文章编号：0258-0926(2018)03-0156-06; doi:10.13832/j.jnpe.2018.03.0156

多方法融合的反应堆紧急停堆子系统安全性分析

刘 华[1]，韩文兴[2]，阳小华[3]，陈 智[2]，刘朝晖[3]

1. 南华大学电气工程学院，湖南衡阳，421001；2. 中国核动力研究设计院，成都，610041；
3. 南华大学计算机学院，湖南衡阳，421001

摘要：针对反应堆紧急停堆子系统，将故障模式影响分析（FMEA）、故障树分析（FTA）、系统理论的过程分析（STPA）3 种独立的基本分析方法进行组合，形成仪表控制系统设计阶段的失效和故障基本项覆盖统计表格。STPA 方法能够很好地弥补了 FMEA 和 FTA 方法的不足。同时，在仪控系统的设计阶段，STPA 方法非常适合发现反应堆紧急停堆子系统涉及的软件类、系统交互以及通信类的故障和安全问题。

关键词：多方法融合；反应堆紧急停堆；安全性分析
中图分类号：TL364 文献标志码：A

Safety Analysis for Reactor Scram Subsystem Based on Multiple Methods

Liu Hua[1], Han Wenxing[2], Yang Xiaohua[3], Chen Zhi[2], Liu Zhaohui[3]

1. School of Electrical Engineering, University of South China, Hengyang, Hunan, 421001, China;
2. Nuclear Power Institute of CHINA, Chengdu, 610041, China;
3. School of Computer Science and Engineering, University of South China, Hengyang, Hunan, 421001, China

Abstract: For the reactor scram subsystem, the failure and fault coverage statistics form for the instrument control system design phase is deduced by the combined use of three independent basic analysis methods FMEA, FTA, and STPA. STPA method can effectively make up for the inadequacy of FMEA and FTA method. At the same time, in the instrument control system design phase, STPA method is very suitable for finding the fault and safety issues in software, system interaction and communication for the reactor scram subsystems.

Key words: Multiple method fusion，Reactor scram subsystem，Safety analysis

0 引 言

核电厂数字化仪表控制系统为电厂安全有效地运行提供了基本信息和控制功能，如持续地为操纵员提供电厂的状态、事件以及对安全和可用性重要的变量信息[1]，帮助操纵员对上述信息进行分析和决策；同时，提供相应方式使得操纵员能够对电厂设备进行操作，并获得电厂的反馈信息[2]。

鉴于数字化仪控系统对核电厂的重要性，需要在安全级仪控系统的设计研发阶段，使用安全分析方法对仪控系统的功能、层次等进行安全分析，检验是否符合安全设计原则，是否存在潜在的失效故障，是否影响安全级仪控系统的核心功能[3]。安全级仪控系统的核心功能是 3 个：反应堆保护自动停堆、事故后监测系统、安全专设及驱动[4]。本文分析对象为反应堆紧急停堆子系统。

收稿日期：2018-04-04；修回日期：2018-05-03
基金项目：反应堆系统设计技术重点实验室开放基金、中核集团高可信计算学科重点实验室共同资助（HT-LW-02-2014005）
作者简介：刘 华，（1979—），男，讲师，现主要从事核电厂数字化仪控系统的安全分析及其研究工作

1　基本安全分析方法的比较和归纳

1.1　故障树分析（FTA）

FTA 广泛用于在系统开发阶段发现设计缺陷，以及在系统操作发生事故或问题时调查起因，是一种由上至下识别关键失效组合的方法，并基于事件链的事故模式。FTA 的输入是已知的危险、失效或事故，以及用于分析的系统设计描述[5]。FTA 过程可以分为 4 个主要步骤：①找到根结点（危害或事故或失效）；②识别出引起根结点的事件或条件的组合，将它们用布尔逻辑整合起来；③分解子结点，直到事件是确定的基本事件；④识别出最小割集，它们是引起顶事件发生的最小基本事件集。

1.2　故障模式影响分析（FMEA）

FMEA 作为一个系统性、主动性方法，主要用来评估和发现潜在失效[6]。FMEA 有助于识别部件在哪里及如何失效，并估计不同失效的相关影响。FMEA 与 FTA 一样，也是基于事件链的事故模型。它是一种由底向上的结构，基于表格，发现和记录一个部件失效的类型，以及这些失效的后果。

