简网科技
EASYNETWORKS

铸造网络的安全防线

针对工业网络的攻击有泛滥化的趋势

2017年影响 工控信息安全 事件最集中爆发的年头之一。安全研究员发现并上报了数百个新漏洞，警告称工控系统和工艺流程中存在新威胁向量，提供了工业系统突发感染数据，并发现了定向攻击（例如， Shamoon 2.0 / StoneDrill）。自从震网（Stuxnet）病毒曝光以来，研究员首次发现了恶意工具包 CrashOverride / Industroyer ，即一种用于攻击物理系统的网络工具。

然而，2017年工业系统遭遇的最严重威胁是加密勒索软件攻击。卡巴斯基实验室发布的ICS CERT（工业控制系统网络应急小组）报告指出，专家上半年发现了33个恶意软件家族的加密勒索软件，虽然全球63个国家的大量攻击被拦截，但是WannaCry 和 ExPetr 毁灭性勒索软件攻击似乎使工业企业对关键生产系统防护的态度开始发生转变。

智造加速了工业网络的开放

简网科技 EASYNETWORKS

《中国制造2025》正式发布后，工业领域设备联网实现智能化将成为必然。随着两化深度融合战略的持续推进，以及物联网等新兴技术在工业领域的应用，智能制造系统安全也倍受企业关注。

智能制造与网络技术的发展密切相关，需要将传统的过程控制网络、企业的内部网络以及工业物联网的数据实时采集、上传，形成工业互联网。这就导致工控系统从传统封闭式系统演变到开放式网络系统，从信息孤岛演变到过程控制和企业信息系统的集成。而在这一转变中，信息安全问题就凸显出来。

2017年国家在原有的《工业控制系统信息安全事件应急管理工作指南》、《工业控制系统信息安全防护能力评估工作管理办法》、《工业控制系统信息安全行动计划（2018-2020年）》等文件

工控防火墙

信息化固有的安全问题，随着“两化融合”，扩展到社会的基石——工业

DCS、SCADA等生产控制系统逐渐与互联网或办公网直接或间接地互联互通，这给黑客透过互联网破坏石油、石化生产装置提供了可能的机会。

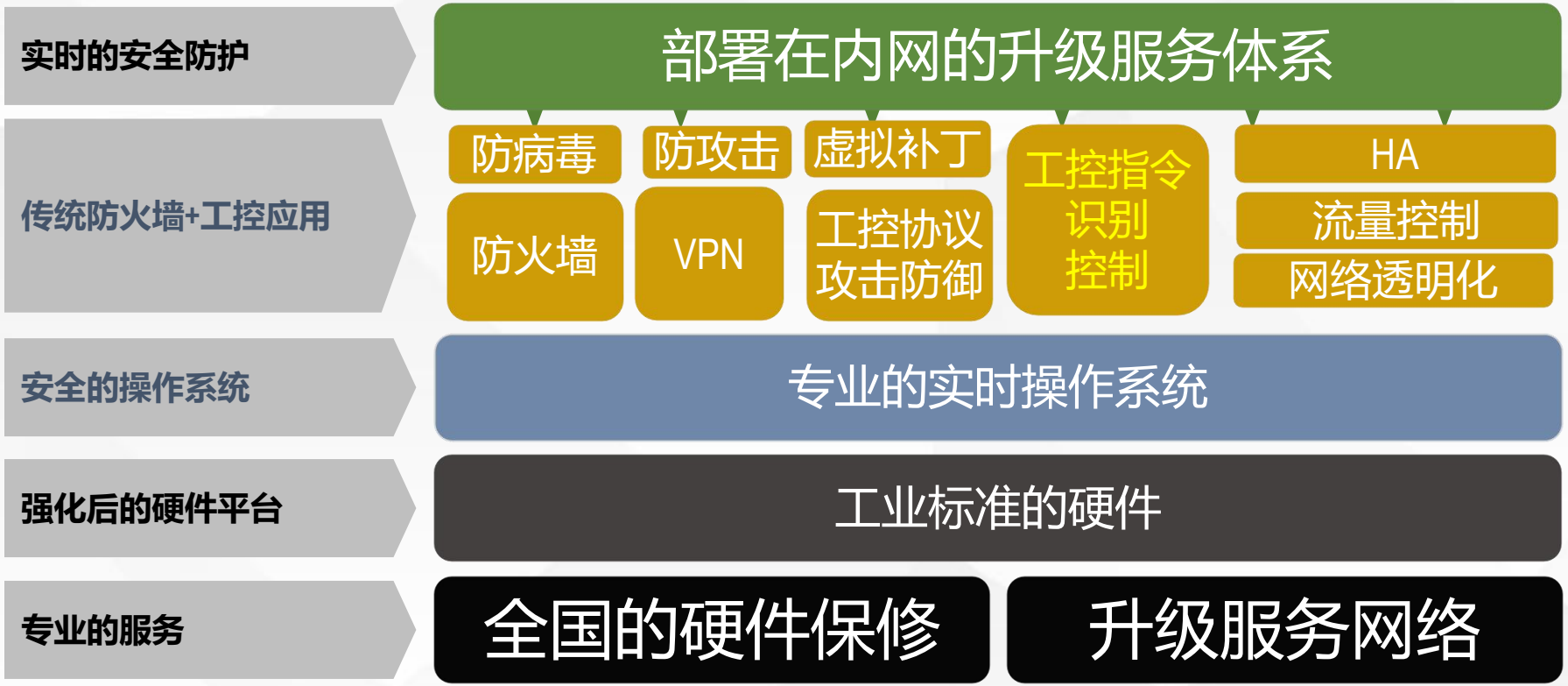
有关安全专家已经开始预警，未来恐怖分子和其他犯罪分子会利用新发现的软件安全漏洞对联合站、输油管道、电站等基础设施进行大规模攻击。而DCS、SCADA等自动控制系统正是他们所要攻击的目标。

