# 2016 年工控安全报告


杭州安恒信息技术有限公司

二〇一七年一月

# 目录

# 1. 工控安全现状分析

工控即工业自动化控制，主要是指使用计算机技术，微电子技术，电气手段，使工厂的生产和制造过程更加自动化、效率化、精确化，并具有可控性及可视性，小到随身使用的电子设备，大到电站电网、航空航天等，但随着工业信息化的发展，生产安全和公共安全正面临巨大的威胁，其造成的后果不容小觑。本章节主要结合 2016 年安恒研究院的分析成果，对全球及全国工控安全现状做简要阐述。

根据 2000 年以来 ics.cnvd.org.cn（CNVD 即国家信息安全漏洞共享平台）披露的工控系统行业的漏洞数量来看，2010 年后越来越多的工控安全漏洞被披露，其中西门子等厂商的产品存在的安全威胁相对较大。

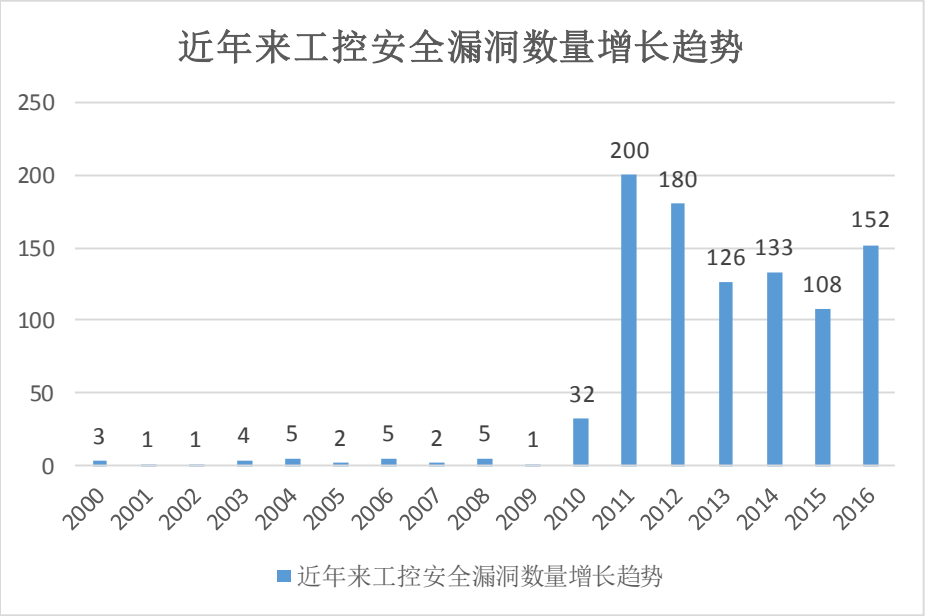


图 1-1 自 2000 年起工控安全漏洞数量增长趋势（数据来源于 CNVD）

工控漏洞在 2010 年之后始终开始保持增长趋势，从整体分析，出现此趋势一方面在于工业信息化的飞速发展，另一方面与受震网病毒的影响后网络安全意识有所提高有着较为直接的关系。综合近几年互联网中爆发的工控安全事件，可发现大部分攻击的根源都来自于利用了脆弱性较大的安全漏洞。

