福昕PDF编辑器

• 永久　• 轻巧　• 自由

升级会员　　批量购买

永久使用

无限制使用次数

极速轻巧

超低资源占用，告别卡顿慢

自由编辑

享受Word一样的编辑自由

扫一扫，关注公众号

测 评 报 告

项目名称：电站控制系统信息安全防护模块

项目编号：CIST HT-2017-12

测评时间：2017年6月10日至2017年7月10日

四川省信息安全测评中心

Sichuan Information Safety Testing Evaluation Center

测 评 报 告

项目名称：电站控制系统信息安全防护模块

项目编号：CIST HT-2017-12

测评时间：2017年6月10日至2017年7月10日

四川省信息安全测评中心

Sichuan Information Safety Testing Evaluation Center

目 录

报告声明

1、本报告仅适用于明确给出的委托单位委托测评的电站控制系统信息安全防护模块项目。

2、本测评报告是依据相关技术标准、技术规范进行的独立、客观、公正的测评结果。在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自增加、修改、伪造或掩盖事实。

3、未经书面批准，不得部分复制本报告（全文复制除外）。

4、为保证委托方的合法权益，本测试报告仅对委托方开放，我方有责任为委托方保守有关的技术秘密和商业秘密。

5、本测评报告不允许拷贝或复制作为广告材料。

6、当被审对象出现更新时，本测试结果便不再适用。涉及到的任何方面都应按要求进行必要的重新测评，更不能将本测评结果应用于其他方面的替代。

7、本测评报告未加盖公章（复印无效），涂改未加盖涂改专用章，均属无效。

测评报告单

项目名称	电站控制系统信息安全防护模块
测评依据	➢ GB/T 20281-2015 《信息安全技术 防火墙安全技术要求和测试评价方法》 ➢ 《电站控制系统信息安全防护模块需求分析说明书》
测评日期	2017 年 6 月 10 日至 2017 年 7 月 10 日

参照国家相关技术要求和项目的设计要求对电站控制系统信息安全防护模块的测评结果如下:

1）功能方面，防火墙能够针对 TCP 层进行有效的通信访问控制，对 ModbusTcp、Profinet、DNP3.0、EtherCAT 和 OPC 协议数据进行深度包过滤；可基于白名单的 MAC 地址、IP 地址、端口匹配访问控制策略，支持 SYSLOG 和告警，可根据控制协议中命令字段或功能码字段的匹配策略，可对 SYS FLOOD/UDP FLOOD/PING OF DEATH 等攻击进行防护，保障了工控系统中通信过程的安全性和可靠性。

2）性能方面，该防火墙设备的最大包吞吐量能够满足工业控制系统通信的要求，支持 IPv4/IPv6 协议。

综合以上测试结果，电站控制系统信息安全防护模块满足相关国家标准和项目设计要求。

主测人（Compiler）：宋海松 日期（Date）：2017.7.7

审核人（Inspector）：张明辉 日期（Date）：2017.7.10

批准人（Approver）：[illegible] 日期（Date）：2017.7.12

批准人职务（Position of approver）：四川省信息安全测评中心授权签字人

（中心签章 Stamp）

1 前言

1.1 测评目的

工业控制系统（ICS）是电力、石油石化、核能等能源行业，航空、铁路、公路等交通行业，水处理、地铁等城市公用设施行业等国家关键基础设施的“大脑”和“中枢神经”，超过 80%的关键基础设施依靠工业控制系统来实现自动化作业。随着信息技术的发展，现代控制系统正逐渐使用通用的 TCP/IP 标准协议、通用的操作系统等，以及同业务系统等其他信息系统的连接也越来越多。

本报告主要测试电站控制系统信息安全防护模块在正常工作环境下的实际吞吐量（Throughput）和响应时间（Response Time），了解防火墙的通信协议访问控制功能和网络性能。