工控防火墙具备双重身份

工控防火墙应具有双重身份，即支持传统防火墙所具备的功能，比如防火墙、防病毒、入侵检测与防护(IPS)、流量控制(QoS)、路由/NAT/透明模式等，同时也支持对工控协议的分析与攻击防护。

我们优势——先进的工控网络安全架构

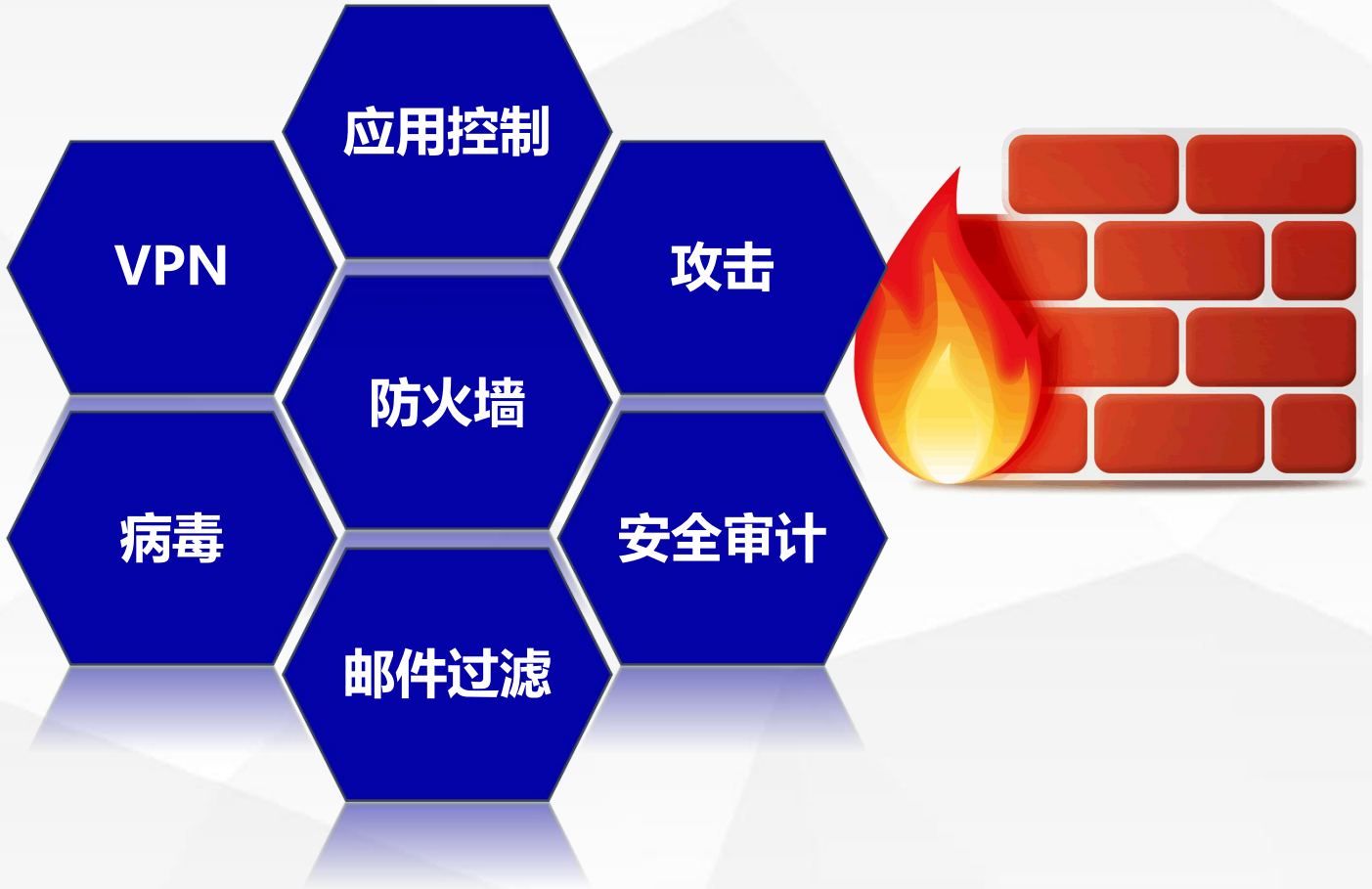
简网科技 EASYNETWORKS



- 专业化设计，工控和数据网的双重身份
- 深度防御，部署灵活

传统网络安全功能

- 高性能防火墙技术
- 高效率VPN技术
- 病毒检测
- IPS技术
- Web过滤
- 邮件过滤
- 应用控制
- 安全审计



工控防火墙技术特点

简网科技 EASYNETWORKS

- 支持的工控协议的自学习

DNP3 Modbus ast OPC RSSP IEC104

- 可设置黑名单和白名单

可以区分读写操作，黑白名单只针对写操作

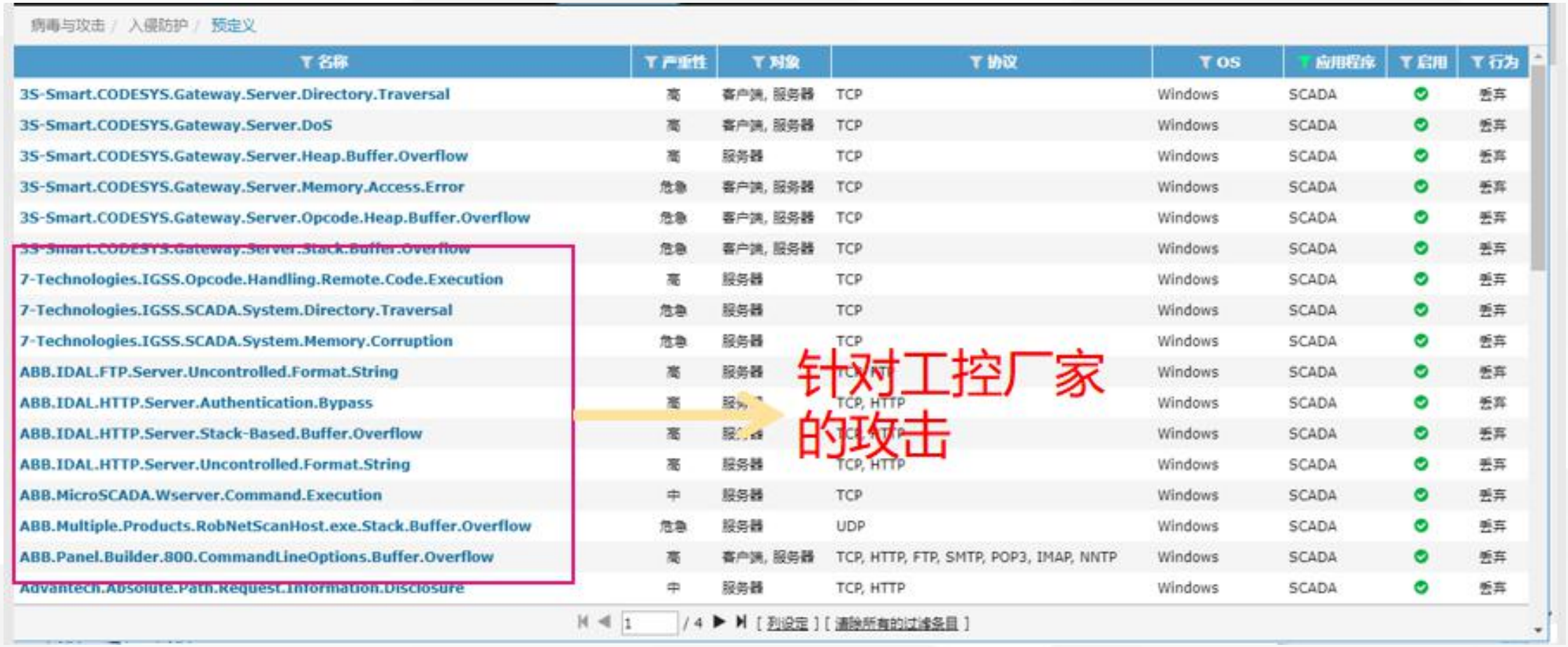
- 监控协议动作和参数

读、写、回滚、寄存器

- 防御协议攻击

一百多种攻击，涵盖了几十厂家

工控协议防御攻击



名称	严重性	对象	协议	OS	应用程序	启用	行为
3S-Smart.CODESYS.Gateway.Server.Directory.Traversal	高	客户端, 服务器	TCP	Windows	SCADA	✓	丢弃
3S-Smart.CODESYS.Gateway.Server.DoS	高	客户端, 服务器	TCP	Windows	SCADA	✓	丢弃
