安全仪控系统分布式控制器可靠性研究

成卫东[1],刘 云[1,2],冷 杉[2]
(1. 西门子电站自动化有限公司,江苏 南京 211000;2. 东南大学 能源与环境学院,江苏 南京 210096)

摘要:安全仪控系统 TXS 的控制逻辑按照功能划分为信号采集、数据逻辑处理、数据逻辑表决以及信号监视和服务 4 个部分。它们被分别下载到不同的控制器中以实现分布式控制。采用 RS 程序自动建立故障树模型并进行定量分析。为了提高建模速度,采用 ActiveX and Visio 对 TXS 硬件设备进行图形化组态和拓扑结构程序分析。以高压安全注入系统的 BA11 功能为例,提出了 2 种控制分布策略,并与原有方法进行了比较。结果表明:所提策略 1 可以提高高压安全注入系统的响应时间,但使其不可用度增长了 0.87%;所提策略 2 将系统的不可用度降低了 3.6%;2 种策略均在安全范围内。

关键词:核电厂;安全;数字化仪控系统;TXS;分布式控制器;可靠性
中图分类号:TM 623.8 **文献标识码**:A DOI:10.3969/j.issn.1006-6047.2014.02.028

0 引言

安全是核电厂设计、运行和维护技术的核心问题。数字化安全仪控系统 TXS 对核电厂实施安全保护和控制,实现对核电厂反应性控制、确保堆芯冷却以及包容放射性产物等安全功能。TXS 自身的可靠性对核电厂安全、经济运行影响极大:误动信号导致核电厂的虚假保护动作,产生安全隐患;拒动信号导致核电厂保护在异常工况下不能正常启动,这是一种危险性故障,严重影响系统或设备的安全[1-3]。

为了保证核电厂 TXS 的可靠性,其采用实体隔离的四重冗余(通道 E、F、G、H)设计,以满足单一故障准则。为了降低共因故障的可能性,TXS 采用 2 个多样性序列 A、B,2 个序列尽可能采用不同的触发参数、处理逻辑和测量仪表。

除了在硬件设备上采用多样性原则以降低和避免共模故障影响外[4-5],①,TXS 通过合理规划软件功能提高系统整体可靠性[6-8]。TXS 的控制功能组态软件是加载到各分布式控制器中运行的,控制器的加载分布策略会影响系统整体可靠性,需有量化的结果。

1 控制器分布规律

TXS 的控制结构见图 1,按功能分为 4 个部分。

a. 信号采集:接收来自各自冗余通道的独立变送器信号,并进行预处理。

b. 数据逻辑处理:将采集的模拟量信号经限值等运算转换为保护指令信号。

c. 数据逻辑表决:将 4 个通道的保护指令进行 4 取 2 表决,然后将指令输出到相应的机柜/开关柜驱动各自的执行机构。

d. 信号监视和服务:监测某些中间信号。

上述 4 种控制逻辑被分别下载到不同的控制器中,以达到分布式控制的作用。

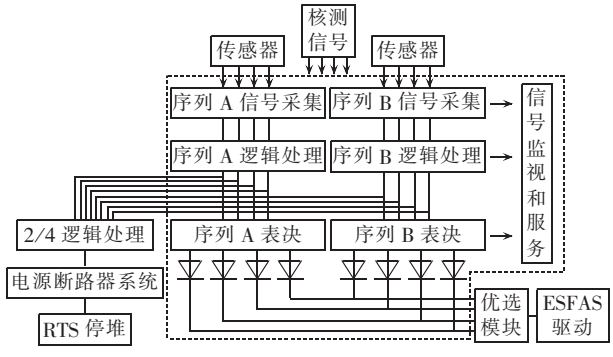

图 1 TXS 的功能结构图
Fig.1 Functional structure of TXS

TXS 的组态被分成功能图组 FDG(Functional Diagram Group)下载到分布式控制器中。如某核电厂的 TXS 中反应堆保护系统就包括 73 个 FDG 组态数据包,分别按 1~73 编号,其分布规律如下:各通道内的 2 个多样性序列中,各分布 2 个 FDG 进行信号采集及处理逻辑、3 个 FDG 处理表决及输出逻辑;另外每通道还各分布 5 个 FDG 以监测本通道相关参数并传送至信号监测与服务单元;剩余 13 个 FDG 完成四通道两序列监测信号的综合处理功能。TXS 的 FDG 分布如表 1 所示,表中 A、B 对应序列 A、B。

