

# 目录

前言	1.1
工控安全概览	1.2
工控协议	1.3
常见协议	1.3.1
ATG	1.3.1.1
Modbus	1.3.1.2
Siemens S7	1.3.1.3
测试脚本	1.3.2
工控产品	1.4
工控安全检索查询	1.5
工控攻击	1.6
工控渗透	1.6.1
工控安全工具和框架	1.7
ATT&CK	1.7.1
STIX and TAXII	1.7.1.1
工控漏洞	1.8
漏洞分析	1.8.1
附录	1.9
名词术语	1.9.1
参考资料	1.9.2

# 工控安全概览

- 最新版本： v0.5
- 更新时间： 20200923

## 简介

整理信息安全领域内的工控安全的基本介绍，包括工控协议，工控协议测试脚本，工控产品，工控相关框架和工具等。

## 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

### Gitbook源码

- [crifan/industrial\\_control\\_security\\_overview: 工控安全概览](#)

### 如何使用此Gitbook源码去生成发布为电子书

详见：[crifan/gitbook\\_template: demo how to use crifan gitbook template and demo](#)

### 在线浏览

- [工控安全概览 book.crifan.com](#)
- [工控安全概览 crifan.github.io](#)

### 离线下载阅读

- [工控安全概览 PDF](#)
- [工控安全概览 ePUB](#)
- [工控安全概览 Mobi](#)

## 版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 [admin 艾特 crifan.com](mailto:admin@crifan.com)，我会尽快删除。谢谢合作。

## 鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 [crifan](#) 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-23  
23:09:16



# 工控安全概览

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
20:40:57

# 工控协议

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
20:45:34

# 常见协议

## 常见协议总结

工控协议	传输协议	端口	说明	zoomeye查询链接
Modbus	TCP	502	工控常用协议，Modbus协议是应用于电子控制器上的一种协议。通过此协议设备间可以通信。它已成为一通用工业标准。 详见： <a href="#">Modbus</a>	<a href="#">port:502</a>
Siemens S7	TCP	102	西门子PLC支持的通讯协议。属于第7层的协议，用于西门子设备之间进行交换数据，通过TSAP，可加载MPI,DP,以太网等不同物理结构总线或网络上，PLC一般可以通过封装好的通讯功能块实现。 S7协议是SIEMENS S7协议族的标准通信协议，使用S7-应用接口的通信不依赖特定的总线系统。 详见： <a href="#">Siemens S7</a>	<a href="#">port:102</a>
BACnet	TCP/UDP ?	47808	楼宇自动控制网络数据通讯协议。楼宇自动控制网络数据通讯协议 (A Data Communication Protocol for Building Automation and Control Networks)。 BACnet 协议是为计算机控制采暖、制冷、空调HVAC系统和其他建筑物设备系统定义服务和协议。 楼宇自动控制网络数据通讯协议(BACnet)是针对采暖、通风、空调、制冷控制设备所设计，同时也为其他楼宇控制系统（例如照明、安保、消防等系统）的集成提供一个基本原则。	<a href="#">port:47808</a>
ATG	TCP	10001	ATG，油罐液位仪，一种储油罐的监测设备；ATG (Automated-Tank-Gauge) 协议是液位仪器的私有通讯协议	<a href="#">port:10001</a>
IEC 104 = IEC 60870-5-104	TCP	2404	输配电通讯协议。IEC 60870-5-104 是国际电工委员会制定的一个规范，用于适应和引导电力系统调度自动化的发展，规范调度自动化及远动设备的技术性能。	<a href="#">port:2404</a>
DNP3 = DNP 3.0	TCP/UDP	20000	DNP = Distributed Network Protocol = 分布式网络协议 是一种应用于自动化组件之间的通讯协议，常见于电力、水处理等行业。分布式网络协议，主要用于电力行业。 SCADA可以使用DNP协议与主站、RTU、及IED进行通讯。 简化OSI模型，只包含了物理层，数据层与应用层的体系结构 (EPA)	<a href="#">port:20000</a>
ICCP			电力控制中心通讯协议	
OPC			过程控制的OLE (OLE for Process Control)。OPC包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统	
OPC DA	TCP	135	OPC (OLE for Process Control, 用于过程控制的OLE) 是一个工业标准。OPC包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统。OPC DA基于微软的OLE、COM和DCOM技术	