3S-Smart.CODESYS.Gateway.Server.Heap.Buffer.Overflow	高	服务器	TCP	Windows	SCADA	✓	丢弃
3S-Smart.CODESYS.Gateway.Server.Memory.Access.Error	危急	客户端, 服务器	TCP	Windows	SCADA	✓	丢弃
3S-Smart.CODESYS.Gateway.Server.Opcode.Heap.Buffer.Overflow	危急	客户端, 服务器	TCP	Windows	SCADA	✓	丢弃
3S-Smart.CODESYS.Gateway.Server.Stack.Buffer.Overflow	危急	客户端, 服务器	TCP	Windows	SCADA	✓	丢弃
7-Technologies.IGSS.Opcode.Handling.Remote.Code.Execution	高	服务器	TCP	Windows	SCADA	✓	丢弃
7-Technologies.IGSS.SCADA.System.Directory.Traversal	危急	服务器	TCP	Windows	SCADA	✓	丢弃
7-Technologies.IGSS.SCADA.System.Memory.Corruption	危急	服务器	TCP	Windows	SCADA	✓	丢弃
ABB.IDAL.FTP.Server.Uncontrolled.Format.String	高	服务器	TCP, FTP	Windows	SCADA	✓	丢弃
ABB.IDAL.HTTP.Server.Authentication.Bypass	高	服务器	TCP, HTTP	Windows	SCADA	✓	丢弃
ABB.IDAL.HTTP.Server.Stack-Based.Buffer.Overflow	高	服务器	TCP, HTTP	Windows	SCADA	✓	丢弃
ABB.IDAL.HTTP.Server.Uncontrolled.Format.String	高	服务器	TCP, HTTP	Windows	SCADA	✓	丢弃
ABB.MicroSCADA.Wserver.Command.Execution	中	服务器	TCP	Windows	SCADA	✓	丢弃
ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow	危急	服务器	UDP	Windows	SCADA	✓	丢弃
ABB.Panel.Builder.800.CommandLineOptions.Buffer.Overflow	高	客户端, 服务器	TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP	Windows	SCADA	✓	丢弃
Advantech.Absolute.Path.Request.Information.Disclosure	中	服务器	TCP, HTTP	Windows	SCADA	✓	丢弃

