第41卷第6期 原 子 能 科 学 技 术 Vol. 41, No. 6
2007年11月 Atomic Energy Science and Technology Nov. 2007

田湾核电厂数字化反应堆保护系统故障模式与后果分析

周海翔

(哈尔滨工程大学 核科学与技术学院,黑龙江 哈尔滨 150001)

摘要:从田湾核电厂数字化反应堆保护系统的结构出发,对数字化保护系统可能出现的故障种类、影响区域和故障后果等进行了详细分析,通过故障模式与后果分析(FMEA)方法,对田湾核电厂数字化反应堆保护系统是否存在设计薄弱环节作出了判断。本工作为国内数字化反应堆保护系统设计提供了一些新思路。

关键词:数字化反应堆保护系统;故障模式;后果分析;核电厂

中图分类号:TP202 **文献标识码**:A **文章编号**:1000-6931(2007)06-0702-05

Failure Mode and Effect Analysis for Digital Reactor Protection System in Tianwan Nuclear Power Plant

ZHOU Hai-xiang

(*Institute of Nuclear Science and Technology, Harbin Engineering University, Harbin* 150001, *China*)

Abstract: The paper describes the structure of digital reactor protection system in Tianwan Nuclear Power Plant, and gives the analysis of the failure mode, effect area and the measure against failure. According to the analysis, the paper evaluates the reliability of digital reactor protection system. At the same time, the paper supplies some new idea for the design of digital reactor protection system.

Key words: digital reactor protection system; failure mode; effect analysis; nuclear power plant

田湾核电厂反应堆保护系统采用了德国西门子公司TXS数字化仪控系统,是目前国内核电厂中唯一的数字化反应堆保护系统。由于反应堆保护系统对核电厂安全起到至关重要的作用,因此,系统设计中的可靠性分析就显得尤为关键。文章将采用故障模式与后果分析(FMEA)的方法,详细地对数字化反应堆保护系统进行定性分析[1]。

1 结构和功能简述

田湾核电厂数字化反应堆保护系统(RPS)结构示于图1。该系统执行反应堆停堆功能和专设安全设施(ESFAS)功能。系统包括4个冗余通道,且每个冗余通道中含有2个多样性

收稿日期:2006-07-11;修回日期:2006-10-10

作者简介:周海翔(1972—),男,江苏淮安人,博士研究生,核能科学与工程专业

组 A 和 B,每个通道中的核心模块为采集处理计算机和表决计算机(VOTER),用于进行信号采集、处理和表决输出。来自 4 个独立冗余通道的变送器信号、外系统的接口信号及主/辅控制室的指令信号在信号采集处理机柜中进行采集分配后送至 RPS 系统。在运算过程中,首先通过总线设备实现 4 个通道输入数据的通信,在每一通道中对 4 个输入值取第二大或第二小,保证数据的可靠性,信号在 RPS 系统中进行采集计算和逻辑功能处理后,反应堆停堆信号(Trip)送反应堆控制棒应急控制机柜采用 4 取 2 逻辑表决后,切除控制棒电源,停闭反应堆;专设安全设施驱动系统信号在 TXS 系统的表决计算机(VOTER)中进行 4 取 2 逻辑表决后,经输出模件输出至优选功能模件,由优选功能模块对来自 RPS 系统、反应堆限值系统(RLS)、正常运行系统的控制指令和后备盘的操作命令信号进行优选控制,选取最高优先级的命令用于控制 ESFAS 功能。

表决计算机采用主从对(Master-Checker)形式,要求 Master 和 Checker 计算机模块在运算周期同步进行功能处理,并比较相互的最终输出值,只有相互的运算结果一致时,输出值才有效。一旦运算结果不同,Master 和 Checker 计算机模块都将不允许输出运算结果,并由 Checker 计算机模块根据故障安全原理直接输出"1"信号(反应堆停堆系统)或"0"信号(ESFAS系统)。

在网络通信方面,采用 1E 级 SINEC L2 总线进行通道内部或冗余通道之间的数据交换,有效地保证了数据在 TXS 系统内的可靠通信。

2　FMEA 分析

FMEA 分析的实质和目的是评估系统在假定故障条件下的动作和响应,即用于证明系统的硬件结构及其安全功能是否能够在事故工况下限制事件的发展和严重程度的加深。其首要任务是分析作为系统基本单元的独立模块和总线设备及其之间的接口可能出现的故障形式。

