从辅变跳闸事件看质量风险分析管理

Analysis and Management of Quality Risk from Auxiliary Transformer Trip Event

杨凯

Kai Yang

台山核电合营有限公司　中国·广东 台山 529200

Taishan Nuclear Power Joint Venture Co., Ltd., Taishan, Guangdong, 529200, China

摘　要：通过对某核电厂辅变跳闸事件的调查，梳理了调试阶段质量风险分析管理问题，包括方法、文件、人员选择、防范措施落实等，并探讨了质量风险分析、风险管理，特别是风险管理与过程方法、质量管理体系、核安全文化的关系。

Abstract: Through the investigation of a nuclear power plant auxiliary transformer trip incident, the problems of quality risk analysis and management in commissioning stage are summarized, including methods, documents, personnel selection, implementation of preventive measures, etc., and the relationship between quality risk analysis and risk management, especially risk management and process methods, quality management system, and nuclear safety culture is discussed.

关键词：辅变跳闸事件；质量管理；风险分析管理

Keywords: auxiliary transformer trip events; quality management; risk analysis and management

DOI: 10.12346/peti.v5i3.8424

1 引言

ISO9100:2015 提出基于风险的思维，指出“应对风险和机遇，为提高质量管理体系有效性、获得改进结果以及防止不利影响奠定基础”。质量风险分析是质量管理的基础，指引着各类管理措施的方向。论文通过辅变跳闸事件分析了核电调试阶段风险分析问题，并探讨了改进风险分析管理的途径，提升风险分析质量。

2 辅变跳闸事件反映出的质量风险分析问题

2.1 事件概述

2015 年 7 月 25 日，电气调试处进行 1LGD0911 间隔（辅变进线开关间隔）的 TP-1LGD-011 试验（定值校验试验），当接入继电保护测试仪给开关本体过流保护装置输送电流时，引发 #1 辅变第二套差动保护装置动作，导致 220kV 辅变电高压侧开关 1GEA1302JA 跳闸，现场丧失 220kV 辅变电源。

2.2 事件直接原因

试验期间开关本体过流保护装置 XI 与 220kV 辅变差动保护装置连接处未短接线，导致差动保护装置中流入电流。如图 1 所示，继电保护测试仪通过试验接口 002BC 向开关本体过流保护装置 XI 输入 3.3A 电流，由于未对 02BN 处（低压控制仓内电气端子 002BN-28、002BN-29、002BN-30、002BN-31）临时短接，电流流入 #1 辅变差动保护装置，电流值大于保护装置动作电流限值（约 0.9A），触发 220kV 辅变电高压侧开关 1GEA1301JA 跳闸。

2.3 事件反映出的质量风险分析问题

①管理程序未要求上下游系统间的影响评价应由上下游人员确认（根本原因）。

1LGD 试验负责人分析图纸后，知晓试验电流从电气端子 002BN-28、002BN-29、002BN-30 流出至 1GEA 保护装置。其在上述四个电气端子端接后，分别测量过 002BN-28、002BN-29、002BN-30 与 002BN-31 之间的电阻，发现端子间是导通的，电流可流通，可执行试验（注：如端子间不导通，电流不流通，则无法注入电流校验定值）。但其并不清楚 1GEA 保护装置的逻辑与工作原理、未向 1GEA 试验负责人核实确认试验电流的影响，认为可执行试验。

检查发现管理程序未要求上下游系统间的影响评价应由上下游人员确认。《调试风险分析与控制》有三方面内容与风险分析相关，即 RAS 单、开工会、班前会。

【作者简介】杨凯（1982-），男，中国山东济宁人，本科，工程师，从事核电工程和生产运营阶段的质量管理研究。

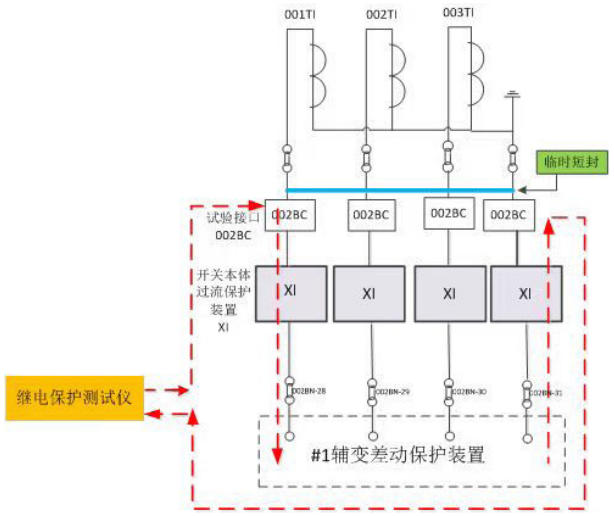

图 1 辅变跳闸事件直接原因示意图

RAS1 单（设备及系统调试分析单）要求分析“系统间冲突：注意各系统间调试活动与窗口是否有冲突，对上下游系统是否存在影响”，但风险分析单准备流程要求“非调试高风险试验清单中的试验，RAS1 单由试验负责人编制、高级主管审核、专业处处长批准即生效并应用”，而 TP-1LGD-011 不在调试高风险试验清单中，未要求上下游系统间的影响评价应由上下游系统人员确认。