1 / 4 [列设定] [清除所有的过滤条目]

工控协议防御攻击

名称	严重性	对象	协议	OS	应用程序	启用	行为
Mitsubishi.MX.ActiveX.ActUWzd.dll.Remote.Code.Execution	高	客户端	TCP, HTTP	Windows, MacOS	SCADA	✓	丢弃
Modbus.TCP.Clear.Counters.Diagnostic.Registers	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Force.Listen.Only	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Function.Code.Scan	信息	客户端	TCP	Other	SCADA	✗	通过
Modbus.TCP.Invalid.Packet.Length	信息	客户端, 服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Points.List.Scan	信息	客户端	TCP	Other	SCADA	✗	通过
Modbus.TCP.Read.Device.ID	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Report.Server.Info	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Restart.Communications.Option	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Unauthorized.Read.Request.PLC	信息	服务器	TCP	Other	SCADA	✗	通过
Modbus.TCP.Write.Request.PLC	信息	服务器	TCP	Other	SCADA	✗	通过
Moxa.AWK-313A.Login.Username.Param.OS.Command.Injection	危急	服务器	TCP, TELNET	Linux	SCADA	✓	丢弃
Moxa.MediaDBPlayback.ActiveX.Control.Buffer.Overflow	高	客户端	TCP, HTTP	Windows	SCADA	✓	丢弃
Moxa.MXView.Private.Key.Information.Disclosure	高	服务器	TCP, HTTP	Windows	SCADA	✓	丢弃
MySCADA.myPRO7.FTP.Hardcoded.Account.Access	危急	服务器	TCP	Other	SCADA	✓	丢弃
OMRON.CX-One.CX-FLnet.Node.Name.Heap-based.Buffer.Overflow	高	客户端, 服务器	TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP	Windows	SCADA	✓	丢弃
OMRON.CX-One.CX-Position.cdmapi32.Stack.Buffer.Overflow	高	客户端, 服务器	TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP	Windows	SCADA	✓	丢弃

◀ 3 / 4 ▶ [列设定] [清除所有的过滤条目]

