一种隐藏的监控系统缺陷处理探讨

于在甫
(华电金沙江上游水电开发有限公司苏洼龙分公司,四川 成都 610041)

摘 要:在水电站监控系统调试中,由于各种原因,使调试人员很难完全真实地模拟机组状态,导致一些隐藏的缺陷很难发现和消除。机组在发生过速事故时,都是从额定转速增加到一级过速,故障继续扩大发展到二级过速。随着事故的扩大,水电站计算机监控系统能够根据事故的级别,正确启动相应的事故停机流程。本文描述的监控系统漏洞,就是一种监控系统在不同级别的事故同时发生时,监控系统事故流程不能正常启动的案例。这类缺陷在计算机监控系统缺陷中,属于典型的程序逻辑错误,给机组稳定运行带来了极大的危害。因为涉及到机组紧急停机,一旦机组发生事故,就可能继续扩大,发生机组二级过速甚至飞逸事故。

关键词:监控系统;下位机;缺陷;二级过速;事故流程
中图分类号:X924.3;O77+9;F618.1 **文献标识码**: B **文章编号**:1001-2184(2022)03-0066-05

Brief Discussion on Treatment of a Kind of Hidden Defects in Monitoring System

YU Zaifu
(Suwalong Branch of Huadian Jinsha River Upstream Hydropower Development Co., LTD, Chengdu, Sichuan, 610041)

Abstract: During debugging of the monitoring system of hydropower station, it is very difficult for the debugging personnel to simulate the status of units completely and some hidden defects are difficult to be discovered and eliminated. In the event of over-speed accident, the unit normally climbs to the level-1 over-speed from the rated speed before coming to level-2 over-speed. With the expansion of the fault, the computer monitoring system of the hydropower station can correctly start the corresponding shutdown process according to the level of the accident. The bugs of the monitoring system described in this paper is a case in which the accident process cannot be started normally when different levels of accidents occur at the same time. Such defects are typical program logic errors in the computer monitoring system, which bring great harm to the stable operation of the unit. Because of emergency shutdown, once accident occurs on the unit, the accident may expand further, and it may lead to level-2 over-speed of the unit or even runaway of the unit.

Key words: monitoring system; slave computer; defect; level-2 over-speed; accident process

0 引 言

随着我国水电建设的不断发展,水电站监控的发展也经历了人工监控、电话调度和远动化监控,以及以计算机为核心、以现代化数据通信为基础的计算机监控系统等阶段。水电厂应用计算机监控系统对提高自动化水平,保证安全运行,提高经济效益,改善劳动条件,促进技术进步都具有十分重要的意义。

根据电力行业相关标准要求,机组现地控制单元,即电站计算机监控系统下位机的顺序控制和调节需要具备机组正常开、停机顺序控制及紧急停机顺序控制[1]。在电站的实际应用中,一般会根据机组事故等级,将机组紧急停机顺序控制程序分为三类:电气事故停机、机械事故停机、紧急事故停机。

同时,水电站各类辅助设备信息化、智能化越来越高,技术人才逐渐紧缺,都对水电站监控系统的稳定性、可靠性带来一定影响。各个监控设备厂家针对这一需求,也对各自的计算机监控系统

收稿日期:2022-03-10

进行了迭代升级。根据相关要求,对监控系统软件的修改,应制定相应的技术方案并经技术管理部门审定后执行。经过模拟测试和现场试验,合格后方可投入正式运行。实施软件改进前,应对当前运行的应用软件进行备份并做好记录。改进实施完成后,应做好最新应用软件的备份,及时更新软件功能手册及相关运行手册。若软件改进涉及到多台设备,且不能一次完成时,宜采用软件改进跟踪表,以便跟踪记录改进的实施情况[2]。

在计算机监控系统不断升级的过程中,仍不可避免地会出现一些 BUG。由于主、客观原因,调试人员在升级完程序后进行调试或者试验时,并不能完全真实地模拟机组所有状态,导致这些 BUG 不能得到及时的处理,给计算机监控系统带来隐藏的故障或缺陷。由于这类故障或缺陷的隐蔽性,在机组正常运行时不会暴露出来,一旦出现往往会带来极大的危害。本文描述的这类缺陷在计算机监控系统缺陷中,属于典型的程序逻辑错误,给机组控制流程带来隐藏缺陷。因为涉及到机组紧急停机流程,一旦机组发生事故,就可能继续扩大,发生机组二级过速甚至飞逸事故。