表 1 TXS 安全保护功能的 FDG 分布
Tab.1 FDG distribution of TXS safety protection function

功能	通道 E		通道 F		通道 G		通道 H	
	A	B	A	B	A	B	A	B
信号采集及处理	1	3	25	25	44	46	59	61
	2	4	26	28	45	47	60	62
	5	6	33	34	48	49	63	64
逻辑表决功能	29	30	35	36	50	51	65	66
	31	32	37	38	52	53	67	68
信号监测	7	10	39	42	54	57	69	72
	8	11	40	43	55	59	70	73
	9		41		56		71	
综合处理	12~24							

收稿日期:2013-06-17;修回日期:2013-12-05

① EDF Framatome Sofinel. Probability safety assessment of China national pressurized water reactor 1 000 MW. 1999.

2 控制器可靠性自动建模

为了分析TXS控制器分布的可靠性,本文采用Risk Spectrum(简称RS)程序建立故障树模型并进行定量分析[9-11],该程序采用RSMCS算法和"下行法"运算法则,需构建体现故障树特点的结构,从而得到最小割集MCS(Minimal Cut Set)①。

TXS信号采集部分的硬件包括信号采集模块SAA1、信号分配模块SNV1、模拟量输入模块S466;逻辑处理和表决部分的硬件包括处理器模块SVE1或SVE2、通信模块SL21、光电转换模块SLLM、通信接口模块SK01、扩展接口模块SBU1、数字量输出模块S451、通信处理器模块SCP1和子机架SBG1或SBG2,每个多样性序列形成的驱动信号经过二极管后进入AV42优选模块驱动相关部件动作。只有当2个多样性序列的表决器全部失效时,安全功能才会失效。

TXS控制器的功能组态和分布十分复杂,人工建立故障树模型不仅费时费力,且无法使故障树模型的风格、编码、假设以及其他在建模中需要考虑的因素保持一致,同时会存在相当多的人为错误。因此,为了简化故障树建模工作,本文采用ActiveX控件开发技术和Visio二次开发技术对TXS硬件设备进行图形化组态和拓扑结构程序分析,完成故障树自动建模。这样可以提高故障树建模效率,简化故障树建模的工作。

Visio具有良好的图形界面和开放性,本文利用Visio二次开发机制并对其定制,实现组态信息自动建模功能[12-13]。为了实现控制器可靠性自动建模软件与RS软件平台数据共享,需要将VSD格式的图形文件进行组态信息提取、简析,并生成RS接口文件,以便导入RS软件中进行故障树的自动生成和可靠性参数的量化分析。

RS软件接口文件由故障树及转移门记录、基本事件记录、门记录和可靠性参数记录4个部分组成。每条记录中包含了多个不同类型的数据项,因此为每种记录定义了一个结构体,并利用动态链表将结构体类型数据按照一定的原则连接起来,最后通过读取链表中的节点数据输出RS接口文件。相关程序流程图如图2所示。