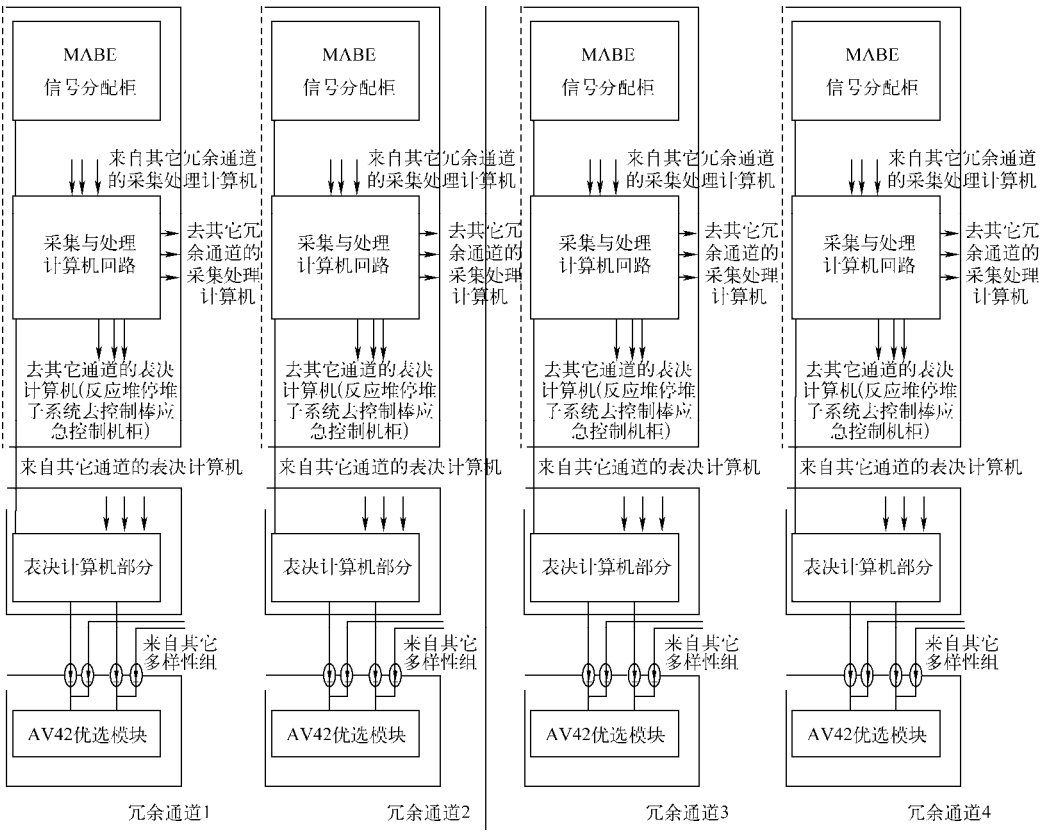

图 1　田湾核电厂数字化反应堆保护系统结构图

Fig. 1　Structure of digital reactor protection system in Tianwan Nuclear Power Plant

2.1 故障的分类

在数字化反应堆保护系统中，有2种故障形式：1）单一信号故障（如测量的输入信号或逻辑运算后的输出信号），它是故障表征的最小单元；2）硬件模块、计算机设备或数据信息的故障，这类故障可能会产生多个单一信号故障。在进行故障分析时，需要将单一信号故障和计算机模块故障（一般为系统的硬件故障）区分开[2]。

1）单一信号故障

对于系统中的每个单一信号，除信号的实际值外，还包括信号的状态信息。状态信息用于区分正常信号、故障信号和测试信号，它们在所有的信号操作过程中具有继承性，即如输入1个故障信号，随之而进行的操作和运算结果通常也视为故障信号。然而，在表决器进行表决运算时例外。例如，表决器的冗余输入中出现故障信号，那么，这些信号将被排除在运算操作之外，只将剩下的有效信号进行表决运算，表决结果仍然为有效信号。

当出现以下几种情况时，信号的状态需设定为故障状态：

（1）输入/输出模块检测存在故障或输入/输出模块没有响应（此类故障通过输入/输出模块的驱动程序来设定）；

（2）数据信息失去完整性或数据信息没有更新（此类故障通过系统实时运行环境中的软件来设定）；

（3）系统在仪控功能运算过程所产生的故障（此类故障通过软件模块功能图来设定）。

信号的状态通常在信号采集（通过I/O模块或网络通信）时业已确定，然后根据相应的运算方法进行处理。

2）计算机模块故障

系统中的计算机模块等硬件模块故障通常由系统的自诊断软件或系统硬件设备（如看门狗等）进行检测。当系统中的计算机等硬件模块被检测出故障，故障处理（Exception Handler）程序将立即中断该模块的在系统中的运行，确保模块在此情况下按照系统要求输出相应的信号，禁止其在总线的通信。此时，根据故障的情况，计算机模块将重新启动或彻底关机。这种计算机模块故障导致的重新启动或按定义关机，能够被与其通信的其他计算机模块检测和标识。

