选煤厂工控网络安全实验分析

韩子彬
(国家能源集团神东煤炭集团公司洗选中心,陕西 榆林 719315)

摘 要:随着信息技术的发展,标准以太网(IEEE 802.3 和 TCP/IP 协议)逐渐应用于工业控制系统(ICS)。它打破了 ICS 的自然隔离,但不包含安全机制。入侵检测系统(IDS),与特定的工业控制过程密切相关,是现代集成电路发展的必然。近年来,工业控制系统安全一直是研究的热点,许多安全问题已广为人知。然而,由于缺乏用于安全研究的开放式虚拟工业控制系统试验装置,选煤厂工控网络安全研究工作受到影响。针对选煤厂煤泥浓缩环节描述了一个虚拟测试框架,创建了测试装置组件,包括虚拟设备和过程模拟器。虚拟试验的设计应确保实验装置可与选煤厂工业控制系统设备进行相互操作,并确保测试可提供类似的工业控制系统网络行为。实验结果表明:其与实际工业控制系统设备可互操作,并且容易受到与实际系统相同的攻击。此外,这些试验装置已被证明在系统附近产生流量,虚拟测试系统在检测渗透攻击、伪造攻击和虚假数据注入攻击方面具有优异的性能。

关键词:选煤厂;工业控制系统;PLC;攻击;网络安全;虚拟测试
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2022)0162-06

Experimental Analysis of Industrial Control Network Security in Coal Preparation Plant

HAN Zi-bin
(Coal Washing Center, Shendong Coal Group Corporation of CHN ENERGY, Yulin 719315, China)

Abstract: With the development of information technology, standard Ethernet (IEEE 802.3 and TCP/IP Protocol) is gradually applied to industrial control system (ICS). It breaks the natural isolation of ICs, but does not include security mechanism. Intrusion detection system (IDS), which is closely related to the specific industrial control process, is the necessity of the development of modern integrated circuits. In recent years, the safety of industrial control system has always been a research hotspot, and many safety problems have been widely known. However, due to the lack of research on the safety of industrial control system in coal preparation plant, it is affected by the lack of open network control system. We describe a virtual test framework for slime concentration in coal preparation plant, and create test device components, including virtual equipment and process simulator. The design of virtual test shall ensure that the experimental device can interoperate with the industrial control system equipment of coal preparation plant, and ensure that the test can provide similar network behavior of industrial control system. The experimental results show that it can interoperate with the actual industrial control system equipment, and is vulnerable to the same attack as the actual system. In addition, these test devices have been proved to generate traffic near the system, and the virtual test system has excellent performance in detecting penetration attack, forgery attack and false data injection attack.

Key words: coal preparation plant; industrial control system; PLC; attack; network security; virtual test

0 引 言

社会生产已经依赖于关键的工业设施,包括能源行业及选煤厂。工控网络故障可能会导致重大安全事故和财产损失。工业控制系统(Industrial Control System)源于计算机控制系统,是 PLC、DCS、SCADA 等工业系统的总称。它从连接到物理过程的传感器收集数据,并通过执行器、开关和阀门等来远程控制生产过程,从而管理复杂和潜在的工业过程。在选煤厂信息化建设高速发展时,其网络安全发展却明显滞后。国外针对工业控制系统的网络攻击,如“震网”事件、委内瑞拉大规模停电事件、挪威铝业集团遭受勒索攻击,以及国内一些工业控制系统网络安全事件引起了高度关注[1]。

目前,工业控制系统领域的技术人员使用的测试方式由实际的控制系统硬件和软件构成,或者由单一类型的系统构成的虚拟环境。测试人员通常会识别他

收稿日期:2022-03-16
作者简介:韩子彬(1982-),男,硕士,高级工程师,研究方向为选煤厂工控网络及自动化。

们的测试系统漏洞,开发针对这些漏洞的攻击,然后捕获正常流量和攻击流量。使用这些私有数据集验证新的入侵检测系统并进行研究。这种测试方法存在两方面问题。首先,私人数据集和试验方式不允许第三方重复实验。基于异常的入侵检测系统需要使用分类器,分类器必须使用预先标记的数据集进行训练。数据集的问题可能会导致分类器依赖数据中与攻击没有真正关联的字段。其次,测试人员还可以根据特定的测试方式定制入侵检测系统。这可能会导致潜在的误导性入侵检测系统的性能结果。