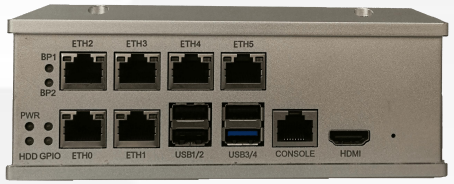
防御攻击案例

我们在中石化油库系统中，多次发现和阻断针对PLC的溢出攻击

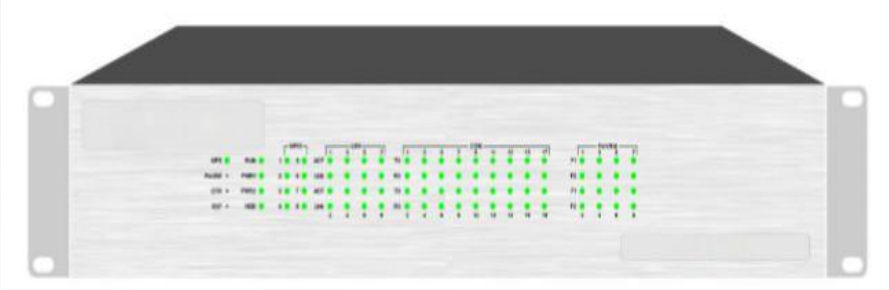
#	Date	Time	级别	子类型	日志ID	源	目的	参考	消息
1	2017-07-11	20:10:10	告警	特征	16384	10.74.49.202	10.183.200.227	43750	SCADA: VIPA.Controls.WinPLC7.Stack.Buffer.Overflow
2	2017-07-11	20:09:47	告警	特征	16384	10.74.49.202	10.183.200.227	43750	SCADA: VIPA.Controls.WinPLC7.Stack.Buffer.Overflow
3	2017-07-11	20:09:24	告警	特征	16384	10.74.49.202	10.183.200.227	43750	SCADA: VIPA.Controls.WinPLC7.Stack.Buffer.Overflow
4	2017-07-11	20:09:02	告警	特征	16384	10.74.49.202	10.183.200.227	43750	SCADA: VIPA.Controls.WinPLC7.Stack.Buffer.Overflow
5	2017-07-11	10:59:37	告警	特征	16384	10.74.50.3	60.28.208.144	38738	针对OpenSSL信息披露漏洞的攻击尝试
6	2017-07-10	15:16:57	告警	特征	16384	10.74.48.246	218.205.68.247	38738	针对OpenSSL信息披露漏洞的攻击尝试
7	2017-07-08	10:53:23	告警	特征	16384	10.74.52.165	10.246.137.243	15621	企图利用通过HTTP请求一个SQL注入漏洞
8	2017-07-07	15:17:34	告警	特征	16384	10.74.50.3	14.17.43.114	38738	针对OpenSSL信息披露漏洞的攻击尝试
9	2017-07-07	13:22:40	告警	特征	16384	10.183.48.249	10.183.101.18	17397	攻击企图对ezip向导一个缓冲区溢出漏洞
10	2017-07-06	09:12:57	告警	特征	16384	10.183.200.174	10.74.49.163	107347976	Apache HTTP服务器是一个开源的可用的Web服务器建立一个安全的现代Web服务器，同时兼容UNIX和Windows操作系统