OPC UA	TCP	4840	opc-ua tcp4840 port:4840 OPC-UA (Unified Architecture) 是下一代的OPC 标准，通过提供一个完整的、安全和可靠的跨平台的架构，以获取实时和历史数据和时间。OPC UA不再依靠DCOM，而是基于面向服务的架构(SOA)	
CIP			通用工业协议，被 DeviceNet 、 ControlNet 、 EtherNet/IP 三种网络所采用	
Tridium Niagara Fox	TCP	1911	Fox协议是Tridium公司开发的Niagara框架的一部分，广泛应用于楼宇自动化控制系统	port:1911
Crimson V3	TCP	789		port:789
PCWorx	TCP	1962	PCWorx协议由菲尼克斯电气公司开发，目前广泛使用于工控系统。PCWORX3.11是菲尼克斯电气公司的专用协议	port:1962
ProConOs	TCP	20547	ProConOS是德国科维公司(KW-Software GmbH)开发的用于PLC的实时操作系统，它是一个高性能的PLC运行时引擎，目前广泛使用于基于嵌入式和PC的工控系统	port:20547
MELSEC-Q	TCP/UDP	tcp 5007 / UDP 5006	MELSEC-Q系列设备使用专用的网络协议进行通讯，该系列设备可以提供高速、大容量的数据处理和机器控制	port:5007, port:5006
IEC-61850 = MMS + goose + SV	TCP	102	输配电通讯协议。IEC 61850标准是电力系统自动化领域唯一的全球通用标准。它通过标准的实现，实现了智能变电站的工程运作标准化。使得智能变电站的工程实施变得规范、统一和透明	
GE SRTP	TCP	18245	GE-SRTP协议由美国通用电气公司开发，GE PLC可以通过GE-SRTP进行数据通信和数据传输	
CANopen			控制局域网通讯协定	
ONVIF	UDP	3702	ONVIF协议的开发目的是通过全球性的开放接口标准来推进网络视频在安防市场的应用，这一接口标准将确保不同厂商生产的网络视频产品具有互通性	
工业现场总线				
PROFIBUS			一种用于工厂自动化车间级监控和现场设备层数据通信与控制的现场总线技术，可实现现场设备层到车间级监控的分散式数字控制和现场通信网络	
EtherNet/IP	TCP/UDP	44818	Ethernet/IP是一个面向工业自动化应用的工业应用层协议。它建立在标准UDP/IP与TCP/IP协议之上，利用固定的以太网硬件和软件，为配置、访问和控制工业自动化设备定义了一个应用层协议。 是一种CIP的实现方式，由罗克韦尔自动化公司开发的工业以太网通讯协定。	port:44818
Profinet			开放式的工业以太网通讯协定	
EtherCAT			德国Beckhoff公司推动的开放式实时以太网通讯协定	

HART-IP	TCP/UDP	5094	HART协议是美国Rosement公司于1985年推出的一种用于现场智能仪表和控制室设备之间的通信协议。现已成为全球智能仪表的工业标准	
PLC通信协议				
MELSEC	TCP/UDP	TCP 5007 UDP 5006	三菱Q PLC支持的通讯协议	
OMRON FINS	TCP/UDP	9600	欧姆龙PLC支持的通讯协定。欧姆龙PLC使用网络协议FINS进行通信，可通过多种不同的物理网络，如以太网、控制器连接等。	port:9600
EGD			GE Fanuc为PLC开发的通讯协定	
Sinec H1			西门子PLC支持的通讯协议	
无线协议				
mqtt				
zigbee			开放式的无线通讯协定	
主流网络协议				
RTSP	TCP	554	RTSP协议是一种实时流传输协议，该协议定义了一对多应用程序如何有效地通过IP网络传送多媒体数据	
SIP	TCP	5060	SIP协议是由IETF制定的多媒体通信协议，SIP的开发目的是用来帮助提供跨越因特网的高级电话业务	
其他协议				
IEC 103				
Power Link			开放式实时以太网通信	
FF HSE			基金会现场总线以太网通信协定	
CoAP			轻量应用层协议	
openSAFETY			开源安全应用协议	
SERCOS III			实时以太网通讯协定	
TTEthernet			实时以太网通讯协定	
CDT			远动规约	
KNXnet/IP			住宅和楼宇控制标准	
Lontalk			埃施朗公司的LonWorks技术所使用的通讯协议	
SAE J1939			一种CAN的变种，适用在农业车辆及商用车辆	
USITT DMX512-A			灯光控制数据传输协议	
BSSAP/BSAP			由Bristol Babcock Inc发展的通讯协定	