1.2 测试依据

- GB/T 20281-2015 《信息安全技术 防火墙安全技术要求和测试评价方法》
- 《电站控制系统信息安全防护模块需求分析说明书》

2 测评环境

2.1 测评对象描述

电站控制系统的信息安全防护模块通过对工业控制系统信息安全攻击、控制系统终端安全防护、控制系统信息安全功能设计、控制系统信息安全防护、控制系统认证授权等多层次多维度的深入研究，解决当前电站控制系统难以抵御信息安全渗透和攻击的问题。本报告主要针对电站控制系统的信息安全防护模块在半实物仿真环境下进行测试。

2.2 测试设备和工具

表1 测评设备及工具

设备和工具名称	数量
台式机	2台
工业防火墙硬件设备	1台
吞吐量测试软件：IxChariot	1套

2.3 测试方式

本次测试采取在实验室模拟测试。

2.4 测试人员

表2 参评人员

姓名	资质/职称	项目职务	项目分工
王丹琛	高级测评师	组长	规范审查，总体把握、质量把控
宋海权	高级测评师	组员	实验环境测试

姓名	资质/职称	项目职务	项目分工
刘勃	高级测评师	组员	实验环境测试
张玥靓	国家注册信息安全人员	组员	测试结果记录、文审

2.5 测评内容

根据客户提出的测试需求，对“电站控制系统信息安全防护模块”进行以下参数的测评。

类别	序号	测 评 项
性能测试	1	64 字节吞吐量
	2	64 字节响应时间
	3	128 字节吞吐量
	4	128 字节响应时间
	5	256 字节吞吐量
	6	256 字节响应时间
	7	512 字节吞吐量
	8	512 字节响应时间
	9	1024 字节吞吐量
	10	1024 字节响应时间
	11	1280 字节吞吐量
	12	1280 字节响应时间
	13	1516 字节吞吐量
	14	1516 字节响应时间
功能测试	15	modbusTcp 深度包检测
	16	OPC 深度包检测功能
	17	抗 SYS FLOOD/UDP FLOOD/PING OF DEATH 攻击测试

类别	序号	测 评 项
	18	DNP3.0 深度包检测功能测试
	19	Profinet 深度包检测
	20	EtherCAT 深度包检测
	21	Tcp/IP 深度包检测
	22	基于白名单的 MAC/IP 地址和端口匹配访问控制策略
	23	SYSLOG 日志记录和告警功能

3 测试结果

3.1 性能测试

序号	测评项	方法	测评结果	结论
1	64 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：64Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):70.942 Mbps(min):63.022 Mbps(max):75.202	满足设计要求
2	64 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：64Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):0.089 Transaction Rate(min):0.079 Transaction Rate(max):0.094	满足设计要求
3	128 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：64Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):142.995 Mbps(min):131.666 Mbps(max):146.145	满足设计要求
4	128 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：64Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):5.593 Transaction Rate(min):5.474 Transaction Rate(max):6.076	满足设计要求

序号	测评项	方法	测评结果	结论
5	256 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：256Byte； （3）发送数据总量：10000000Byt。	Mbps(avg):194.438 Mbps(min):175.246 Mbps(max):206.932	满足设计要求
6	256 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：256Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):4.114 Transaction Rate(min):3.866 Transaction Rate(max):4.565	满足设计要求
7	512 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：512Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):393.512 Mbps(min):378.430 Mbps(max):402.617	满足设计要求
8	512 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：512Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):2.033 Transaction Rate(min):1.987 Transaction Rate(max):2.114	满足设计要求
9	1024 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1024Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):594.006 Mbps(min):552.486 Mbps(max):623.539	满足设计要求
10	1024 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1024Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):1.346 Transaction Rate(min):1.283 Transaction Rate(max):1.448	满足设计要求
11	1280 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1280Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):736.292 Mbps(min):689.061 Mbps(max):800.000	满足设计要求

