**使用AND\_THEN与OR\_ELSE为内存安全增设防护**

|  |  |  |
| --- | --- | --- |
|  | 作者：云龙  职务：华东区 技术支持工程师  邮箱：long.yun@beckhoff.com.cn  日期：2022-11-10 | |
| **摘 要：**  在PLC程序代码编辑时，我们经常会使用到数组和指针的功能，当我们使用这两个功能时一定需要特别留意在程序的运行过程中是否会存在超过数组越界、指向非法/无效地址的问题，虽然也有一些方法可以在后期对这些问题进行检查，但是在程序设计的时候就应该先考虑到这部分代码的内存安全，以此我们建议合理的使用AND\_THEN和OR\_ELSE运算符，在设计时就尽量避免类似问题。同时，上述两个运算符的使用还能有效优化程序的执行时间、提升效率。后文将对此详细描述。 | |
| **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：**  [**InfoSys中关于AND\_THEN的信息**](https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_plc_intro/2528923787.html&id=2639569006076492326)  [**InfoSys中关于OR\_ELSE的信息**](https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_plc_intro/2528929163.html&id=8504778572887165500) | |

目 录

[1. 软硬件版本 4](#_Toc118986675)

[1.1. 倍福Beckhoff 4](#_Toc118986676)

[1.1.1. 控制器硬件 4](#_Toc118986677)

[1.1.2. 控制软件 4](#_Toc118986678)

[2. 运算符说明 4](#_Toc118986679)

[2.1. AND\_THEN 4](#_Toc118986680)

[2.2. OR\_ELSE 4](#_Toc118986681)

[2.3. 短路求值 4](#_Toc118986682)

[3. 应用演示 4](#_Toc118986683)

[3.1. 在指针引用时的应用 4](#_Toc118986684)

[3.2. 在数组索引时的应用 6](#_Toc118986685)

[3.3. 不同优先级的错误判断与状态输出 7](#_Toc118986686)

[4. 总结 8](#_Toc118986687)

# 软硬件版本

## 倍福Beckhoff

### 控制器硬件

TwinCAT控制器，IPC、EPC或者PC，

此处使用：个人笔记本电脑

### 控制软件

个人笔记本电脑安装Full TwinCAT3：TwinCAT 3.1 Build 4024.22版本

# 运算符说明

## AND\_THEN

该运算符是IEC 61131-3标准的拓展，只允许在ST编程中使用，是对BOOL和BIT类型的操作数进行逻辑“与运算”，并具有短路求值（short-circuit evaluation）的属性。

与“AND”运算符的功能类似，当所有的操作数都为 "TRUE"时，运算的结果也为 "TRUE"，否则就为 "FALSE"。

使用“AND\_THEN”运算符时，只有在前一个操作数为“TRUE”时，TwinCAT才会继续运算后续操作数的表达式。例如在IF (ptr < > 0 AND\_THEN ptr ^ = 99) THEN的条件中，只有当ptr < > 0条件满足时，才会执行后面的(prt^)取值动作，这样的特性可以在程序设计时有效的避免出现引用空指针的问题。

相反，如果使用“AND”运算符，TwinCAT 总是会运算所有操作数，那么在上例中，如prt = 0时，再执行(ptr^)取值动作就会出现引用空指针的问题。

## OR\_ELSE

该运算符是IEC 61131-3标准的拓展。只允许在ST编程中使用，是对BOOL和BIT操作数进行逻辑“或运算”，并具有短路求值（short-circuit evaluation）的属性。

与“OR”运算符的功能类似，当至少一个操作数产生“TRUE”结果时，操作的结果也为“TRUE”，否则为“FALSE”。

与使用“OR”运算符相比，对于“OR\_ELSE”来说，只要其中一个操作数产生为“TRUE”的结果，所有其他操作数上的表达式就不会被运算。

## 短路求值

只要最终的结果已经可以确定是真或假，求值过程便告终止，这称之为短路求值（short-circuit evaluation）

# 应用演示

## 在指针引用时的应用

变量声明：

PROGRAM MAIN

VAR

 pData  :POINTER TO INT;

 iData  :INT;

 bSwitch,bResult

     :BOOL;

