DCS 系统时钟同步及跳变机制研究与改进

王五妹，季 诚
（福建福清核电有限公司，福建 福清 350318）

摘　要：福清核电站采用了先进的全厂数字化（DCS）控制系统，作为分布式实时系统，对时钟信号的处理提出了非常高的要求。文章针对 DCS 时钟同步及时钟跳变机制进行相关研究，并结合福清 1 号机组出现的上游时钟跳变对 DCS 系统产生的影响，研究上游时钟发生跳变时 DCS 系统的应对机制，通过自主搭建的时钟授时 DCS 系统开展系列测试，提出并实现了两种预防 DCS 系统时钟跳变对 DCS 影响的改进方法，消除了上游 GPS 时钟跳变对 DCS 系统的影响，避免因上游时钟跳变后 DCS 不可用造成的机组非计划后撤，本研究对核电厂机组安全稳定运行具有实际应用价值，并对后续机组及同行电厂 DCS 时钟同步机制研究具有借鉴意义。

关键词：DCS；IRIG-B；时钟同步；时钟跳变
中图分类号：TM623　　**文献标识码：**A　　**DOI:** 10.16157/j.issn.0258-7998.2023.S1.052

中文引用格式：王五妹，季诚 . DCS 系统时钟同步及跳变机制研究与改进 [J]. 电子技术应用，2023, 49（S1）: 245-250.
英文引用格式：Wang Wumei, Ji Cheng. Research and improvement of clock synchronization and jump on DCS system [J].Application of Electronic Technique,2023,49(S1):245-250.

Research and improvement of clock synchronization and jump on DCS system

Wang Wumei, Ji Cheng
(Fujian Fuqing Nuclear Power Co., Ltd., Fuqing 350318,China)

Abstract: DCS control system is used in Fuqing Nuclear power plant. AS a distributed real-time system, clock signal processing is high important. Combined with the influence of the upstream clock jump in Fuqing Unit 1 on the DCS system, the response mechanism of the DCS system when the upstream clock jumps is researched. Based on a series of tests, the article imposes and realizes two methods to prevent the clock jump and eliminated the impact of the upstream GPS clock jump on DCS system. The research is useful for the safe and stable operation of the nuclear power plant unit, which has practical application value and significant for subsequent research on the DCS clock synchronization mechanism of peer power plants.

Key words: distribute control system; IRIG-B; clock synchronization; clock jump

0 引言

随着核电技术的发展，数字化集散控制系统（DCS）已广泛应用于国内核电机组。对比传统模拟盘台控制系统，数字化集散控制系统最大特点是在分散的机柜控制基础上，增加数字信号集中处理单元，用于 DCS 二层人机交互界面（HMI）的实时数据显示、日志与报警信息查看、以及历史趋势的调用分析等，同时利用计算机化处理手段模拟传统控制模块，在主控室操纵员站（OWP）上实现对就地设备的远程信息监视和控制。

传统模拟盘台控制系统采用继电器回路实现信号控制与显示，时钟信号对其影响不大，而数字化 DCS 系统作为分布式实时系统，则对时钟信号的处理提出了非常高的要求。为确保现场上万个不同仪表信号能够被分布的上百个控制机柜同步采集计算，采集后通过计算机化手段将这些信息同步显示在操纵员站，以确保机组事故瞬态时，DCS 二层人机接口能够按真实的时间顺序记录

现场瞬间触发的大量日志、报警以及趋势信息。其前提是确保 DCS 分布式的系统都基于同一时间标准，其次要求所有参与计算显示的数据有一个正确的时间标签，且能够被 DCS 系统正确解析与处理。

基于上述实时集散控制系统的需求，本文对 DCS 时钟同步及时钟跳变机制进行相关研究，并结合福清 1 号机组在 2020 年 5 月出现的上游时钟跳变对 DCS 系统产生的影响，研究上游时钟发生跳变时 DCS 系统的应对机制，通过自主搭建的时钟授时 DCS 系统开展系列测试，提出并实现两种消除时钟跳变对 DCS 系统影响方法，避免因上游时钟跳变后 DCS 不可用造成的机组非计划后撤，本文研究具有实际应用价值，并对后续机组的 DCS 时钟同步机制研发具有借鉴意义。