FMEA 的输入是系统和组件的设计描述；FMEA 过程可以分为 4 个子任务：①建立分析范围；②识别每个模块的失效模式；③确定每一个潜在失效模式的效果和它们的潜在起因；④以最坏结果的方式评估每一个失效模式，并分配给它们假定严重性的相关值等等，最终计算出风险度。设计人员需要开发出所需的控制动作，以减低与失效模式的潜在致因相关的风险。

1.3　系统理论的过程分析（STPA）

STPA 方法是一种基于系统理论事故模型和过程的安全性分析技术，它能够适用于大型复杂系统[7]。STPA 能够更完全地识别在复杂的安全关键系统中的致因因素，包括软件设计错误。在 STPA 中，系统被视为交互控制环，事故被认为是源于在设计、开发和操作过程中安全约束没有得到充分的实施[8]。

与 FTA 有所不同的是，STPA 包括了没有发生失效，却由于系统部件间的非安全和非意图交互而引发问题的情况，因此 STPA 可以涵盖更为广泛的事故场景。STPA 提供了指导与识别潜在不充分控制动作，导致危险状态等相应功能。它的实现包括 3 个主要步骤：①通过识别出系统事故或不可接受的损失事故，画出系统初步控制结构图等方式，来建立进行 STPA 分析所需的基础信息；②识别以导致危险状态的潜在非安全控制动作；③确定这些非安全控制动作为什么会发生。

2　反应堆紧急停堆子系统简介

反应堆保护系统所需的现场传感器信号（含模拟量输入/开关量输入电阻式温度探测器（RTD）温度信号/泵转速脉冲信号）首先被送至保护仪表预处理（PIPS）机柜，由 PIPS 机柜中的信号采集/隔离/分配模块处理后送至反应堆保护机柜（RPC）机柜。

在 RPC 机柜中，现场信号将在进行必要的处理后（例如开方、滤波、超前-滞后等）将与保护定值进行比较从而产生用于保护系统逻辑表决的“局部脱扣”信号。该信号除了参与自身所属保护组的逻辑表决之外，同时通过光纤网络送至其他 3 个保护组。由于每个保护组均采取这种处理方式，从而每个保护组都能获得与传感器冗余度相当的“局部脱扣”信号。然后，每个保护组对这些“局部脱扣”信号进行逻辑表决，产生通道级的紧急停堆信号和专设安全设施驱动信号。其中，2 个多样性子组的通道级紧急停堆信号均进行基于硬件的“或”运算后被送至对应的停堆断路器。

反应堆自动停堆保护系统的功能要求和设计准则应体现多样性和冗余性的设计理念[9]，整个系统由多个保护系统序列组（一般是 3 ~4 组）和多个逻辑序列（一般是 2 个）组成，功能多样性设计要求在处理保护信号参数时，将其分成多个多样性子组分别在不同的计算机处理器单元进行处理[10]。同时，核电厂数字化保护系统在设计上要保证电厂在整个寿命期内可维修和试验，冗余性设计是解决在线试验的主要技术手段。

基于以上的系统设计特点，在现行的核电厂数字化保护系统中的反应堆紧急停堆功能，主要采用单向信号序列，多重信号逻辑判断的设计思路。为提高保护系统的可靠性，在系统通道的设计中一般以无源常开触点的方式输出故障信号，

表 1 紧急停堆子系统的失效和故障基本项覆盖统计表

Table 1 Failure and Failure Coverage Statistics for Emergency Shutdown Subsystem

①基本项编号	②分析对象	③可能的失效（故障）模式及原因	④安全分析方法的覆盖			⑤系统设计中已有的应对措施	⑥应该补充的应对措施	⑦措施标记栏
			FMEA	FTA	STPA			
1	保护仪表预处理 PIPS	隔离失效，信号直通	√	√	√	电路测试	仪控系统需补充考虑	●

表 2 设计阶段紧急停堆子系统的失效和故障基本项覆盖统计节选

Table 2 Selection of Failure and Failure Basic Items for Emergency Shutdown Subsystem in Design Phase

基本项编号	分析对象	可能的失效（故障）模式及原因	安全分析方法的覆盖			系统设计中已有的应对措施	应该补充的应对措施	措施标记栏
			FMEA	FTA	STPA			
1	保护仪表预处理 PIPS	隔离失效，信号直通	√	√	√	电路测试	仪控系统需补充考虑	●
2	保护仪表预处理 PIPS	信号不能完成隔离转换	√	√	√	电路测试	仪控系统需补充考虑	●
3	主控模块电源	电路故障：虚焊，封装等	√	×	√	电路测试	—	○
4	逻辑表决模块	硬接线故障	√	√	√	自诊断	硬件监测	●
5	逻辑表决模块	数据处理软件故障（软表决）	√	√	√	多级软表决	软件自诊断	●
6	停堆相关整定值	停堆相关整定值设置错误，设置过高	√	×	×	无	参数验证	★
7	现场控制站之间的通信	通信间歇中断	√	×	√	自诊断，安全状态	共因失效分析；通信的冗余和多样性	●
8	停堆断路器	断路器失电线圈硬件故障	√	√	√	超出设计阶段的范围	定期检修，提高供货质量	△