该文描述了一种虚拟测试方法,该测试方式首先减少了重复工作,可以不必创建自己的试验台。可以模拟工业控制网络系统,这为测试人员提供了便捷的测试方式,提高了工作效率。其次,可以共享代码,将已发布的结果进行复制和比较。第三,虚拟测试方式可用于为入侵检测人员捕获正常网络流量或异常网络流量。第四,目前工业控制系统的研究需要大量投资。应用此种测试方式,无需购买大型设备即可开展研究测试应用[2-3]。

1　系统组成

与虚拟系统相比,实验室规模的系统具有许多优点。首先,数据将反映实际控制系统过程中存在的实际测量变化。其次,通信模式和延迟将完全准确,不易受到操作系统调度负载等模拟变量不准确的影响。第三,工业控制系统网络设备单独容易受到许多攻击。这些漏洞可能不存在于用于模拟的系统中。比如包括导致设备易受泪滴攻击、web 应用程序攻击或缓冲区溢出攻击的协议实现漏洞。其他安全问题,如设备的保护不善或硬编码默认密码,也不会出现。通过实验室规模的过程控制系统,除了基于协议的攻击和正常背景流量之外,还可以捕获这些攻击。

虚拟测试分为几个独立的组件。主要组件包括过程模拟器、虚拟设备、实际设备、配置文件和数据记录器,用于捕获和存储网络流量和过程状态,如图 1 所示。

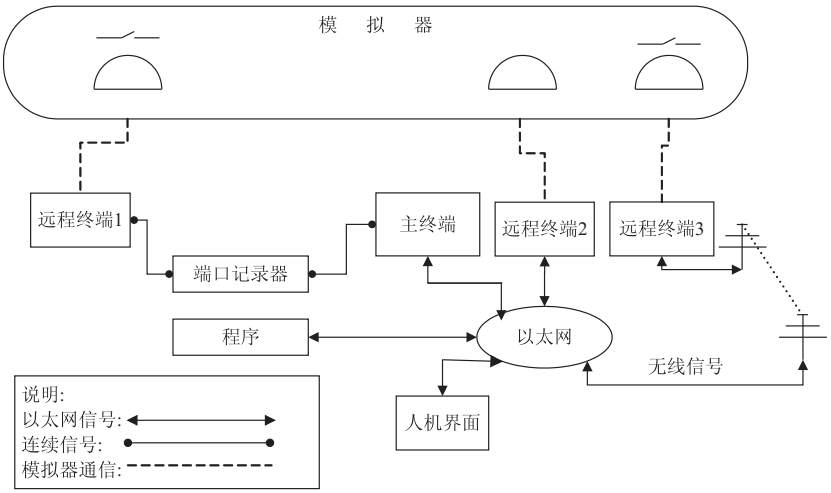

图 1　系统结构

过程模拟器可通过编程或模拟器实现。在工业控制系统网络中,虚拟设备取代了主终端单元和远程终端单元。虚拟设备包括用编程语言实现的控制逻辑,以模拟内部主逻辑或远程终端逻辑功能。虚拟设备和过程模拟器通过单独的模拟器通信信道进行通信。虚拟试验支持与实际设备的接口。配置文件用于描述测试组件之间的连接,并为每个接口设置通信协议和速率。数据记录器可用于捕获和存储过程信息和网络流量。

测试功能主要是能够模拟真实的工业控制系统串行和 TCP/IP 协议通信。测试方式可以模拟工控网络及协议,包括工业控制系统数据。除工业控制系统流量外,虚拟工业控制系统控制过程也与实际选煤厂生产过程相似。为有效地用于生产实践,须可靠地记录对网络流量的捕获,记录对工控网络流量影响很小,并具有足够的精确度和准确性,可以充分体现系统的行为。测试方式还能够与实际的选煤厂工业控制系统设备连接,确保与实际工业控制系统兼容[4]。

为了实现开放系统的性能,虚拟试验系统应灵活且易于扩展。每个组件应独立于其他组件,任何单独的组件都是操作所需的。这有助于实现虚拟试验与现有系统集成。它还允许测试人员调整测试项目,与这个虚拟装置一起工作。例如,能够包含开放主域控制器项目中的相量测量和主域控制器实例,或者集成其他虚拟测试软件。

