NSFOCUS

绿盟工控漏洞扫描系统

产品白皮书

目录

一. 概述

实现以“数字化、智能化、网络化”为特点的工业信息化建设已经成为我国两化融合的重要目标，党的十八大提出要“坚持走中国特色新型工业化、信息化、城镇化、农业现代化道路”。相比西方发达国家因为历史原因形成的“先工业化再信息化”的发展路径(比如德国政府在 2013 年提出的“工业 4.0”国家战略)，我国成功抓住了新一轮全球科技革命和产业变革机遇，实现了工业化和信息化同步发展。

而工业控制系统在工业信息化中有着举足轻重的位置，其广泛应用于工业、电力、能源、交通运输、水利、公用事业和生产企业，被控对象的范围包括生产过程、机械装置、交通工具、实验装置、仪器仪表、家庭生活设施、家用电器等。它通过对工作过程进行自动化监测、指挥、控制和调节，保证工业设施的正常运转，是国家关键基础设施和信息系统的重要组成部分。

同时，正因为这些关键基础设施在国计民生中的重要性，也往往成为国际敌对势力、敌对组织、黑客的攻击目标。ICS-CERT 公布数据中，2013 年全年的工控安全事件达 632 件，其中多集中能源行业（59%）和关键制造业（20%），工控安全事件呈快速增长的趋势(如图 1-1 所示)。

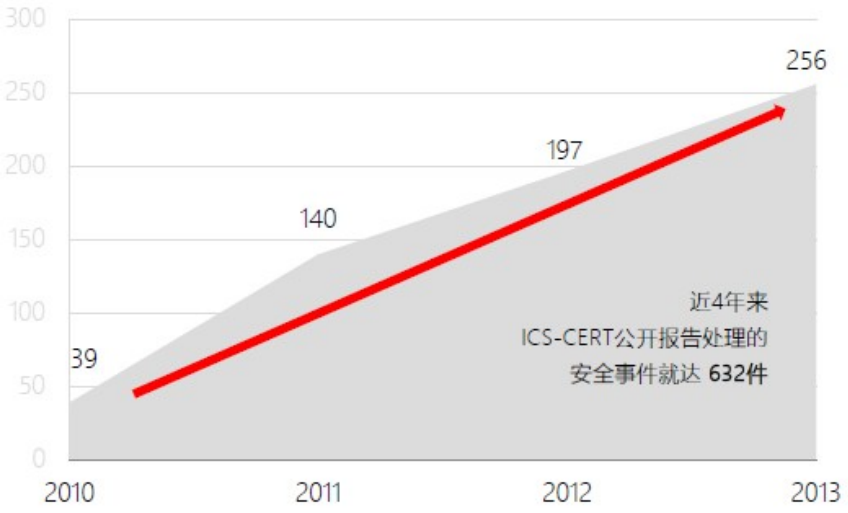

图 1-1 ICS-CERT 历年的公布工控安全事件统计分析

其中：

① 代表性的伊朗布什尔核电站震网病毒事件

自从 2010 年震网病毒、Flame、Duqu7 事件的爆发，因其危害的规模、发起者的属性(国家级别)、操作的复杂性，震惊了全世界，也极大促使了各国政府对工控安全的重视。

② 专门针对工控系统的新型攻击—Havex

2014 年又出现了继震网病毒以后的超级病毒，专门针对工控系统的新型攻击—Havex ，其变种多(F-Secure 声称他们已收集和分析了 Havex RAT 的 88 个变种)、危害大（Havex 可感染 SCADA 和工控系统中使用的工业控制软件，这种木马可能有能力禁用水电大坝、使核电站过载，甚至可以做到按一下键盘就能关闭一个国家的电网）、范围广(ICS-CERT 的安全通告称当前至少已发现 3 个著名的工业控制系统提供商的 Web 网站已受到该恶意代码的感染)。

③ 持续威胁的黑客组织—“蜻蜓组织”

在 2014 年 1 月，网络安全公司 CrowdStrike 曾披露了一项被称为“Energetic Bear”的网络间谍活动，在这项活动中黑客们可能试图渗透欧洲、美国和亚洲能源公司的计算机网络。根据赛门铁克的研究报告称，黑客组织 Energetic Bear 也被称为“蜻蜓 Dragonfly”，这是一个至少自 2011 年起便开始活跃的东欧黑客团体。蜻蜓组织最初的攻击目标是美国和加拿大的国防和航空企业，但从 2013 年开始，蜻蜓组织的主要目标转向许多国家的石油管道运营商、发电企业和其他能源工控设备提供商，即以那些使用工控系统来管理电、水、油、气和数据系统的机构为新的攻击目标。