以硬接线的方式发送到数字化仪控系统（DCS）执行报警功能的输入输出（I/O）通道中[1]。因此，传感器→信号切换→信号处理→逻辑符合判断→保护驱动的信号传递过程，构成反应堆停堆保护子系统紧急停堆功能的核心过程。

3 多方法融合的紧急停堆子系统设计阶段的安全性分析

3.1 分析流程与步骤

（1）选择的分析对象为安全级仪控系统下的反应堆紧急停堆子系统。

（2）基于反应堆停堆保护子系统紧急停堆信号的信号产生通路，采用 FMEA、FTA、STPA 方法独立分析反应堆紧急停堆子系统，将 3 种方法得到的安全分析基本项的覆盖情况，进行叠加和统计整理，完成失效和故障基本项覆盖统计表中的①~④对应列的内容见表 1。

（3）通过设计文档的审核和对应，审核已有应对措施，完成失效和故障基本项覆盖统计表中的⑤对应列的内容。

（4）在上述步骤的基础上，将设计改进、优化，补充应对的措施填入统计表中⑥对应列的内容。

（5）结合统计表中⑤、⑥列的内容，将 4 种符号○、符号●、符号★、符号△填入统计表⑦对应列中。

多方法融合的仪控系统安全性分析的最终结果是以紧急停堆子系统的失效和故障基本项覆盖统计表来体现。

失效和故障基本项覆盖统计表中，基本项编号用来标记基本的故障或安全问题；分析对象对应具体的仪控系统里软件、硬件或通信相关的模块或单元；可能的失效模式及原因是通过已有的设计文档，结合背景知识，覆盖软件、硬件或通信相关的故障和安全问题，例如表决组合逻辑电路故障、通信链路故障、组态算法的下载错误等；安全分析方法的分析覆盖这一栏，当 FMEA、FTA、STPA 方法能够覆盖某个可能的失效（故障）模式，就标记√，如果不能检测，则标记为×；系统设计中已有的应对措施这一栏，针对设计阶段