1 DCS 系统时钟同步机制研究

福清核电 1-4 号机组采用全厂数字化 DCS，其中 DCS 自动控制与保护层（DCS 一层）采用的是美国 Foxboro 的 I/A 平台；信息监视与操作控制层（DCS 二层）采用的是法国 Atos 的 ADACS_N 平台。两个平台之间数据交换通过基于 TCP/IP 协议开发的 NetFox API 接口程序实现。

1.1 DCS 一二层系统时钟架构

在标准 IA 的时钟架构中，如图 1 所示，对系统内的设备定义有三种：一是 MTK 时钟服务器，它是承担时钟服务功能的工作站，允许对外发送包含时间和日期的授时广播信号给 ADD MTK 和 STK，告知 ADD MTK 和 STK 当前正确的时间和日期；一个完整的 DCS 系统中仅允许存在一个主 MTK 和一个备用 MTK(BTK) 相互冗余备用。二是 ADD MTK，它是除时钟服务器外的其他工作站，ADD MTK 正常情况下接受 MTK 发送的授时广播信号，并根据此信号进行工作站时钟同步，它又能在 MTK 故障时承担时钟服务授时功能。三是 STK 时钟服务从站，它不具备时钟服务功能，仅能被动接收时钟同步信号，所有的控制器都是 STK。

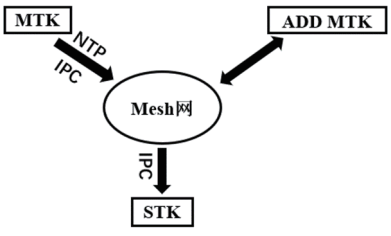

图 1 IA 时钟服务设备分类

为确保整个 DCS 系统一二层时钟保持同步，且与电厂其他系统时间保持一致，福清核电 DCS 采用了全厂时钟系统授时信号。全厂时钟系统接收 GPS 的国际标准时钟授时（UTC）信号作为时间基准，分别送至两个扩展时钟信号分配柜，如图 2 所示，分配器 1 负责给一号机组 DCS 一层 MTK 时钟服务器、一号机组 DCS 二层的 A、B 列前端服务器 1CFR1 和 1CFR2 时钟服务器授时。分配器 2 负责给二号机组 DCS 一层 BTK 时钟服务器、二号机组 DCS 二层 2CFR1 和 2CFR2 时钟服务器授时。其中一、二号机组 DCS 二层为相互独立的网络结构，正常 CFR1 主用，CFR2 备用。一、二号机组 DCS 一层在同一个网络架构中，依靠 1MTK 和 2BTK 时钟实现时钟冗余，正常 1MTK 主用 2BTK 备用。

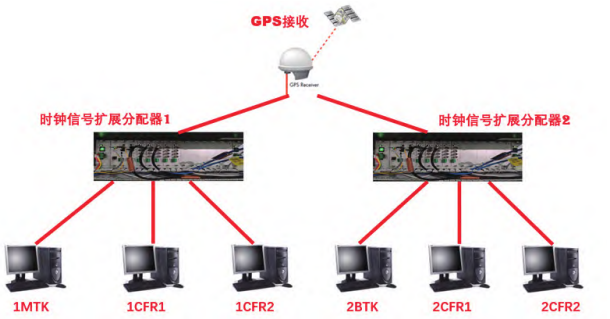

图 2 福清核电 DCS 时钟网络架构图

1.2 DCS 一层工作站和控制器授时原理

IA 系统中的时间服务器 MTK 接收 IRGB 码，结合自身工作站时区设置产生 DCS 系统授时信号，依靠 NTP 协议每隔 16 s 在 MESH 网络中发送一次广播，完成所有工作站强制时间同步工作，保证各工作站的本地时间和 MTK 时间保持一致。各工作站在未接收到 MTK 时钟广播信号期间，依靠工作站本地时间计时，NTP 授时偏差在 50 ms 内。

在 GPS 同步时间脉冲模式下，控制处理器在未收到 MTK 时钟信号时以基本处理周期 (bpc) 为基础进行自走时。如图 3 所示，MTK 每分钟通过网络依靠 ISO 协议发送“time at the next pulse”消息给控制器，纠正控制器的时间。控制器同时接受主用 MTK 和 BTK 的对时脉冲 , 主用 MTK 和 BTK 各自通过时钟脉冲调制解调器每隔 5 s 发送一个主 / 备用对时脉冲，备用对时脉冲作为主用对时脉冲的冗余，控制器只有在接收到对时脉冲且同时收到“time at the next pulse”消息，才会强制更新控制器时间和时区。