2.2 故障的标识

单一信号故障主要是由于系统功能运算过程中信号值与实际工程设定值相比较时出现超限值或与设定值不一致造成的，因此，主要体现为测量信号检测过程中的信号故障、冗余通道运算结果的一致性判断过程中的信号故障及执行机构的反馈所产生的故障信号。单一信号故障检测的结果将在软件模块功能图中标识出，并将其传送至监视服务接口计算机（MSI），用于信息系统的显示。

计算机等模块故障主要是系统本身的硬件故障，同样也在功能图中用特殊的功能块标识出来，并将其通过监视服务接口计算机（MSI）传至服务单元（SU）储存起来，或通过MSI传至主控室，用于后备盘的显示。

2.3 FMEA分析的假定

FMEA分析前须严格区分系统外部事件和系统内部事件所引起的系统故障。例如，火灾、洪水或地震等事件是通过土建设计或其它设计措施来防范其对系统的不利影响，因此，在FMEA分析中不包括此类事件的故障分析。

在FMEA分析中，数字化反应堆保护系统内潜在的故障对系统的影响是FMEA分析的起点，必须找出那些对保护系统功能具有消极影响的子系统或模块故障。通过分析，要求随机故障及其后续故障或假定故障的发生不会导致设计基准事故处于失控状态。

为方便进行FMEA分析，将独立的计算机模块和总线设备作为系统分析的最小元件（尽管计算机模块内部也可能出现很多故障，但这些故障最终的影响均体现在计算机模块及其接口中）。在此基础上，分析研究它们或与它们相连的接口模块的故障。在分析过程中，通常分析的是故障所影响的区域或模块而不是故障发生的区域或模块。根据故障的不同将其影响的区域分为以下几部分。

1）随机故障影响的单一计算机模块

对随机故障所导致的单一计算机模块故障进一步的分析可知，这种故障通常分为硬接线通信的信号故障和串口通信的数据信息故障。硬接线通信的信号故障一般输出值为无效信号

值或"冻结"信号状态,冻结状态直到新的有效值出现才能被检测出来;串口通信的信息故障如能被系统的自诊断程序检测出来,它则仅影响信息的传输过程,如信息故障不能被检测出来,它的影响范围将扩大到接收数据信息的所有计算机模块,但这些影响也只发生在故障所在的多样性组中。当然,还有些不能被检测出的故障,如测量信号的故障,由于在表决器运算过程中能够被有效的屏蔽,因此,也不会将其影响范围扩大。

2) 随机故障影响的单一总线设备

对于总线故障,其等同于信号丢失或信号无效的情况。

3) 产品质量等共因故障所影响的某一通道所有计算机模块

对于影响某一通道的所有计算机模块的故障,无论是来自环境影响还是计算机本身都将影响到整个通道功能的实现。这其中也包括了共因故障。由于 1E 级设备的高可靠性要求,所以,这些故障发生的可能性较小。

4) 产品质量等共因故障所影响的某一多样性组的所有计算机模块

对于影响多样性组中所有计算机的故障,多为产品质量所导致,同样这种故障也包括共因故障。由于 1E 级设备的高可靠性要求,所以,这种故障发生的概率很小,一般,这种故障是可控的,例如,可将故障计算机模块的外部响应设定为"no-voltage"的安全模式。

5) 与初始故障进行通信所影响的计算机模块

在数据校验中不能被检测出来的信息故障会导致随后接受此数据的计算机出现故障并影响到数据通信链上的所有计算机,这种故障同样被限制在同一多样性组中。

综上所述,被假定的故障种类列于表 1。

2.4　FMEA 分析过程

当进行 FMEA 分析时,由于结构或功能对称和相似等因素,可对系统中假定故障的计算机模块数量进行简化,所有多样性组中结构对称的计算机模块及对称的多样性组间功能相似的计算机模块均可参照在某个计算机模块上的故障进行分析。这样,整个系统中 24 个功能计算机模块都可简化成 1 个计算机模块来分析其故障模式。

4 个监视服务接口计算机(MSI)同样具有这样的对称结构,因此,同样可以简化成 1 个计算机模块进行分析。

表 1　田湾核电厂数字化反应堆保护系统故障种类

Table 1　Failure mode of digital reactor protection system in Tianwan Nuclear Power Plant

