井平台上 SIS 的组成及其关键指标，开展系统功能设计和常用安全度的计算，采用可靠性框图法完成典型安全控制流程的安全度计算。

关键词：安全度等级；可用性；表决结构；逻辑；切断
中图分类号：U674.38^{+}1　　**文献标志码：**A　　**文章编号：**2095-4069 (2017) 02-0040-06

Design of the Security System for Jack-Up Drilling Rig

YUAN Fei-hui，CHEN Lin
（Shanghai Waigaoqiao Shipbuilding Co., Ltd., Shanghai 200137, China）

Abstract: Security system of Jack-up drilling rig is a kind of protection system for the purpose of accident pre-caution, people and equipment protection and production benefit maximization on the premise of safety. This paper introduces the composition of the security system and its key index, the function design of the system and the methods used in safety integrity level calculation, where reliability block diagram is used in calculating the safety integrity level of the typical safety control process.

Key words: safety integrity level; availability; voting architecture; logic; shutdown

1　平台安全系统概述

平台安全系统（Safety Instrument System，SIS）又称安全切断、安全保护系统，主要包括火灾和气体探测报警系统及应急切断系统 2 套子系统，使其正常运行是自升式钻井平台安全生产作业的前提和保证。

1.1　系统组成

平台安全系统是基于继电器或 PLC（Programmable Logic Controller）技术，由输入、输出和控制器组成的控制系统。其工作原理为：读取来自于可寻址的火灾探测系统、气体和火焰探测器、CO_2 系统及应急切断按钮等外部系统的输入信号，经逻辑控制器处理后输出至执行结构，完成通风设备或油气设备关闭及消防设备启动等动作，使设备和人员处于安全状态，达到控制事故、减轻事故影响和消除事故的目标。自升式钻井平台安全系统流程图见图 1。

收稿日期：2016-09-23
作者简介：袁飞晖，男，高级工程师，工程硕士，1978 年生。2011 年毕业于华中科技大学工业工程专业，现从事船舶和海洋工程电气自动化设计及技术管理工作。