如下图，基于近几年披露的工控安全漏洞的等级来看，可以看到近 94%的漏洞属于高中危漏洞，而高中危漏洞的严重性相比于其它漏洞而言危害更大。

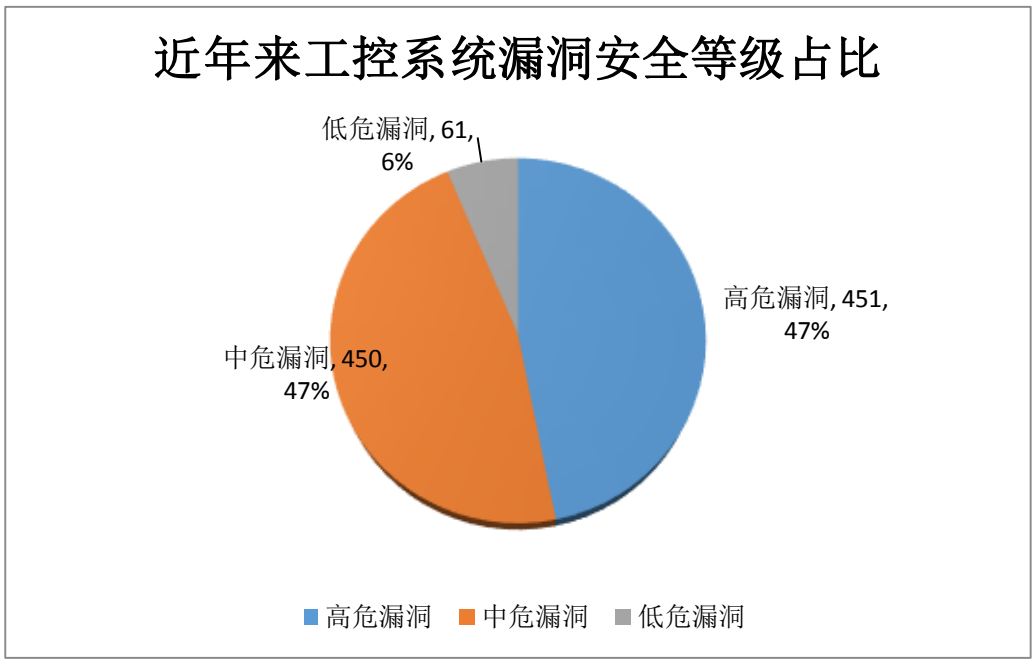


图 1-2 近年来工控系统安全漏洞安全等级数量及其占比

# 2. 2016 年工控安全事件分析

1）BLACKENERGY(黑暗力量)攻击导致的断电事故

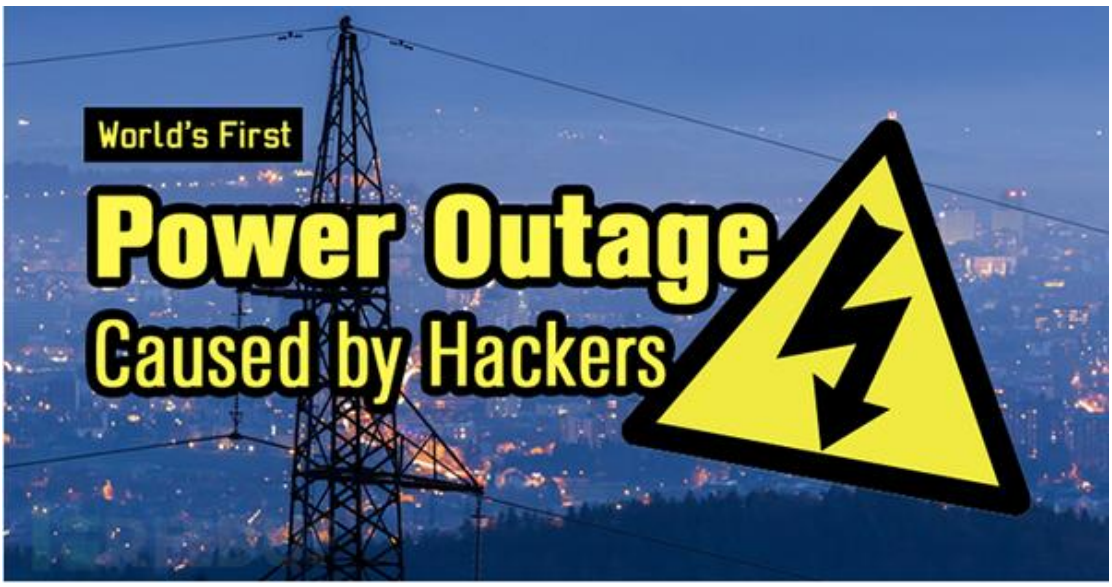


图 2-1 乌克兰大面积停电示例图（1）

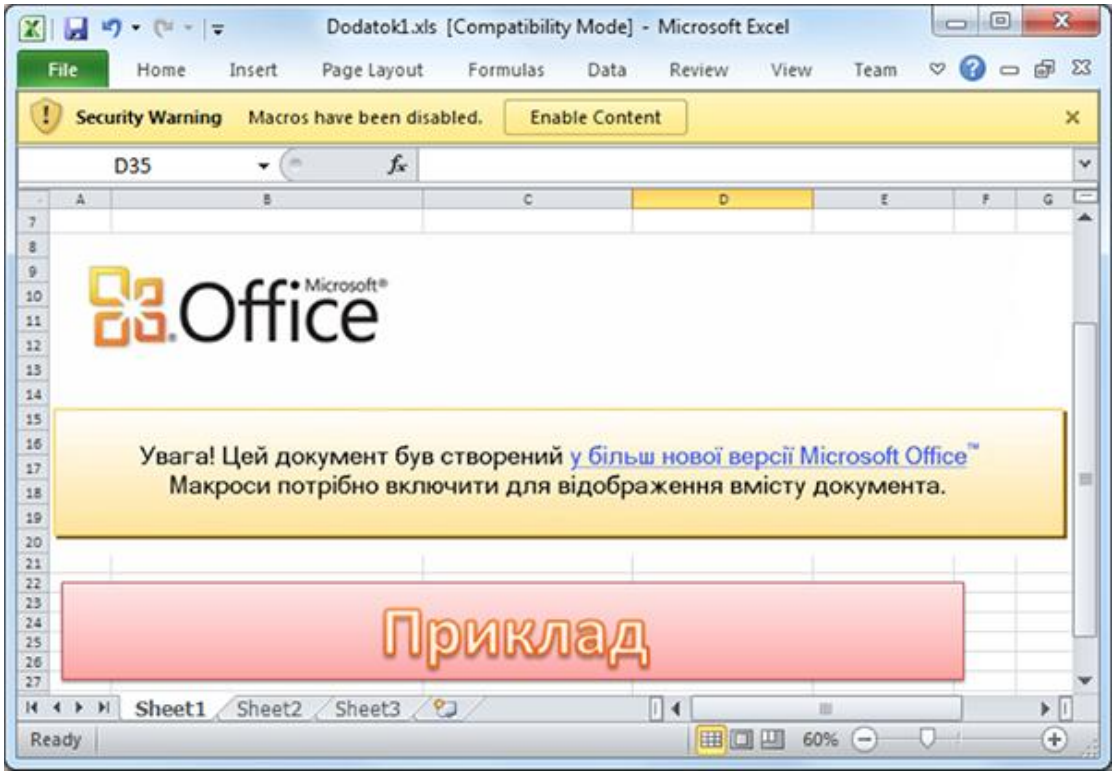


图 2-2 乌克兰大面积停电示例图（2）

2015 年 12 月 23 日，乌克兰电力供应商 Prykarpattyaoblenergo 通报了持续三个小时的大面积停电事故，受影响地区涉及伊万诺-弗兰科夫斯克、卡卢什、多利纳等多个乌克兰城市。后经调查发现，停电事故为网络攻击导致。攻击者使用附带有恶意代码的 Excel 邮件附件渗透了某电网工作站人员系统，向电网网络植入了 BlackEnergy 恶意软件，获得对发电系统的远程接入和控制能力。

2) 伊朗黑客攻击美国大坝事件


图 2-3 伊朗黑客攻击美国大坝事件示例图（1）

2016 年 3 月 24 日，美国司法部公开指责 7 名伊朗黑客入侵了纽约鲍曼水坝(Bowman Avenue Dam)的一个小型防洪控制系统。幸运的是，经执法部门后期调查确认，黑客还没有完全获得整个大坝计算机系统的控制权，仅只是进行了一些信息获取和攻击尝试。这些伊朗黑客可能为伊朗伊斯兰革命卫队服务，他们还涉嫌攻击了包括摩根大通、美国银行、纽约证券交易所在内的 46 家金融机构。