编号	检测单元	功能	种类	故障模式
1	独立的计算机模块	硬接线信号	单一故障	1) 故障信号输出
				2) "冻结"信号
		串口通信	单一故障	1) 被检测出的信息故障
				2) 未被检测出的信息故障,但无严重后果
			共因故障	未被检测出的信息故障,有严重后果
2	总线设备	串口通信	单一故障	被检测出的信息故障
3	通道中所有计算机模块	硬接线信号	共因故障	1) 故障信号输出
				2) "冻结"信号
		串口通信	共因故障	1) 被检测出的信息故障
				2) 未被检测出的信息故障,但无严重后果
4	多样性组中所有计算机模块	硬接线信号	共因故障	所有信号的输出为"no-voltage"状态
		总线通信	共因故障	信息故障
5	数据链接中的计算机模块	硬接线信号	后续故障	故障信号输出
		总线通信	后续故障	被检测出的信息故障

2个冗余的网关计算机(GATEWAY)将保护系统中的数据传送至外部系统,对于反应堆保护系统,与它们接口的设备是MSI计算机,MSI计算机模块可保证GATEWAY计算机的任何故障均不会影响到反应堆保护系统功能实现。因此,GATEWAY计算机故障在FMEA分析中仅视为MSI计算机模块的一部分。

由于2个多样性组的网络结构一致,因此,对于网络数据链接过程中的故障只要分析1个多样性组即可。同样,由于各通道的结构也基本相似,因此,都在FMEA分析中只考虑某一通道和多样性组。

对于与MSI计算机模块连接的SINEC H1总线,由于其在网络结构上属于反应堆保护系统安全功能通道以外的部分,其故障对于完成反应堆停堆功能或者ESFAS功能没有影响,因此,这部分的故障只在系统测试或系统维护时进行检测。

2.5 FMEA分析结果

通过分析可看出,田湾核电厂数字化反应堆保护系统的4冗余通道采用4取2的表决逻辑,保证了计算机模块单一信号故障不会对反应堆保护系统的安全功能产生严重的影响。这些故障信号既不可能产生虚假的驱动信号,也不可能对正常的保护指令的执行产生影响。同样,在反应堆保护系统冗余通道之间进行数据交换后,软件的信号有效性选择防止了数据传输过程中产生的故障影响后续的安全功能。只有多样性组中或数据通信链中的所有计算机的共因故障才有可能影响到反应堆保护系统某个多样性组的安全功能。因此,避免此类故障的发生的唯一途径是通过不断提高产品质量,减少模块的故障率。

对于反应堆停堆系统,正常运行时控制棒的驱动回路处于闭合状态,在信号故障情况下为故障安全模式,"0"信号输出,结果将导致控制棒落棒,保证了堆芯安全。而ESFAS系统的驱动回路在正常运行时处于断开状态,只有采用多样性的方法才能保证多样性组内的共因故障不会影响到ESFAS系统安全功能的执行。

由于GATEWAY计算机是冗余的,因此,系统与外部的数据通信网络也完全冗余。这样,随机的信号故障将不会导致数据丢失,因而进一步影响主控室信息系统的信息显示。

由于SU计算机运行的是离线软件,因此,SU计算机没有冗余。即使这样,SU的故障或数据在传送至SU过程中的故障也不会导致故障信息的丢失。因为在没有得到SU计算机接收到故障信息的确认之前,反应堆保护系统的功能计算机模块将始终存储自身所发生的所有故障信息。

对于硬接线信号的输出故障,除冻结信号需要在新的有效信号出现后或在定期试验中才能检测到外,其他的信号均能被系统自动检测。

3 小结

通过对田湾核电厂数字化反应堆保护系统的故障模式和后果分析可看出,德国西门子公司的TXS系统能够满足系统安全要求。文章同时给出了数字化反应堆保护系统可靠性定性分析的基本方法,它可为核电厂数字化反应堆保护系统的国产化设计提供有益的帮助。

参考文献:

[1] GB/T 9225-1999 核电厂安全系统可靠性分析的一般原则[S]. 北京:标准出版社,1999.

[2] 王华金,刘立新,李谢晋,等. 核电站数字化反应堆保护系统研究[J]. 核动力工程, 2002, 23(A02):74-78.
WANG Huajin, LIU Lixin, LI Xiejin, et al. Research of digital reactor protection system for nuclear power plant[J]. Nuclear Power Engineering, 2002, 23(A02): 74-78(in Chinese).