文章编号：0258-0926(2018)03-0086-04; doi:10.13832/j.jnpe.2018.03.0086

核电厂安全级 DCS T2 试验方案研究

张亮亮，张 瑜，周 粲，陈 杰，刘东波

深圳中广核工程设计有限公司上海分公司，上海，200241

摘要：核电厂安全级分布式控制系统（DCS）的 T2 试验对于保证其逻辑功能的可靠性有重要作用。基于安全级 DCS 定期试验、定期试验相关法规、标准，对各安全级 DCS 平台 T2 试验的方案及特性进行了论述，分析了其优缺点。提出 T2 试验设计中需要综合考虑的因素，给出 T2 试验的建议方案及改进建议。

关键词：安全级分布式控制系统（DCS）；T2 试验；交迭；旁通；周期；自动化

中图分类号：TL362 文献标志码：A

Research on Periodical T2 Test for Reactor Protection System

Zhang Liangliang, Zhang Yu, Zhou Can, Chen Jie, Liu Dongbo

Shanghai Branch of Shenzhen China Nuclear Power Design Co. Ltd., Shanghai, 200241, China

Abstract: T2 test of the safety DCS of the nuclear power plant is important for the reliability of logic function. Based on safety-related regulations and standards, this paper introduces different safety DCS platforms, and analyzes their advantages and disadvantages respectively. Finally, the factors that should be considered in the design of T2 test are proposed. A proposal of T2 test on a regular basis and suggestions for its improvement is given.

Key words: Safety DCS, T2 test, Overlap, Bypass, Test period, Automation level

0 引 言

核电厂安全级分布式控制系统（DCS）用于实时监测反应堆的工艺保护参数，当参数超过整定阈值时，自动触发紧急停堆信号及必要的专用安全设施，以维持安全屏障的完整性。安全级 DCS 的定期试验用于检查安全功能的预期可用性，尤其是检查可能会阻止安全功能正确执行的故障。虽然目前核电厂都采用了先进的数字化仪控技术，相对于传统的模拟平台，不存在定值漂移和功能退化等问题，同时还具有强大的系统自诊断功能。但是针对自检无法检测的故障，仍有必要进行定期试验来保证安全级 DCS 正常实现安全功能。核电厂安全级 DCS 一般采用多重冗余结构，为保证安全级 DCS 在试验状态下满足单一故障准则提供了条件。

本文主要对定期试验相关法规标准、不同平台 T2 试验的差异、T2 试验设计中需要考虑的主要因素及改进策略进行论述。

1 安全级 DCS 定期试验

核电厂安全级 DCS 的定期试验一般分为 3 段，分别为 T1、T2 和 T3 试验，如图 1 所示。

（1）T1 试验：主要对过程仪表及核仪表系统的通道进行验证；一般包括传感器交叉比较及通道校准。

（2）T2 试验：主要验证反应堆停堆系统和专设安全系统的保护逻辑。

（3）T3 试验：主要验证保护逻辑的输出信号和相关设备（断路器、阀门等）的驱动，T3.1 试验分别对每一序列的一对停堆断路器进行试验；

收稿日期：2017-06-28；修回日期：2018-04-02

作者简介：张亮亮（1988—），男，工程师，现主要从事核电厂安全级 DCS 设计工作

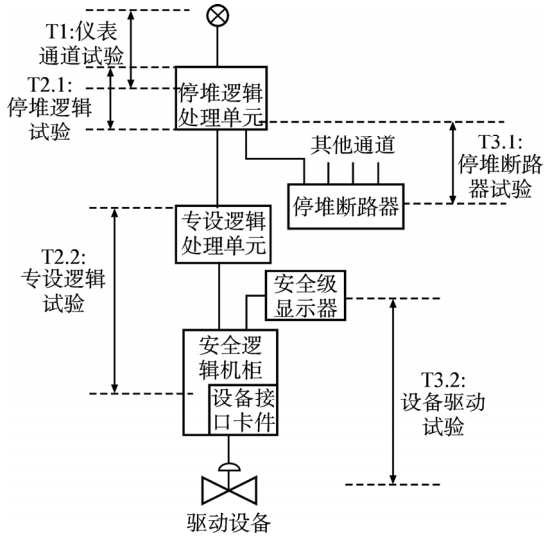

图 1 安全级 DCS 定期试验简图

Fig. 1 Diagram of Periodic Test for Safety DCS

T3.2 试验一般通过安全级显示器驱动来实现（另外，设备接口卡件至驱动设备的短脉冲电气连续性自检测试可作为定期测试的补充）。因此针对不同安全级 DCS 平台，T1、T3 试验总体来说一致性较强。