每年的工控安全事件造成的后果已经很严重,这就有必要我们针对工控的安全更加重视,同时针对工控的攻击已经上升到到每时每刻都可能潜在的发生着,所以对工控的安全隐患,更应该有效的做好安全工作,发现安全隐患,进一步保障工控安全。

# 3. 互联网中工控协议识别

工控系统中通信协议存在众多标准，也存在众多私有协议，如果有过使用组态软件的经历，你便会发现，在第一步连接设备时除连接设备的方式有以太网/串行等方式外，各家基本上都存在自己的私有通信协议。同时对于工控协议在传输的过程不加密、协议上无认证，往往可以通过协议分析识别协议。在众多公开

或私有协议中可分为这大概几类，标准协议：国际标准或公认的标准协议，如Modbus、DNP3、IEC104等。私有公开：只有厂商自己设备支持并提供官方协议文档，如Omron FINS协议、三菱Melsec协议等。

私有不公开协议只有厂商自己设备支持且官方不提供协议文档，如S7、西门子PPI协议、GE SRTP等。

**下面我们针对主流的工控协议简单的描述和说明。**

1） SIEMENS

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。

2） CoDeSys

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。

3） GE-SRTP

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。

4） omron

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。

5） Modbus

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。

6） fox

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。

7） EtherNet/IP

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。

8） dnp

DNP(Distributed Network Protocol，分布式网络规约)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。SCADA 可> 以使用 DNP 协议与主站、RTU、及 IED 进行通讯。

9) BACnet

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。

10) MELSEC-Qmelsecq

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。

11) HART-IP

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 。

12) PCWorx

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。

# 4.工控设备暴露互联网中分布

工控协议在传输的过程不加密、协议上无认证，也就说明每发现一台工控设备都存在安全漏洞和安全风险，由于各个区域对暴露出来的设备数量以及协议类型不同，所以存在的安全风险也是不同的。例如下文我们将从全球,国内,协议三个角度来说明这些安全隐患。

## 4.1 全球范围内暴露在互联网中工控设备

通过安恒研究院探测发现，全球范围内暴露在互联网中的设备数量已经达到 53,831 台，其中黄色的点代表工控设备，越集中代表工控设备数量越多，也可以认为其风险也较为集中。注意此次分析的数据为截止到 2016 年 12 月存活使用的工控设备，不同于部分第三方平台中提供的历史所有工控设备数量（存在大量设

备已经不再使用的情况），更能代表当前最新的工控设备情况。


图 4-1 全球暴露在互联网中的工控设备数量散点图

从图中可以看到，美国区域暴露的工控设备最多，其数量已达到 27,104 个，远远超于其它国家，这是由于美国是工业化最为发达的国家，工业网络也较为开放。从互联网披露的事件来看，美国地区发生的工控安全事件相较于其它区域更多，这与其政治背景、军事力量及工业发展等有较为直接的关系。从图中来看，中国在互联网中暴露出来的工控设备仅次于美国、加拿大，所带来的安全隐患也比其他国家相对更高一些，需要引起重视。

下表基于以上数据，就各个工控协议在全球工控系统中使用的数量进行统计：

| 协议 | 数量 |
|---|---|
| fox | 24759 |
| modbus | 18241 |
| enip | 7019 |
| s7 | 1203 |
| crimson | 1089 |
| iec104 | 577 |
| pcworx | 395 |
| dnp3 | 232 |
| proconos | 192 |
| melsecq | 124 |

