西门子S7-300,接口模块IM365西门子代理商

产品名称	西门子S7-300,接口模块IM365西门子代理商
公司名称	湖南西控自动化设备有限公司
价格	.00/件
规格参数	西门子:S7300 PLC:6ES73650BA010AA0 德国:用于连接扩展架, W/O K-BUS,2
公司地址	中国（湖南）自由贸易试验区长沙片区开元东路1306号开阳智能制造产业园（一期）4#栋301
联系电话	17838383235 17838383235

产品详情

技术干货|基于西门子软PLC的虚拟SCADA系统的工控安全实践

一、概述/

近几年，随着国家政策和工业数字化发展的推动，工控安全行业发展迅速，造成了对工控安全研究人员需求的巨大缺口的同时，提出了对度更高的要求。一方面，工控网络安全是集成了信息安全技术与工业自动化控制技术的跨学科的全新领域， 需要了解并掌握更多领域的相关知识，有着较高的技术门槛；

另一方面，缺乏可研究和学习的便利环境。对于企业和个人层面来说，成本耗费较高，从事相关研究的公司或人才，需自行采购一些硬件设备，搭建模拟环境，再进行相应的安全研究。为了解决这些难题，我们做了很多相关的技术研究，通过构建一套虚拟的工业控制环境，从而降低了解和学习工控安全的门槛，推动相关人才的培养和技术攻防的实战演练。

二、控制器虚拟化技术介绍/

可编程控制器，即PLC。PLC的实现分为硬PLC和软PLC。 所谓硬PLC从严格意义上来说是由硬件或者一块专用的ASIC芯片来实现PLC指令的执行。而软PLC是用一些通用的CPU或者MCU来实现PLC指令的解释或者编译持行。

软件PLC（SoftPLC，也称为软逻辑SoftLogic）是一种基于PC机开发结构的控制系统，它具有硬PLC在功能、可靠性、速度、故障查找等方面的特点，利用软件技术可以将标准的工业PC转换成全功能的PLC过程控制器。

软件PLC综合了计算机和PLC的开关量控制、模拟量控制、数学运算、数值处理、网络通信、PID调节等功能，通过一个多任务控制内核，提供强大的指令集、快速而准确的扫描周期、可靠的操作和可连接各种I/O系统的及网络的开放式结构。所以，软件PLC
提供了与硬PLC同样的功能，同时又提供了PC环境的各种优点。

虚拟机技术是虚拟化技术的一种，所谓虚拟化技术就是将事物从一种形式转变成另一种形式，常用的虚拟化技术有操作系统中内存的虚拟化，实际运行时用户需要的内存空间可能远远大于物理机器的内存大小，利用内存的虚拟化技术，用户可以将一部分硬盘虚拟化为内存，而这对用户是透明的。

如果将软PLC安装在虚拟机下，在软PLC出现故障时，用备份的虚拟机代替当前的虚拟机，即可快速恢复系统运行；此外，开发人员不必在现场，即可开发调试项目，在调试完成后，将包含软PLC的虚拟机直接放在现场的工控计算机上就直接可以完全运行。

三、构建虚拟SCADA系统/

使用西门子WinCC V7.3上位机组态软件和西门子软PLC，可以实现一个虚拟化运行的SCADA系统。

3.1 通讯拓扑

3.2 运行西门子软PLC

SIMATIC软PLC是西门子公司开发的基于PC控制的核心组件，它的出现扩展了SIMATIC S7的控制范围。软PLC是一个名副其实的控制中心，它将PLC控制、数据处理、通讯、可视化及工艺集成于一台PC机上。

在虚拟机中安装PLC后，运行如下：

虚拟PLC的运行环境搭建好了之后，下面就可以往虚拟PLC里面写配置和程序了。

3.3 配置虚拟PLC

（1）打开step7软件

创建工程，并进行组态配置

（2）定义变量

（3）编写一个简单的测试程序

（4）下载程序

将程序下载至CPU中，就可以运行程序。

（5）执行程序

程序下载完成后，就可以运行程序。

通过修改值改变运行状态，经验证程序逻辑正确。

3.4 配置虚拟SCADA系统

（1）变量管理

（2）通讯连接设置

（3）创建一个新图形

（4）组态图形

（5）项目激活

3.5 SCADA运行界面

通过点击“ 启动按钮 ”和“ 停止按钮 ”可以看到阀门运行状态会改变，至此，说明上位机WinCC和虚拟PLC通讯没有任何问题，虚拟PLC能够和硬件PLC一样，实现同样功能。

四 针对西门子PLC的攻击行为/

4.1 s7comm协议简介

和Modbus的应用层协议不同，S7comm的协议栈修改程度更高，在应用层组织的数据经过COTP协议、TPKT协议的进一步处理后，终通过TCP进行传输，wireshark wiki给出的S7comm的协议栈如下：

OSI layer	Protocol
Application Layer	S7 communication
Presentation Layer	S7 communication(COTP)
Session Layer	S7 communication(TPKT)