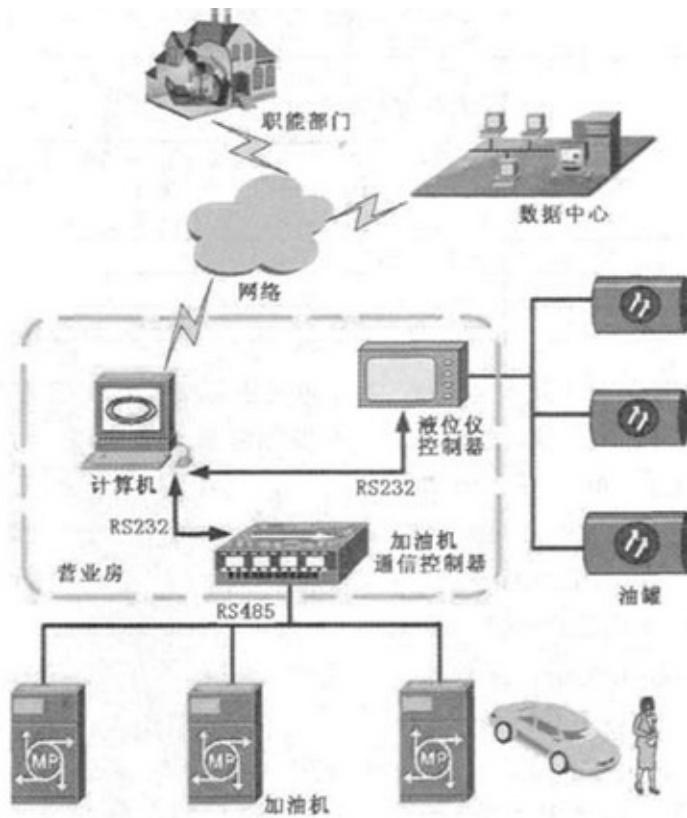
Gryphon			车用通讯协定	
Doip			汽车诊断协议	
AUTOSAR			汽车开放系统协议	
redlion-crimson3	TCP	789	协议被Crimson桌面软件用于与Red Lion G306工控系统的HMI人机接口	
Fox	TCP	1911	Fox协议是Tridium公司开发的Niagara框架的一部分，广泛应用于楼宇自动化控制系统	
secure-fox	TCP	4911	Fox协议是Tridium公司开发的Niagara框架的一部分，广泛应用于楼宇自动化控制系统	
moxa-nport	UDP	4800	Moxa串口服务器专为工业应用而设计。不通配置组合的串口服务器更能符合不同工业现场的需求。NPort系列串口服务器让传统RS-232/422/485设备立即联网，提供您基于IP的串口联网解决方案	
codesys	TCP	2455	CoDeSys编程接口在全球范围内使用广泛，全球上百个设备制造商的自动化设备中都是用了该编程接口	
ddp	TCP/UDP	5002	DDP协议(DTU DSC Protocol)是DTU与DSC之间的通讯协议，DDP是一种厂商定义的私有公开性质的通信协议，用于数据的传输和DTU管理	
lantronix-udp	TCP	30718	Lantronix串口服务器专为工业应用而设计。串口服务器是一种具有串口转以太网功能的设备，它能将RS-232/485/422串口转换成TCP/IP网络接口，串口服务器广泛的应用在SCADA数据采集环节上，用于解决串口和以太网的通信问题	
wdbrpc	TCP	17185	VxWorks是世界上使用最广泛的一种在嵌入式系统中部署的实时操作系统，是由美国WindRiver公司于1983年设计开发的。VxWorks系统在工业控制领域应用较广泛。WDB RPC是VxWorks的远程调试协议	
dahua-dvr	TCP	37777	DAHUA-DVR协议是浙江大华安防监控设备的私有通信协议，该协议用于实时视频流量的传输	
vstarcam-udp	UDP	8600	VSTARCAM-UDP协议是威视达康安防监控设备的私有通信协议该协议用于获取安防监控设备的网络配置等信息	
CSPV4	TCP	2222	CSPV4是可以识别PLC5/SLC 500控制器的服务；罗克韦尔的SLC 500功能强大，拥有先进的指令集、丰富的输入输出模块，专门针对工业现场恶劣的工作环境而设计	
general-electric-srtsp	TCP	18245	GE-SRTP协议由美国通用电气公司开发，GE PLC可以通过GE-SRTP进行数据通信和数据传输	
私有协议				
bachmann-tcp	TCP	3500	Bachmann是一种私有协议，用于Bachmann PLC的通讯，常见于风力发电等行业	