2　过程模拟

过程模拟不仅模拟工业控制系统的物理特性,还必须对来自工业控制系统的控制输入做出响应。对于工业控制系统安全实验而言,能够对网络攻防进行建

模至关重要,这影响着工业控制系统设备和实际控制过程。如果设计了一个试验装置来模拟一个选煤厂浓缩过程,那么就需要一个过程模拟器来管理浓缩池的物理过程。选煤厂浓缩池是煤泥浓缩设施,主要用来处理煤泥水,以提高底流中煤泥的含量,为后续煤泥处理流程做准备。通过添加凝聚剂与絮凝剂,煤泥水中的煤泥在自身重力的作用下在浓缩池的内部发生自由沉降,最终在浓缩池的底部得到浓度较高的煤泥浆液。在传动部件的带动下耙架将煤泥浆液刮集到浓缩池的中心并从排料管排出成为底流。浓缩池上部的清水则从四周排出成为溢流。通过处理后,这部分水可以回收利用形成选煤厂洗水闭路循环。控制过程包括启用水泵和排水阀。

过程模拟器直接与虚拟测试中的选煤厂浓缩池 PLC 通信。该通信发生在与工业控制系统通信分离的后通道上。通信包括模拟器的测量信号和设备的输入信号。模拟器的数据模拟 PLC 和用于液位、压力、流量和其他仪表设备中的模拟和数字信号输入。输出信号用于控制电机、泵和阀门等执行器。

模拟器模块执行过程模拟并存储物理过程的当前状态。通信接口接收来自虚拟设备的周期性过程控制更新和过程测量更新请求。请求由通信接口排队,并按照更新队列接收的顺序应用。配置文件用于设置物理过程的初始条件[5]。

过程模拟器由四个组件组成:模拟器模块、通信接口、堆栈更新和配置文件。模拟器模块执行过程模拟并存储物理过程的当前状态。通信接口接收来自虚拟设备的周期性过程控制更新和过程测量更新请求。来自虚拟设备的请求由通信接口排队,并按照更新堆栈接收的顺序应用。配置文件用于设置物理过程的初始条件。虚拟设备和过程模拟器之间的接口与通信通道是分开的。过程模拟器至虚拟设备接口对模拟和数字输入输出进行建模,这些输入和输出通常位于远程终端装置或智能设备上。过程模拟器体系结构如图 2 所示。

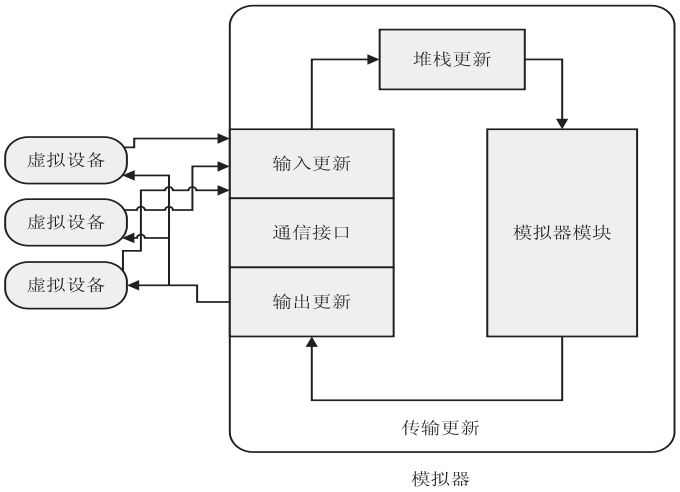

图 2 过程模拟器体系结构

流程模拟利用 Python 编程软件实现。启动时,模拟器模块读取配置文件以配置流程变量,如流量、电机转速等,并设置初始模拟状态。模拟是基于离散时间的。模拟器接口接受并向模拟器提供有关设备相关输入和输出的更新。输入和输出在配置文件名中定义。文件名的值在流程模拟器之间传输。这模拟了远程终端装置与过程测量装置和过程执行器之间的模拟和数字输入输出连接。

3 配 置

为了实现协议接口,可以创建客户端模块和服务器模块。这些模块可以利用在 Python 或其他语言(如 C++或 Java)现有的代码中创建。通常由工业控制系统设备执行的其他任务包括充当 FTP 或 HTTP 服务器。虚拟设备中没有本机提供此功能。但是,可以通过在虚拟机中与虚拟设备一起运行 FTP 或 HTTP 服务器来模拟该功能。