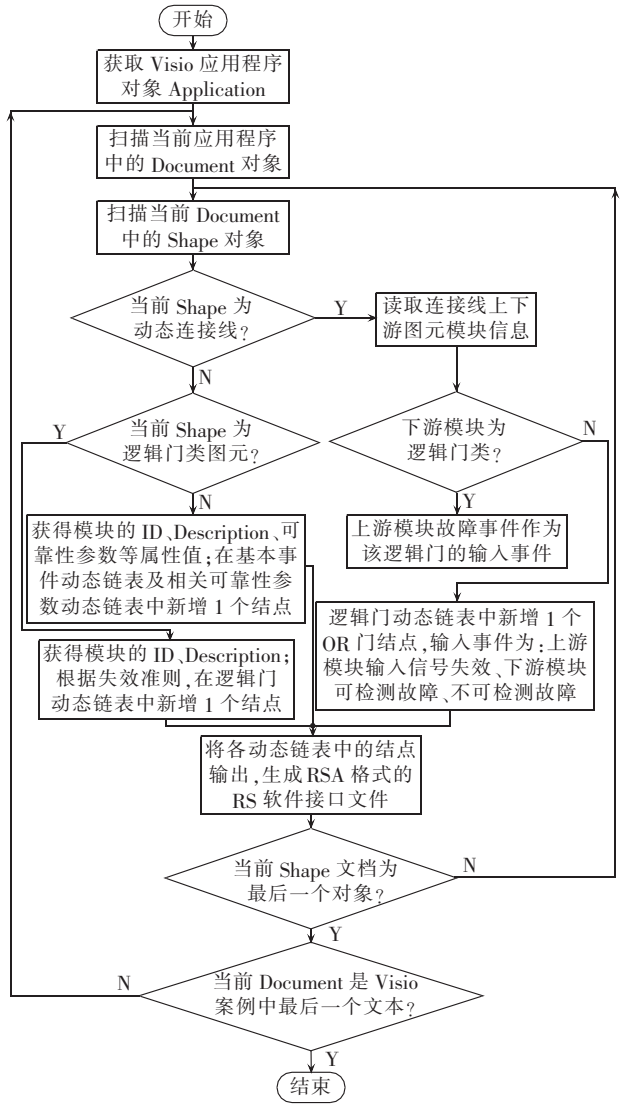

图2 组态信息自动建模功能程序流程图

Fig.2 Flowchart of automatic modeling for configuration information

3 控制器分布可靠性分析

以高压安全注入(下文简称安注)系统仪控功能BA11为例,其功能逻辑如图3所示,控制器分布如下。

a. 多样性序列A:激发高压安全注入功能的输出信号被启动,当操纵员发出命令,或冷却剂热段温度高于150℃且一回路冷却剂的过冷度(反应堆内偏离冷却剂沸腾温度)$\Delta t<10$℃时,使用传感器组A。四通道相关逻辑分别下载在控制器1、25、44、59中。

b. 多样性序列B:激发高压安全注入功能的输出信号被启动,当安全壳内大气压力高于0.129 MPa或操纵员发出命令时,使用传感器组B。四通道相关逻辑分别下载在功能控制器3、27、46、61中。

c. 四通道产生的逻辑信号经4取2表决后输入AV42模块并驱动相关阀门开关及安注泵启动,其中序列A表决逻辑分布在控制器5、33、48、63中,序列B表决逻辑分布在控制器6、34、49、64中。

根据TXS的硬件结构结合BA11功能逻辑,以及本文开发的控制器可靠性自动建模软件,设计了通道E的仪控功能组态图如图4所示。

利用该软件在RS程序中自动建立以"高压安注启动信号(BA11信号)失效"为顶事件的故障树模型。由于篇幅限制,本文只给出部分故障树图如图5所示。

① RELCON A B. Risk spectrum theory manual. 1998.