开工会、班前会要求进行补充风险分析，但均未明确要求进行上下游系统间的影响评价，也未要求由上下游人员确认。

进一步访谈 1LGD 试验负责人，在辅变高压侧开关跳闸事件发生前，其在调试其他系统时也存在未通知上下游系统相关人员的情况，导致相关系统出现报警并向其询问原因。此种工作习惯也导致其未向 1GEA 试验负责人核实确认试验电流对 1GEA 的影响。这表明，在管理程序没有明确要求的情况下，由一个系统的试验负责人包办上下游系统间的影响评价是一种常态。

②管理程序未明确何时需要重新填写 RAS1 单（促成原因 1）。

2013 年 8 月 20 日 1LGD 试验负责人执行过此试验，未出现辅变跳闸，因为当时辅变尚未投入使用，相关保护也未投入。后续因定值变更，需要在 2015 年 7 月重新执行试验进行定值校验。

进一步检查发现，1LGD 试验负责人在 2015 年 7 月 13 日提交“1BAS101 试验及 1LGD 系统单体调试”工作申请时所附 RAS1 单为 2013 年 8 月 15 日批准生效的 RAS1 单（此 RAS1 单针对的是 2013 年 8 月 20 日需要执行的试验），试验负责人未重新填写 RAS1 单进行风险分析，而此时辅变已投运。管理程序要求《调试风险分析与控制》4.6.1 节要求“试验负责人向接口工程师提交试验许可证申请时，必须同时提交 RAS1/RAS2 分析单”，但当重新进行试验时，是否需要重新填写 RAS1 单，程序未有明确规定。

③信息系统限制一个 TP 只能填写一次 RAS1 单（促成原因 2）。

调试管理信息系统对 RAS1 单的填写进行了限制，对于一个试验只能填写一次 RAS1 单，导致 1LGD 试验负责人在 2015 年 7 月 13 日不可能重新填写 RAS1 单。这一软件设置未考虑到调试试验重新执行的可能性、未考虑到重新执行调试试验时由于可能的变化因素而导致需要重新进行风险分析的必要性。

④管理程序无相关要求，导致提出工作申请时工作文件准备不充分，未发出 TCR（试验澄清）向设计部门澄清（促成原因 3）。

2015 年 7 月 13 日，电气调试处 1LGD 试验负责人提交“1BAS101 试验及 1LGD 系统单体调试”工作申请，此时 TP-1LGD-011 试验的文件《装置就地试验》第 6 节 INITIALSTATUS（初始状态）仍要求“ANT and AST are not energized”（主变和辅变不带电），直到试验实施当天 7 月 25 日才由 1LGD 的试验负责人助理、试验负责人、电气调试处厂用配电组主管确认“AST is energizing which will not affect this test.”（辅变带电不影响本试验），即提出工作申请时的工作依据文件并没有完成准备或准备不充分。这也导致试验执行当天在确认“AST is energizing which will not affect this test（辅变带电不影响本试验）”前，调试部门没有时间发出 TCR 向设计部门澄清辅变带电执行试验的可行性与风险。

检查管理程序发现，管理程序未要求提出工作申请附上 RAS1 单时相关工作文件必须已出版或重新试验时应再次检查 CFA 文件确认可执行性。在工作文件准备不充分的情况下，风险分析无从谈起。

需要指出的是，事件发生后，部分人员认为是试验人员未掌握不同类型设备间的不同点，是人员的惯性思维造成的后果。但笔者有不同意见，依靠识别不同点去进行风险分析管理是徒劳的，一方面我们很难有精力和时间去识别不同点，另一方面我们也没有必要去识别不同点。我们需要的是遵守程序（包括管理程序和技术程序），通过程序控制风险，而且通过遵守程序才能避免人员的惯性思维。

3 风险分析的几项思考

3.1 风险分析的前提条件：风险分析对应的活动必须是明确的

风险基于活动，只有活动明确，才有可能被正确地分析。对于核电厂，将活动明确的方法一般是将活动分步骤地明确写出并形成文件。活动的明确需要达到此种程度，即确保合格授权人员在看到文件要求后，所执行的活动是一致而没有偏差的。

3.2 风险分析与变更：变更引入风险

虽然活动是相同的、活动的自身风险是相同的，但是活

动不是单独存在的，活动需要人员、在一定的时空下执行，不同的人、不同的执行时间、不同的执行环境将通过活动带来风险。这反映出的就是变更所带来的风险。变更很容易出现风险，一方面是因为事物具有关联性，变更前的关联性容易被充分完整地分析，而变更将引入新的关联性，这种关联性不容易察觉或者因为缺少相关方的介入而无法被察觉，容易出现牵一发而动全身，另一方面是因为变更容易引起信息丢失或偏差。对于辅变跳闸事件，与之前已执行过的试验相比，变更表现在试验是在辅变带电的条件下执行的，这引入了 1LGD 与 1GEA 的关联性。