图 3 DCS 一层控制器授时原理图

2 DCS 时钟源故障影响分析

2.1 DCS 最小系统测试平台搭建

DCS 最小测试平台如图 4 所示，主要包括：A/B 扩展钟、MTK/BTK、2ALMHC/2HS1HC、A/B 时钟脉冲解调器、A/B 时钟脉冲分配器、一对 FCP270、一个交换机、WIRSHARK 数据抓取平台。在不影响时钟授时的情况下，取消外部 GPS 信号源改为扩展钟内部晶振授时，因为只有一对 CP，取消时钟对时脉冲分配 HUB。

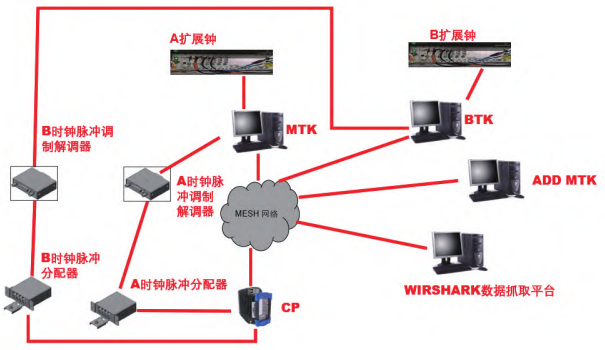

图 4 DCS 最小系统测试平台

2.2 时钟跳变对 DCS 一层系统的影响测试

本次测试结合 DCS 时钟授时系统的原理并结合以往的时钟故障案例，共设置 7 个标准测试模式，依靠 WIRSHARK 软件抓取的相关数据包经过人工分析，测试检查在 GPS 同步时间脉冲模式前提条件下，不同时钟授时故障模式下 DCS 系统和控制器时间变化规律。

本次试验主要关注 WIRSHARK 软件抓取两个方面异常，一是提取相关数据包，检查如下源地址为 151.128.152.18（MTK 物理地址）和源地址为 151.128.152.24（BTK 物理地址）的相关数据包，主要分析其对应的 SMB 和 NTP 数据包，检查工作站授时机是否正常，确认发生异常的主备时钟服务器功能切换功能；二是提取目的地地址为 01:00:6c:11:11:11 的 ISO 数据包，观察每分钟一次的控制器授时消息，确认其下发的 UTC 时间戳，因篇幅关系，下述仅给出测试结果。

(1) MTK 正常 /BTK 正常 :DCS 系统以 MTK 时钟作为参考，每 16 s 进行一次 NTP 时钟同步工作 , 检查工作站发现时间正常 , 控制器的时钟信号不是由时钟服务器决定的，也并没有事先进行主备选择，其授时信号的取舍主要由控制器决定。

(2) MTK 故障 /BTK 正常 : 人为手动设置主时钟故障，备用时钟工作正常，检查发现系统由 MTK 授时改为 BTK 授时，检查工作站发现时间正常，控制器时间正常。

(3) MTK 负偏 /BTK 正常：人为设置主时钟后退一小时，DCS 系统以 MTK 时钟作为参考，工作站除 BTK 外，其余工作站时间跳变后退一小时，观察控制器时间未发生跳变。

(4) MTK 正常 /BTK 负偏：人为设置备用时钟后退一小时，系统仍旧以 MTK 为时钟源，工作站除 BTK 后退一小时外，其余工作站时钟均正常，观察控制器时间未发生跳变。

(5) MTK 正常 /BTK 故障: 系统仍以 MTK 授时为主。

(6) MTK 正常 /BTK 正偏：手动拨快备用时钟超前一小时，系统以 MTK 时钟作为参考，工作站除 BTK 工作站时钟超前一小时，其余工作站时钟均正常，观察控制器时间发生正的时钟跳变。

(7) MTK 正偏 /BTK 正常：主用时钟超前一小时，系统以 MTK 时钟作为参考，除 BTK 工作站时钟正常外，其余工作站时钟均超前一小时，观察控制器时间发生正的时钟跳变。