bachmann-udp	UDP	3003	Bachmann是一种私有协议，用于Bachmann PLC的通讯，常见于风力发电等行业	
beckoff-ads	UDP	48899	Beckoff-ads是一种私有协议，用于Beckoff PLC的通讯，常见于风力发电等行业	
hollysys-lk	UDP	6000	Hollysys-lk协议是一种私有协议，用于Hollysys PLC的通讯，常见于电力、石油、化工等行业	
hollysys-macs	UDP	8000	Hollysys-macs协议是一种私有协议，用于Hollysys DCS的通讯，常见于电力、石油、化工等行业	
siemens-license	TCP	4410	Siemens License协议是一种私有协议，用于西门子上位机软件的License服务	
igss	TCP	12397	IGSS协议是一种私有协议，用于IGSS (Interactive Graphical SCADA System) 软件之间的通讯	
foxboro	TCP	20476	Foxboro是一种私有协议，用于Foxboro PLC的通讯，常见于电力、石油、化工等行业	
ilon-smartserver	TCP	1628	ILON-SMARTSERVER协议是ECHELON公司生产的iLon系列产品的私有通信协议，iLon系列产品可以广泛的应用于工业控制领域；iLon SmartServer类似于一台服务器，起着指令分发，数据存储等作用	

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23 23:07:58

# ATG

- ATG
  - =油罐液位仪=加油站液位仪
  - 是什么：一种储油罐的监测设备
  - 现状
    - 全球有高达5800多站点的设备接入了互联网
    - 其中5300多位于美国
    - 仪表主要供应商为维德路特（Vedeer-Root）
    - 仪表设备经由串转网（串口转以太网）的方式接入互联网（主要用于运营商远程监控数据）
    - 因为设备协议上没有认证
      - 攻击者可以轻易通过网络更改仪表的门限和阀值、产生警报等引起安全事故
  - 加油站监测的系统结构图



# Modbus

- Modbus
  - MODBUS协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。特定总线或网络上的MODBUS协议映射能够在应用数据单元（ADU）上引入一些附加域。
  - 安全问题：
    - 缺乏认证：仅需要使用一个合法的Modbus地址和合法的功能码即可以建立一个Modbus会话
    - 缺乏授权：没有基于角色的访问控制机制，任意用户可以执行任意的功能。
    - 缺乏加密：地址和命令明文传输，可以很容易地捕获和解析

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-23  
22:27:54

# Siemens S7

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
22:26:15

## 产品

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
20:49:40

# 检索查询

- 工控安全全球检索网站和系统

  - ICS-Radar

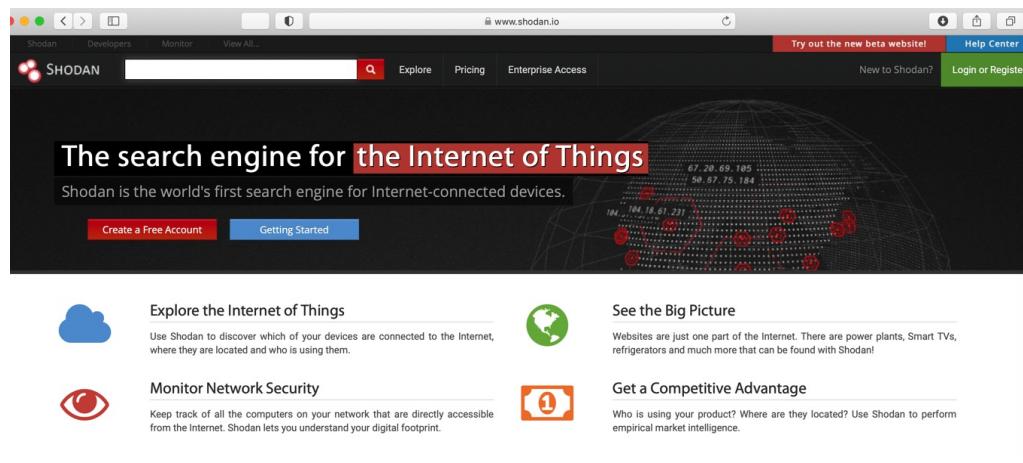
    - [http://radar.wincssec.com/html/search/search\\_topic.html](http://radar.wincssec.com/html/search/search_topic.html)





