程序错误造成的监控机死机两案例分析

李智勇
(云南电网公司德宏分公司 调度中心,云南 德宏 678400)

摘要:以 SL300 和 DISA100 型系统为例,根据实际工作中遇到的故障,就非法和错误报文而引起的处理程序运行出错造成死机现象作了深入分析。SL300 前置机死机的直接原因是接收了数据库没有配置的参数,进一步找到了内存管理问题,提出了增加寻址出错处理机制的修补措施。DISA100 监控后台机死机的直接原因是接收了协议未规定的非法报文,诱因是保护管理机内存管理出错,反映了规约处理程序容错性不够的问题。

关键词:死机;接口;内存;数据空间;监控;过滤器
中图分类号:TM 76 **文献标识码**:B **文章编号**:1006-6047(2006)10-0114-03

计算机死机的原因有很多,例如操作系统进程冲突、软/硬件冲突、程序出错、系统文件损坏、遭黑客软件或病毒程序攻击、硬件损坏、灰尘等。本文以当前系统内较常用的 SL300 和 DISA100 型系统为例,就变电站自动化系统监控程序接收了非法数据而造成程序死锁、分析了监控模块退出的问题[1]。

1 SL300 前置机死机问题

某工程 A 变电站监控系统为集成电子 SL300,变压器保护及测控采用 PST1200、PSR651,监控系统与变压器保护装置经通信转换器采用 IEC-60870-5-103 规约作接口通信,同时还与其他保护、直流等设备通信。

SL300 在正常运行 20 d 后,频繁死机并重启,无规律可循。在检查中偶然发现,当 PSR651 装置运行时,SL300 前置机就死机。于是,从 SL300 与 PSR651 通信着手,发现当 SL300 收到下列报文就死机:68 0A 0A 68 08 05 09 01 09 05 C7 D0 2C 01 E9 16。

通过分析,该报文为 PSR651 装置地址为 05 单元(DIO)上送的遥测量报文,其<FUN>为 199(C7),<INF>为 208(D0),从厂方提供的信息表中查得,该遥测为档位遥测,<012C>表示 3 档。在 SL300 系统固定库 SLFixDB_M.mdb 里,DBtype 表"PSR650-DIO 数字量输入/输出模块(103)" BT_YCDataNum(为开辟遥测数据空间用)设置为 0,DBTypeYCInf 表里也没有相关遥测的定义,相应的规约配置文件 IEC103Cfg.ini 里也没有档位遥测的定义。

于是,在 IEC103Cfg.ini 里[设备参数 _PSR650DIO]项下加入如下定义:

```
;      3) 遥测
遥测个数=2
遥测 0=C7D0          ;dc1
遥测 1=C7D1          ;dc2
;      7) 遥测模式
遥测模式=1
满码遥测 0=2000,1        ;T1
满码遥测 1=2000,1        ;T2
```

固定库 SLFixDB_M.mdb 里增加档位遥测的设置,开辟数据空间[2-4]。再模拟档位报文,前置程序模块 ccs 不再出错。还原成原来的配置,模拟档位报文,每次都造成 ccs 前置程序死锁。

按照 IEC-60870-5-103 规约原理,智能设备(IED)单元只要接收到<总召唤>命令,就会将其全数据回传给监控。而本例中,监控死机的直接原因在于接收了没有配置数据库的数据而造成的。这个问题可以通过 2 种比较简易的方法避免:按厂方提供的信息表完整地配置数据库;通信转换器只固化监控需要转发的数据。这 2 种途径实际都是统一双方数据库的做法。

为什么 ccs 在接收到未配置的数据就会死机呢?首先分析 SL300 的程序流程。ccs 模块在系统初始化时,根据<固定库>里的配置,预先分配好内存空间以供存取;正常运行时,将接收的数据根据预留的内存空间进行存放;当接收到错误数据(如报文校验和错误)就直接舍弃;而当接收到合法但数据库里又没有配备的数据时(如本例),程序仍然按常规到内存里寻找存放数据的空间,这时,因为内存里实际并没有分配给该数据的空间,最终造成内存寻址出错[2]、程序死锁。因此,死机的根本原因还在于 ccs 程序设计有漏洞。该漏洞可以通过 2 种方式修补:

a. 在接收到合法数据时,先判断该数据是否需要,如果不需要就舍弃,需要才进行存储;

b. 存取数据的子程序里加入寻址出错处理机制。

由于系统正常时大量接收的都是合法数据,如果按照 **a** 方式处理,势必浪费大量的系统资源而使实时性受到影响;**b** 方式是比较合理的选择,在完善的程序里是必不可少的机制。

收稿日期:2005-12-19;修回日期:2006-03-06

2　DISA 100 监控后台死机问题

DISA 100 系统是 20 世纪 90 年代后期推出的 DISA 2 型变电站自动化系统，是技术较为成熟、功能较为完备、短小精悍的系统。某工程自 1999 年来共采用了 6 套 DISA 2 型监控系统，系统均按图 1 配置。