2.3 时钟跳变对 DCS 系统的影响测试结果及分析

结合对福清核电 DCS 授时系统各项测试，福清核电 DCS 授时系统使用了完全独立的 A/B 列冗余授时模式，只要 MTK 授时服务器及网络正常，工作站默认只会从 MTK 取时间，在 MTK 获得下发 NTP 授时广播权限的情况下，ADD MTK 不会判断其从 MTK 获取的时钟信号是否发生正 / 负跳变。因此当 MTK 因为外部 GPS 时钟跳变，导致其下发的 NTP 时间信号正 / 负跳变，系统内除 BTK 外的所有 ADD MTK 将同步发生时间正 / 负跳变。BTK 因为有接外部 GPS 信号源将跟随其外部 GPS 信号时间，即使 BTK 发生时钟正 / 负跳变，系统内除 BTK 发生时间超前或者滞后外，其他的 ADD MTK 不会跟随 BTK 发

生时间跳变。在 MTK 时钟回路异常时，MTK 和 BTK 的授时角色发生转换， DCS 系统授时服务功能会切换至 BTK，BTK 会同步给 MTK 和 ADD MTK 同时发送 NTP 时间信号，此时 DCS 系统内的工作站时间将跟随 BTK 时间，但一旦 MTK 恢复正常系统授时角色仍将自动回归至 MTK。具体判断机制如图 5 所示。

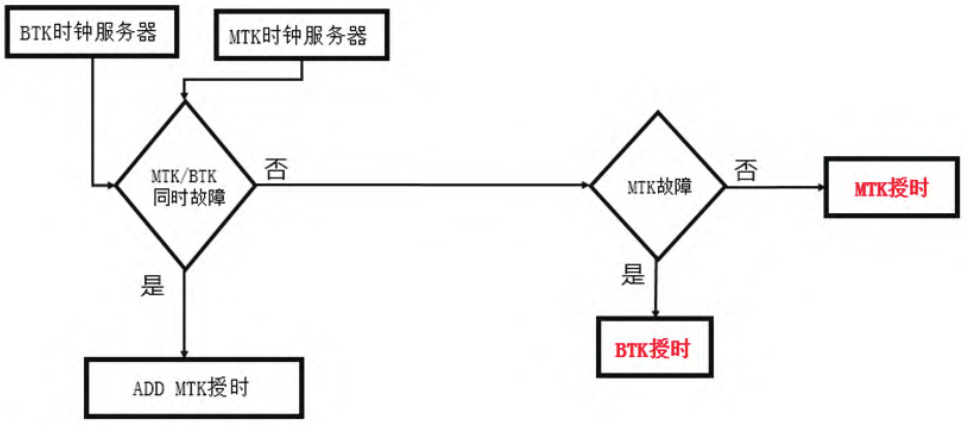

图 5 福清核电 DCS 工作站授时机制原理图

对福清核电 DCS 工作站授时机制解析，我们发现 DCS 工作站之间的 NTP 授时机制是冗余且有严格主备之分的，只要 MTK 授时回路正常，系统将只接受 MTK 授时信号，但福清核电 DCS 工作授时机制未考虑上游 GPS 时钟异常的情况，只判断 MTK 或者 BTK 的时钟回路是否异常，缺少对 MTK 或者 BTK 的 NTP 服务有效性进行比较和分析，无法预防外部 GPS 时钟信号的跳变带来的影响。

对福清核电 DCS 控制系统控制器时钟授时协议解析发现，如图 6 所示，MTK 和 BTK 对控制器的授时权限没有经过预先的分配，正常情况下 MTK 和 BTK 的 ISO 协议没有主备之分，其只是单纯的向控制器发送“time at next pulse”授时信号，其取舍由控制器判断，判断依据主要是对比同一时刻 MTK 和 BTK 的时标，滞后的将被自动舍弃。若 MTK 或者 BTK 其中一个发送的“time at next pulse”消息超前，则控制器将自动跟随超前的时钟服务器。此授时机制优点是能够避免时钟服务器故障或者上游时钟源滞后带来的影响，但无法在外部时钟正跳变信号时，对系统进行保护。