  - Shodan搜索

    - <https://www.shodan.io>





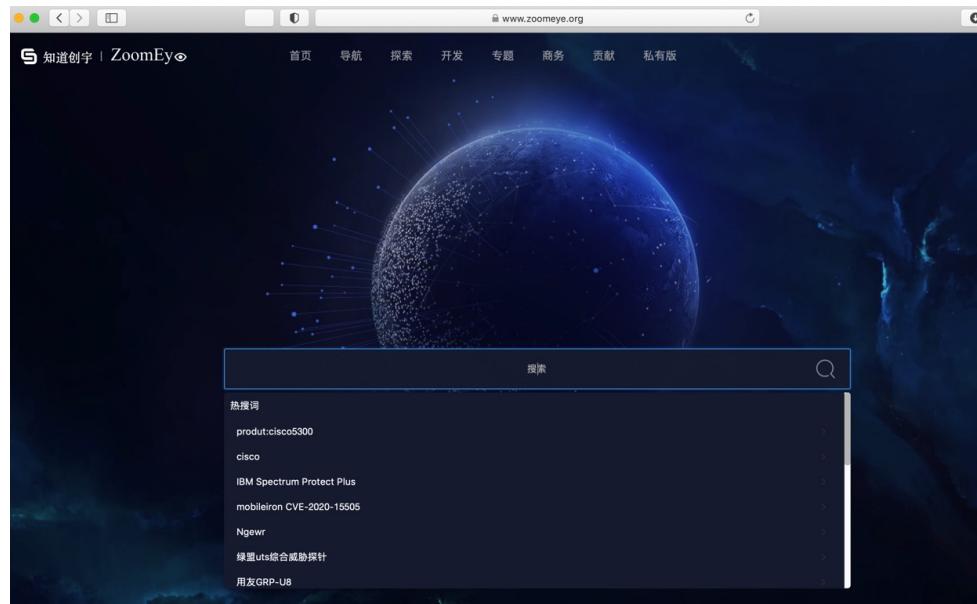
  - 举例





  - Zoomeye搜索

    - ZoomEye - Cyberspace Search Engine
    - <https://www.zoomeye.org>

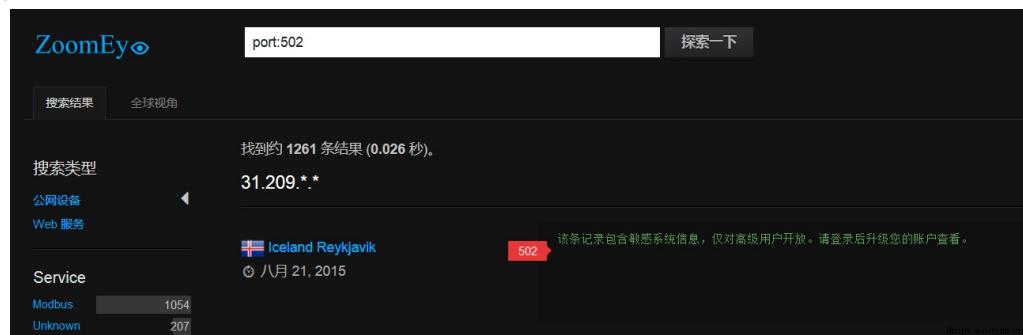


### ■ ZoomEye - Cyberspace Search Engine

■ <https://www.zoomeye.org/statistics>



### ■ 举例



crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23 22:39:59



# 工控攻击

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
22:33:09

# 工控渗透

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
22:33:19

# 工具和框架

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
20:49:05

# 工控漏洞

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
22:43:18

# 漏洞分析

## 乌云工控漏洞的分析

针对乌云主站的漏洞进行关键字搜索：工控(31)、SCADA(15)、Modbus(9)、PLC并进一步整合得到如下列表。

缺陷编号	漏洞起因	漏洞标签
<a href="#">wooyun-2015-132010</a>	弱口令	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控配置/阀门可控未测）
<a href="#">wooyun-2015-129388</a>	注入	华润化工控股有限公司信息门户设置缺陷/sql注入
<a href="#">wooyun-2015-125651</a>	弱口令	某地有线电视内网沦陷可能修改推送广告内容等
<a href="#">wooyun-2015-125399</a>	注入	中华工控网SQL注入导致全网数据沦陷 90W会员数据#打包
<a href="#">wooyun-2015-122677</a>	弱口令	某工控系统配置不当危及船只安全
<a href="#">wooyun-2015-117227</a>	弱口令	某水库工控系统存在弱口令(成功渗透)
<a href="#">wooyun-2015-116558</a>	配置不当	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC 可被操控执行任何命令）
<a href="#">wooyun-2015-107326</a>	注入	某油田开发公司工控系统sql注入
<a href="#">wooyun-2015-96729</a>	配置错误	VIA 弱密码致华北工控内网远程桌面服务器/内网穿透/涉及敏感信息
<a href="#">wooyun-2014-87708</a>	弱口令	温州市管道燃气公司 SCADA 系统弱口令
<a href="#">wooyun-2014-86726</a>	逻辑漏洞	中国工控网任意用户密码重置漏洞
<a href="#">wooyun-2014-83839</a>	弱口令	大量外网 web 监控系统后台存在弱口令(涉及两款监控产品，涵盖宾馆、车间、仓库、企业内部等)
<a href="#">wooyun-2014-71890</a>	弱口令	某财政信息网系统管理系统密码泄露