总的来说，面对攻击技术与手段日益先进、复杂、成熟的针对工控系统进行攻击的行为，工控系统所面临的安全威胁也将日益严峻。

而通过对这些众多的工控安全事件深入分析可以看到，其有一个核心的关键环节就是利用了工业控制系统的“漏洞”，进而攻陷了整个工业控制系统。而工业控制系统公开的漏洞也是呈现出快速增长的趋势(如图 1-2 所示)。

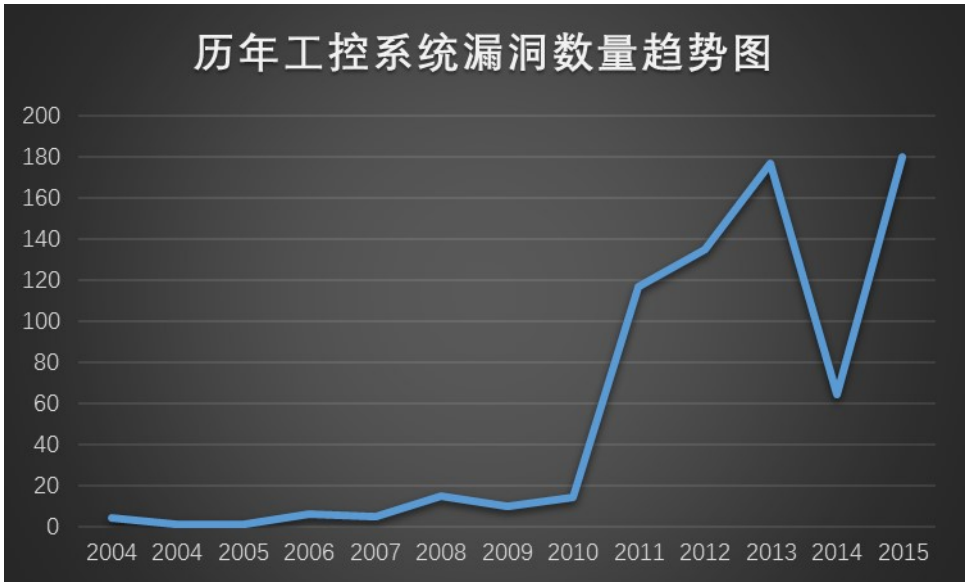

图 1-2 公开的 ICS 漏洞的年度变化趋势

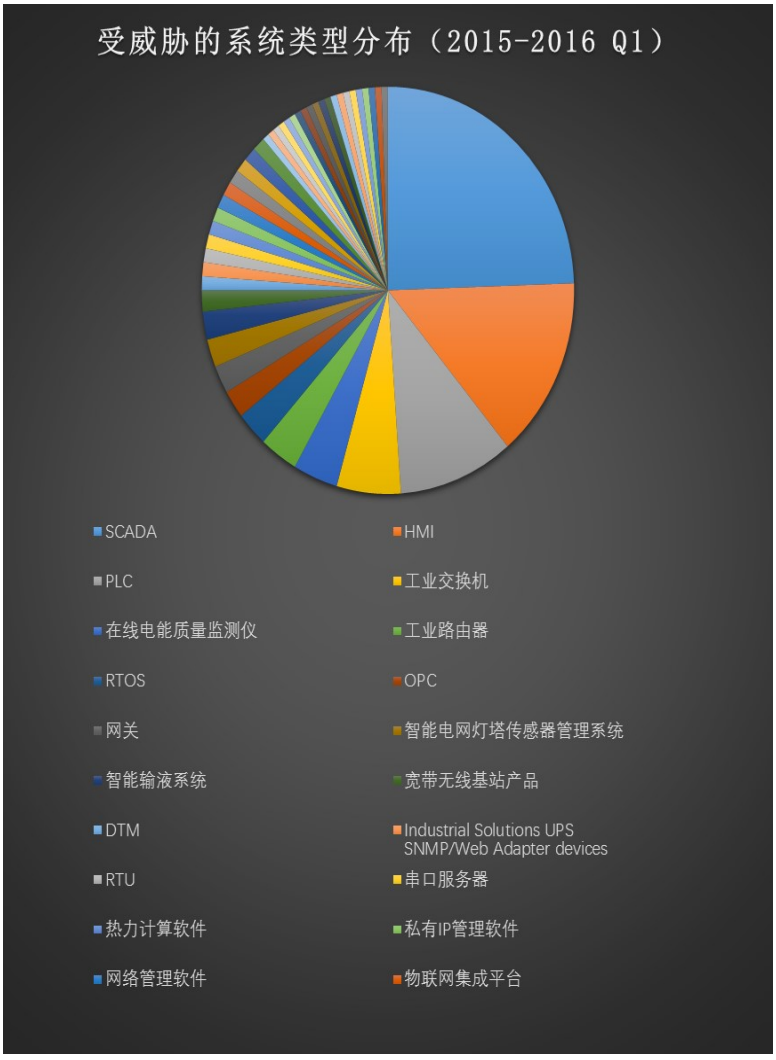

图 1-3 受威胁的系统类型分布

其中：

① 公开漏洞中以 SCADA/HMI 系统相关的漏洞为主，其占比超过 40%

② 公开漏洞所涉及的工业控制系统厂商仍然是以国际著名的工业控制系统厂商为主，西门子（Siemens）、施耐德电气（Schneider）、研华科技（Advantech）、摩莎（MOXA）、通用电气（GE）与罗克韦尔（Rockwell）占据漏洞数排行榜的前几名

因此，如何在黑客成功攻击工业控制系统之前帮助企业发现漏洞，进而促使其完善系统，成为保障工业控制系统安全运行、增强企业安全健壮性的必要手段。

二. 工控安全评估面临的挑战

2.1 工业控制系统面临更加苛刻的安全性要求

在工业控制系统中，无论是一次系统还是二次系统，以及间隔层还是过程层，业务的连续性、健康性是至关重要的，尤其对石化、电力、交通、核工业、水利等行业的核心监控、生产系统。而工业控制系统由于其长期封闭、独立的特性，造成了在安全方面建设的欠缺，不具备更多的容错处理，比如异常指令的处理，不具备较大压力的处理，比如快速数据传输、访问等。工业控制系统安全性相比 IT 环境的一些主要区别包括：

① 工业控制系统安全问题将直接对物理环境造成影响，有可能导致人员伤亡，环境破坏和大规模关键业务中断等

② 工业控制系统安全相比 IT 安全有更广泛的威胁向量，包括安全限制和特有网络协议的支持

③ 工业控制系统安全涉及的系统厂商多，测试和开发环境多种多样

④ 一些工业控制系统安全环境面临预算限制，这是与那些需要严格监管的 IT 不同之处