2 安全级 DCS 定期试验主要法规、标准对比

美国电气和电子工程师协会标准 IEEE Std.338[1]要求，定期试验过程中要保证安全级 DCS 满足独立性要求；功能试验最好采用从敏感元件到被驱动设备同时试验的方法（完整性）；在不能采用上述方法时，可以采用分段交迭试验的方法；定期试验过程不会对核电厂正常运行带来不可接受的影响。美国核管会标准审查大纲 NUREG 0800、BTP 7-17 以及美国核管委会导则 RG 1.118（电力系统及保护系统定期测试）、GB/T 5204 与 IEEE Std.338 的要求基本一致。

国际电工委员会（IEC）60671-2007[2]提出了采用计算机自检功能作为定期监督试验的替代方案。计算机的仪控系统通过自检功能，若能在故障出现后短时间内识别出故障，可以排除在定期试验范围之外，但必须证明自检功能可以识别所有可能的故障模式。如果存在自检功能无法识别的其他故障，必须证明这些故障不会影响设备的安全功能，否则必须按照标准设计该部分的定期试验[3]。另外，自检功能发现的故障应以适当的报警以及指示功能通知操纵员。

3 不同安全级 DCS 平台 T2 定期试验方案比较

目前国内核电厂常用的安全级 DCS 平台主要包括三菱公司 MELTAC-N plus、AREVA 公司 TXS、Invensys 的 TRICON 平台以及西屋公司 Common Q 平台等。

3.1 MELTAC-N plus 的 T2 试验方案

MELTAC-N plus 平台 T2 逻辑试验功能包括紧急停堆和专设驱动功能逻辑试验，分别由相应的自动试验装置（AT）[4-5]完成。进行紧急停堆功能的 T2 逻辑试验时，需在通道旁通[6]状态下进行。以四取二停堆功能为例，定期试验状态下，该通道的反应堆停堆断路器（RTB）始终处于闭合状态，其余 3 个通道的表决逻辑从四取二退化成三取二。专设驱动功能的 T2 逻辑试验时，每次只针对冗余驱动逻辑的一个系列。2 个系列至驱动接口卡件（PIF）的输出采用“或”逻辑。处于测试状态的系列，其输出在“或”逻辑之前被闭锁。而处于非测试状态的另一系列可在真实的安全信号触发时输出相关安全动作命令。

MELTAC-N plus 平台定期试验在停堆换料期间执行，其良好的旁通逻辑设计最大程度降低了对安全功能的影响，保证了安全级 DCS 的可靠性。另外强大的批处理自动测试功能及良好的人-机界面、报告输出功能，使其在执行效率、节约人工时方面也有一定优势。

3.2 TXS 平台的 T2 试验方案

TXS 平台应用于国内田湾核电厂、岭澳核电站二期等。T2 试验用于检查信号采集与处理单元（APU）、逻辑表决单元（ALU）逻辑运算是否正确。由于反应堆保护系统采用数字化系统并且具备高度自检功能，因此 TXS 平台的 T2 试验仅通过平台内置的启动时以及正常运行期间的自检测/监视功能（主要包括 CPU、内存、看门狗以及通讯等的测试）实现[7]。TXS 平台基于自检功能进行 T2 试验，具有以下优点：迅速发现故障、无需人工干预、现场运维人员操作压力小以及不影响安全级系统的正常运行。

3.3 TRICON 平台的 T2 试验方案

TRICON 平台反应堆保护系统由四重冗余的保护组和两重冗余逻辑系列组成。其 T2 试验装置[8]主要由 1 台工作站、交换机以及光线组成，

工作站中的应用程序被称为“ 自动测试应用程序 ”（ATA）。TRICON 平台 T2 试验内容主要包括逻辑功能验证以及硬接线连接检查（用于保护系统结构内部，“ DO—DI ”）。试验信号的自动注入及试验结果的比较均在工作站中进行。