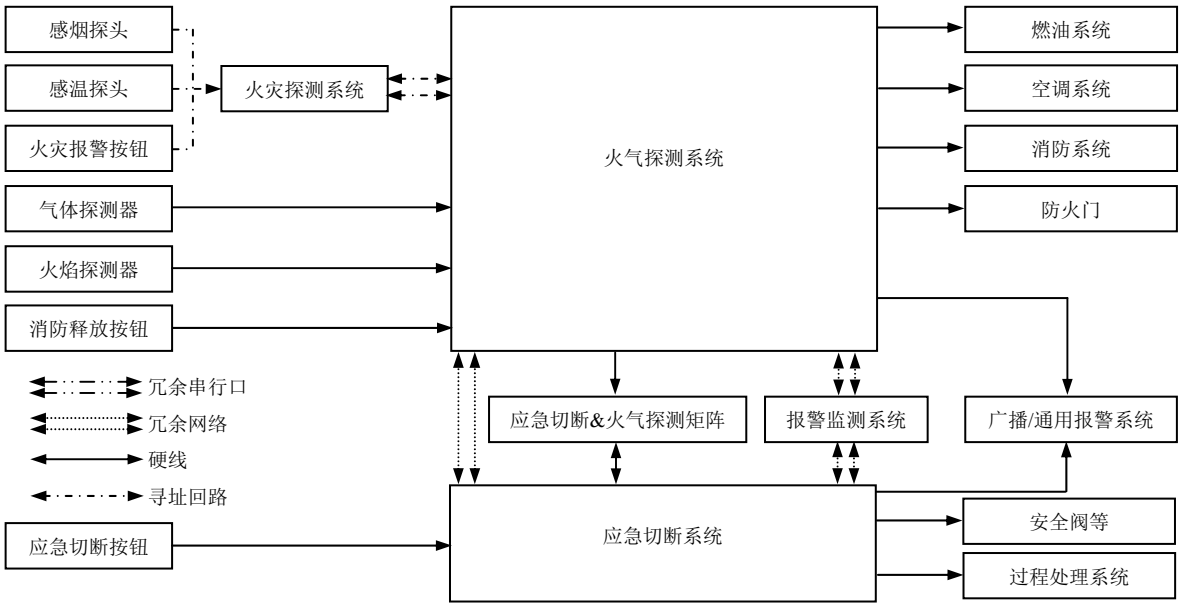

图 1　自升式钻井平台安全系统流程图

1.2　系统设计指标

安全系统设计的目标包括：

1) 功能安全满足平台的安全要求，即功能安全性；

2) 安全系统本身的安全等级达到相关规范的要求，即安全度等级。

1.2.1　功能安全性

系统功能安全性是指安全系统的动作结果安全性。安全系统主要用于对平台危险因素进行监测、控制、减轻和消除。在发生危险或安全系统自身出现故障时，系统的动作应能有效控制、减轻（甚至是清除）事故和风险，同时不会带来新的风险。系统的设计结果应是动作后所有设备都处于安全状态，以保证人员和设备的安全。

1.2.2　系统安全性

系统安全性是指系统执行安全动作的可靠性，用安全度等级来度量，定义为 PFD（Probability of Failure on Demand）。其含义是系统响应并执行时失败的概率，即当发生需求时未能满足需求（即不能正常完成保护功能）的概率，具体安全度等级描述见表 1。

表 1　安全度等级描述

ISA-S84.01	IEC 61508	DINV19520 (TüV)	PFD	说明
SIL.1	SIL.1	AK1~3	10^{-2}～10^{-1}	仅对少量的财产和简单的生产及产品进行保护
SIL.2	SIL.2	AK4	10^{-3}～10^{-2}	既对大量的财产和复杂的生产及产品进行保护，又对生产操作人员进行保护
SIL.3	SIL.3	AK5~6	10^{-4}～10^{-3}	对工厂的财产、全体员工的生命和整个社区的安全进行保护
—	SIL.4	AK7~8	10^{-5}～10^{-4}	避免会对整个社区带来巨大冲击的灾难性事故（例如核事故）

1.2.3 系统可用性

系统的可靠性采用平均无故障时间（t_{MTTF}）来度量；系统的可维护性采用平均维护时间（t_{MTTR}）来度量；而计算机可用性定义为

$$可用性 = t_{MTTF}/(t_{MTTF}+t_{MTTR})\times 100\% \tag{1}$$

在自升式钻井平台中，通常采用定期维护的管理方式。参照运行项目经验，t_{MTTR} 均以小时计，而 t_{MTTF} 在 1 000 h 以上，因此可用性和可靠性通常是一致的。

系统安全性和系统可用性是衡量安全仪表系统优劣的重要指标，无论是安全性低还是可用性低，都会使损失的概率提高。从某种意义上说，安全性和可用性是矛盾的 2 个方面：某些措施会提高安全性，但会导致可用性下降；反之亦然。因此，设计时要兼顾安全性和可用性。安全性是前提，可用性是基础，可用性必须服从于安全性。

2 安全系统设计

安全系统的本质作用是保证生产安全，同时服务于生产。因此，在设计系统时，应在保证功能安全性和系统安全性的前提下兼顾系统可用性设计。

2.1 设计步骤

参考美国仪器、系统和自动化协会（The Instrumentation, System, and Automation Society，ISA）关于安全系统设计生命周期流程[1]见图 2。

