**通过Eventlog文件分析故障**

|  |  |
| --- | --- |
|  | 作者：范小军  职务：风电部 技术工程师  公司：BECKHOFF中国  邮箱：x.fan@beckhoff.com.cn  日期：2022-12-26 |
| **摘 要：**  本文档介绍了Eventlog工具的各类功能，以及如何通过Eventlog分析故障。 | |
| **附 件：**   |  |  |  | | --- | --- | --- | | 序 号 | 文件名 | 备注 | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | |
| **历史版本：**   |  |  |  | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | |
| **免责声明：**  我们已对本文档描述的内容做测试。但是差错在所难免，无法保证绝对正确并完全满足您的使用需求。本文档的内容可能随时更新，如有改动，恕不事先通知，也欢迎您提出改进建议。 | |
| **参考信息：** | |

目 录

[1. Windows系统日志 3](#_Toc126921193)

[1.1. Tcsyslog和Eventlog 3](#_Toc126921194)

[1.2. Eventlog日志文件打开的方式 3](#_Toc126921195)

[1.2.1. 方法一 3](#_Toc126921196)

[1.2.2. 方法二 3](#_Toc126921197)

[1.2.3. 方法三 4](#_Toc126921198)

[2. Eventlog信息查看 5](#_Toc126921199)

[2.1. Eventlog文件记录 5](#_Toc126921200)

[2.2. 文件记录的保存 5](#_Toc126921201)

[3. 日志文件的分析 6](#_Toc126921202)

[3.1. 故障文件的打开及筛选 6](#_Toc126921203)

[3.2. Application事件记录 6](#_Toc126921204)

[3.2.1. 模块状态的变化 6](#_Toc126921205)

[3.2.2. 光纤通讯问题 7](#_Toc126921206)

[3.2.3. 模拟量模块问题 8](#_Toc126921207)

[3.2.4. 耦合器通讯问题（子站问题） 8](#_Toc126921208)

[3.2.5. 主站初始化问题 10](#_Toc126921209)

[3.3. System时间记录 12](#_Toc126921210)

[3.4. Security事件记录 12](#_Toc126921211)

# Windows系统日志

## Tcsyslog和Eventlog

在Windows CE系统中使用的记录TwinCAT运行状态的是TcSyslog文件，但是在Windows 7或者Windows 10的系统中不再是Tcsyslog文件记录状态，而是用Windows系统日志Eventlog记录事件。

Windows操作系统在运行过程中会记录大量日志信息。这些日志主要包括Windows 事件日志、IIS日志、FTP日志、Exchange Server邮件服务日志、SQL Server 数据库日志。

Windows 日志文件以特定的数据结构存储，每个记录事件的数据结构包含9个元素：日期/时间、事件类型、用户、计算机、事件ID、来源、类别、描述、数据。 查看日志可以通过系统自带的事件查看器查看。

Windows系统内置三个核心日志文件：System、Security、Application，默认大小均为20480kB也就是20MB，记录数据超过20MB时会覆盖过期的日志记录；其他的应用程序以及服务日志默认大小均为1MB，超过这个大小一样的处理方法。

如下是核心日志记录的内容表：



那么我们如何得到这样的故障文件？

## Eventlog日志文件打开的方式

### 方法一

在TwinCAT软件的图标点击右键→Tools→Event Viewer。

图形用户界面, 应用程序

描述已自动生成

### 方法二

选中Computer，鼠标右击 “管理工具”**，**然后单击“事件查看器”。

图形用户界面, 应用程序

描述已自动生成

### 方法三

使用Win+R，输入eventvwr.msc，直接进入事件查看器。

1. 同时按住键盘上的Windows以及字母R键。

图形用户界面, 应用程序

描述已自动生成

1. 在新弹出的窗口中，输入eventvwr.msc。

图形用户界面, 应用程序

描述已自动生成

通过以上三种方式我们带来了日志浏览窗口可以看到有Application、Security、System，是我们需要收集的Event log信息。

# Eventlog信息查看

## Eventlog文件记录

如下图是我们需要收集的Eventlog记录文件，包含三个文件：System.evtx、Security.evtx、Application.evtx。

文本

描述已自动生成

## 文件记录的保存

先选中所要保存的日志文件项目如Application，按照如下图中的顺序保存，需要注意要选择保存的位置及名称（名称自己命名）。如下图，分别保存我们需要的日志文件System.evtx、Security.evtx、Application.evtx。

图形用户界面, 应用程序

描述已自动生成

# 日志文件的分析

## 故障文件的打开及筛选

在我们的电脑上双击打开日志文件，就可以直接打开查看故障信息，可以筛选当前日志，选在关键，错误，警告等信息查看日志，便于快速的定位，找到故障信息所在的那一行。

图形用户界面

描述已自动生成

当点击一条故障信息时在下方常规中就可以看到具体的故障信息。如下图：

图形用户界面, 表格

描述已自动生成

## Application事件记录

主要是对Application文件进行分析，应为Application记录的是应用程序需要报告的信息。

### 模块状态的变化

TwinCAT System Manager中显示模块的状态不在OP，EtherCAT通讯中断，模块的状态不在OP

日志文件Application 中可以看到事件的ID为20000。

一般事件的ID为20000TwinCAT System Service的信息，其中包含了倍福设备的一些运行状态，如下图：

图形用户界面, 应用程序

描述已自动生成

主要信息是：

10/27/2019 12:25:13 PM 674 ms

'Tower301CO2(EL6731)' (1033): abnormal state change (from 'OP' to 'SAFEOP') with code 0x1b, 'Sync manager watchdog'. Try to go back to 'OP'...