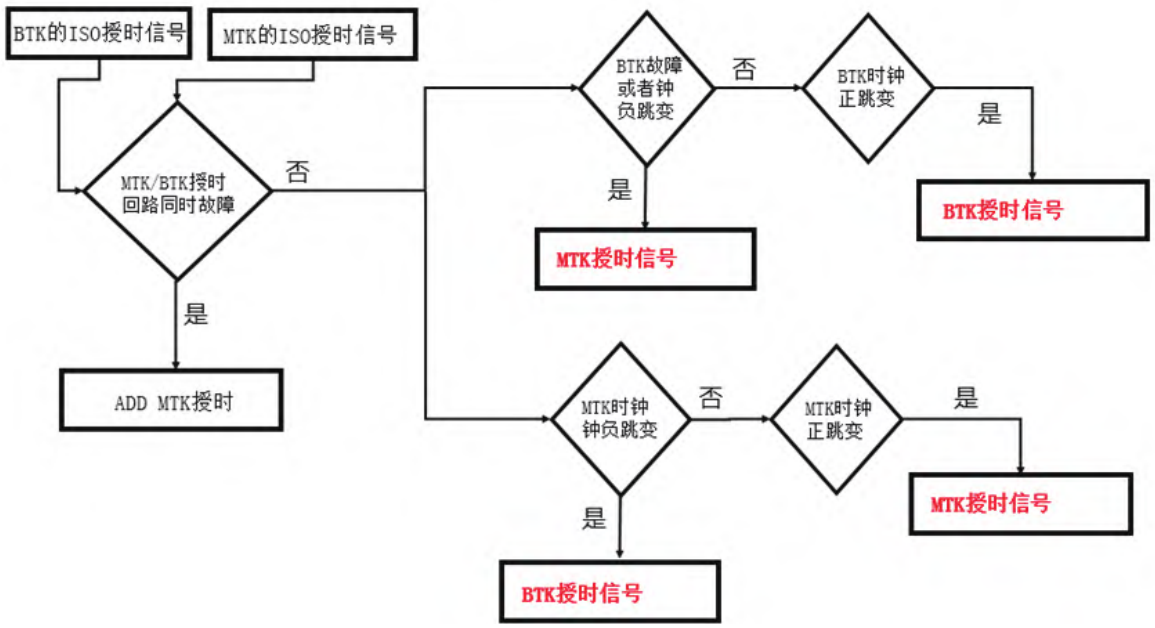

图 6 福清核电 DCS 控制器授时机制原理图

结合对福清核电 DCS 时钟授时机制分析和 8 种情况测试结果，得出如下结论：

（1）针对工作站的 NTP 授时模式，其对外部 GPS 时钟源异常跳变无抵御能力。

（2）针对控制器的“time at next pulse”授时模式，其对外部 GPS 时钟源滞后有抵御能力，但无法处理时钟源超前跳变问题。当外部时钟源正跳变的时候，I/A 系统无法识别该时钟信号的是否正常，默认跟随时钟信号超前的服务器，导致控制器时钟发生跳变，当外部时钟源恢复正常时，因为对时脉冲一直存在，控制器无法自动回拨时间。需要断开对时脉冲控制器时间才能恢复。

（3）DCS 二层中 CFR 服务器不允许外部时钟向历史跳变，一旦时钟向历史跳变，直接导致 DCS 一二层断开连接，CFR 停运，DCS 二层不可用，主控失去监视和控制功能。

3 DCS 时钟可靠性提升措施

3.1DCS 一层系统授时机制优化

通过对 DCS 一层时钟的性能分析发现，当外部 GPS 时钟源故障的情况下，DCS 一层正向或者逆向的时钟跳变，都会给系统带来严重的影响，威胁 DCS 系统的稳定运行，最好的办法是在外部时钟源发生故障的情况下，DCS 时钟服务器能够及时发现并转为 DCS 内部时钟源能够保持当前时钟状态，依靠服务器内部的晶振时间自走时，维持 DCS 系统的稳定运行，等待外部时钟的恢复。