工控产品

- 导轨式

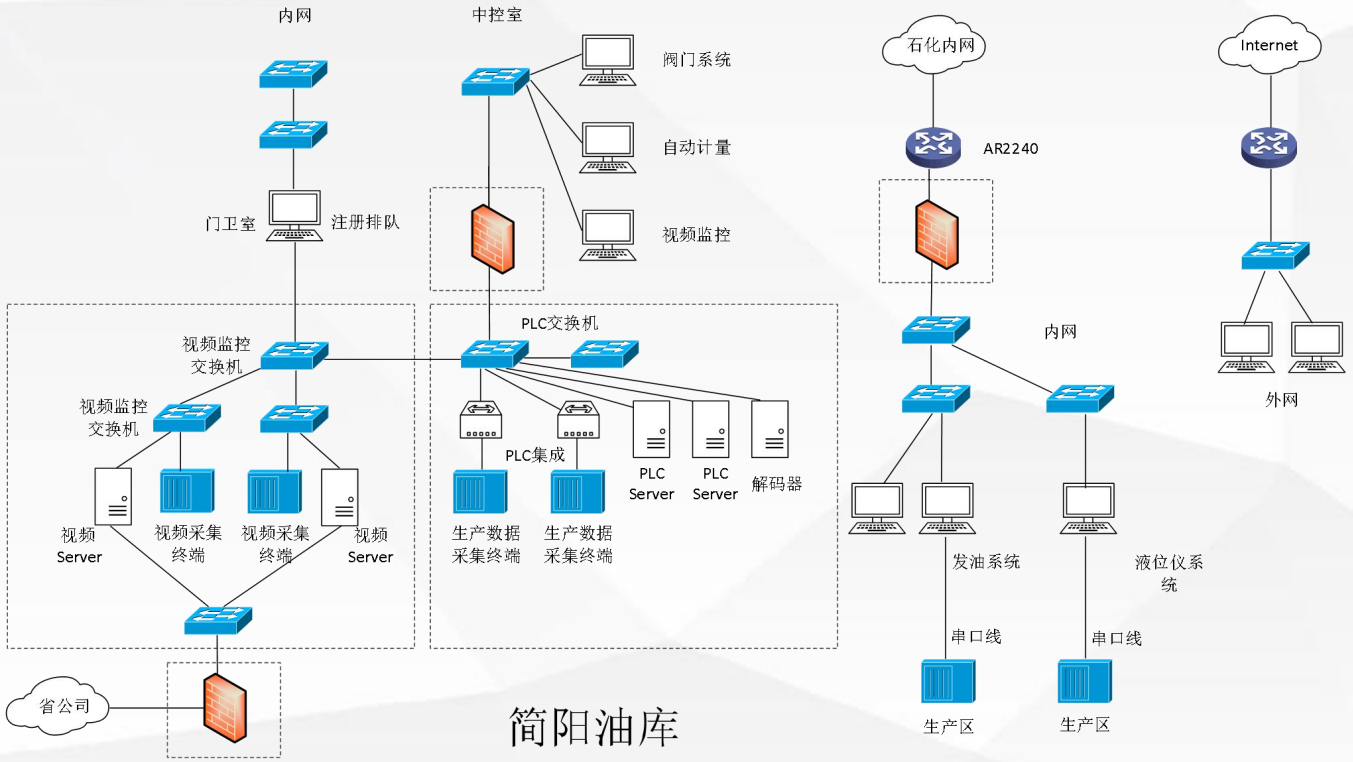

ETH2
ETH3
ETH4
ETH5
BP1
BP2
PWR
HDD GPIO
ETH0
ETH1
USB1/2
USB3/4
CONSOLE
HDMI

- 机架式



案例 | 中石化油库安全体系

某典型油库的拓扑如下，在工控网络边界部署安全防御体系



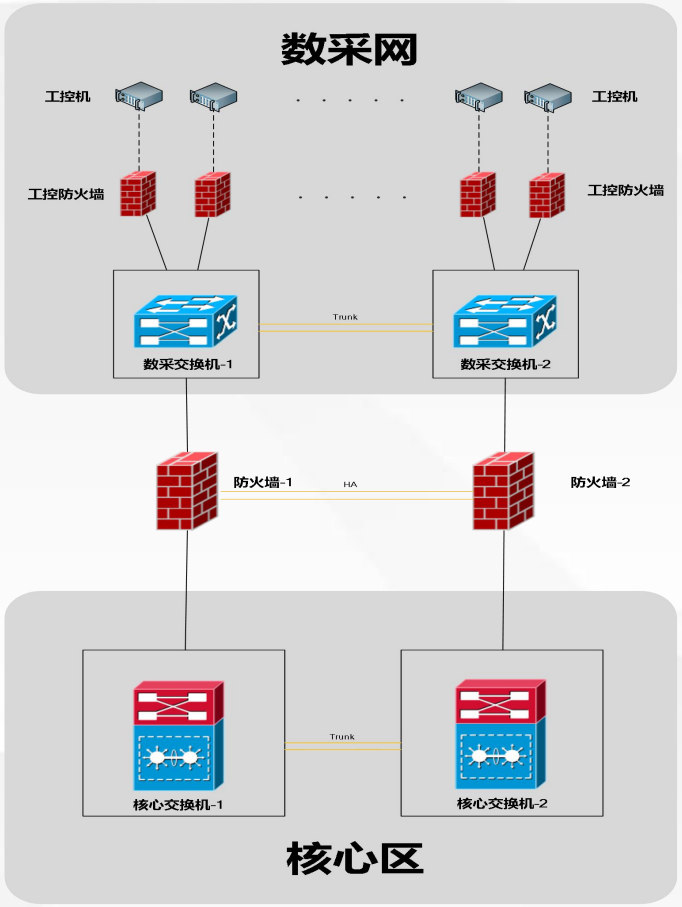
简阳油库

- 部署位置：
  - 在工控网与办公网互联点
  - 在工控网上联省公司节点
  - 在工控网与控制室边界
- 部署模式：
  - 支持bypass的透明模式。
- 部署地点：
  - 中石化四川销售公司
  - 中石化河南销售公司
  - 中石化浙江销售公司
  - 中石化吉林销售公司
  - 中石化辽宁销售公司
  - 中石化内蒙古销售公司
  - 中石化云南销售公司
  - 中石化江苏销售公司
  - 中石化福建森美