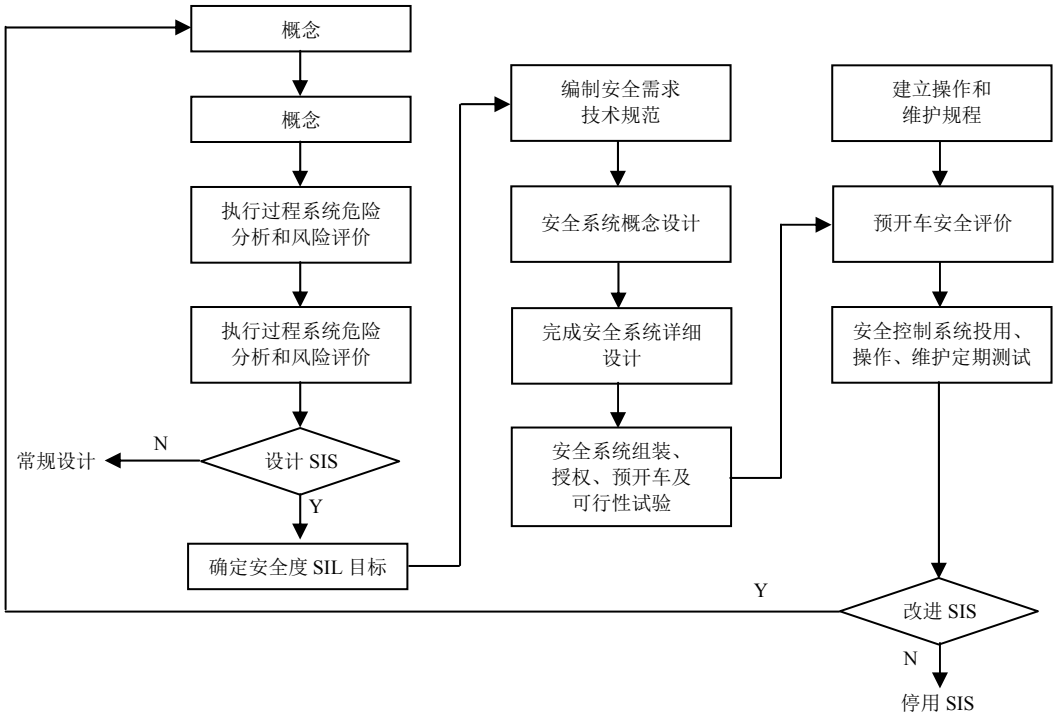

图 2 安全系统设计生命周期流程

自升式钻井平台自身无航行能力，适合在近海区域进行钻井勘探作业。其风险主要来自于火灾、可燃和有毒性气体泄漏及设备故障等。因此，自升式钻井平台安全系统的设计以应对上述危险的需求进行，安全功能应以预防、控制和消除上述危险为目的，避免故障扩大。

在标准安全系统的设计流程中，通过风险评估明确需降低的风险值[2]，通过评定计算确定需要的安全度等级，主要采用的定性计算法有风险矩阵法、定量计算法和基于频率定性法等。然而，在平台安全系统的设计中，相对于化工、矿产等行业，系统功能在流程上更加简单，且产品通用性更强，因此，安全度等级的需求一般都在满足船级社安全规范的基础上由建造及技术规格书予以明确。由此，相较于标准安全系统的设计，自升式钻井平台安全系统的设计步骤可简化为以下形式。

1) 总体目标：应对火灾、可燃性和有毒性气体泄漏和误操作；
2) 控制技术选择：电动、气动及 PLC 控制技术等；
3) 安全度等级(SIL)：参照建造及技术规格书要求；
4) 体系结构：综合考虑系统的安全性和可用性，对系统的结构进行合理配置；
5) 详细设计：包括功能安全性和系统安全性。

2.2 功能设计

自升式钻井平台的主要危险来自于火灾事故、可燃性或有毒性气体泄漏事故等，因此应将这些危险发生后有效进行报警、隔离、灭火和关闭设备等操作包含在安全系统的设计中，以保护人员和设备的安全。

2.2.1 控制技术和结构

在自升式平台系统设计中，安全度等级通常选择为 SIL1 或 SIL2；同时，为满足系统的集成需求，一般选择基于 PLC 技术构建的安全控制系统。表决结构采用 1oo2D，以提高系统的安全性。冗余 PLC 热备技术，实现无扰动转换，确保系统的可靠性，并兼顾系统的可用性。传感器系统和现场子系统间普遍采用 1oo1 架构，在满足安全度目标的前提下，尽可能地简化系统，降低成本。若有特殊情况和需求，可单独进行设计。

2.2.2 典型控制流程设计

根据图 1，自升式钻井平台安全系统主要包括火灾和气体探测系统及应急切断系统 2 部分，每个流程都涵盖输入、逻辑控制和输出等 3 个环节。平台安全系统的典型控制流程有应急切断按钮手动触发和火气警报自动触发 2 种模式。