⑤ 在传统的安全性和可用性作为主要安全特性的 IT 行业，工业控制系统行业还会关注对产品质量的协调影响，运营资产和下游后果的安全问题

2.2 如何把成熟的 IT 风险评估技术移植到工业控制系统环境中

在面对与 IT 系统不一样的安全性要求的工业控制系统时，如果把成熟的 IT 风险评估技术移植到工业控制系统中成为必须解决的问题，主要包括两个方面：

① 如何覆盖多样的工业控制系统

在安全风险评估时，不仅需要对在工业控制系统中使用的传统 IT 设备/系统，比如操作系统、交换机、路由器、弱口令、FTP 服务器、Web 服务器等，进行安全评估，还需要覆盖工业控制系统中所特有的设备/系统，比如 SCADA、DCS、PLC 等，以及处于上游的数字化设

计制造软件等；同时，不仅要包括对漏洞的评估，还需要对一些关键系统的配置进行安全性评估；以及需要对主流的工控协议的支持。

同时，根据 IHS 最近的研究报告“2013 全球工业以太网和现场总线技术”中的调查显示，从 2011 年到 2016 年，虽然新增加网络节点的总数量将会增加超过 30%，但是现场总线和以太网产品的混合产品数量将会基本维持不变，从 23%到 26%仅仅增加 3 个百分点。由于技术更新的成本、难度，老式工业总线很难都替换成支持以太网的新式总线。因此，需要有一种有效地手段，可以对基于老式总线工业控制系统进行漏洞扫描。

② 如何保障业务的连续性和健康性

工业控制系统因为其使用特性，相比传统的 IT 系统，其连续性和健康性要求会更高，尤其像电网、交通、市政等这些行业，工业控制系统的中止或故障将带来非常大的经济、社会影响；同时，有的系统上线后甚至要求几年、十几年不能停止。因此这对这种更加苛刻的要求，需要在安全评估工作中保障业务的连续性和健康性。

三. 绿盟工控漏洞扫描系统

3.1 概述

面对全新的工控安全威胁，主管/监管机构在检查和评估其安全问题，以及企业在安全自查时急需一款专门面向工业控制系统的漏洞扫描工具，为了满足此需求，绿盟科技推出了专门面向工业控制系统的漏洞扫描产品——绿盟工控漏洞扫描系统(NSFOCUS Industrial Control Systems Vulnerability Scanning System，简称 NSFOCUS ICSScan)。