的文档，审查是否有针对具体失效和故障的应对措施，有，就简单标注，没有就需要改进、补充、优化。

多方法融合的分析表格里，措施标记栏内的符号含义有 4 种情况。

（1）符号○：系统设计已有应对措施，无需补充。

（2）符号●：系统设计已有应对措施，建议补充，加强。

（3）符号★：系统设计无应对措施，建议补充。

（4）符号△：超出系统设计范围，建议关注和补充。

失效和故障基本项覆盖统计表的样表见表 1。

限于篇幅，将失效和故障基本项覆盖表格内容，截取一部分，得到表 2。

3.2　分析结果比较

（1）失效（故障）模式及原因的基本项数量统计。

通过多方法融合安全性分析，将每种方法覆盖到的可能失效或故障原因基本项数量叠加到一起，不重复计算，得到设计阶段发现的失效或故障原因基本项 SUM=143 项。

FMEA 安全分析方法分析覆盖的基本项数量 X1=106 项。

FTA 安全分析方法分析覆盖的基本项数量 X2=87 项。

STPA 安全分析方法分析覆盖的基本项数量 X3=136 项。

设计阶段的安全级仪控系统反应堆停堆子系统已有应对措施分析覆盖的基本项数量 X4=86 项。

对那些安全级仪控系统没有的应对措施，表格中★的数量，即项目组做了建议补充的基本项数量 Y1=44 项。

对那些安全级仪控系统已有的应对措施，表格中●的数量，即项目组又做了建议补充的基本项数量 Y2=59 项。

提出改进意见或在设计研发、验证测试、运行维护等阶段应加强的基本项数量，即 44 个★和 59 个●数量之和：共计 E=103 项。

超出系统设计范围，表格中△的数量即建议关注和补充的基本项数量 C=13 项。

系统设计已有应对措施，表格中○的数量即无需补充的基本项数量 W=27 项。

（2）失效（故障）原因应对措施的覆盖率量化计算

已知设计阶段发现的失效或故障原因基本项 SUM=143 项。

基于 FMEA 安全分析方法，对安全级仪控系统可能的失效（故障）原因，分析覆盖率的量化计算：X1/SUM=106/143=74.1%。

基于 FTA 安全分析方法，对安全级仪控系统可能的失效（故障）原因，分析覆盖率的量化计算：X2/SUM=87/143=64.0%。

基于 STPA 安全分析方法，对安全级仪控系统可能的失效（故障）原因，分析覆盖率的量化计算：X3/SUM=136/143=95.1%。

安全级仪控系统项目已有的应对措施，对安全级仪控系统可能的失效（故障）原因，分析覆盖率的量化计算：X4/SUM=86/143=60.1%。

针对已有系统设计和应对措施，通过多方法融合的安全性分析，一共有 143 个故障基本项。基于这 143 个故障基本项，分析表格得到的相应的数字化仪控系统的处理措施和设计改进。

（3）多方法融合的安全分析对不同分析类别的适应性

仪控系统的设计阶段，为了完成反应堆紧急停堆子系统的故障和安全分析，将故障和安全分析的对象分为 3 个类别：硬件、软件、系统交互和通信。

硬件包括保护仪表预处理、输入输出模块、优选逻辑模块等对应的机箱或板卡。相对硬件，安全级 DCS 仪控系统的重要特点就是在仪控系统不同层次上，在不同级别的站点、机柜、机箱、板卡上，诸多软件和通信接口嵌入在对应的硬件里，共同完成复杂的控制、安全功能等[11]。反应堆紧急停堆子系统设计阶段的故障和安全分析，软件和通信功能自然成为故障和安全分析的重点对象[12]。

反应堆紧急停堆子系统涉及的软件包括：组态软件、应用软件、操作系统、支持软件等。在不同级别的站点、机柜、机箱、板卡上，DCS 仪控系统使用的软件更丰富，形态更多样，行使的功能更多[13]。软件安全分析本身就是业界的难点。本文通过多方法融合，对软件安全分析做些初步尝试和实践。

系统交互和通信功能的范围界定：除去电源接口、硬接线之外的不同板卡间、不同机箱间的所有接口，都归口到通信接口。基于通信接口执行的功能，即系统交互和通信功能。系统交互和通信功能将整个系统紧密联系在一起，完成不同子系统、不同层次设备间的有效、快速、正确连接。通信功能的正确与否直接影响系统性能。基于此，反应堆紧急停堆子系统的故障和安全分析必须重点关注系统交互和通信功能。

FTA 方法非常适合结构清晰、没有反馈、与时序关联不强的系统故障和安全分析，而紧急停堆子系统中，FTA 对硬件故障的分析是最合适的。基于 FTA 方法，硬件故障和安全问题的检测覆盖率达到 100%。但 FTA 不适合耦合度高、存在时序关联、控制约束的软件和通信故障和安全问题的发现。因此，FTA 对软件和通信故障、安全问题的发现能力是很有限的，分别只有 85%和 80%。

FMEA 方法，分析层次和粒度对故障和安全问题的检测覆盖率影响很大。本文 FMEA 方法分析层次和粒度，最低层次截止到板卡层，暂时不对元器件的单一失效作出分析，否则分析难以收敛。设计阶段的 FMEA 特点，是假定单一故障产生，分析对应的故障影响。分析对象突破了硬件的局限，考虑了软件 FMEA 和通信功能 FMEA 的情况。FMEA 方法对硬件、软件和通信 3 类故障和安全问题的分析能力相对折中，具体见表 3 的数据。

STPA 方法是基于系统角度的安全分析方法，强调系统的安全问题源于系统控制约束的缺失或不理想。分析流程是形成一个控制闭环。STPA 对硬件的故障分析能力要弱于 FTA 方法，但对软件和通信两类故障和安全问题的分析能力，明显优于 FMEA 和 FTA 方法。

表 3 多方法融合的安全分析对不同分析类别的适应性

Table 3 Adaptability of Multi-Method Fusion Security Analysis to Different Analysis Categories

分析方法	检测覆盖率/%		
	硬件	软件	系统交互和通信
FMEA	80	85	80
FTA	100	65	75
STPA	90	90	100

3.3 分析结论

通过量化对比，得到如下结论：在数字化仪控系统的设计阶段，反应堆紧急停堆子系统由于是一个硬件、软件、系统交互和通信的复杂系统，单一的分析方法 FMEA 或 FTA 方法，都有局限性。由于大量软件、通信功能的存在，FMEA 或 FTA 对故障和安全问题的发现能力是很有限的，对反应堆紧急停堆子系统的故障和安全问题检测覆盖率分别只有 74.1%和 64.0%。STPA 由于注重系统结构，适合硬件、软件、系统交互和通信的混合系统，因此在设计阶段，对反应堆紧急停堆子系统的故障和安全问题检测覆盖率达到 95.1%。