2.2.2.1 应急切断按钮手动触发流程

应急切断按钮被触发之后，系统会触发平台上的相应报警，并切断风、油等设备，属于典型的开环控制，流程见图 3。

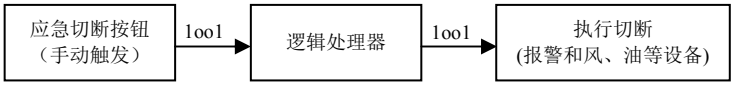

图 3 应急切断按钮触发流程

2.2.2.2 火气警报自动触发流程

火灾和气体传感器触发流程属于自动触发流程。以气体探测器为例，一旦检测到高位报警，信号经逻辑处理器处理后触发相应的切断风、油等设备并报警；启动消防措施等流程。详细流程见图 4。

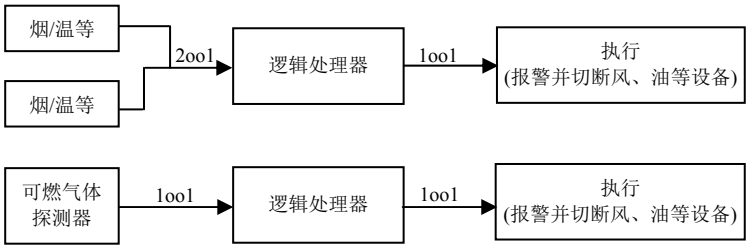

图 4 气体探测器触发流程

系统的安全状态应由设备服务目的、设备所处的环境及设备在整套流程中的控制作用来定义。平台上普通机械处所内的风、油设备应是关闭或停止运行的，因此图 3 和图 4 中的设备都是在事故发生后被切断，进入安全状态。然而，对于平台上的动力处所（如发电机间）和危险气体产生处所（如泥浆池），应在火灾或气体事故发生之后维持运行或加大排风，以达到控制事故和减轻事故影响的目的。设备的安全状态并非都是停止状态，应根据服务处所和服务对象进行具体分析、区别定义。

2.3 系统安全性验证——安全度计算

在系统设计完成之后，需对其安全性进行评估，确保其安全功能达到设计的安全度等级。若计算值不符合设计需求，则应重新对系统进行设计或改造。

2.3.1 安全度计算方法

针对安全度等级，主流的计算方法有可靠性框图、故障树和马尔可夫模型（Markov）等[3-4]。

1) 可靠性框图是一种传统的可靠性分析方法，使用图形结构标示系统内部的串并联关系，简单、直观。1oo2 可靠性框图见图 5。

2) 故障树根据布尔逻辑图标示系统特定的故障，推理分析故障发生的基本原因，建立从结构到原因的有效逻辑图。1oo1 故障树模型见图 6。

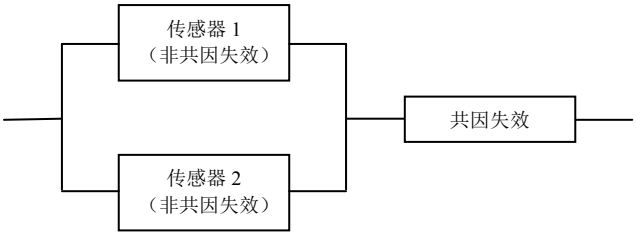

图 5　1oo2 可靠性框图

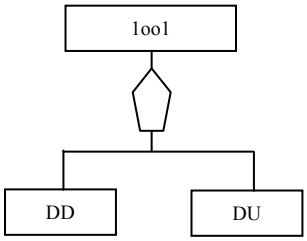

图 6　1oo1 故障树模型

3) 马尔可夫模型定义系统中全部互斥的成功/失效状态，由已编码的圆圈标示。系统以某种概率由一种状态转向另一种状态，无论是失效还是维修，状态转移都用箭头转移弧标示，并注明失效率或维修率，从而描述系统随时间变化的行为[5]。1oo1 马尔可夫模型见图 7。