<a href="#">wooyun-2014-58681</a>	配置不当	对电厂生产控制网络的一次漫游（针对工控网络的小型 APT 攻击）
<a href="#">wooyun-2013-42212</a>	目录遍历	北京市一工控系统多处漏洞可内网渗透（已经发现 webshell）
<a href="#">wooyun-2013-22961</a>	网络未授权访问	301 基础设施系列-国外基础设施 1（鲍里斯波尔国际机场地面照明控制和监测系统）暴露
<a href="#">wooyun-2013-21848</a>	弱口令	从对某电厂 DCS 控制系统的实体控制浅谈工控安全（可控制电厂实体设备）
<a href="#">wooyun-2013-21314</a>	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透 第二份案例ops.wooyun.org

<a href="#">wooyun-2013-21250</a>	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网的渗透
<a href="#">wooyun-2012-16328</a>	未授权访问	美国一工业操作系统越权访问,可控制能源基础设施
<a href="#">wooyun-2012-10818</a>	弱口令	武汉市某工控系统弱口令导致信息泄漏，企业各种记录在内
<a href="#">wooyun-2012-09565</a>	命令执行	放统计代码，站长一秒钟变 APT 攻击专家 ( <a href="#">wooyun-2012-09025</a> 级)
<a href="#">wooyun-2012-09025</a>	设计缺陷	UC 云端加速引擎存在非正常泄露 referer 问题
<a href="#">wooyun-2012-07340</a>	账户体系控制不严	某省级能源集团旗下 XX 存在安全隐患
<a href="#">wooyun-2012-07172</a>	配置错误	某环境集成平台存在严重问题！获得客户端控制实权！
<a href="#">wooyun-2012-07084</a>	弱口令	中国电信某 GPS 监控平台存在严重问题
<a href="#">wooyun-2012-06997</a>	SQL注入	天津鑫然智能 DCS 监控平台
<a href="#">wooyun-2012-06196</a>	配置不当	国内某大型风电工控系统应用配置失误
<a href="#">wooyun-2012-04702</a>	信息泄露	南京国电自动化股份有限公司厂站监控系统源代码及配置文件泄露漏洞
<a href="#">wooyun-2014-84258</a>	未授权访问	姜堰市自来水公司 SCADA 管网综合监测系统漏洞
<a href="#">wooyun-2014-80994</a>	注入	哈药集团分公司 sql 注入(影响大量同服网站数据库)
<a href="#">wooyun-2014-58654</a>	命令执行	CenturyStar9.0 SCADA 组态软件存在远程命令执行漏洞
<a href="#">wooyun-2014-58130</a>	上传漏洞	某电厂 SCADA 测试文件未清理存在任意上传漏洞(可导致服务器沦陷)
<a href="#">wooyun-2013-34711</a>	弱口令	天能集团某 SCADA 系统弱口令登陆
<a href="#">wooyun-2013-21086</a>	SQL注入	某煤矿 SCADA 系统存在严重缺陷可导致服务器沦陷
<a href="#">wooyun-2012-07334</a>	未授权访问	某市燃气管道 SCADA 系统登录绕过
<a href="#">wooyun-2012-06952</a>	设计缺陷	某 SCADA 电力监控系统漏洞 <a href="http://www.wooyun.org">http://www.wooyun.org</a>