表 4-1 全球范围内单个工控协议暴露在互联网中的数量 TOP10

所有暴露在互联网中的工控协议，FOX 安全风险最高，数量达到 24,759 个，

目前 Tridium 公司的专用协议 Tridium Niagara Fox 被广泛应用于智能建筑、基础设施管理、电信设施管理、安防系统、智能电网、暖通空调设备等领域，因此其数量也较多。而排行第二的 Modbus 协议是全球第一个真正用于工业现场的总线协议，因其公开发表无版税要求，工业网络部署相对容易，对供应商来说，修改移动原生的位元或字节没有很多限制等优点，得到全球的广泛应用。

就使用率较高的工控协议来看，所有协议在美国的使用率均远大于其他区域，加拿大、荷兰、西班牙、法国、中国等区域使用也较大。

## 4.2 单个工控协议暴露在互联网中的数量(全球范围)

下图为就全球而言，各类协议使用数量排名 TOP10 的汇总表：

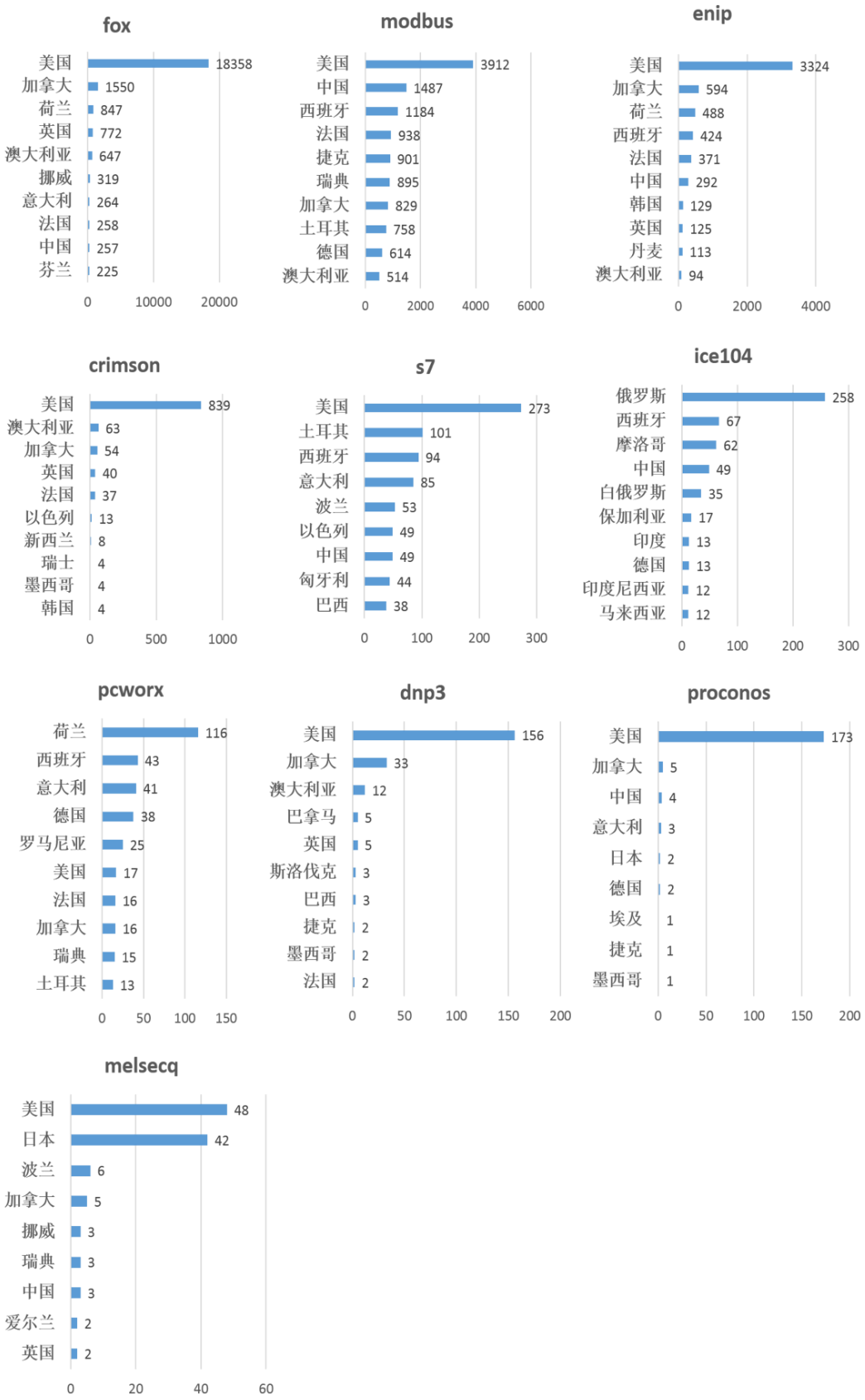


图 4-2 单个工控协议暴露在互联网中的数量 TOP10 图示