表 4 安全分析方法的故障率覆盖

Table 4 Failure Rate Coverage of Security Analysis Methods

分析方法	FMEA	FTA	STPA	设计阶段已有仪控功能应对措施
检测覆盖率/%	74.1	64.0	95.1	60.1
覆盖的基本项数量	106	87	136	86

表 4 中的设计阶段已有仪控功能应对措施，对应的检测覆盖率为 60.1%，那么初期设计阶段，未考虑的仪控功能应对措施有 39.9%。通过该指标，明确了设计阶段的改进、补充的总体要求，从而推动反应堆停堆子系统的设计改进，最终覆盖到 FMEA、FTA、STPA 这 3 种方法共同映射的基本项总数量 143 项。

从设计优化改进、故障和安全分析的角度，多方法融合的停堆子系统安全性分析给出了足够充分的建议和补充，这些建议和补充不是强制性的，但与核电仪控系统的设计准则是吻合的。这些建议和补充，既可以作为设计阶段设计人员的

重要参考，又可以是验证与确认的辅助审查参考，同时还是仪控系统运行维护阶段的参考文档。

4 结　论

通过本文分析，针对核电厂数字化仪控系统的反应堆停堆子系统，FMEA、FTA、STPA 3 种独立的基本分析方法，都能够有效地找出系统潜在可能的故障失效或设计缺陷；但没有一种覆盖率能够达到理想的 100%故障检测覆盖率；STPA 方法由于基于系统理论的控制结构和功能非线性分析，能够很好地弥补 FMEA 和 FTA 方法的不足。同时，STPA 方法在仪控系统的设计阶段，非常适合发现反应堆紧急停堆子系统涉及的软件类、系统交互以及通信类的故障和安全问题。作为创新点的基于多方法融合的故障和安全分析，给数字化仪控系统工程项目设计阶段的验证与确认，提供一个详细、可操作的审查方法和实施方案。

参考文献：

[1] 郭晓明. 核电站数字化仪控系统可靠性分析方法研究[D]. 北京：清华大学，2011.

[2] 任德曦，胡泊. 核电站安全分析方法与安全评价标准初探[J]. 人类工效学, 1996, 2(3): 35-40.

[3] 李静霞，于劲松. 核电站安全级 DCS 缺陷危害性分级的研究与应用[J]. 自动化博览，2015,16 (3): 64-67.

[4] 尹宝娟. 提高核电仪控系统软件安全性的验证技术研究[J]. 自动化博览，2012, 13(9): 68-70.DOI: 10. 3969 /j. issn. 1003-0492. 2012. 09. 018.

[5] 张永发，童节娟，周羽，等. 核电厂概率安全分析中动态可靠性方法综述[J]. 原子能科学技术, 2012, 46(4): 472-479.

[6] IEC 60812-2006, Analysis techniques for system reliability- Procedure for failure mode and effect analysis (FMEA)[S].2006.

[7] 阳小华，刘朝晖，陈智，等. 核电厂数字化仪控系统全状态监测机制[J]. 核动力工程，2014, 35(03): 138-141.

[8] 刘朝晖，陈智，吴志强，等. STPA 方法在数字化反应堆紧急停堆系统安全性分析中的研究与应用[J]. 核动力工程，2015(s2): 157-161.

[9] IEEE 352-1987, IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems[S].1987.

[10] IEC 61508-2010, Functional safety of electrical/ electronic/programmable electronic safety-related systems [S]. 2010.

[11] 艾九斤，李运坚，李相建. 核电厂 DCS 安全级应用软件开发的危险分析[J]. 计算机工程与设计, 2012, 33(6): 2323- 2327. DOI: 10.3969/ j.issn.1000- 7024. 2012. 06. 045.

[12] 李熊，程康，张春雷，等. 浅谈核电仪控系统中安全性与可靠性的关系及区别[J]. 自动化博览, 2013, (8): 60-63.DOI: 10. 3969/j. issn.1003-0492. 2013. 08. 022.

[13] 郑伟智，张礼兵，刘静波，等. 核电站安全级 DCS 应用软件设计过程浅析[J]. 自动化仪表, 2014, 35(2): 53-57. DOI: 10. 3969/j. issn. 1000-0380. 2014. 02. 015.

（责任编辑：杨洁蕾）