案例 | 广石化数采网边界安全

简网科技 EASYNETWORKS

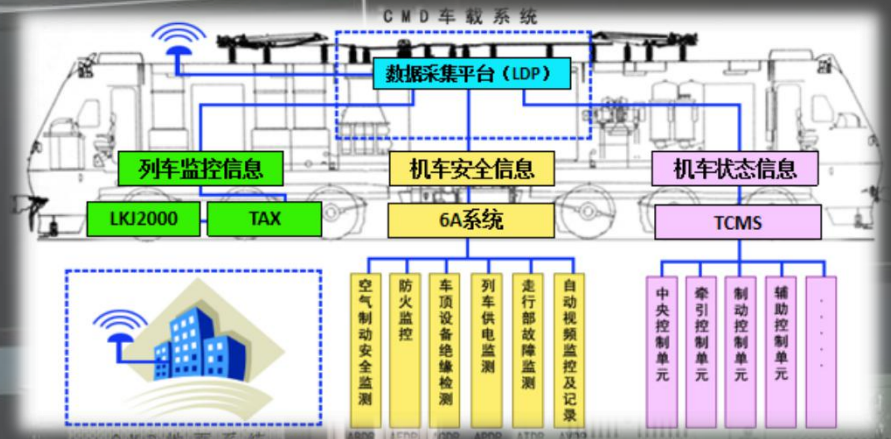
广石化的工控网边界和内部部署我们的安全设备实现数采网的安全



序号	名称	型号	机柜位置	序列号	质保开始时间	质保结束时间
1	厂外业务区防火墙-1	KFW-3800	1-8柜	APW2KMA0A1000017	2018.4.15	2021.4.15
2	厂外业务区防火墙-2	KFW-3800	1-9柜	APW2KMA0A1000019	2018.4.15	2021.4.15
3	无线接入区防火墙-1	KFW-3800	1-6柜	APW2KMA0A1000024	2018.4.15	2021.4.15
4	无线接入区防火墙-2	KFW-3800	1-7柜	APW2KMA0A1000027	2018.4.15	2021.4.15
5	集团网防火墙-1	KFW-3800	1-2柜	APW2KMA0A1000018	2018.4.15	2021.4.15
6	集团网防火墙-2	KFW-3800	1-2柜	APW2KMA0A1000048	2018.4.15	2021.4.15
7	DMZ区防火墙	KFW-3800	2-4柜	APW2KMA0A1000023	2018.4.15	2021.4.15
8	集中管理	Kcentre-3000	2-3柜	APW1KSC001000136	2018.4.15	2021.4.15
9	日志审计	Klog-3000	2-3柜	APW1KSC001000126	2018.4.15	2021.4.15
10	厂内业务区防火墙-1	KFW-3800	1-3柜	APW2KMA0A1000026	2018.4.15	2021.4.15
11	厂内业务区防火墙-2	KFW-3800	1-3柜	APW2KMA0A1000021	2018.4.15	2021.4.15
12	数采区防火墙-1	KFW-3800	1-4柜	APW2KMA0A1000016	2018.4.15	2021.4.15
13	数采区防火墙-2	KFW-3800	1-4柜	APW2KMA0A1000022	2018.4.15	2021.4.15
14	改制单位防火墙	KFW-3800	1-3柜	APW2KMA0A1000025	2018.4.15	2021.4.15

案例 | 高铁机车定制版

部署高铁机车上，用于高铁机车控制系统和6A系统的安全防御和安全审计



强大的合作伙伴

简网科技 EASYNETWORKS

铁科院 CARS 中国铁道科学研究院集团有限公司 CHINA ACADEMY OF RAILWAY SCIENCES CORPORATION LIMITED

与铁科院合作推进高铁的安全建设，目前京张高铁作为样本工程

HollySys

与和利时合作推进铁路信号安全体系建设

CIC 国家工业信息安全发展研究中心 CHINA INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

与工信部一所推进工控安全标准建设

简网科技
EASYNETWORKS

THANK YOU

北京简网科技有限公司