序号	测评项	方法	测评结果	结论
12	1280 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1280Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):1.086 Transaction Rate(min):1.000 Transaction Rate(max):1.161	满足设计要求
13	1516 字节吞吐量测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1516Byte； （3）发送数据总量：10000000Byte。	Mbps(avg):706.651 Mbps(min):509.879 Mbps(max):794.439	满足设计要求
14	1516 字节响应时间测试	（1）测试数据类型：基于 TCP 层之上的随机数据； （2）数据包大小：1516Byte； （3）发送数据总量：10000000Byte。	Transaction Rate(avg):1.132 Transaction Rate(min):1.007 Transaction Rate(max):1.569	满足设计要求

3.2 功能测试

序号	测评项	方法	结论
1	modbusTcp 深度包检测	1）构建测试环境； 2）通过分别在模拟攻击端和模拟控制端分别安装 ModbusTcp 客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。	通过
2	OPC 深度包检测	1）构建测试环境； 2）白名单测试； 3）过滤 opnum； 4）过滤 opnum 和 ctx_id。	通过
3	DNP3.0 深度包检测	1）构建测试环境； 2）测试通过分别在模拟攻击端和模拟控制端分别安装 DNP3.0 客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。	通过

序号	测评项	方法	结论
4	Profinet 深度包检测	1）构建测试环境； 2）测试通过分别在模拟攻击端和模拟控制端分别安装 Profinet 客户端软件与服务器软件建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。	通过
5	EtherCAT 深度包检测	1）构建测试环境； 2）测试通过分别在模拟攻击端和模拟控制端分别安装 EtherCAT 客户端软件 SOEM 与服务器软件 SOES 建立通信过程，客户端发送数据包通过工业控制防护系统到服务器端来进行验证。	通过
6	Tcp/IP 深度包检测	1）测试环境搭建； 2)通过发送 TCP/IP 数据包来观察防护模块对于数据包检测与防护能力。	通过
7	SYSLOG 日志记录和告警功能	1）测试环境搭建； 2）模拟一个简单的工业控制环境，通过 PC 机、TCP&UDP 测试软件以及防火墙配置管理软件等，来模拟工业控制网络中的数据通信，测试防火墙的 syslog 日志记录功能和告警。	通过
8	基于白名单的 MAC/IP 地址和端口匹配访问控制策略	1）测试环境搭建； 2）模拟一个简单的工业控制环境，通过 PC 机、TCP&UDP 测试软件以及 modbus poll/slave 软件等，来模拟工业控制网络中的数据通信，并使用 hping 软件实现 syn flood 攻击。	通过
9	抗 SYS FLOOD /UDPFLOOD /PING OF DEATH 攻击	1）构建测试环境； 2）配置攻击电脑和被攻击电脑、配置防火墙。	通过

4 结论及意见

四川省信息安全测评中心受电子科技大学委托，于2017年6月10日-2017年7月10日，对“电站控制系统信息安全防护模块”，依据国家标准进行安全测试。

通过测试表明：

1）性能方面，该防护设备的最大包吞吐量能够满足工业控制系统通信的要求，支持IPv4/IPv6协议。

2）功能方面，防火墙能够针对TCP层进行有效的通信访问控制，对ModbusTcp、Profinet、DNP3.0、EtherCAT和OPC协议数据进行深度包过滤；可基于白名单的MAC地址、IP地址、端口匹配访问控制策略，支持SYSLOG和告警，可根据控制协议中命令字段或功能码字段的匹配策略，可对SYS FLOOD/UDP FLOOD/PING OF DEATH等攻击进行防护，保障了工控系统中通信过程的安全性和可靠性。综合测试记录，以上测评的性能指标及防火墙功能基本上达到项目设计要求。

5 注意事项

- 本报告正文页码编号从第三页开始。
- 本报告未加盖“四川省信息安全测评中心”公章无效。
- 本报告仅对本次被测评对象有效。
- 本报告共印三份，客户执第一、二份，本中心保存第三份。
- 未经本中心书面批准，不得部分复印报告。