

工业梯形图分析1

发表于 2021-02-16 更新于 2021-02-19 分类于 [Challenge](#) , [2019](#) , [工业信息安全技能大赛](#) , [成都站](#)
[Challenge](#) | [2019](#) | [工业信息安全技能大赛](#) | [成都站](#) | [工业梯形图分析1](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

[纵横网络靶场社区](#)

题目描述

这是一个常见的工控梯形图。当PIW的值为4096时，DB2.DBDO的值为多少？

题目考点

- 梯形图编辑

解题思路

首先安装好西门子编程软件STEP7,软件版本随意，我安装的版本是V5.4

第二是需要安装西门子的仿真PLC程序，S7-PLCSIM

□

□

以上两个软件安装完成后，使用SIMATIC Manager打开题目附件，步骤，文件—打开—浏览—，找到题目附件

□

打开后，可以看到有几个功能块，其中OB是主程序，FC是功能块（子程序），DB是数据块，OB和FC里面找，程序很简单，根据题目说明，在OB1中找到了PIW和DB2.DBDO

□

直接把PIW256改成4096，接下来，启动模块仿真：

S7-PLCSIM会自动弹出来

□

注意：这里需要把仿真PLC设置为STOP模式才能下载程序

然后把程序下载到仿真PLC

□

如果有弹出窗口，点击是

□

接下来把仿真PLC切换到RUN模式，下一步，连线PLC，并在线监视

□

因为最开始我们已经把PIW256值改为了4096，所以程序会自动计算结果，在DB2.DBDO上显示的值即为flag。

注意：flag格式为自动计算的结果，不是16进制，也不是10进制

□

Flag

```
1 flag{37091.9}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/成都站/wbmoiQQei4iYeoxxfFniLx.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[# Challenge # 2019 # 工业信息安全技能大赛 # 成都站](#)

[工业梯形图分析2](#)

[TCP-urgent-pointer](#)