1 电厂及故障状况

四川某水电站,计算机监控系统按照“无人值班(少人值守)”的原则设计,能受到现地控制单元(LCU)、中控室、四川省电力调度中心的监视和控制[3]。上位机采用北京中水科技水电科技开发有限公司开发的 H9000 水电厂计算机监控系统结构及配置:下位机 LCU 采用国电南京自动化股份有限公司供货,以施耐德可编程控制器(PLC)为基础构成(在建的远程控制系统亦由国电南京自动化股份有限公司供货及技术支持)。

该电站计算机监控系统具有以下主要功能:

(1)数据采集和处理;

(2)安全运行监视;

(3)自动发电控制(AGC);

(4)自动电压控制(AVC);

(5)人机接口及操作;

(6)设备运行管理指导;

(7)系统自动诊断与自动恢复;

(8)系统通信。

在一次机组检修过程中,开展机组监控系统事故流程模拟试验,发现当模拟“机组转速大于二级过速(145% Ne)”事故源,机组能够按照要求启动紧急停机流程,并“动作快速门”(紧急落门)。但是,当同时模拟“调速器手动,且转速大于 115%”、“机组转速大于二级过速(145%Ne)”时,机组并不能正常“动作快速门”。

该电站采用引水调压式,通过压力钢管将水库水源引致调压室,经过调压室工作闸门控制将水源送至水轮机组。在机组正常运转时,只通过导叶控制机组转速及机组状态转换过程。当机组发生严重事故,导叶关闭失败或者机组转速过快(大于额定转速 145%),就要通过落下调压室工作闸门来切断水源,防止事故扩大。

在监控系统机组 LCU 控制程序中,对机组事故进行了分类,分别有电气事故、机械事故、紧急事故。对于紧急事故,根据事故原因的不同,动作结果分为落工作门与不落工作门两种。经过本次检修测试发现,当同时发生导致落门与不落门的事故时,不落门的事故源会覆盖需要落门的事故启动源,导致工作门不再需要时及时落下,造成极大的安全隐患。

2 缺陷原因

机组事故流程控制主要由计算机监控系统下位机控制,主控为机组 LCU,辅控为水机保护柜 PLC。该电站下位机由国电南京自动化股份有限公司供货,采用施耐德品牌可编程控制器。经分析,此缺陷的原因主要是下位机 PLC 控制程序 BUG 导致。

该电站下位机 LCU 采用施耐德品牌昆腾系列 PLC,调试软件为 UNITY Pro,主程序及程序段根据具体需求,采用以下语言编写:

功能块图 FBD、梯形图(LD) 语言、指令列表 IL、结构化文本 ST、序列控制 SFC。

所有编程语言可在同一项目中混用,并符合 IEC 61131-3 标准。UNITY Pro 附带的扩展功能块库中包含各种功能,从简单布尔运算的功能块、进行字符串和数组操作的功能块到对复杂控制回路进行控制的功能块都有[4]。

一个完整的控制程序可由以下元素构成:

主任务(MAST)、快速任务(FAST)、1~4 个 Aux 任务、为其分配一项已定义任务的段、用于处理由时间控制的事件的段(Tlmerx)、用于处理由硬件控制的事件的段(EVTx)、子程序段。

该电站下位机 LCU 控制程序有一个主程序 MAIN-PROC 和许多子程序段构成。机组运行

至今，机组 LCU 及水机保护 PLC 控制程序共进行过“加装机组运行过程中主轴密封水中断启动事故停机流程”、“区分机组事故停机、紧急停机过程”、“将事故停机、紧急停机事故过程分优先级”等多项修正和升级。

在机组 LCU 及水机保护 PLC 控制程序升级过程中，监控厂家及业主单位都对监控系统各项功能进行了测试，并对机组流程进行了试验。历次试验中，均未发现监控系统 BUG 出现故障。