ICSScan 支持对传统 IT 系统的漏洞扫描、配置核查、Web 扫描，包含主流操作系统、应用软件、数据库、网络组件等信息模块漏洞；

ICSScan 支持工业现场资产设备网络拓扑功能，并以资产管理为导向，帮助客户对现场设备进行全局风险管控查看；

ICSScan 支持现场控制器设备信息静态导入扫描风险评估，零风险扫描；

ICSScan 针对工业现场 SCADA 软件、数字化设计制造，各厂商组态软件等上位机软件的漏洞扫描；

ICSScan 支持针对 Schneider、Siemens、AB 等各大主流厂商 DCS、PLC、RTU 等控制器的漏洞扫描；

ICSScan 支持针对主流的工控通讯协议（ModbusTCP、S7、ProfiNet、DNP3.0、IEC-60870-5-104、IEC-61850-MMS）进行 Fuzzing 漏洞挖掘测试，支持对高危拒绝服务漏洞数据包全程回放验证，支持对高危漏洞收藏验证；

ICSScan 漏洞库标识兼容 CVE、CNNVD、CNCD、CVSS 等各大漏洞平台信息；

ICSScan 是国内首款工控系统漏洞扫描器，并入选国外 Gartner 魔力象限，集资产发现、信息收集、漏洞扫描、漏洞挖掘、漏洞回放验证、风险评估、报表展示、漏洞跟踪等完备的漏洞管理能力于一体。

3.2 产品架构

NSFOCUS ICSScan 主要由系统接入层、系统核心层、基础平台层三个部分组成，可以在各种网络环境中进行灵活的部署和管理，如图 3-1：

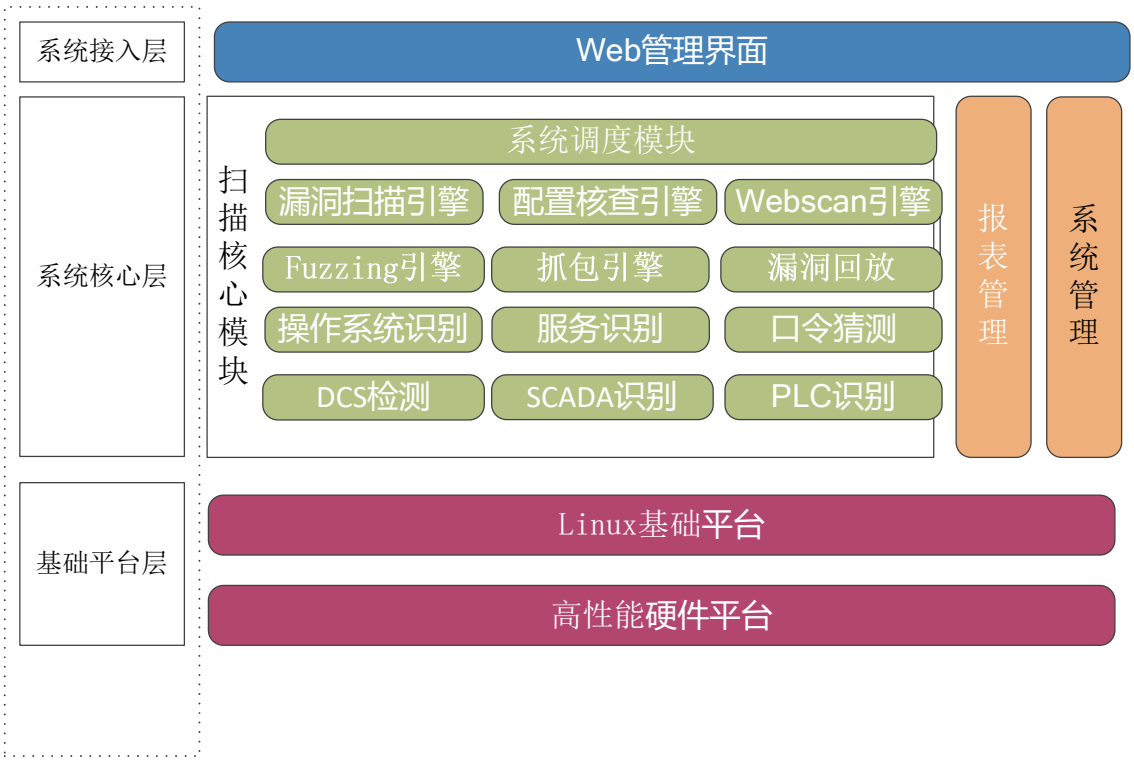

图 3-1 绿盟工控漏洞扫描系统架构图

① 基础平台层

使用专用的硬件平台，提供可靠稳定的硬件环境，辅助以系统运行的必须软件，组成基础平台层，支持传统 IT 网络协议，支持工业网络协议。

② 系统核心层

主要是漏洞扫描引擎，包含传统主机完整扫描过程的一系列核心功能，存活判断，端口扫描，服务识别，OS 判断，口令猜测等；包含 PLC 资产识别，PLC 漏洞扫描；

- 支持传统 IT 主机的配置核查功能；
- 支持 Web 站点的扫描功能；
- 具备完善的报表展示功能，支持 Html、Word、PDF、Excel 等多模式报表输出模块；
- 证书系统辅助控制模块输出，并加入升级系统保证系统的可维护性