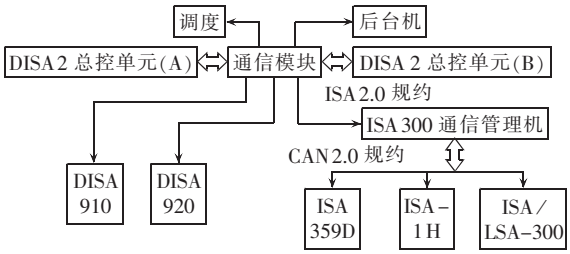

图 1　原监控系统与保护连接示意图

Fig.1 The original connections between supervisory system and protections

保护设备采用 ISA 系列，通过 ISA－300(E)与监控通信。B 变电站因扩容需要，增加了 2 台电容器，保护设备采用 ISA－359 F 保护测控一体化装置，并同时增加 1 台 ISA 301A 保护通信管理机，新系统按图 2 连接(实际并非最佳配置结构)，并升级总控、后台和调度的规约处理程序，实现 F 系列保护测控装置信息的接入和处理，且不能影响老系统的运行[5-7]。

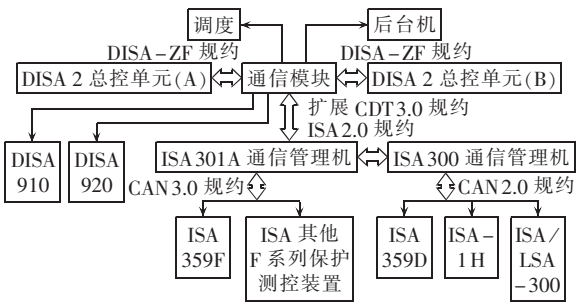

图 2　新监控系统与保护连接示意图

Fig.2 The expanded connections between supervisory system and protections

新系统按图 2 建立后，ISA 359F 装置保护测控功能均能正确实现，连接的保护信息能正确报告，可以远方修改定值，系统功能均能实现。但运行一段时间后，当地后台机监控程序频繁死锁，信息出错。监控程序死锁后，只有将计算机重启才能正常进入监控系统，如果仅重启监控程序，就会报告“系统为演示版”的信息，“确定”后随即退出。

现场检查时发现，多次调用保护定值后就会出现程序死锁现象，且通信模块在报告出错信息前就自动退出运行。故可初步判断与保护装置上传的保护报文有关。基于此判断，随即进行了验证①-③。

2.1　非法报文

后台机调用保护定值，同时监视总控 810 发给后台机的报文，发现了大量协议未规定的非法报文，有以下情况。

a. 非法报文，不该有 72 帧。例 1　EB 90 EB 90 EB 90　72 00 01 00 00 CE ……。例 2　EB 90 EB 90 EB 90　72 00 01 00 00 CE　00 00 00 00 00 FF。

b. 连续的非法报文，造成死机的元凶。例 1　EB 90 EB 90 EB 90　74 92 01 05 01 B9　00 00 BA EA (导致死机的 2 个字) 00 53。例 2　EB 90 EB 90 EB 90　74 92 01 05 01 B9　00 00 18 26(报文长度) 00 DC。

c. D 系列 4 号柜、1 号单元保护装置正常的定值上传报文出错(字长度)。

EB 90 EB 90 EB 90　74 92 2F 05 01 D6　00 04(保护单元柜号) B6 00(出错字长度) 01(单元地址)……

上述报文，均有严重的问题。按《DISA 通信规约(v2.01)》所述及该系统的组建情况①，保护报文的控制字都应该是“74”，而 **a** 报文的控制字为“72”，并且其特征码、源站址、目的站址、功能码、单元柜号及地址、报文长度均为 00；是不正确的。

a 中例 1 帧的信息字长为 01，实际应为 17 个信息字；参阅规约文本②-③可知，**b** 中 2 帧报文都有严重错误：其柜号地址号均为 00 H，在实际配置中没有这个装置，定值报文长度 BA EA，18 26 均大于协议规定的报文最大长度 512 Byte[1]，但报文中只有 1 个信息字，没有定值报文真正实体。因此可以判断，监控程序通信模块退出与此密切相关。随后，对系统进行了如下试验。

用串口收/发程序将上述报文逐一发给监控机，发现通信模块在接收处理 **a** 帧报文时，都没有死机，而是报告 ISA 定值包有错，接收 **b** 例 1 帧报文时，出现死机，而与 **b** 例 1 帧相似的 **b** 例 2 不会引起死机，还进行了分解，报告是定值报文。**b** 是非法报文，为何会有截然相反的结果？2 帧的区别仅在于报文的长度不同而已，死机是否与此相关？为了验证是否相关，就不断改变报文长度字节做试验。测试发现，当报文长度字节大于 6 476 (HEX：4B 19)时，监控程序就会出错，小于或等于时不会出错，但从已有的资料中无法判断 6476 为什么会造成死机。厂家程序开发人员认为该数值与死机没有关键的联系，死机问题可以通过在规约程序中设置过滤器予以解决。这个解释虽然不能令人信服，但问题终究找到了，通过提供的上述试验数据，厂家纠正了后台监控软件的错误。