虚拟设备包括一个与过程模拟器通信的接口。过程模拟器接口接受并向模拟器提供设备相关输入和输出的信息。过程模拟器接口模拟从远程终端到测量设备(输入)和执行器(输出)的连接。远程终端通常包括数字输入和输出,以及到模数转换器(ADC)和数模转换器(DAC)的链路[6]。

控制逻辑直接模拟实际控制设备的控制和监控功能。控制逻辑被指定为独立于虚拟设备实现的单个 Python 函数。控制逻辑由逻辑控制线程调用;该线程还同步模拟器通信。相同的控制逻辑功能可用于多个设备,以允许代码重用。实际工业控制系统中的过程控制逻辑包括读取输入、执行逻辑和数字计算,然后设置适当的输出。该行为由虚拟设备控制逻辑建模。对

设备内存中的点的读取和写入由 get( ) 和 set( ) 函数处理。控制逻辑可以由组合逻辑、循环、条件编程和算术组成。

下段代码表示选煤厂浓缩池水泵的控制逻辑示例。

```
#determine if pump should be turned on
If( points[ 'SystemInAuto' ]. get( ) and
        not points[ 'HighLevelFloat' ]. get( ) and
        ( points[ 'LowLevelFloat' ]. get( ) or
        points[ 'PumpRunCmd' ]. get( ) ) :
points[ 'PumpRunCmd' ]. set( TURE)
elif( points[ 'SystemInMAN' ]. get( ) and
          points[ 'MANPumpRunCmd' ]. get( ) ) :
points[ 'PumpRunCmd' ]. set( TURE)
else:
points[ 'PumpRunCmd' ]. set( TURE)
```

该段代码检查控制系统模式(手动或自动)的状态,读取高位和低位液位传感器的值。这段代码不直接寻址存储点。点是通过名称来表示的。此外,控制逻辑不包括特定于协议的命令。get( ) 和 set( ) 函数是在协议层之上实现的,以允许在多个通信协议中使用控制逻辑。Points 为数据对象提供了接口。通过允许虚拟设备中的控制逻辑按名称引用数据对象,独立于通信协议或内存分配。使通信协议或内存分配可以更改,而无需更改控制逻辑或其他代码[7-9]。

因为虚拟设备是在虚拟机中实现的,并且使用标准的通信接口和经过验证的网络软件堆栈,可以测试新设备,并捕获数据日志,包括与设备的交互。比如虚拟试验可以与实际的人机界面(HMI)软件连接。HMI 可以在一个虚拟机中运行,并与模拟远程终端单元的虚拟设备通信。

过程模拟器和虚拟设备都是模块化的,除过程控制逻辑和过程模拟外,系统特性和行为由单个配置文件描述。该文件基于文本,可以手动编辑或机器生成。文件内容包括模拟器配置信息和系统中每个虚拟设备的配置。模拟器配置信息包括模拟器接口类型、接口配置信息和模拟器变量初始化。虚拟设备配置信息包括系统中每个设备的编号和名称、要存储的数据对象、通信协议、服务器和客户端协议类型和编号,以及工业控制系统接口配置(地址、端口等)。

虚拟试验的主要需求是生成有用的数据集以支持研究。理想情况下,流量捕获不应影响测试的运行。通过 tcpdump 或 Wireshark 可以捕获 MODBUS/TCP 网络流量。这些工具可以在混合模式下运行,以便在不干扰控制系统通信的情况下捕获流量。使用客户端 TCP 端口号来区分虚拟设备。将每个设备托管在自己的虚拟机中,可以为每个虚拟设备分配唯一的 IP 地址。

MODBUS 协议终端数据记录需要一个特殊的端口记录器。端口记录器为每个需要串行端口的虚拟设备创建一个伪终端主从对;创建从端口到设备预期读取的文件链接,主端口由端口记录器打开。当一个设备发送消息时,记录器会读取该消息,并将其回显到其他设备,然后进行记录。端口记录器还可以打开一个物理串行端口,并将其作为伪终端进行回显。也可以将单个设备指定为主设备,以模拟主设备到从设备的多点 RS-485 系统。端口记录器还可以在接收消息和重新传输消息之间插入延迟,以模拟传输延迟。