③ 系统接入层

- 主要负责系统自身和任务下发的接入管理
- 系统自身提供 Web 和 Consle 两种管理模式，更为完善的进行配置管理；
- 任务下发可从 Web 端以及开发的二次开发接口远程下发

其子系统如下：

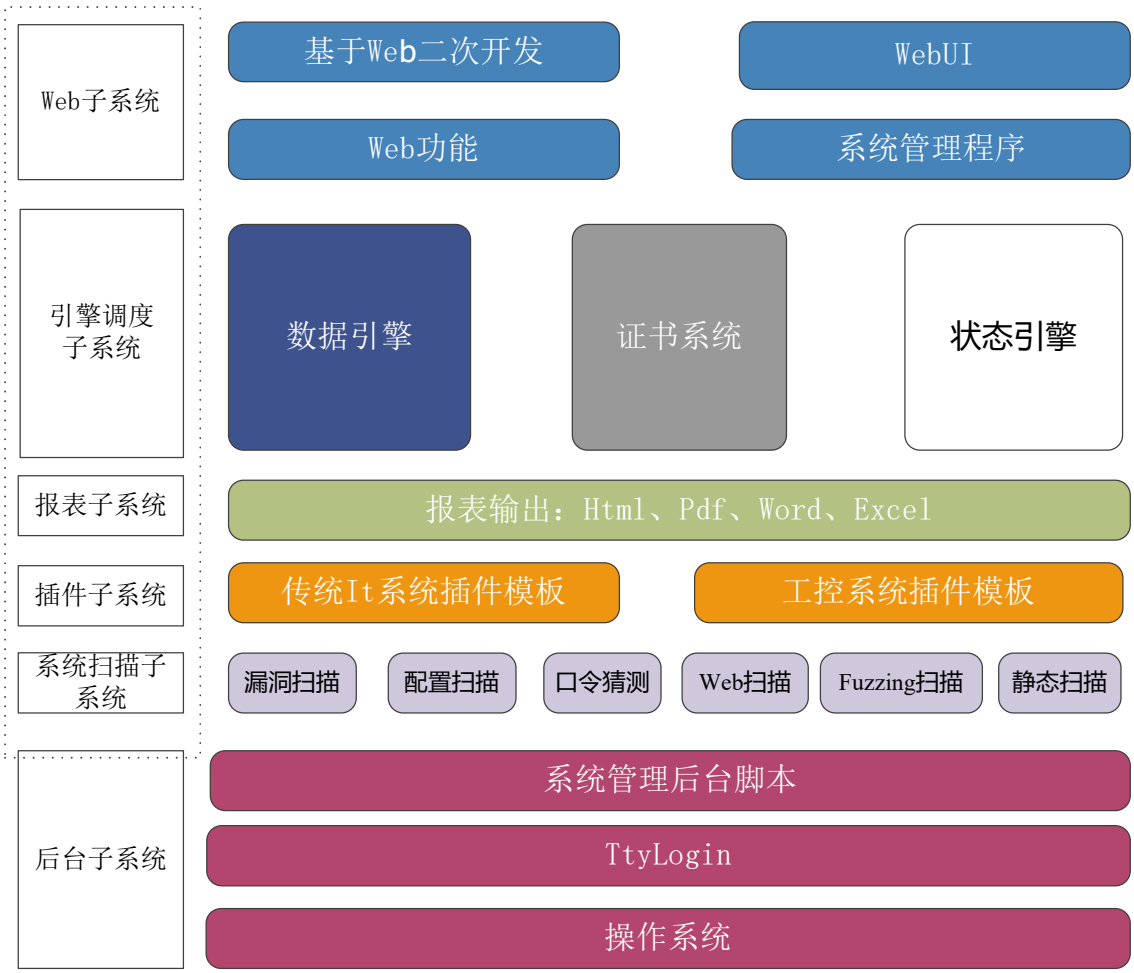

图 3-2 绿盟工控漏洞扫描系统工作原理示意图

四. 绿盟工控漏洞扫描系统产品特性

4.1 传统 IT 类设备扫描

NSFOCUS ICSScan 支持对传统 IT 类设备主机发现、端口扫描、服务识别，支持 Windows、Unix/Linux 各类操作系统识别，支持各类网络设备及防火墙识别、支持各主流数据库（Oracle、MySql、Postgresql 等）漏洞扫描，支持虚拟化组件漏洞扫描。