END\_VAR

测试程序：

pData := ADR(iData) \* TO\_UDINT(bSwitch);

IF pData <> 0 AND\_THEN pData^ > 99 THEN

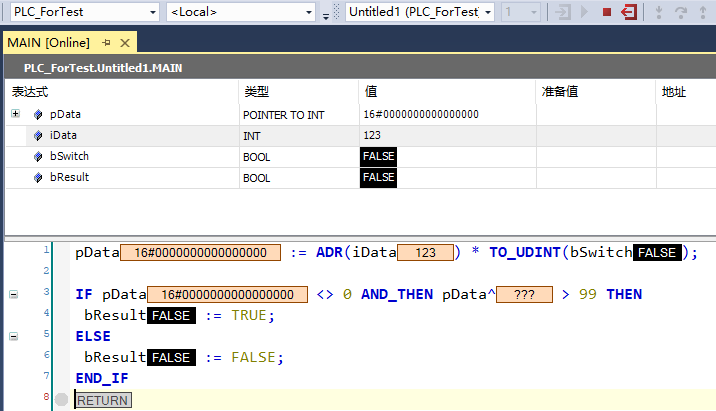
 bResult := TRUE;

ELSE

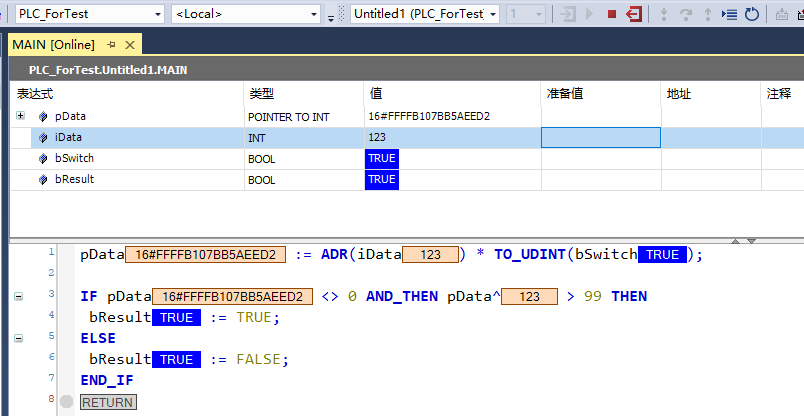
 bResult := FALSE;

END\_IF

运行效果：



AND\_THEN检查到没有满足前提条件，后续的操作数不再进行运算，即使后续操作数中出现空指针引用的表达式也不会导致PLC程序停止运行。



当所有条件都满足时，执行IF中要输出的表达式。

## 在数组索引时的应用

变量声明：

PROGRAM MAIN

VAR

 aData  :ARRAY[2..9] OF INT;

 iIndex  :INT;

 bSwitch,bResult

    :BOOL;

END\_VAR

程序主体：

IF bSwitch THEN

 iIndex := 5;

ELSE

 iIndex := 999;