具体设计参考图 7 系统，在 BTK 上通过修改 D:/usr/fox/sp/tk.cfg 文件，将 BTK 由外部 GPS 授时切换为无 GPS 授时模式，在 MTK 时钟服务器的前端增加一个时钟扩展服务器，将冗余的 GPS 信号同时接入一个扩展时钟服务器上，扩展时钟服务器的 CPU 主控制板卡上带有实时时钟芯片，当 CPU 主控制板接收到外部输入的时钟信号时，主控制板会对实时时钟芯片进行校对。当没有接收到外部的时钟信号时，主控制板还可以根据本地时钟提供的时间信息产生秒脉冲、分脉冲、时脉冲、IRIG-B 码和时间报文等时间信号，且这些信号仍保持着较高的准确度。外部时钟服务器能够判断外部时钟信号的情况，当时钟信号 A 和时钟信号 B 同时故障，自动切换至时钟服务器内部晶振授时，如果时钟 |A-B|<10 s 且 A 回路正常则，优先使用 A 授时，当 |A- 本地时间 |>10 s 且 |B- 本地时间 |<10 s，则授时服务切换为 B 授时，当 |A- 本地时间 |>10 s 且 |B- 本地时间 |>10 s 则切换回内部晶振授时。其授时机制如图 8 所示。

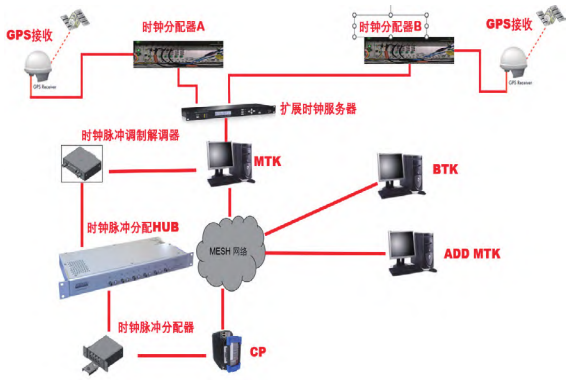

图 7 DCS 一层新时钟架构

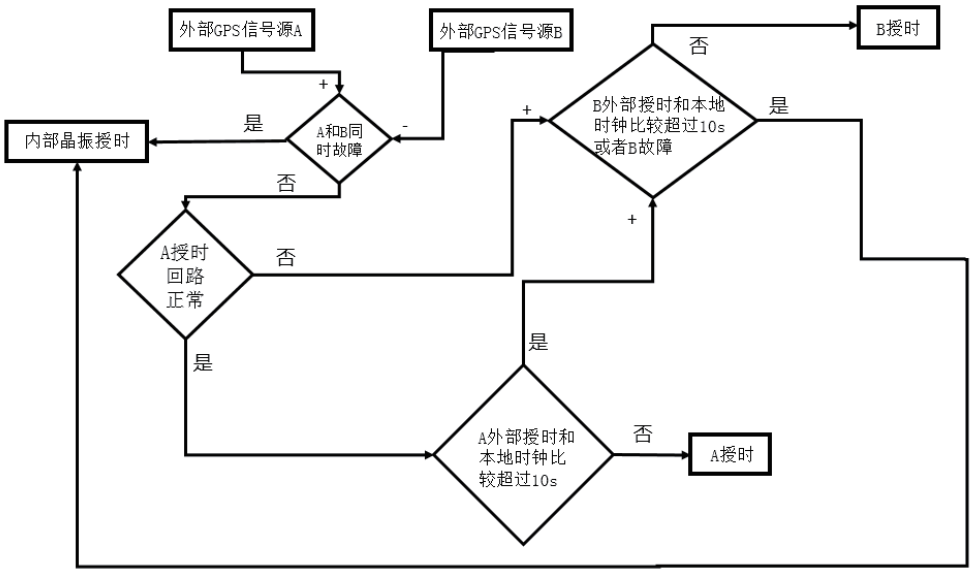

图 8 新增时钟服务器判断机制

此方法应用于现场，既满足了外部 GPS 同步授时精度较高的优点，又可以避免外部时钟跳变导致 DCS 时钟信号突变，同时依靠无 GPS 授时模式 MTK/BTK 自走时功能，能够保证外部时钟服务器故障的情况下 DCS 仍然能够正常地运行一段时间，有效地提升了 DCS 的可靠性。

3.2 增加外部时钟监测

基于 FPGA 执行 IRIG-B 标准的 AC/DC 编码技术，利用精密授时型 GPS 引擎作为系统时基，检测同步信号和经串口输出的绝对时间信号，编码后输出到 DC/AC 接口模块，再输出到物理链路，系统结构如图 9 所示。