4.2 上位机配置信息核查

NSFOCUS ICSScan 支持对上位机设备信息配合核查功能，从账户管理、口令设置、端口管理、应用程序管理、网络服务管理、操作系统安全设置、磁盘管理、日志审计、更新设置、补丁管理等多角度进行配置安全基线核查。

4.3 信息网、控制器 Web 扫描

工业现场内部设备物理隔离，信息网站作为对外的唯一接口并与内网级联，信息网的安全直接影响着整个后场的信息安全，另多数的 PLC 等控制器均自带 Web 配置页面，Web 组件多为自主实现，健壮性差，很容易被拒绝服进而影响到 PLC 控制器正常运转；

NSFOCUS ICSScan 支持对信息网及各控制器 Web 页面的漏洞扫描，包括 SQL 注入、XSS 检测、挂马检测等常见的 Web 攻击手段，更多维度的支持安全检测

4.4 覆盖多样的工业控制系统

NSFOCUS ICSScan 不仅能对在工业控制系统中使用的传统 IT 设备/系统，更针对工业控制系统中所特有的设备/系统，比如 SCADA、DCS、PLC 等，以及处于上游的数字化设计制造软件进行漏洞扫描

- 支持对 Advantech BroadWin、Citect、7-Technologies、Measuresoft、WellinTech 等 SCADA/HMI 应用进行漏洞扫描
- 支持对 Schneider、Siemens、AB 等组态软件及 PLC、DCS 等控制器进行漏洞扫描

- 支持 ModbusRTu、IEC101 等串口总线方式扫描
- 支持对数字化设计制造软件平台（如产品数据管理 PDM、专用数控机床通信软件 eXtremeDNC、高级设计系统 ADS 等）进行漏洞扫描

4.5 工业通讯协议 Fuzzing 漏洞挖掘

工业现场自动化集成度高，厂家多样复杂，各厂家通讯协议自主实现，以规约为主，无明确的代码实现要求，实现能力参差不齐，以功能接口实现为主，无深入的安全健壮性测试，给黑客提供了便利的利用条件；

对此，绿盟工控漏洞扫描系统对厂商设备出厂自检，工业现场环境入围测评，检测机构设备送检安全测试提供了更有力的工控协议 Fuzzing 漏洞挖掘模块，对 PLC 等控制器进行更深一步的漏洞挖掘功能。

4.5.1 通讯协议

ICSScan 当前选择主流的现场通讯协议，如：

ModbusTCP， 支持施耐德、HoneyWell、AB 等厂商及支持该通讯的其他厂商；

ProfinetIO、S7，支持西门子全系的 PLC 及组态软件；

DNP3.0 ，支持大型分布式网络部署的工业现场，应用于电力、水务等行业；

IEC-60870-5-104，覆盖广泛应用于配电网络的终端设备；

IEC-61850-MMS，覆盖广泛应用于变电站网络的自动化设备。

选取主流协议匹配到主流厂商，可覆盖电力、石化、烟草、水务、交通等主要基础设施的终端控制设备。

4.5.2 漏洞挖掘

ICSScan Fuzzing 挖掘模块参考各协议的国际/国家/行业标准的规约要求，对协议通讯进行深度学习，研究其格式，通讯方式，应答规约，异常处理；构造丰富的 Fuzzing 测试数据集合，编写精准的测试用例套件，利用完善的数据分析功能，配合多样的过程监听手段，进行高效的漏洞挖掘扫描，对 DUT 进行全面的协议实现分析，以期发现拒绝服务漏洞。

4.5.3 数据回放

传统的漏洞挖掘测试过程环境可能受其他影响，发现问题不能精准定位，不能复现，不能帮助客户定位问题，解决问题；

ICSScan Fuzzing 漏洞挖掘模块，在发现问题的过程，对 Fuzzing 过程进行全程路径记录及抓包存储，可对发现的问题及时高效的回放验证，帮助使用者精准高效的定位问题。

4.5.4 漏洞收藏

漏洞挖掘的结果是否影响到其他批次的设备，是否受当前环境的影响，能否对该漏洞进行统一的命名管理验证，才是对客户真正的帮助。

ICSScan 漏洞挖掘以客户为导向，对客户使用测评过的 DUT 设备漏洞，进行统一的收藏管理，可自定义描述，并根据新的 DUT 进行有效的验证测试，可以以收藏的漏洞情况直接验证测试，方便有效，不用再进行长时间的测试。

4.6 工业控制系统资产网络拓扑

在部分工业控制系统环境中，由于系统使用者和系统管理者很有可能分属于两个部门，所以没有相关人员对工业控制系统进行过资产的梳理，拓扑的更新等操作，并且由于工控设备大多数部署在工控现场，可能位于不同机柜甚至位于不同的地区，在进行工业控制系统资产梳理和拓扑编制的过程中存在较多困难点。