2.2　产生错误报文的原因

为什么 810 总控会向后台机发送错误报文呢？究竟是转发出了问题还是保护通信管理机出了问题？通过监视总控 810 与保护通信管理机通信报文发现，当后台机召唤定值时，通信管理机就会回答大量的非法报文。报文内容在此不再列出，但通过上述报文摘录 **a** 分析可以发现，报文中实际包含了类似遥测报文的内容。在 301A 内存中也查到了向 810 发送的非法报文。经软件开发人员分析，内存管理出

① 《DISA 通信规约(v2.01)》4.12.④.
② 《ISA 300 扩展 CDT 通信规约(Ver102)》2.4.
③ 《ISA 300 基于串口保护通信规约(Ver302)》.

现了问题。通过对程序检查发现,读/写内存的指针在循环读取中发生了非预期的偏移,通过对其进行修改后上述问题就消除了[4-5,7]。

在该案例中,监控程序和保护管理机程序都有错误。保护管理机程序的错误直接导致了后台机死机,是监控程序错误发作的诱因,如果没有保护管理机程序的错误,监控程序错误也许永远不会呈现出来。查找此类错误,即可以像本案例一样逆向查找,逐步地排除问题;也可以从诸多故障现象的分析中直接找到故障的源发点,如在本案例中,由于增加了一台ISA 301A保护管理机而出现了故障,就可以直接从ISA 301A入手进行排除。

3 结语

上述2套监控系统的开发人员对笔者反映的问题都给予了积极的回应,并根据笔者提供的资料,纠正了程序中存在的错误,在新版的程序中已不存在上述问题,用户如遇到此类问题,可以让厂家直接提供最新版本的程序就可以了。

正如上述案例一样,所有的程序都难免会有错误的存在,即便通过严格的调试和长时间的运行实际,也不可避免,只不过有的错误容易发现,有的错误直到程序"退役"也未必能够被发现。并且它们表现的现象各不相同,造成的危害程度也各不相同,有的很难发现也很难查找。但作为用户,即便无法准确判断或难以查找到问题所在,也可以将故障的触发条件、现象、时间等信息记录详细,这些信息能为厂家分析和解决问题提供最为重要的信息。因为有些故障是间歇性的,厂家人员在现场时,这些故障并不一定会发作,如果再没有比较详实的信息可以提供,将对厂家解决问题造成很大的难度。

参考文献:

[1] 吴维宁,张文亮. 提高电力系统软件可靠性措施的研究[J]. 电力自动化设备,2003,23(3):53-55.
WU Wei-ning,ZHANG Wen-liang. Measures to enhance electric monitoring software reliability[J]. Electric Power Automation Equipment,2003,23(3):53-55.
[2] 王忠明. 微机计算机原理[M]. 西安:西安电子科技大学出版社,2003.
[3] 熊静琪. 计算机控制技术[M]. 北京:电子工业出版社,2003.
[4] 孙涵芳. Intel 16位单片机[M]. 北京:北京航空航天大学出版社,1998.
[5] 李现勇. Visual C++串口通信技术与工程实践[M]. 北京:人民出版社,2002.
[6] NELSON M. 串行通信开发指南[M]. 潇湘工作室,译. 北京:中国水利水电出版社,2000.
[7] 刘红玲. 微机接口实用技术[M]. 北京:电子工业出版社,2003.
[8] 邬宽明. 现场总线技术应用选编(上)[M]. 北京:北京航空航天大学出版社,2003.

(责任编辑:汪仪珍)

作者简介:
李智勇(1978-),男,云南泸西人,工程师,主要从事电力自动化工作(**E-mail**:zhiyongli1@163.com)。

Two cases of computer halt caused by program bugs

LI Zhi-yong
(Dehong Sub-company Dispatch Center,Yunnan Power Grid Co.,Ltd.,Dehong 678400,China)

Abstract: Taking SL 300 and DISA 100 systems as examples,according to real faults occurred in operation,the computer halt phenomena caused by illegal and wrong messages are analyzed. The halting of SL 300 front-end computer is found due to receiving parameters not configured in database,causing memory management problem. Addressing mistake processing mechanism is added for it. The halting of DISA 100 supervisory computer is found due to receiving an illegal message undefined in protocols,causing memory management problem of protection manager. Poor errortolerance of protocol processing program is shown.

Key words: halt; interface; memory; data space; monitoring; filters