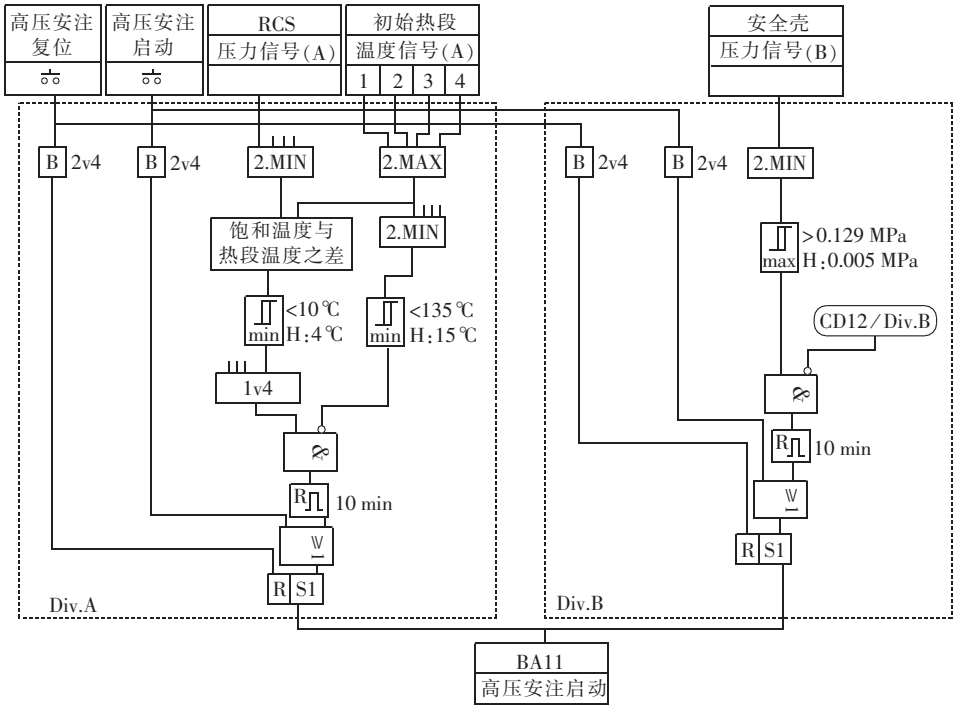

图 3 高压安注系统 BA11 功能的逻辑图

Fig.3 Logic of function module BA11 of HP-injection system

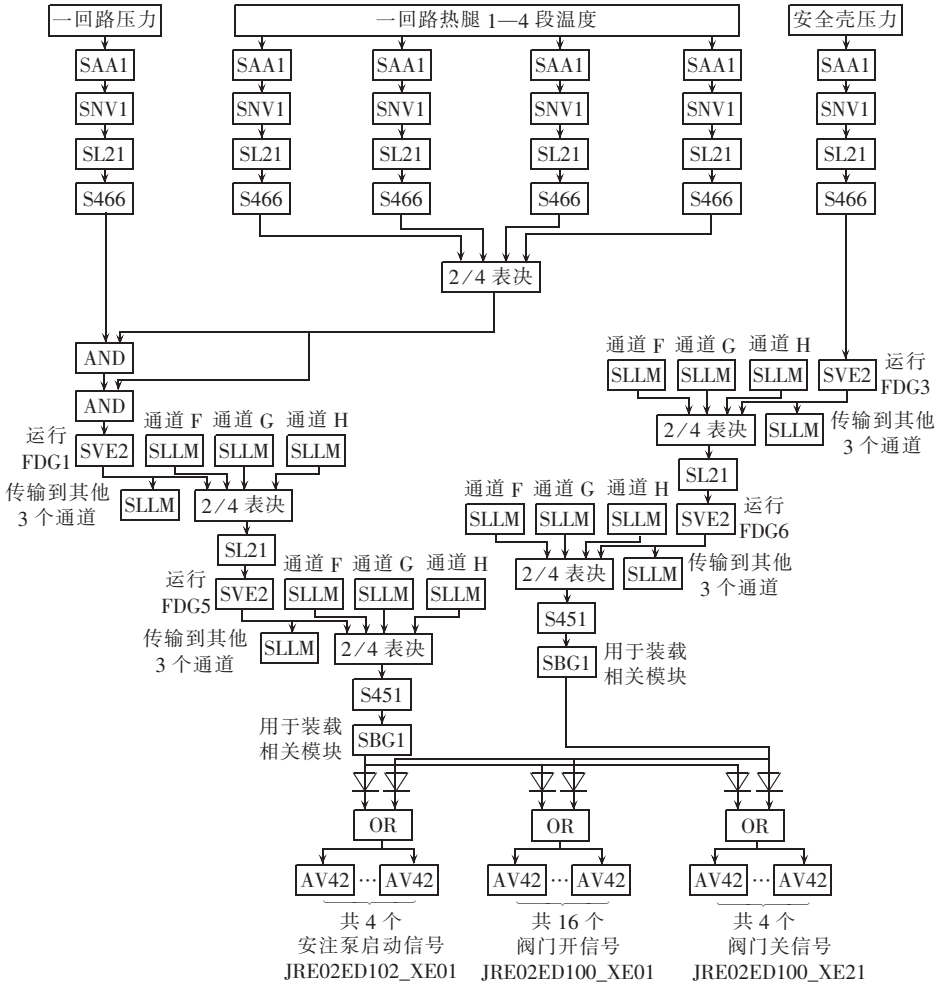

图 4 BA11 功能组态逻辑图(通道 E)

Fig.4 Configuration logic of BA11(channel E)