针对此种情况，绿盟工控漏洞扫描系统以资产管理为导向，先进行现场环境网络资产设备发现，并进行网络拓扑展示详细信息，能够对所在工控系统进行拓扑的自动生成操作，并支持后期人工修改，操作快捷，方便跟踪最新的设备漏洞信息。

4.7 基于串行总线的漏洞扫描技术（ICSScan-H 具备该功能）

根据最近的研究报告，老式现场总线和以太网总线混合的现状将长期存在。如 RS232，RS422，RS485 接口的 ModbusRTU、ProfiBus、IEC101 等协议，此类串行总线协议广泛应用于石化、电力、交通、烟草、制造行业等工业自动化控制领域。

绿盟工控漏洞扫描系统具有对使用串行总线接口设备的漏洞扫描能力，使得漏洞扫描产品可以与基于 RS232，RS422，RS485 通讯接口的工控设备进行通讯，加上漏洞扫描产品对工控协议的支持，实现了对基于 RS232，RS422，RS485 串口的老式工业总线设备的漏洞扫描。

4.8 轻量化扫描技术

在工业控制系统中，业务的连续性、健康性是至关重要的，尤其是对一些核心监控、生产系统，因此，对其进行漏洞扫描时也需要做到轻量化，以尽可能减轻工业控制系统的负担。绿盟工控漏洞扫描系统采用把扫描融入到正常的业务中的思路，也就是说，部分扫描行为与正常的业务行为是一致的，这样就能避免非正常的操作而造成对系统的影响。同时，绿盟科技的这种独创的技术已经在石化、电力、交通、政府、企业等传统 IT 系统上获得了上千个实际用户场景的验证，通过引进这种成熟的技术，以实现对工业控制系统的轻量级漏洞扫描。

4.9 无损扫描技术

在一些对业务连续性特别敏感的行业领域，客户无法提供停机或检修的时机对工业控制系统进行脆弱性的扫描，但是迫于业务本身的安全需求或合规性的要求必须进行评估，为了实现对工业控制系统完全的无害评估，绿盟工控漏洞扫描系统独家采用了无损扫描技术，通过对支持的工控资产进行梳理和信息收集，绿盟工控漏洞扫描系统可以实现远程，非接触式的安全评估。在不影响业务的前提下完成漏洞扫描。

4.10 可视化的工控风险展示

风险“可视化”是进行风险管控必不可少的特性。科学的风险发现、风险跟踪技术可以很好的提高整体风险控制的水平，可为企业带来更高的效率，有的甚至可以提高效果。

绿盟科技根据多年的经验积累，采用了更具实效性的仪表盘技术，从不同的角度展示设备风险及趋势。

- 包含资产整体的风险值、资产分析趋势图
- 包含主机风险等级分布、资产风险分布趋势

- 能够可视化的显示当前资产的风险值及过去一段时间的变化趋势

4.11 基于工控资产的漏洞跟踪

工控系统一般规模大，资产数量、漏洞数量、脆弱性问题也很多，汇总成大量的风险数据，会使安全管理人员疲于应付，又不能保证对重要资产的及时修补。

因此在漏洞跟踪是需要尽量收集工控系统环境信息，建立起工控资产关系列表，系统基于资产信息进行脆弱性扫描和分析报告；需要从风险发生区域、类型、严重程度进行不同维度的分类分析报告，用户可以全局掌握安全风险，关注重点区域、重点资产，对严重问题优先修补。对于需要定位工控资产安全脆弱性的安全维护人员，通过直接点击仪表盘风险数据，可以逐级定位风险，直至定位到具体主机具体漏洞；同时需要提供了强大的搜索功能，可以根据资产范围、风险程度等条件搜索定位风险

4.12 完善的漏洞管理流程

安全管理不只是技术，更重要的是通过流程制度对安全脆弱性风险进行控制，很多公司制定了安全流程制度，但仍然有安全事故发生，人员对流程制度的执行起到关键作用，如何融入管理流程，并促进流程的执行是安全脆弱性管理产品需要解决的问题。

图 4-1 工控漏洞管理流程

安全管理流程制度一般包括预警、检测、分析管理、修补、审计等几个环节，结合安全流程中的预警、检测、分析管理、审计环节，并通过事件告警督促安全管理人员进行风险修补。

4.13 高可靠的自身安全性

产品本身采用独立的硬件平台，数据分区加密，Web 站点访问采用 HTTPS 方式访问；产品本身屏蔽关键扫描服务外的其他服务端口；产品涉及用户更密码的地方都加密处理，保证密码的安全性；产品相关任务，日志，数据等导出都采用独立的加密处理；产品升级及证书系统采用高等的数据加密处理；提供独立的产品诊断 Consle，保证系统的可维护性。