此时我们就可以和Tcsyslog一样看到过去机组运行时的报错信息。

当前的报错信息时间时：10/27/2019 12:25:13 PM 674 ms

报错的模块及信息为：Tower301CO2(EL6731)' (1033): abnormal state change (from 'OP' to 'SAFEOP') with code 0x1b, 'Sync manager watchdog'. Try to go back to 'OP'...

就可以知道在模块EL6731状态发生变化，从op变为safeop。

### 光纤通讯问题

TwinCAT System Manager中显示EtherCAT通讯中断或者显示为OP LINK\_MIS D

1. 在TwinCAT软件Online中查看信息如下：

表格

描述已自动生成

1. 在EventLog中查看记录如下：

TwinCAT System Message: Timestamp: 12/10/2021 8:58:53 PM 152 ms Message: 'Term 3 (EK1501) (1002) - Term 9 (EL2004) (1008)' Communication interrupted。

表格

描述已自动生成

### 模拟量模块问题

例如：

8/30/2019 4:52:04 PM 607 ms

'Cms304AI6(EL3204) (1032)' Communication re-established

图形用户界面, 文本

描述已自动生成

### 耦合器通讯问题（子站问题）

EventLog文件中出现 from‘OP’to‘SAFEOP’或‘Communication interrupted’

例1：

10/27/2019 8:33:47 AM 991 ms

'Nac300BC0(EK1501)' (1002): 'INIT to PREOP' failed! Error: 'check device state for PREOP'. Communication Error '1823'。

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

例2：

9/14/2019 5:02:42 PM 742 ms

'Cms304BC0(EK1100) (1029) - Cms304AI6(EL3204) (1032)' Communication interrupted

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

例3：

9/3/2019 12:19:40 PM 455 ms

'Nac300BC0(EK1501) (1002)' Communication interrupted

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

### 主站初始化问题

1. 主站初始化问题：

通讯过程：

第一步：EtherCAT主站发送Frame，发现连续10次（10个PLC周期，200ms）没有从站响应之后，主站会报错Frame missed 10 times (frame no. 0)；

第二步：主站不再发送模块的读写命令，只发送BRD（广播查找命令）

第三步：等到主站接收到从站的返回命令之后，主站认为总线从重大问题中恢复，主站会把自己的状态变为Init；Frame returned -> force reinitialization!

第四步：主站会刷新从站的状态，重新建立通讯，建立连接需要很多步骤；主站会把自身的状态从INIT变为PREOP，准备下一步的OP。

第五步：如果主站从INIT变为PREOP失败，主站的状态就变回Init。如果主站从INIT变为PREOP成功，再变为OP，最后主站的状态就是OP。

在EventLog中会如下显示：

首先第一条信息为：

图形用户界面, 文本

中度可信度描述已自动生成

TwinCAT System Message: Timestamp: 11/4/2021 4:57:07 PM 694 ms Message: Device 1 (EtherCAT): Frame missed 10 times (frame no. 1)。

第二条信息：

表格

描述已自动生成

TwinCAT System Message: Timestamp: 11/4/2021 4:56:40 PM 244 ms Message: Device 1 (EtherCAT): Frame returned -> force reinitialization!

当然此时可以用运行Read\_EcSlaveStatus21\_V27.exe文件，查看TXT记录。

2. 对于这样的故障排查：

这样的问题有可能就是网线虚接或者有模块损坏（模块没有完全损坏），此时我们可以设置EtherCAT主站。

## System时间记录

系统信息，包括蓝屏等的信息，此处略。

## Security事件记录

Security是用户的登录等信息的记录。

图形用户界面

低可信度描述已自动生成

**上海（ 中国区总部）**

中国上海市静安区汶水路 299 弄 9号（市北智汇园）

电话: 021-66312666

**北京分公司**

北京市西城区新街口北大街 3 号新街高和大厦 407 室

电话: 010-82200036 邮箱: beijing@beckhoff.com.cn

**广州分公司**

广州市天河区珠江新城珠江东路32号利通广场1303室

电话: 020-38010300/1/2 邮箱: guangzhou@beckhoff.com.cn

**成都分公司**

成都市锦江区东御街18号 百扬大厦2305 室

电话: 028-86202581 邮箱: chengdu@beckhoff.com.cn

|  |  |
| --- | --- |
| 请用微信扫描二维码  通过公众号与技术支持交流 | 倍福官方网站：  https://www.beckhoff.com.cn  在线帮助系统：  https://infosys.beckhoff.com/index\_en.htm |
| 倍福虚拟学院：  https://tr.beckhoff.com.cn/ |
| 招贤纳士：job@beckhoff.com.cn  技术支持：support@beckhoff.com.cn  产品维修：service@beckhoff.com.cn  方案咨询：sales@beckhoff.com.cn |
|  |