4　流量比较

为了验证虚拟试验,对选煤厂浓缩池控制系统进行建模。PLC 连接到每个物理过程,充当远程终端单元。PLC 包括梯形图逻辑,用于监控过程测量并执行控制逻辑。控制逻辑以梯形图逻辑的形式描述。主终端与两个远程终端通信。主终端包括监控逻辑,并充当中继器,将查询信息从系统人机界面转发至寻址远程终端。人机界面定期查询每个远程终端。人机界面还可以通过改变远程终端设置点对物理过程进行监控。

网络流量捕获一般使用相似性度量进行对比。相似性度量是一种比较 IP 网络捕获的方法,它可以产生一个从 0 到 1 的标量值,表示两个捕获基于网络和流量特征的相似程度。1 被视为相同,而 0 被视为不相同。每个指标衡量的是被比较捕获的特征。相似性度量的关键是积分度量,也就是说,为一组有限的键值计算一个整数分。离散度量的相似性由下式定义,其中 x_1 是第一次捕获中的第 i 个标量,依此类推,度量每个主机传输的字节数[10]。

$$\text{similarity} = 1 - \frac{1}{n}\sum_{i=0}^{n}\frac{|x_{1,i} - x_{2,i}|}{x_{1,i} + x_{2,i}}$$

表 1　系统相似性度量

名称	相似性	平均误差	最大误差	误差比/%
字节吞吐量	0.984 93	4.326 41	4	-2.969
错误计数	1	-	-	-
函数代码计数	0.999 96	-	0 000 32	0
函数代码序列	0.999 64	-	-	-
ID 序列	0.999 95	-	-	-
到达时间	0.935 33	0.003 66	0 066 16	3.046
无效 CRC	1	-	-	-
主主间到达时间	0.949 12	0.007 31	0 072 20	3.038
主从间到达时间	0.913 56	0.005 48	0.019 5	14.42
数据包大小	0.999 99	-0.000 83	0	-0.004
数据包吞吐量	0.984 95	0.246 93	0.246 93	-2.966

表 1 给出了系统比较的相似性度量。通过使用通信线缆直接连接主设备和从设备并记录流量。系统在关闭模式下保持 291 秒,捕获了 2 419 个数据包。从虚拟系统获取的流量捕获是使用波特率模拟的端口记录器创建的,虚拟系统也处于关闭模式;在 393 秒内捕获 3 173 个数据包。

重复相同的过程以获得自动模式下系统的流量捕获。虚拟系统自动模式捕获了 2 045 个数据包,占用时间为 255 秒。字节吞吐量和包吞吐量相似性度量非常接近统一(分别为 0.984 93 和 0.984 95),说明从系统响应主系统,主系统在从系统响应后发送请求。测试结果表明,该测试方式能够根据报文解析结果,拦截报文中与功能实现无关的部分以及潜在的安全威胁,从而验证了选煤厂基于应用层协议解析的工业控制系统网络安全防护策略的有效性[11]。

5 与实际设备集成

虚拟试验设备通过实际串行端口与虚拟主设备和从设备之间的工业控制系统无线信号相互连接。虚拟主机与实验室从机配对,实验室主机控制虚拟从机设备。这也说明了与工业控制系统通信设备的互操作性。使用的无线信号为 900 MHz 专有工业无线频率。这些无线信号连接到一个 USB 串行端口设备和虚拟试验主机。两个虚拟试验装置中的每个虚拟设备都连接到单独的端口记录器实例。每个实例都连接到一个串行端口,并创建一个虚拟设备连接到的伪终端。端口记录器充当两个物理串行端口的虚拟链路记录器。实验室通信是在每个 PLC 和无线信号之间放置串行分接线缆进行的,只记录收到的数据包。通过将虚拟选煤厂浓缩系统与集成工业无线链路进行比较,计算相似性度量。自动模式实验室捕获了 248 个数据包,而自动模式虚拟捕捉器捕获了 2 195 个数据包[12]。关闭模式实验室捕获了在 715 秒内发送的 2 789 个数据包,关闭模式下虚拟捕捉器捕获了在 1 052 秒内发送的 2 142 个数据包。在关闭模式下,实际系统有一个带有循环冗余校验错误的数据包,但虚拟系统没有。主要原因为:首先,实验室系统使用非延迟诱导进行日志记录,而模拟系统使用两个端口记录器,它们充当存储转发记录器。测试方法使模拟系统的计时结果出现偏差。其次,虚拟系统使用 USB 到串行适配器连接两个端口,虚拟系统数据包必须通过两个串行口缓冲区,而不仅是一个缓冲区。这增加了传输时间延迟。尽管在计时方面的相似性很低,但结果表明虚拟系统的所有非计时行为都与实验室系统相似[13]。对于工业控制系统测试人员来说,在这种情况下,实施或测试主要依赖于此设置的定时特性的项目(如入侵检测系统)可能会导致错误结果。而不依赖时间安排的项目的结果是准确的。