4.14 持续快速漏洞响应机制

绿盟科技组建了专门的工控漏洞研究和分析小组，通过多种渠道持续跟踪国内外最新发布的工控漏洞，并通过自建、合作等方式搭建工控漏洞实验环境，对工控漏洞进行分析和解剖，并把漏洞扫描的能力持续添加到产品中。这种严谨科学的漏洞规则添加方式，可以更加有效地保证检测的准确性，以及减少从漏洞发现到漏洞检测之间的时间窗口，达到持续快速的漏洞响应效果。

4.15 多样化部署模式

采用远程访问的方式，网络可达即可；并连接现有的网络，不做网络的任何修改；可覆盖传统的 IT 系统，也可覆盖工控系统，如下图所示：

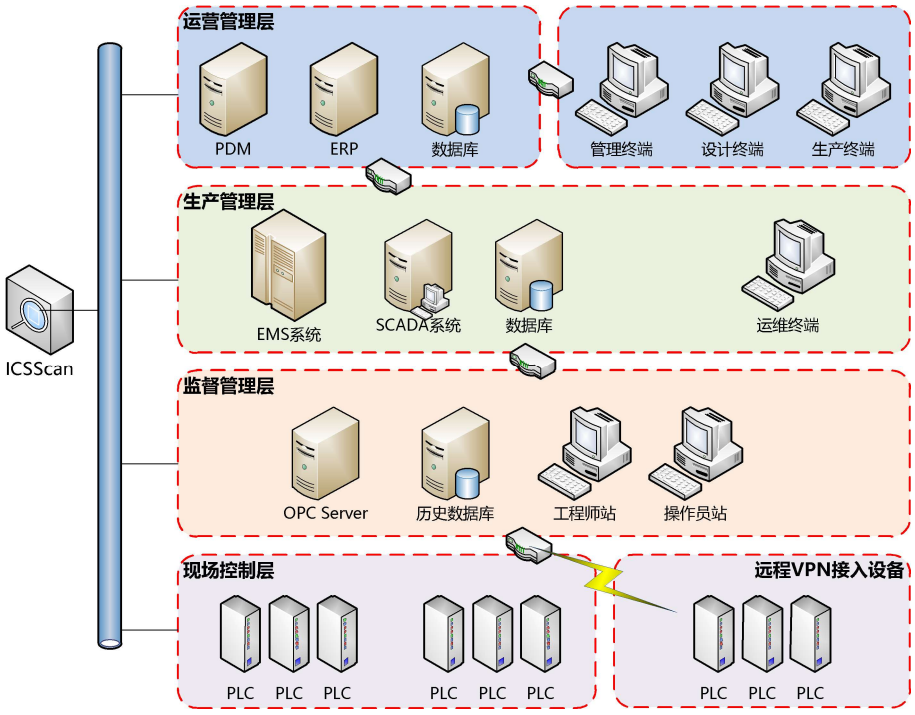

图 4-2 绿盟工控漏洞扫描系统典型部署方式

五. 结语

由于工业控制系统所覆盖的行业重要性，比如油化、电力、核电厂、水利、交通、市政、军事、高端制造业等，其安全性问题也越发的重要，并且牵涉到国计民生。对于这些重要的基础工业设施，如何进行安全性检查，如何发现潜在的问题，成为亟待解决的问题。

NSFOCUS ICSScan 作为国内首款可以专门针对这些工业控制系统进行安全评估的工具，可以很好地帮助国家监管机构、测试评级、行业主管机构等对工业控制系统进行全方位的风险评估；同时，也很好地帮助把成熟的 IT 风险评估技术成功移植到全新的工业控制系统环境中。

六. 附录

参考文献：

① [工信部 451] 关于加强工业控制系统信息安全管理的通知，工信部协[2011]451 号

② [（原）电监会 2005] （原）电监会 5 号令《电力二次系统安全防护规定》

③ [发改委] 第 14 号令《电力监控系统安全防护规定》

④ [电监会 2013] 电监会 2013 年 50 号文，《电力工控信息安全专项监管工作方案》

⑤ [国家烟草局 2013] 国家烟草局《烟草工业企业生产区与管理区网络互联安全规范》

⑥ [国家能源局,2013] 国家能源局国家能源局关于近期重点专项监管工作的通知（国能监管〔2013〕432 号）

⑦ [绿盟科技] 绿盟科技 《2014 绿盟科技工控系统安全态势报告》

⑧ [绿盟科技] 《2015 绿盟工控安保框架白皮书》

⑨ [Gartner] Gartner 《Definition: Operational Technology Security 2013》

⑩ CONTROL ENGINEERING ® China 2014.3 《如何实现以太网的快速迁移》