该方案具有较高的自动化程度及执行效率，操作简便，同时成本低，便于实现。

3.4 Common Q 平台的 T2 试验方案[9]

Common Q 平台的定期试验[9]自身无 T1、T2、T3 划分，参照其他平台，其 T2 试验主要包括：通道运行性试验（COT）及驱动逻辑试验，且保护系统每个序列 COT 的测试频率均为 92 天 ，驱动逻辑试验的测试频率为 92 天/次（各序列轮流执行）。试验通过各序列维护测试盘（MTP）子系统实现，可根据试验要求点击相关试验按钮或选择试验参数、输入数值，监测对应输出状态。

该方案的优点主要是测试用的 MTP 子系统为 Common Q 平台的一部分，测试时无需连接专用测试装置；测试过程无需测试旁通。

该方案的缺点主要是：T2 试验交迭程度较高，造成测试程序较多，且部分试验测试周期很短，运维人员工作量较大；试验自动化程度较低，需要在 MTP 上人为输入试验值，操作比较繁琐，且由于测试程度较多导致测试时间长，容易引起人因失误。

4 安全级 DCS T2 试验设计需考虑的主要因素

4.1 自检功能与定期监督试验的关系

目前国内的法规、标准对通过自检功能来替换定期试验尚缺乏明确的要求，另外，自检功能还可能会增加软件的复杂程度。但核安全监管部门认可 TXS 平台 T2 定期测试方案，同时随着安全级平台自检功能及技术的进一步完善，为后续更多安全级平台采用自检功能替代全部或部分定期试验带来了可能。目前安全级 DCS 的自检功能多为定期试验的补充，而不能替代定期测验，与 IEEE Std.338-2006 的要求一致。

4.2 保护逻辑试验交迭方式的简洁性

为满足保护系统逻辑的整体试验，交迭试验是一种具有可执行性的常见试验方式。为了提高试验效率，缩短测试时间，在满足通道试验完整性的前提下，应充分考虑交迭试验的简洁性，即分段试验应尽可能简洁。特别是针对人工手动干预过多、测试周期较短的定期测试，交迭试验分段过多将会带来更多人因风险。

4.3 试验中的旁通及防止安全功能的误触发

在停堆换料期间对保护系统的逻辑通道定期测试时，通过保护逻辑中的允许信号可有效地防止安全功能的误触发。而在功率运行期间执行 T2 试验，以 4 个通道的安全功能为例，修改信号变量值等测试过程可能会造成通道的局部脱扣，此时该功能的四取二表决逻辑相当于三取一逻辑，即只需要其他 3 个通道产生一个局部脱扣信号，就会引起安全功能的误触发。因此，为了防止 T2 试验对核电厂正常运行带来不利影响，试验通道旁通是一种常用的做法。在通道旁通状态下，四取二表决逻辑降级为三取二。

另外，试验时的某个分段交迭过程需满足安全表决逻辑，这些安全命令直接输出至该通道所控制的反应堆停堆断路器（RTB）或专设驱动设备。试验过程中可能会影响到 RTB，由于 RTB 一般由 4 对断路器组成，每次试验只针对其中的 1 对。试验过程满足单一故障准则。若测试过程中核电厂出现异常工况，不会阻止安全级 DCS 正常触发安全功能。而 CPR 设计中，停堆相关的 T2 测试逻辑可能会引起该通道停堆断路器处于打开状态，若此时存在另一保护通道误触发，将满足停堆“ 四取二逻辑 ”，造成反应堆停堆误触发。在 CPR 的设计中，测试中通道的 RTB 处于强制闭合状态，此方法有利于防止测试过程停堆功能的误触发。

当试验可能造成专设驱动设备动作时，可在测试时将设备接口卡件的控制方式设置为“ 就地控制 ”，以旁通安全级控制器的试验命令。另外，由于专设控制器多为冗余控制，可对冗余控制器独立进行测试，以防止误触发。

4.4 保护逻辑试验装置的安全分级

按照国际电工委员会 IEC60671-2007 要求，一般情况下，测试装置的安全分级低于所测试的系统或设备。但是如果测试装置会干扰系统/设备执行安全重要功能，测试装置的安全分级应与所测试的系统或设备一致。NUREG 0800，BTP7-17 也要求执行定期测试的软硬件的安全分级与被测

试系统相同。

另外 GB/T 5204[10]推荐试验装置与安全系统装在一起，以便在进行定期试验中无需加设或拆除导线，但是试验装置不能干扰部件或系统可运行性或安全功能。特别是在测试周期较短的情况下，将试验装置直接作为安全级 DCS 的一部分，可以减少操作中可能引起的人因失效。