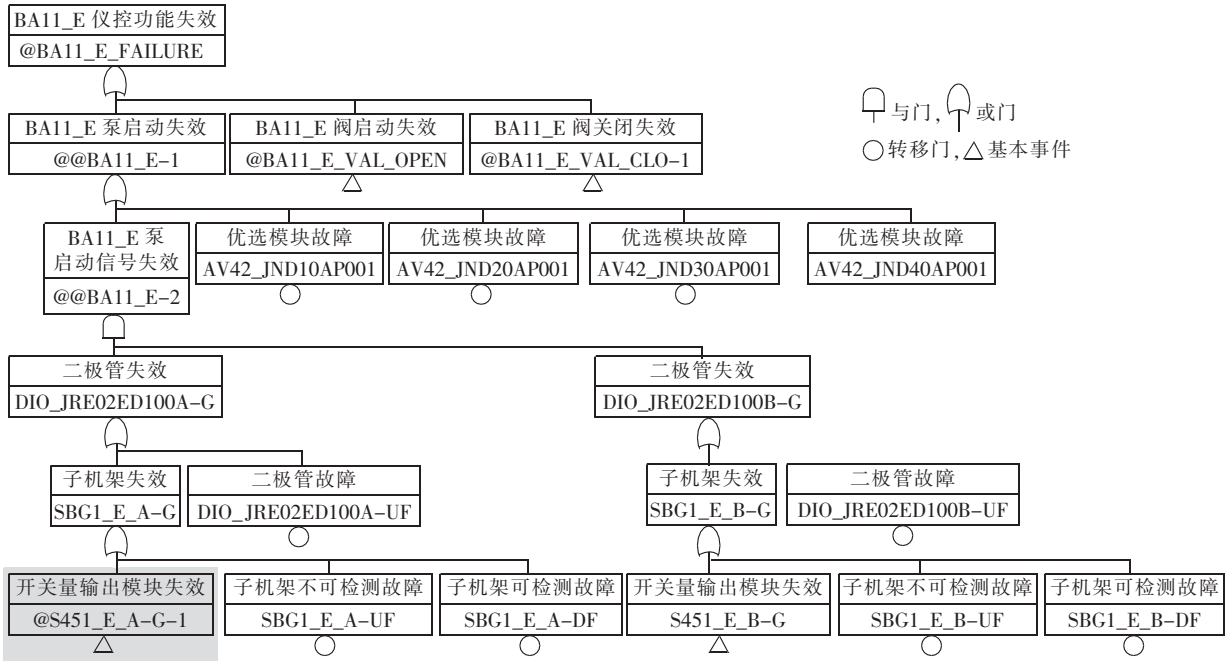

图 5 BA11 功能失效故障树

Fig.5 Fault tree of BA11 failure

量化结果举例:计算得到通道 E 高压安注仪控功能的平均不可用度为 8.05×10^{-4}。同时可以得到对通道 E 高压安注仪控功能失效贡献最高的 10 个最小割集 MCS(Minimal Cut Set)如表 2 所示。