6 模拟攻击

对测试装置执行攻击,以验证其可用于测试攻击,而不仅仅是生成正常的工业控制系统流量。如果虚拟试验要用于安全研究,这种模拟是必不可少的。攻击方式有如下两种。

第一次攻击假设内部人员或具有物理访问权限的其他攻击者已将设备放置在系统中主设备和从设备之间的串行线上;该设备可以监控通信,并输入命令和响应。对于该测试,攻击设备每秒向主读取请求注入一次预定响应;该响应表示水池液位为 22.3%。这种攻击被称为注入攻击,它是在实验室和虚拟系统上进行的,攻击对两个系统都有效。然而,与实验室系统相比,该攻击对虚拟系统更有效。根据系统的请求与响应节奏,发送攻击包的时间是随机的;当主机发送读取请求,并且它收到的第一个数据包是注入的数据包时,攻击成功。在实验室系统中,在发送请求之前发送到 PLC 的任何数据都将被忽略。在虚拟系统中,数据被缓冲,直到工业控制系统客户端代码读取。由于攻击到达虚拟系统的时间阈值大于实验室系统,因此攻击对虚拟系统更有效。在工业控制系统客户端代码中发送请求之前,需要添加一个 flush() 调用,才能实现此攻击的完全逼真度。在任何情况下,两个不同的工业控制系统设备在受到攻击时都可能出现这种行为。比如西门子 PLC 和罗克韦尔 PLC 会以完全相同的方式受到攻击[14]。

其余的攻击利用实验室和与专有无线系统相连的虚拟管道系统。这些攻击假定攻击者已渗入无线系统。一台从机连接到一台 PC 上,用于运行攻击指令。将其连接到虚拟试验装置主机的 USB 串行端口设备。虚拟测试台中的每个虚拟设备都连接到各个端口记录器实例;每个实例都连接到一个串行端口,并创建一个虚拟设备连接到的伪终端。实验室系统通信是通过在每个 PLC 和无线系统之间放置串行分接线缆进行的,只记录收到的数据包。使用工控网络无线系统对通信系统进行从属拒绝服务攻击。攻击者使用自己的从机无线信号持续传输数据,导致无法接收合法从机的数据包。最终的结果是,主服务器不会对从服务器发送的响应进行更新,只要攻击持续,就会存储相同的值。在攻击中,攻击者持续传输无意义的数据,从而在响应读取请求的同时,向从属服务器创建拒绝服务。这会为主机创建一个可供选择的响应,并保证主机只接收攻击者选择的值。一旦攻击停止,信息会在几秒钟内恢复到正确的值。这种攻击对实验室和虚拟试验装置

都有效[15]。

系统中无线攻击的相似行为表明,虚拟试验装置可用于测试工业控制系统设备。虽然在某些情况下,攻击似乎对虚拟系统更有效,但它们仍然可以用于开发针对工业控制系统的验证攻击。

7　结束语

随工业控制技术的发展,工控网络安全防护日益成为不可忽视的问题。该文介绍了虚拟攻击试验方法,提供了独立的工业控制系统虚拟设备、模拟器和日志记录设备。这些虚拟设备可以模拟控制过程。根据模拟选煤工控网络和数据采集,可实现工业控制网络防护安全和数据安全,强化了工控网络安全管理、防范和追溯能力,提高了安全防护的科学性、整体性、针对性,保证了工业数据合理利用。结合工控系统数据传输和监管需求,稳定、可靠、先进、高效的工控安全防护系统,既保证了数据传输,又提升了工控安全防御能力,为工控业务正常运行打下基础。实验表明网络流量中 84% 的相似性度量,保证了其与真实设备的完美互操作性,可以模拟工控网络攻击行为,全面提升了选煤厂工控安全纵深防御管理及预警能力。

参考文献:

[1] 张春坡. 黑岱沟露天煤矿工业控制网络安全防护技术研究与应用[J]. 煤炭工程,2021,53(z1):144-148.