4.5 保护逻辑定期试验周期

根据 GB/T 5204[10]的要求，初始试验间隔时间或以后的试验间隔时间的改变应利用确定论的方法或基于风险的方法（或两者的结合）来决定。核电厂安全级 DCS 平台的设计与开发不仅要考虑自身架构满足单一故障、独立性等特征，也应充分考虑其平台产品的试验要求（如试验周期等），以满足核电厂运行维护人员的实际需求，尽可能缩短定期试验的工作量。

如果 T2 试验均在停堆换料期间进行，那么发生误驱动的可能性（如不满足允许信号）及误驱动的后果相对正常运行期间也相对较小。

4.6 保护逻辑试验的自动化水平

为满足保护系统自身的可靠性要求及单一故障准则，每次只能对单个通道进行定期试验，而不能同时对多个通道进行试验。因此，通过增加试验设备或试验人员数量来缩短试验时间不可行。提高保护逻辑试验装置的自动化水平可以提高执行效率，满足 IEEE 试验时间应尽量短的要求，降低人因风险，以保证安全级 DCS 可靠地运行。另外，当定期试验在停堆换料期间执行时，由于换料窗口的限制，定期试验装置自身的执行效率非常重要。目前，MELTAC-N plus 等平台采用可以成批/组对停堆及专设功能进行自动试验，有较高的执行效率。

另外，试验结果报告的自动生成、检测到的故障以直观方式提供给操纵员等功能也会进一步提高试验装置的人-机交互能力及自动化水平。

5 保护系统 T2 试验方案的建议

基于以上分析，推荐安全级 DCS 的 T2 试验装置的安全分级采用 1E 级，各保护序列均配置 1 套测试装置。这样可避免跳线等操作带来的人因问题，同时通过软件、硬件鉴定的试验装置不会对安全级 DCS 的正常运行带来不利影响。试验过程应尽可能自动化，人为干预少，执行效率高，还应具有良好的人-机交互功能。

为了降低试验中的通道旁通对安全级 DCS 运行造成的影响，测试过程各交迭过程的数据通讯可设置适当的信号质量标识或状态位，既能满足通道试验完整性的要求，又能保证试验过程不会带来逻辑降级的影响。

6 结束语

在满足相关法规标准的前提下，结合现有各安全级 DCS 平台保护逻辑定期测试方案的优缺点，在保证可靠性目标的前提下，综合考虑成本等因素，降低保护逻辑试验中的人因风险，尽可能提高其自动化程度，对于核电厂及安全级 DCS 的正常运行有着重要的意义。

参考文献：

[1] Institute of electrical and electronics engineers. Standard criteria for the periodic surveillance testing of nuclear power generating station safety systems. IEEE Std.338-2006 [S]. New York：IEEE，2006：4-9.

[2] International Electrotechnical Commision. IEC 60671-2007.Nuclear Power Plants–Instrumentation and Control Systems Important to Safety-Surveillance testing[S]. Geneva：IEC，2007：12-13.

[3] 张龙强，江辉，田亚杰. CPR1000 新项目安全级仪控系统定期试验方案[J]. 核科学与工程，2010 (S1)：103-109.

[4] 朱攀，王银丽，冯威，等. 红沿河核电厂反应堆保护系统定期试验方案设计[J]. 核动力工程，2015，36(02)：96-100.

[5] 王强，朱雯，张岚，等. 基于 MELTAC 平台的反应堆保护系统 T2 试验方案分析[J]. 核动力工程，2014，(04):106-109.

[6] 王巧燕，张黎明，李恒. CPR1000 新项目保护系统旁通功能设计[J]. 核科学与工程，2010 (S1): 97-102.

[7] 王强，黎国民，况德军. 基于 TXS 平台的数字化反应堆保护系统实现特性[J]. 核科学与工程，2014，34(03): 390-396.

[8] 尤兵，宫成军，李逊存. 福清核电站反应堆保护系统 T2 试验方案的优化[J]. 中国核电，2016, 9(03): 261-266.

[9] 罗慧. AP1000 反应堆保护和安全监视系统定期试验分析[J]. 中国仪器仪表，2015 (07): 35-39.

[10] 国家质量监督检验检疫总局. 核电厂安全系统定期试验与监测：GB/T 5204 [S]. 北京: 中国标准出版社，2008.

（责任编辑：张明军）