表 2 高压安注仪控功能的不可用度

Tab.2 Unavailability of HP-injection system

事件	事件描述	不可用度	贡献/%
DIO_JRE02ED100A_XE01 DIO_JRE02ED100B_XE01	二极管故障	2.51×10^{-5}	3.12
DIO_JRE02ED100A_XE21 DIO_JRE02ED100B_XE21	二极管故障	2.51×10^{-5}	3.12
DIO_JRE02ED102A_XE01 DIO_JRE02ED102B_XE01	二极管故障	2.51×10^{-5}	3.12
AV42_JND10AP001	优选模块故障	2.16×10^{-5}	2.68
AV42_JND11AA101	优选模块故障	2.16×10^{-5}	2.68
AV42_JND11AA201	优选模块故障	2.16×10^{-5}	2.68
AV42_JND10AA801	优选模块故障	2.16×10^{-5}	2.68
AV42_JET53AA101	优选模块故障	2.16×10^{-5}	2.68
AV42_JET53AA102	优选模块故障	2.16×10^{-5}	2.68
AV42_JET53AA103	优选模块故障	2.16×10^{-5}	2.68

从表 2 可以看出,通道 E 高压安注仪控功能的不可用度前 10 位最小割集占总不可用率的 28.12%。贡献最大的设备是二极管元件和 AV42 优选模块,其中共有 24 个 AV42 模块,对系统失效贡献达到 64.32%。

a. 分布策略 1。从图 1 可知,安注系统仪控功能可以分为现场数据(压力、温度)的采集、功能逻辑运算及表决输出 3 个部分,若将 3 个部分功能分别加载到不同的控制器中,将能提高系统的响应时间。利用本文开发的软件,可以得到通道 E 高压安注仪控功能的平均不可用度为 8.12×10^{-4},对比原有设计,可靠性降低了 0.87%。

b. 分布策略 2。控制器(SVE2)之间通过通信模块 SL21、光电转换模块 SLLM 传输数据,这些模块对系统可靠性产生消极影响。将 2 个控制器的功能逻辑加载到同一个控制器中完成,这样可以减少系统模块的使用数量,从而减小系统的不可用度。设计对应的组态逻辑图,可以得到通道 E 高压安注仪控功能的平均不可用度为 7.76×10^{-4},比原有设计降低了 3.6%。

对比原有的控制器分布策略量化结果,本文提出的 2 种分布策略的高压安注系统仪控功能的不可用度前 10 位最小割集分布尚能保持一致,处在安全范围之内。

4 结语

TXS 采用分布式控制器实现安全仪控功能,本文深入研究了其分布规律。为了简化分布式控制器可靠性研究的故障树建模工作,本文运用 ActiveX 控件技术和 Visio 二次开发技术专门开发了图形化的控制器可靠性自动建模软件。

以高压安注仪控功能为例,分析了 TXS 控制器不同分布策略下的可靠性,为安全仪控系统的可靠设计和组态提供了量化的结果。

参考文献:

[1] 刘宇,吴中旺. 核电厂运行安全性能指标体系[J]. 清华大学学报:自然科学版,2006,46(3):421-424.