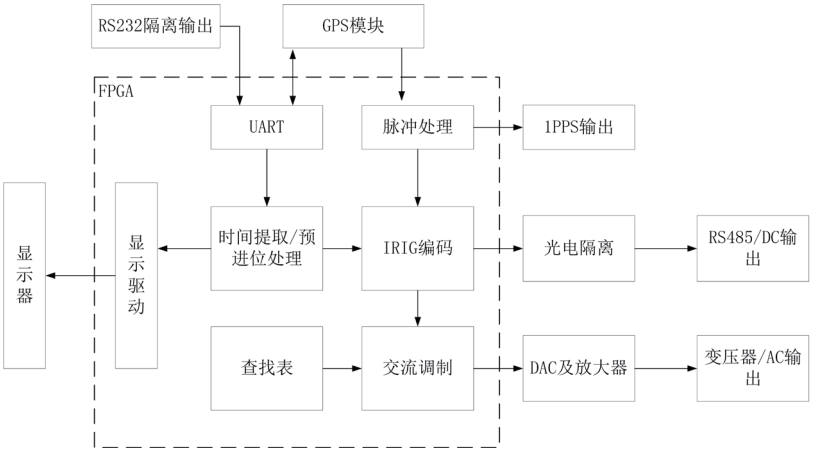

图 9 基于 FPGA 的 IRIG-B 编码器系统框图

上述系统首先实现了 B 码直流编码，而后在直流的基础上实现交流调制，以得到交流码，同时提供恢复每秒脉冲输出和隔离串口输出时间码，以及显示器显示。

要保证 B 码每个码元的上升沿时刻准确，需要 100 ps 的精确时基和 pps 的参考点。一般的做法是用 pps 作为基准，每个码元的起点由前两个秒脉冲的间隔等分得到。这种方法使用上一时刻来预测下秒，每秒脉冲有抖动时会导致最后一个码元宽度不足或超过 10 ms，这将无法利用 B 码来实现时间同步和数据等间隔同步的采集。

使用外置 GPS 引擎产生的 100 ps 信号作为每个码元的起始时刻然后再从 100 ps 信号中恢复出 1pps 由于 B 码参考标记 P=1pps 的上升沿，所以这种方法既保证 P 的准确性，又保证各个码元和索引标记时刻的准确性。在有等间隔同步数据采样要求的场合，可使用每个 B 码码元的上升沿校准本地时基，确保采样同步和时间同步。

时钟信号调理单元主要由时钟信号解码输入单元和编码输出单元组成，解码输入单元可通过外置时钟信号输入接口，接收外部输入的时钟信号 IRIG-B，进行信号处理、解码分析，提取出传送的时间信息，可供 DCS 维修人员分析使用。

编码输出单元可根据测试装置模拟仿真的时间信息，进行信号编码，生成各种时钟信号 IRIG-B，再通过外置时钟信号输出接口，将模拟的时钟信号发送给下游 DCS 系统 MTK 时钟服务站测试和使用。

便携式时钟检测装置，不仅为 DCS 维修人员提供了一种可视化、简洁、明了的时钟检测手段，避免时钟服务器更换过程中，人为设置错误导致 DCS 时钟系统故障，提升维修人员对 DCS 时钟的判断能力。同时也提供了一种便捷、快速的标准时钟源信号，可以在全厂时钟授时系统故障期间，作为标准时源使用。

4 结论

文章基于福清核电 204 大修期间 GPS 时钟改造工作造成的福清 1 号机组 DCS 二层系统主控历史趋势呈直线、数据时标超前 8 小时问题，展开系列分析研究与测试，深入核电厂时钟同步及 DCS 授时机制研究，通过对 DCS 一层、二层系统时钟同步、授时、数据收发机制的剖析，结合自主搭建带有上游时钟的 DCS 测试平台，从增加报警、优化 DCS 一二层时钟授时机制、增加外部时钟监测等四种方法，多重预防时钟跳变，降低上游 GPS 时钟跳变对 DCS 系统的影响，对 DCS 系统的安全可靠运行具有实际指导意义，同时，对同行电厂 DCS 时钟授时机制优化具有借鉴意义。

（收稿日期：2023-11-13）

作者简介

王五妹（1984-），女，硕士研究生，正高级工程师，主要研究方向：DCS、仪控维修技术、设备管理技术。

季诚（1986-），男，本科，高级工程师，主要研究方向：DCS、仪控维修技术。