在自升式钻井平台安全系统中，主要使用 1oo1 和 1oo2D 2 种结构，这里采用 IEC 61508-6 中推荐的可靠性框图对安全度等级进行验证。

2.3.2　安全度等级验证

1) 以应急切断按钮手动触发为例，流程可转化为应急切断表决框图（见图 8），以此进行计算。

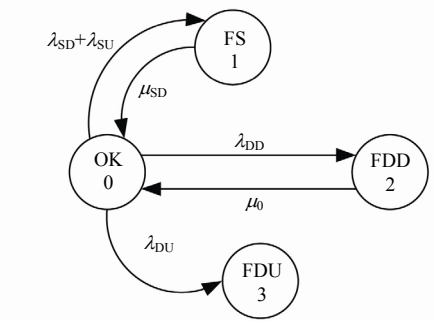

图 7　1oo1 马尔可夫模型

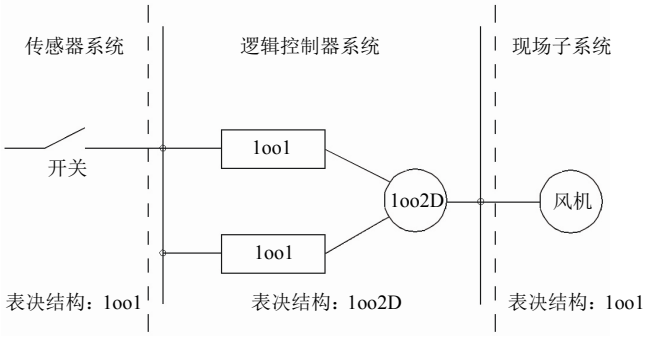

图 8　应急切断按钮手动触发表决框图

系统由传感器系统、逻辑控制器系统和现场子系统等 3 部分组成，其安全度计算应为

$$P_{\mathrm{PFDSYS}} = P_{\mathrm{PFDS}} + P_{\mathrm{PFDL}} + P_{\mathrm{PFDFE}} \tag{2}$$

式(2)中：P_{PFDSYS} 为 E/E/PE 安全相关系统的安全功能在要求时的平均失效概率；P_{PFDS} 为传感器子系统要求时的平均失效概率；P_{PFDL} 为逻辑子系统要求时的平均失效概率；P_{PFDFE} 为现场子系统要求时的平均失效概率。

2) 参照 IEC 61508 – 6，可查出 1oo1 结构和 1oo2D 结构的 PFD 计算式[6]为

$$\begin{cases} P_{\mathrm{PFD_G}} = (\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}})t_{\mathrm{CE}} \\ \lambda_{\mathrm{DU}} = \lambda / 2(1 - P_{\mathrm{DC}}) \\ \lambda_{\mathrm{DD}} = \lambda / 2P_{\mathrm{DC}} \\ t_{\mathrm{CE}} = \lambda_{\mathrm{DU}} / \lambda_{\mathrm{D}} \left(T_1 / 2 + t_{\mathrm{MTTR}}\right) + \lambda_{\mathrm{DD}} / \lambda_{\mathrm{D}} t_{\mathrm{MTTR}} \end{cases} \tag{3}$$

$$\begin{cases} P_{\mathrm{PFD_G}} = 2(1-\beta)\lambda_{\mathrm{DU}} + [(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}}]t'_{\mathrm{CE}}t'_{\mathrm{GE}} + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}t_{\mathrm{MTTR}} + \beta\lambda_{\mathrm{DU}}(T_1/2 + t_{\mathrm{MTTR}}) \\ \lambda_{\mathrm{SD}} = \lambda / 2P_{\mathrm{DC}} \\ t'_{\mathrm{CE}} = \left[\lambda_{\mathrm{DU}} / (T_1/2 + t_{\mathrm{MTTR}}) + (\lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}})t_{\mathrm{MTTR}}\right] / (\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}}) \\ t'_{\mathrm{GE}} = \left[\lambda_{\mathrm{DU}} / (T_1/3 + t_{\mathrm{MTTR}}) + (\lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}})t_{\mathrm{MTTR}}\right] / (\lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{SD}}) \end{cases} \tag{4}$$