END\_IF

IF iIndex >=2

 AND\_THEN iIndex <= 9

 AND\_THEN aData[iIndex] > 99 THEN

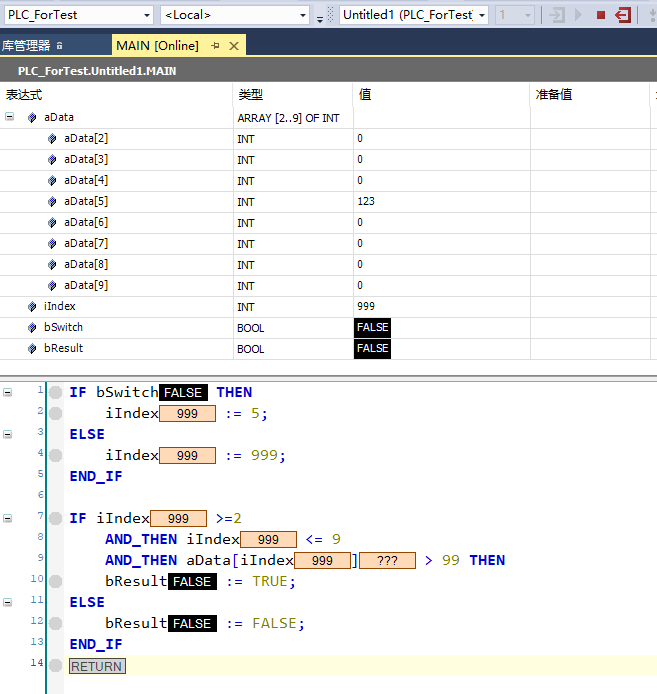
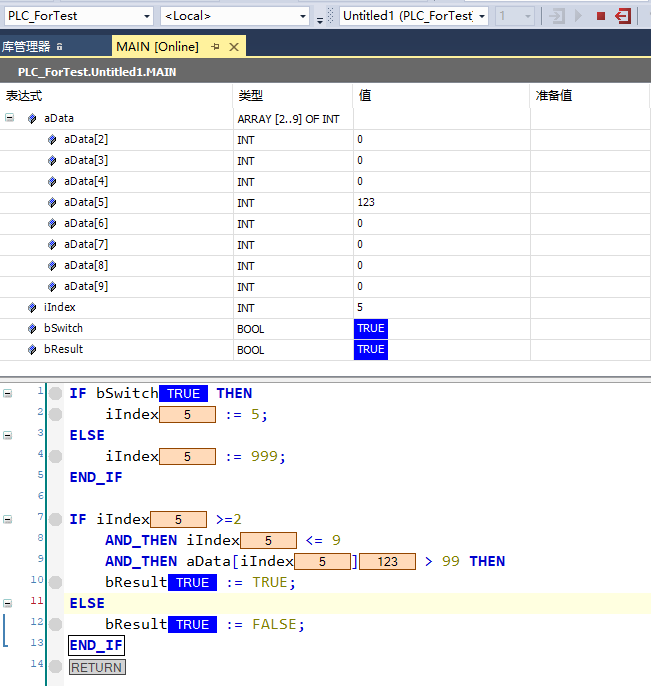
 bResult := TRUE;

ELSE

 bResult := FALSE;

END\_IF

运行效果：

如上左图，当数组索引序号超过了数组边界时也不会出现PLC程序运行异常的情况；

右图中数组索引序号在声明的数组范围后并满足了所有运行条件后，执行输出语句。

## 不同优先级的错误判断与状态输出

变量声明：

PROGRAM MAIN

VAR

 bError,bWarn,bInfo :BOOL; *//Error Level Error>Warn>Info*

 bErrored   :BOOL;

 iErrorID   :INT;

END\_VAR

程序主体：

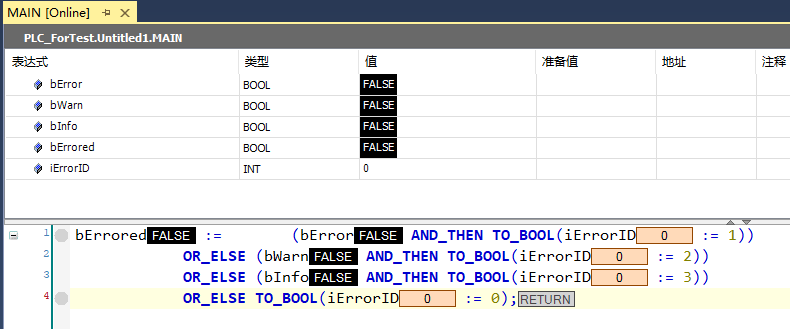
bErrored :=   (bError AND\_THEN TO\_BOOL(iErrorID := 1))

   OR\_ELSE (bWarn AND\_THEN TO\_BOOL(iErrorID := 2))

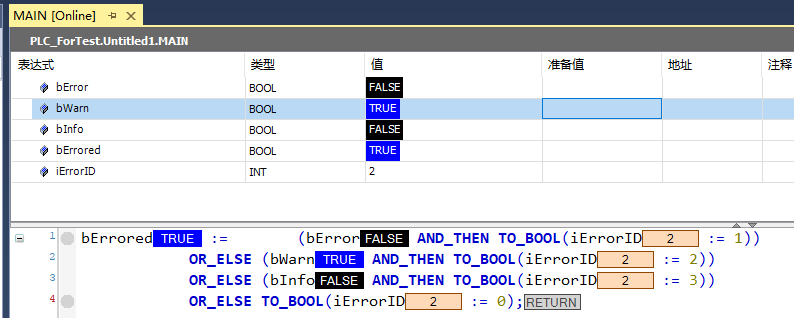
   OR\_ELSE (bInfo AND\_THEN TO\_BOOL(iErrorID := 3))