经查，此次 BUG 故障发生在几种不同语言编写的程序段中，其中机组紧急停机事故判定程序采用功能块图 FBD 语言编写，程序段主要内容见图 1。

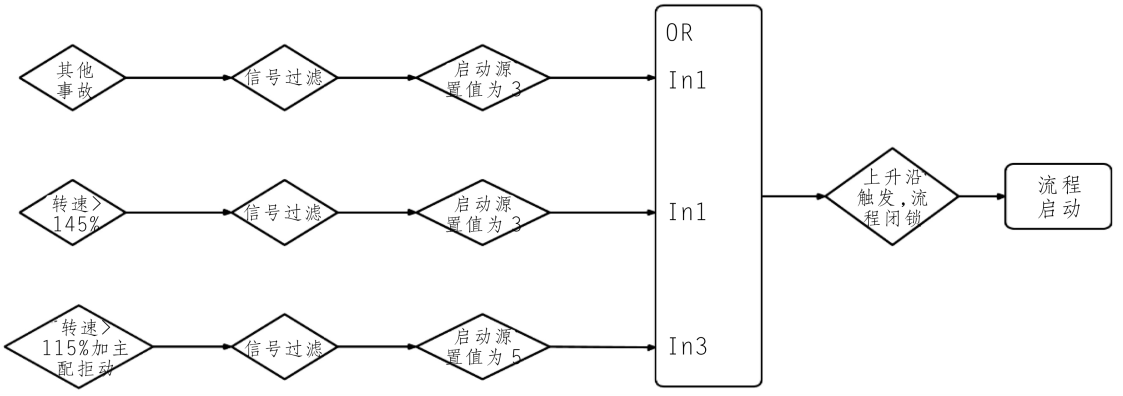

图 1　程序段主要内容

如图 1 所示，在机组开关量、中断量同时报“机组转速大于 145%Ne 故障”信号时（图 1 中转速大于 145% 信号满足），且信号保持时长大于 300 毫秒（途中信号过滤），将会给事故启动源中间变量“RESON”置值为 3（图 1 中启动源置为 3），然后经综合判定、上升沿触发、流程闭锁等一系列程序流，再分别对控制对象置值、对控制接受置值、对流程步骤置值、对启动原因置值、对下位机 LCU 号置值，并执行子程序调用。在此过程中，流程将机组控制流程控制接受值“RCEVIVE. CMMD”置为 2。当机组控制流程接受值“RCEVIVE. CMMD”等于“2”时，流程跳转到另一组由结构化文本 ST 语言编写的程序段，此后将机组流程转为紧急事故停机流程，再将机组工况转换流程步骤跳转到第 200 步，进入机组紧急停机流程见图 2。

当模拟“机组转速大于二级过速”事故时，机组 LCU 监控程序按照以上方式，触发紧急停机流程，然后根据事故源中间变量 REASON 的值来判定动作快速门，即：当“REASON”大于 0 且小于 5 时给落门控制零，并保持 120 秒确保工作门落门到位，然后继续执行投数固配压阀、向电调柜发出紧急停机令、事故跳发电机出口断路器 DL2 第 1 组跳闸线圈、事故跳发电机出口断路器 DL2 第 2 组跳闸线圈、跳灭磁开关等一系列操作。当“REASON”的值不是 0～5 之间时，不执行落门程序，直接执行投数固配压阀、向电调柜发出紧急停机令、事故跳发电机出口断路器 DL2 第 1 组跳闸线圈、事故跳发电机出口断路器 DL2 第 2 组跳闸线圈、跳灭磁开关等一系列操作。

当同时模拟“调速器手动且转速大于 115%”、“机组转速大于二级过速（145% Ne）”时，存在两个事故判定源。“调速器手动且转速大于 115%”事故将事故源中间变量 REASON 的值置为 7，而“机组转速大于二级过速（145%Ne）”将事故源中间变量 REASON 置为 3。

根据施耐德编程手册可知，FBD 功能块程序执行的顺序由信号流决定，并行功能块执行顺序由功能块的执行编号指示，执行编号数值代表执行次序。由图 1 可以看出，将事故源中间变量 REASON 置为 3 的功能块执行编号为 16，将事故源中间变量 REASON 置为 6 的功能块执行编号为 51。由此可知，当这两个事故源同时存在时，程序执行过程中，中间变量 REASON 先被置为 3，后被置为 7，最后按照 REASON 置为 7 来执行后续程序，此时，程序将判定机组紧急停机状态为不落门的一种。这也是在本次检修中，当同时模拟的两个事故源时，机组不能正常动作快速门的原因。而且，一旦进入紧急停机流程，将按照当前紧急停机流程启动源执行，即便事故扩大至需要动作工作门的事故时，由于已经在紧急停机流程中，新的事故源即便被识别也不会执行。当