[2] 方捷睿,曹卫民,白建涛,等. 基于协议解析的工控网络安全仿真平台设计[J]. 自动化仪表,2021,42(2):102-106.

[3] 顾　闯. 煤炭企业工控网络安全防护与预测方法研究[J]. 煤炭科学技术,2019,47(11):143-147.

[4] WU P,WU M,ZHU J. The overall design and application of safety protection for industrial control systems[J]. Journal of Physics Conference Series,2020,1650:022033.

[5] YONG W,LIU J,YANG C,et al. Access control attacks on PLC vulnerabilities[J]. Information Security,2018(6):311-325.

[6] 吴开兴,王文鼎,李丽宏. 煤矿企业工业控制系统入侵检测算法[J]. 工矿自动化,2018,44(11):75-79.

[7] 黄健华. 斜沟煤矿选煤厂构建智能工厂的探索与实践[J]. 选煤技术,2021(3):31-37.

[8] 黄培松. 对工业控制网络安全脆弱性分析技术的研究分析[J]. 电子测试,2021(18):74-75.

[9] SERHANE A,RAAD M,RAAD R,et al. Programmable logic controllers based systems (PLC-BS):vulnerabilities and threats[J]. SN Applied Sciences,2019,1(8):924.

[10] YU W,WANG Y,SONG L. A two stage intrusion detection system for industrial control networks based on Ethernet/IP[J]. Electronics,2019,8(12):1545.

[11] MO Xiaojin. Industrial control network anomaly data identification method based on wireless communication[C]//Proceedings of 2019 9th international conference on information and social science (ICISS 2019). [s. l.]:Francis Academic Press,2019:31-37.

[12] 龚　俭,杨　望. 计算机网络安全导论[M]. 南京:东南大学出版社,2020.

[13] 胡一名. 工控网络异常检测系统的设计与实现[D]. 北京:北京邮电大学,2021.

[14] 李　威,李建俊,何晓霞,等. 基于流量分析的工业控制系统网络安全基线确定方法研究[J]. 科技通报,2018,34(9):176-179.

[15] 罗　野,王　英,闫怀超,等. 高交互式工控蜜罐系统设计与实现[J]. 自动化仪表,2021,42(3):98-101.

(上接第 161 页)

参考文献:

[1] 刘　军,张　洋,严汉宇. 原子教你玩 STM32(寄存器版)[M]. 北京:北京航空航天大学出版社,2013:341-351.

[2] 朱　斌,张　磊,怯肇乾. STM32-MCU 片内 IIC 接口的驱动程序设计[J]. 电子世界,2018(16):113-115.

[3] 刘　静,余小平,奚大顺,等. 基于 STM32 的Ⅱ C-DAC 6571 程序设计[J]. 电子设计工程,2018(4):172-175.

[4] 姬占涛,毛惠丰. TMS320F28335 的 I~2C 总线与 ADS 1115 的通信设计[J]. 单片机与嵌入式系统应用,2016(1):45-48.

[5] 刘　宁,陈冬琼,杨克磊. 基于 STM32 最小系统串口通信显示系统设计[J]. 工业控制计算机,2017,30(8):33-36.

[6] 蔡培君. 基于单个三轴加速传感器的人体运动状态识别[J]. 安庆师范学院学报:自然科学版,2016(1):83-86.

[7] 薛喜红,宋建锋,梁晓敏. 加速度传感器快速检测装置的开发[J]. 天津职业技术师范大学学报,2019(3):25-29.

[8] 宗　赤. 基于加速传感器的船舶振动检测系统设计[J]. 电子产品世界,2011(4):46-47.

[9] 冯仰刚,谢乾坤,强立宏,等. STM32F103ZET6 最小系统设计[J]. 电子世界,2013(5):141-142.

[10] 意法半导体. STM32 中文参考手册(第 10 版)[S]. 北京:意法半导体(中国)投资公司,2010.