   OR\_ELSE TO\_BOOL(iErrorID := 0);

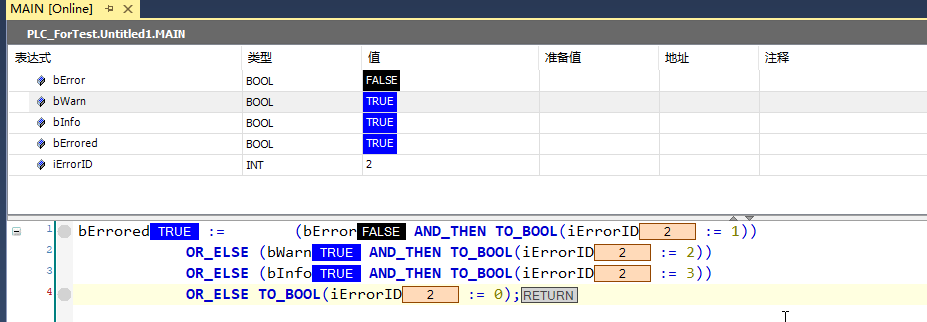
运行效果：



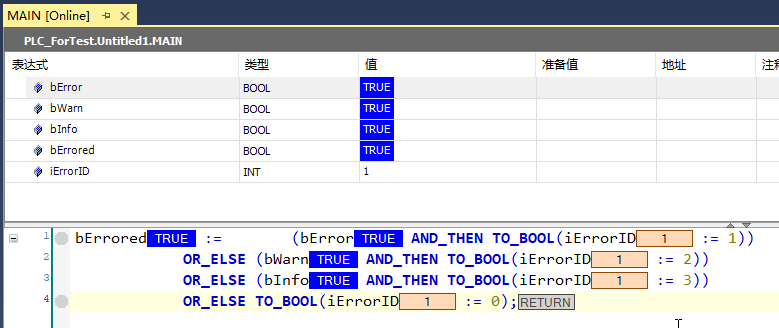
没有任何状态触发时，ErrorID输出为0，Errored状态为false



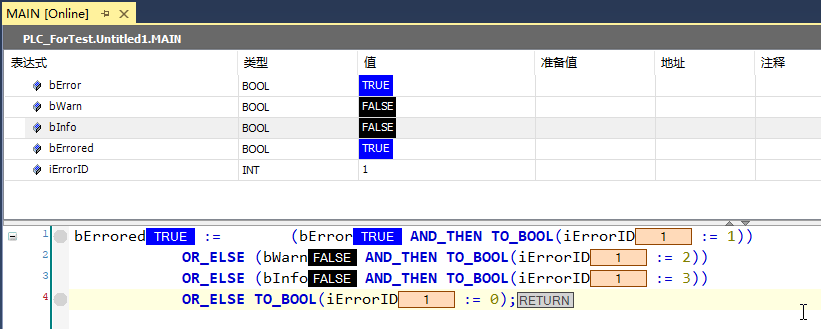
当警告的状态被触发时，ErrorID输出为2，Errored状态输出为true



当消息的状态被触发时，ErrorID输出保持为2，Errored状态输出为true



当所有状态都被触发时，ErrorID输出为1，Errored状态输出为true



当只有错误的状态被触发时，ErrorID输出为1，Errored状态输出为true

# 总结

在ST语言编程中使用AND、OR运算符时，所有条件判断都会被执行。而使用AND\_THEN、OR\_ELSE运算符时，当操作数确定满足执行条件后，后续操作数的表达式将不会被执行。由此，我们不仅可以在数组、指针引用等地方增强程序代码在内存引用上的安全性，还能有效减少CPU对表达式的处理时间，以提升代码的执行效率，使代码风格更加干净整洁。

**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 |
|  |