存在两种情况会导致需要落工作门的事故时,工作门无法落下:

```
*紧急事故停机闭锁紧急事故停机过程**)
 IF RECEIVE.CMMD=2 AND (JZ.JJSG_GC OR JZ.YJGS_GC) THEN
    CTRL.ALARM:=6;
 END_IF;
*紧急事故停机闭锁紧急事故停机过程**)
 IF RECEIVE.CMMD=1 AND JZ.YJGS_GC THEN
    CTRL.ALARM:=6;
 END_IF;
*控制启动记录报警**)
 OBJ_TEMP[1]:=NO.GEN_OBJ+NO.BREAKER_OBJ;
 OBJ_TEMP[2]:=NO.GEN_OBJ+NO.BREAKER_OBJ+NO.SWITCH_OBJ;
 OBJ_TEMP[3]:=NO.GEN_OBJ+NO.BREAKER_OBJ+NO.SWITCH_OBJ+NO.GATE_OBJ;
制条件满足,置进入流程标志,若条件不满足则退出报警*)
 IF CTRL.ALARM=0 THEN
    CTRL.BUSY:=1;(*置控制忙标志*)
    CTRL.OBJECT:=RECEIVE.OBJECT;
    CTRL.CMMD:=RECEIVE.CMMD;
    CTRL.S_TEP:=RECEIVE.CMMD*100;(*给流程起始步骤赋值*)
     IF RECEIVE.OBJECT=1 THEN
        JZ_CTRL();(*机组命令调用解释程序*)
     END_IF;
 ELSE
    ALARM_SD();(*报警退出*)
 END_IF;

IF CTRL.OBJECT =1 THEN(*对应控制对象2-8,紧急停机,电气事故,机械事故,停机,空转,空载,发电,调相*)
  CASE CTRL.S_TEP OF
    200:(*紧急停机*)
        JZ.JJSG_GC:=1;
        JZ_KON(IN1:=1,T1:=T#1S);(*调定时器*)
        IF NOT JZ.TJT THEN
        CTRL.S_TEP:=602;
        ELSE
        CTRL.ALARM:=9;(*报警:机组已在停机态,流程无效*)
        CTRL.FINISH:=1;
        END_IF;
```

图 2 进入机组紧急停机流程

(1)同时发生需要落门和不需要落门的紧急停机事故;

(2)先发生了不需要落门的紧急停机事故,然后事故扩大发生了需要落门的紧急停机事故。

从图 1 可以看出,不仅事故源“调速器手动,且转速大于 115%”存在时,会导致“机组转速大于二级过速(145% Ne)”事故源无法触发,紧急停机的最后三个事故源存在时(分别将 REASON 置为 5、6、7),都将闭锁前四个需要动作事故门,使紧急停机流程无法触发。如果最后三个事故源先满足条件的话,也将占用紧急停机流程,导致前四个事故源无法触发。

根据《NB /T 35004— 2013 水力发电厂自动化设计技术规范》规定,当机组发生下列事故时,应关闭快速事故闸门或蝶阀、球阀、圆筒阀,并启动水力机械事故停机流程:

(1)机组过速到最大瞬态转速的规定值加 3%额定转速(二级过速)时,电气转速信号器动作;

(2)机组过速到最大瞬态转速的规定值加 5%额定转速(二级过速)时,机械液压过速保护装置或机械过速开关动作。

机组在发生事故的时候,特别是过速事故时,都是从额定转速增加到一级过速(115% Ne),然后发展到二级过速。如果监控系统不能正确动作,将会给机组稳定运行带来极大的安全隐患。

3 缺陷处理

为了消除缺陷,修复机组监控流程 BUG,可以采取两种方式:

第一种方式:将需要动作于落门的紧急停机事故与不动作落门紧急停机流程独立开,即将紧急停机流程分为两个,不动作于落门的一级紧急流程独立动作,当动作于落门的二级停机流程动作后,闭锁一级紧急停机流程,执行二级紧急停机流程,确保在事故扩大时工作闸门能够可靠动作。这样修改的优点是:不管两事故同时发生、还是不需要动作落门的事故先发生,一旦需要动作落门