LIU Yu,WU Zhongwang. Operational safety performance indicators

for nuclear power plants[J]. Journal of Tsinghua University: Science and Technology Edition,2006,46(3):421-424.
[2] WU Jie. Overview of probabilistic risk assessment and applications [C]//Progress in Safety Science and Technology Part B-Proceedings of the 2004 International Symposium on Safety Science and Technology. Beijing,China:[s.n.],2004:61-67.
[3] 王翠芳. 核电站数字化仪控系统开发过程及其验证与确认[J]. 自动化仪表,2012,33(7):49-52.
WANG Cuifang. Development process,verification & validation of the digitized instrument & control system for nuclear power plant [J]. Process Automation Instrumentation,2012,33(7):49-52.
[4] 周海翔. 田湾核电厂安全仪控系统(TXS 系统)失效概率估算[J]. 核科学与工程,2007,27(1):86-92.
ZHOU Haixiang. Estimation of reliability for safety I&C system (TXS system) in Tianwan NPP[J]. Chinese Journal of Nuclear Science and Engineering,2007,27(1):86-92.
[5] 于文革,张志俭,黄卫刚,等. 大亚湾核电站反应堆保护系统可靠性分析[J]. 核动力工程,2003,24(1):63-67.
YU Wenge,ZHANG Zhijian,HUANG Weigang,et al. Reactor protection system reliability analysis of Daya bay NPP[J]. Nuclear Power Engineering,2003,24(1):63-67.
[6] 曹建亭. 采用 DCS 实现核电站多样性保护控制分析[J]. 现代电力,2007(6):34-39.
CAO Jianting. Analysis of diversified protection and control functions implemented in DCS for nuclear power plants[J]. Modern Electric Power,2007(6):34-39.
[7] 郭春. 宁德核电站与田湾核电站数字化保护系统设计分析[J]. 电力科学与工程,2010,26(7):20-24.
GUO Chun. Design analysis of digital reactor protection system between Ningde and Tianwan NPP[J]. Electric Power Science and Engineering,2010,26(7):20-24.
[8] 李建,许可新,史瑛杰. 核电站反应堆保护系统架构分析[J]. 自动化仪表,2010,31(10):44-47.
LI Jian,XU Kexin,SHI Yingjie. Analysis of the frameworks of reactor protection system in nuclear power plant[J]. Process Automation Instrumentation,2010,31(10):44-47.
[9] LIU P,WU Y C,HUANG D S,et al. LOCA probabilistic analysis of FLL-TBM[C]//23rd Symposium on Fusion Technology. Venice, Italy:[s.n.],2004:86-91.
[10] WU Jie. Overview of probabilistic risk assessment and applications [C]//Progress in Safety Science and Technology Part B-Proceedings of the 2004 International Symposium on Safety Science and Technology. Toulouse,France:Taylor & Francis Group,2004:61-67.
[11] FRANKLIN L C M. Preventive maintenance policy optimization of a nuclear reactor high pressure injection system using a reliability-cost model[J]. IEEE Latin America Transactions,2005 (3):159-164.
[12] 刘强,刘向君,马旭勃. 利用 Visio 二次开发技术实现逻辑图自动分析[J]. 软件导刊,2009,8(1):13-15.
LIU Qiang,LIU Xiangjun,MA Xubo. Analysis of logic graph based on Visio automation[J]. Software Guide,2009,8(1):13-15.
[13] Microsoft 公司. 开发 Microsoft Visio 解决方案[M]. 北京:北京大学出版社,2002:106-125.

作者简介:


成卫东

成卫东(1969–),男,江苏泰州人,工程师,从事核电数字化仪控系统工程技术方面的研究工作;

刘　云(1988–),女,江苏盐城人,硕士研究生,研究方向为核电可靠性(**E-mail**:liushui_xingyun@163.com);

冷　杉(1958–),男,江苏镇江人,教授,博士,现从事核电和火电系统仿真和可靠性技术方面的研究工作。

Reliability of distributed controller in safety I&C system

CHENG Weidong[1],LIU Yun[1,2],LENG Shan[2]
(1. Siemens Power Plant Automation Co.,Ltd.,Nanjing 211000,China;
2. School of Energy and Environment,Southeast University,Nanjing 210096,China)

Abstract: The control logics of digital safety I&C system TXS are downloaded to different controllers for distributed control,which are classified according to functions into four kinds:signal acquisition,data logic processing,data logic voting,and signal monitoring & service. RS(Risk Spectrum) program is applied to automatically build the fault tree model for quantitative analysis. In order to improve the modeling efficiency,ActiveX and Visio are applied in graphical configuration and analysis of topological structure for the hardware components of TXS. With the function module BA11 of HP-injection system as an example, two control distribution strategies are proposed and compared with the original method. Results show that, within the safety range,the response time of HP-injection system can be improved by the proposed strategy No.1 with its unavailability increased by 0.87 %,which can be reduced by 3.6 %,adopting the proposed strategy No.2.

Key words: nuclear power plants; safety; digital I&C system; TXS; distributed controller; reliability