Transport Layer	ISO-on-TCP (RFC 1006)
Network Layer	IP
Data Link Layer	Ethernet
Physical Layer	Ethernet

COTP与TPKT协议涉及到网络与PLC设备的连接问题，有兴趣的朋友可以自行上网搜索。

S7Comm数据作为COTP数据包的有效载荷，个字节总是0x32作为协议标识符。S7Comm协议包含三部分：

Header

Parameter

Data

S7Comm Header如下图所示：

我们通过两个表来了解Header的结构：

其中为重要的就是ROSCTR字段，其定义如下表：

S7comm 协议的 Parameter 部分与 Data 部分，则是根据 Header 中 PDU type 的功能码的不同、协议扩展（Userdata）的内容不同而变得不同。

当PUD类型为JOB和ACK_Data时，Parameter项的个字段为Function code，其类型为Unsigned interger，长度为1byte，其详细的功能码如下：

采用S7comm协议进行读写操作时，Parameter结构相同，只是写操作多了Data结构。

当PDU类型是JOB时，Parameter部分的结构如下：

其中一个Item的结构如下

当PDU类型是ACK_DATA时，Parameter部分的结构如下：

Data 部分存储 Item 结构体，其中一个 Item 的结构如下

4.2 抓包分析

通过对虚拟PLC与SCADA系统的通讯进行抓包分析，过滤出func为0x05，即写入操作的数据包：

查看wireshark中的包信息：

PDU类型为0x01(JOB)；

Function Code为0x05(Write)；

Item中的DB number为1，地址为0x000000；

Data中写入的数据为01。

查看响应数据如下：

PDU类型为 0x03(ACK_DATA)；

Function Code为0x05(Write)；

Return Code在Data中，为0xff(Success)。

4.3 非法接入实施网络攻击

由于虚拟PLC与SCADA系统未进行授权访问，在未配置工控安全防护设备时，极易受到未授权访问（非法接入）或数据篡改类型的攻击。

在了解到工控系统中某些写入的DB编号和地址后，可通过多种脚本方式轻易对工控环境中的PLC设备或S

CADA系统等进行攻击，如通过python脚本连接s7comm协议的设备，进行数据篡改或操控plc的启停等。

五、 虚拟PLC和SCADA系统对工控网络安全实践的意义

由于工控现场对设备运行具有高安全性和高可靠性的强需求，加之工控领域使用的技术和产品具有高度的非标准化特点，对工控领域的技术研究及防护不可能像在实验室中那样轻易地、快速地进行。

而虚拟PLC和SCADA系统的利用为解决上述问题提供了便利和技术可行性，同时也为安全厂商提供了一种快速搭建贴近客户现场仿真环境的方法，便于其对防护技术及效果进行验证，这对于安全厂商帮助工业领域的企业提高其自身运行的安全性具有积极的推动作用。

虚拟PLC和SCADA系统还可以将工业网络安全靶场提升到一个新的高度，原有环境的工业网络安全靶场受硬件条件的约束，对场地、人员等的要求，不便于环境的搭建和迁移；

但基于虚拟SCADA系统的工业网络安全靶场可以完全虚拟化，上传到云环境中，可以实现工业网络安全靶场的攻防实训平台、网上教学、举办大型的工业网络安全攻防大赛等。

快速部署

在搭建传统的工业网络安全靶场时，使用硬件PLC会带来各种不便并加大调试时间，增加人力和物力的投入成本；但使用虚拟SCADA系统来搭建工业网络安全靶场，仅仅只通过软件设置就可以还原真实的工业网络环境，效果一样而且操作便捷，可减少很多时间，满足了真正意义上的快速部署需求。

攻防试验

虚拟SCADA系统具有真实SCADA系统的特性，可以通过该平台实时获取到工业生产环境中工业网络的流量，经过流量分析后可以在线对工业设备进行攻击，例如常见的USB木马攻击、数据篡改攻击、控制器攻击等行为。如下图就是模拟的数据篡改攻击，模拟攻击者接入过程控制网交换机，针对生产中的重要数据进行篡改，软件PLC误以为是上位机发送的指令，将错误的数据通过PLC输出控制板发送给现场设备执行。

教育培训

基于虚拟SCADA系统的工业网络安全靶场可以作为教学与培训的实验环境，集合各类工控领域行业级安全产品（如攻防对抗、网络威胁管理、漏洞挖掘检测、工控安全大数据、全网检测审计、数据采集隔离、系统安全监管、智能保护等设备），及工业网络相关元器件及过程控制系统（PLC、DCS、SCADA、上位机等）。

该平台在还原真实的工业网络环境的基础上，可让不同学员通过网络就能进入该环境进行学习。

攻防大赛

能够通过云搭建工业网络安全靶场，意味着以后关于工业网络安全的攻防大赛不必在现场搭建环境，不仅能节约场地费用，还能满足快速搭建，不受人数的限制，不受地理位置的制约，只要有网络就可以通过云平台进入模拟的工业网络安全靶场，这样收益人群更广，具有传统的工业网络安全大赛环境所不能比拟的优势。