事故发生，就会执行落门的紧急停机事故。缺点是：程序改动较大，在程序改动的过程中，有带来其他漏洞的风险。

第二种方式：在紧急停机 7 个启动源中，将需要落门的紧急停机事故启动源程序块（FBD 功能块）调整到不需要落门的紧急停机事故启动源程序块之后。这样修改的优点是：当同时发生需要落工作门和不需要落工作门的紧急停机事故时，能够保证机组紧急停机事故正常落门，程序改动较小。缺点是：如果不需要落门的紧急停机事故先发生，后续事故扩大发生了需要落门的紧急停机事故时，工作门不能正常落下。

经该电站与监控系统供应商共同协商后，计划先按照方案 2 执行，待后期改造时再处理遗留问题。检修单位根据业主意见，将机组 LCU 及水机保护 PLC 控制程序根据方案 2 进行了修改，并对机组重新进行了流程试验。经试验验证：当发生机组紧急停机事故时（模拟事故信号），机组紧急流程能够正常动作；当同时发生需要落门的紧急停机事故以及不需要落门的紧急停机事故时，机组紧急停机流程能够正常动作，并能够正常地动作于落工作闸门。

4　结　语

根据计算机监控系统试验验收规程要求，监控系统试验验收工作中，需要通过各种人机接口设备（如现地/厂站，键盘/按钮等）发出控制命令或模拟启动条件启动控制流程。各种命令或启动条件所引发的控制操作（包括成功与失败）、提示、登录、报警及相应处理等应满足受检产品技术条件规定，且最终的控制流程及设置的有关参数应与现场设备要求一致[5]。在水电站监控系统设备调试过程中，需要模拟各类机组事故来验证机组事故流程能否正常启动。然而，机组事故发生时存在很多不确定性，甚至可能多类事同时发生。在面对各类复杂情况下，怎样验证监控系统流程是否正常启动，怎样检查各类设备动作情况，是监控调试人员需要重点关注的事情。

为实现国家“碳达峰”和“碳中和”的总体目标，清洁能源必将迎来新的发展。而计算机监控系统作为电站的大脑，如何在不断的迭代发展中，保证电站的安全稳定运行，就显得尤为重要。在电站建设中，特别是电站计算机监控系统建设中，一定要大胆验证。同时，在电站检修调试过程中，应尽量模拟机组真实的故障现象，并以发展的眼光看待机组事故，让机组安全稳定运行的各种保障措施真正发挥作用。

参考文献：

[1] 水电厂计算机监控系统基本技术条件[S]，DLT 578-2008. 国家发展改革委员会，2008.6.4.

[2] 水电厂计算机监控系统运行及维护规程[S]，DLT 1009-2006. 国家发展改革委员会，2006.9.4.

[3] 桂雪芹. 泸定水电站计算机监控系统结构及特点[J]. 水力发电，2011，37(05)：80-82+94.

[4] 施耐德 UNITY Pro 程序语言和结构参考手册[S]. 2008.7.

[5] 水电厂计算机监控系统试验验收规程[S]，DLT822-2002. 国家经济贸易委员会，2002.9.16.

作者简介：

于在甫（1988-），男，河南濮阳人，工程师，学士，从事电力生产、检修及运维工作.

（责任编辑：卓政昌）

（上接第 65 页）

在水利水电工程的前期规划设计中，坚持创新、协调、绿色、开放、共享的新发展理念已经成为一种必然，也是新发展理念的一种贯彻方式。以新发展理念贯穿于昌波水电站的预可研和可研全过程，优化了整体水利枢纽的功能，并将新发展理念融入到水电站各个建筑物中，在取得较好经济效益的同时也使工程质量得到很大程度的提高。因此，以新发展理念主导水电站前期管理工作，对于破解发展难题、增强发展动力、厚植发展优势具有重大指导意义。

参考文献：

[1] 周雅程，刘建华. 新发展理念引领下实现水利建设高质量发展问题研究[J]. 价格理论与实践，2020，(12)：27-30.

[2] 汪安南. 深入推动黄河流域生态保护和高质量发展[J]. 人民黄河，2022，44(01)：167-169.

[3] 吴浓娣. 把握新发展理念 推动水利高质量发展[J]. 水利发展研究，2021，21(04)：7-10.

[4] 吴海峰. 共享发展理念下充分发挥南水北调中线工程效益研究[J]. 经济研究参考，2019，(17)：75-85.

[5] 陈勇. 用新发展理念引领企业高质量发展[J]. 企业文明，2022，(1)：119-121.

作者简介：

赵林涛（1989-），男，河南林州人，工程师，学士，主要从事昌波水电站前期管理工作.

（责任编辑：卓政昌）