3.3 风险分析由谁实施：需要活动相关的专业负责人员分析

辅变跳闸事件表明 1LGD 系统试验时有电流流入 1GEA 系统，1GEA 系统受 1LGD 系统试验影响，但 1LGD 系统试验负责人未通知 1GEA 系统试验负责人介入风险分析工作，而是由 1LGD 系统试验负责人包办，但其并不清楚 1GEA 保护装置的逻辑与工作原理；在辅变带电的情况下实施 1LGD 系统试验，需要修改文件，文件的修改需设计部门确认，但是实际设计部门未介入。风险不是由系统、活动的专业负责人员进行分析，无法确保分析质量。

3.4 与边界活动相关的风险分析方法：管理输出

边界意味着有上下游、上下游之间有输入输出，假定边界活动的划分没有重复、遗漏，则边界活动的风险来自边界的受影响方没有介入，而边界活动的执行方又没有知识背景，处于知识盲区。解决的方法是边界活动的执行方明确自身的边界、明确活动边界上是否有输出、将输出的受影响方纳入风险分析。

4 风险管理的几项思考

4.1 风险与人

虽然辅变跳闸事件体现的是试验环境变化，无法看出人员引入的风险，但在此有必要特别说明风险与人的关系。人员引入风险的途径主要有两个方面，一方面来源于执行活动时的人员变更，此时需要确保信息无丢失、无偏差地传递以便抑制风险；另一方面是人因失效，人不是无差别的，人员具有生物和社会差异性，相同的培训授权无法保证消除人员间行为模式、心理状态等的差异性，这从大量事件的执行人员均是培训授权合格的人员造成的就可以看出。消除此类风险，一方面需要人员的多样性，即实施监护，让具有不同行为模式、心理状态等的人员监护另一名实施人员；另一方面需要文化引导，规范大家的思考、行为模式。

4.2 风险管理与过程方法

辅变跳闸事件反映出管理过程本身存在着风险，最终导致了管理过程的非预期输出，这说明过程的策划存在着问题。ISO9001:2015 在修订过程中考虑了风险管理，提出“确定产生非预期的输出或过程失效对产品、服务和顾客满意带来的风险”“组织应策划：a）应对这些风险和机遇的措施；b）如何在质量管理体系过程中整合并实施这些措施，评价这些措施的有效性”，就是使用风险管理的方法完善过程的策划，防止过程的非预期输出，防范过程自身的风险，将风险管理与过程方法相结合融入质量管理体系 [1]。

4.3 风险管理与质量管理体系

ISO31000:2018 指出“风险管理是整合在所有组织过程中的部分”“风险管理的成功取决于将风险管理嵌入整个组织所有层次的基础和安排的管理框架的有效性”“风险管理宜以相关、有效和有效率的方式嵌入到所有组织的实践和过程中。风险管理过程宜变成组织过程的部分，而不是分离的”。

从辅变跳闸事件看，一个原因是防范措施未落实在相关的工作执行文件中，如工作程序、工作指令，很容易出现遗忘、遗漏。这说明风险管理未很好地与已有的质量管理体系相融合。

4.4 风险管理与核安全文化

ISO31000:2018 指出“风险管理应考虑人力和文化因素。风险管理应考虑外部和内部人员的能力、观点和倾向，这些因素可以促进或阻碍组织目标的实现 [2]。”

辅变跳闸事件暴露出的问题“1LGD 试验负责人知晓试验电流流出其设备管辖边界至 1GEA 保护装置，但并不清楚试验电流流经的 1GEA 保护装置的逻辑与工作原理，在其不清楚的情况下未向 1GEA 试验负责人核实确认试验电流对 1GEA 的影响，并认为可以执行试验”，说明试验负责人是带疑问操作的，不符合安全文化中的“质疑的态度”（质疑未知：面临着不确定的条件时个人停止工作。在工作进行前先进行风险评估和管理。）、没有进行保守决策。

抛开知识技能，风险的辨识分析明显地与个人的责任心、意识、态度相关，因为风险未被辨识前很难被其他非专业人员所认知，这导致风险辨识和分析活动非常容易被隐藏、应付了事，甚至是有意地绕过。这也导致一个常见的现象，大量的事件在发生后寻找原因时，都被归为了风险分析不到位。而核安全文化强调个人投入、责任心、意识，且培育核安全文化的目的之一就是促使人员有责任心地去执行程序，主动汇报异常、寻求支持。这体现了文化因素对风险管理的支撑 [3]。

5 结语

作为质量管理基础的质量风险分析，要求关联人员完整参与、针对的活动具体明确、关注变更等。为提升质量管理有效性，应将风险管理与过程方法、核安全文化相结合，尤其关注人这一具有意识及主观能动性的变量。

参考文献

[1] ISO9001—2015 质量管理体系要求[S].

[2] ISO31000—2018 风险管理标准[S].

[3] 国际核安全咨询组.安全文化[R].维也纳:1991.