以上的漏洞列表中，可以得出如下结论：

- 乌云工控漏洞的案例中，绝大多数起因是弱口令(弱口令最多的是123456，其次是admin)、注入类漏洞
- 能够挖出工控的精华漏洞的人也是特定的那几位，且在Kcon2015也有过演讲
- 挖掘此类漏洞主要解决两个问题
  - 如何找到工控相关的系统和地址
  - Getshell后，基于工控知识如何操控系统
- 根据漏洞中的细节可以进一步的复测和拓展，进而为工控系统的漏洞挖掘提供非线性思路
  - 结合GHDB关键字的搜索：例如 inurl:SCADA 等
  - 链接地址含SCADA、Modbus等协议的关键字等
  - 其他KEY：MIS、SIS、DCS、PLC、ICS、监控系统等
  - 相关公司：南京科远、金风科技、天能集团、国电南瑞、华润燃气、积成电子、重庆三峰、东方电子等

## 工控精华漏洞分析

乌云工控相关的精华漏洞如下7个，在思路亮点中分析了漏洞的核心，同样也可能是获得打雷精华的理由。几乎共同点均是操控了对应的工控系统

缺陷编号	漏洞标题	思路亮点	作者
wooyun-2015-132010	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控/配置/阀门可控未测）	燃气系统 Getshell+内网渗透+敏感信息	jianFen
wooyun-2015-125651	某地有线电视内网沦陷可能修改推送广告内容等	Getshell+集群指令下达+敏感信息	scanf
wooyun-2015-116558	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC 可被操控执行任何命令）	发电厂 getshell+内网 DB+操控 DCS+拓扑分析	zph
wooyun-2014-58681	对电厂生产控制网络的一次漫游（针对工控网络的小型 APT 攻击）	MIS&SIS 分析 +Getshell+内网	Z-one
wooyun-2013-21314	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透 第二份案例	在线 DCS 采集系统操控	Z-one
wooyun-2013-21250	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透	软件厂商+未授权敏感信息+Getshell+操控 Syncmb	Z-one
wooyun-2015-127849	某大型 SCADA 系统缺陷导致多地多个工控基础设施被沦陷（影响电力、自来水、运营商等）	-	zph drops.wooyun.org

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook 最后更新: 2020-09-23 22:47:14

## 附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2018-06-15  
20:45:43

# 名词术语

- 专业术语

- DCS = 分布式控制系统 = 集散控制系统
- PCS = 过程控制系统
- ESD = 应急停车系统
- PLC = Programmable Logic Controller = 可编程序控制器
- RTU = 远程终端控制系统
- IED = 智能监测单元
- HMI = Human Machine Interface = 人机界面
- MIS = Management Information System = 管理信息系统
- SIS = Supervisory Information System = 生产过程自动化监控和管理系统
- MES = 制造执行管理系统

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23  
22:42:25

## 参考资料

- 全国首个工业互联网安全研究院落户园区-名城苏州新闻中心
- 160077346356.mp4
- 2015年1月 – 灯塔实验室
- 加油站实时监测设备的一次全球统计报告 (Tank Gauges Vulnerability Global Census Report) – 灯塔实验室
- 【工控网络协议专题】
- 【工控网络协议专题-汇总】工控协议整理集合（更新ing）\_qq\_29864185的博客-CSDN博客
- ICS-Radar
- ZoomEye - Cyberspace Search Engine
- 【工控协议专题01】Modbus协议原理与安全性分析\_qq\_29864185的博客-CSDN博客
- 工控安全入门分析 - 路人甲
- 罗克韦尔自动化主页-罗克韦尔自动化（中国）有限公司
- 

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-23 22:51:51