式(3)和式(4)中：T_1 为检验测试时间间隔，h；t_{MTTR} 为平均恢复时间，h；P_{DC} 为诊断覆盖率，在公式中以分数或百分比的形式表示；λ 为子系统中一个通道的失效率（每小时）；λ_{D} 为子系统中通道的危险失效率（每小时），$\lambda_{\mathrm{D}} = 0.5\lambda$（假设 50%的危险失效和 50%的安全失效）；$\lambda_{\mathrm{DD}}$ 为检测到的子系统中通道每小时的危险失效率（子系统通道中所有检测到的危险失效率的总和）；c 为未检测到的子系统中通道每小时的危险失效率（子系统通道中所有未检测到的危险失效率的总和）；t_{CE} 为 1oo1，1oo2，2oo2，1oo2D，2oo3 结

构中通道的等效平均停止工作时间（子系统通道中所有部件的组合关闭时间），h；λ_{SD} 为子系统中被检测到的通道每小时的安全失效率（子系统通道中所有检测到的安全失效率的总和）；t'_{CE} 为 1oo2D 结构中通道的等效平均停止工作时间（子系统通道中所有部件的组合关闭时间），h；t'_{GE} 为 1oo2D 结构中表决组的等效平均停止工作时间（表决组中所有部件的组合关闭时间），h；β 为具有共同原因、没有被检测到的失效分数（在公式中用分数或百分比的形式表示）；β_D 为具有共同原因、已被诊断测试检测到的失效分数（在公式中用分数或百分比的形式表示），假设 $\beta = 2\beta_D$。

3) 设定维护时间间隔为 1 a，平均维护时间 $t_{MTTR} = 8\,\text{h}$。

(1) 开关：$P_{DC} = 90\%$；$\lambda = 5\times10^{-6}$。

(2) 逻辑处理器：$P_{DC} = 90\%$；$\lambda = 10\times10^{-6}$；$\beta = 2\%$；$\beta_D = 1\%$。

(3) 风机：$P_{DC} = 60\%$；$\lambda = 5\times10^{-6}$。

事实上，根据上述参数，从 IEC 61508–6 表 B.3 中可直接查得：$P_{PFD_{开关}} = 1.1\times10^{-3}$；$P_{PFD_{逻辑处理器}} = 4.8\times10^{-6}$；$P_{PFD_{风机}} = 4.4\times10^{-3}$。整个系统 $P_{PFD} = P_{PFD_{开关}} + P_{PFD_{逻辑处理器}} + P_{PFD_{风机}} = 5.5\times10^{-3} =$ 安全度等级2。

因此，安全系统部分的设计达到 SIL2 等级。从 PFD 结果分析看，安全系统中所有部件都是相互制约的，安全度等级受制于安全度最低的部分。从 IEC 61508–6 表 B.3 中可看出，在参数相同的情况下，1oo2D 结构的 PFD 值明显优于 1oo1 结构，因此改变表决结构是提高系统安全度等级的可行方法，这也是目前系统改造的常用方案之一。

3 结 语

自升式钻井平台安全系统的设计以确保系统的功能安全性和系统安全性为目标，通过采用多样的控制技术和系统结构来实现。功能安全性应基于对实际环境的危险分析，对各安全控制流程进行逐一分析设计；而系统安全性则是对整套安全控制流程进行评定。通过计算分析可知，系统安全度等级受限于控制流程中传感器、逻辑控制器和执行仪表等设备的PFD值，因此在安全控制系统设计中不要忽略对逻辑控制器以外的其他部件的技术和系统结构进行评估。

【参 考 文 献】

[1] ISA. Safety Instrumented Systems (SIS) — Safety integrity level (SIL) evaluation techniques: ISA. TR84.0.02[S]. 1998.

[2] SAMMARCO J J. Safety framework for programmable electronics in mining[J]. Society of Mining Engineers, 1999: 30-33.

[3] 靳江红，吴宗之，赵寿堂，等. 安全系统的功能安全国内外发展综述[J]. 化工自动化及仪表，2010, 37 (5): 1-6.

[4] IEC. Functional safety of electrical/electronic/programmable electronic safety related systems, Part 5: examples of methods for the determination of safety integrity levels[S]. 2000.

[5] GUO H T, YANG X H. A simple reliability block diagram method for safety integrity verification [J]. Reliability Engineering and System Safety, 2007, 92: 1267-1273.

[6] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508-6[S]. 2000.