## 4.3 中国范围内暴露在互联网中的工控设备

近年来，我国政府高度重视工控系统安全，曾经爆发的“黑天鹅”安全门、某城市可远程访问和控制的数据采集与监控系统、某市自来水厂系统等事件给各行各业敲响了警钟，工控系统安全正如计算机系统安全一样面临着越来越多的黑客攻击。


**图 4-3 全国范围内暴露在互联网中的工控设备**

通过探测发现中国范围内暴露在互联网的工控设备数量已达到 2143 台，由于工控协议直接暴露在互联网中所以攻击者很容易接触到这些工控设备，通过漏洞和 APT 攻击的手法来对这些设备进行攻击，也就说明在互联网中暴露出来的工控设备数量越多说明存在的安全风险越高。

我们针对每个地区来详细分析存在的工控安全风险，每个地区面对的风险等级，以及面对工控协议是不一样的所以存在的安全风险高低不一样。

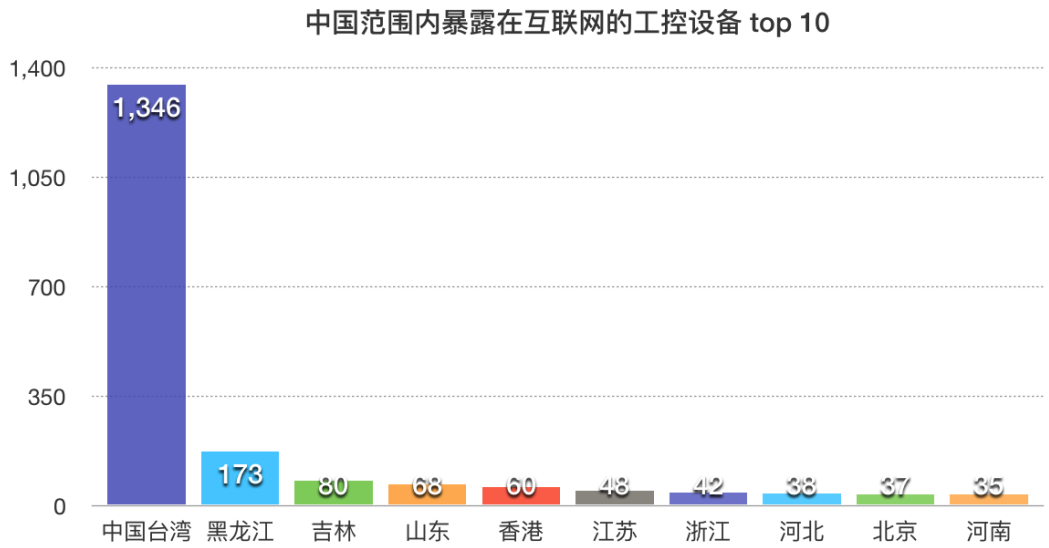


图 4-4 暴露在互联网中的工控协议数量 TOP10

| 区域 | 数量 |
| --- | --- |
| 中国台湾 | 1,346 |
| 黑龙江 | 173 |
| 吉林 | 80 |
| 山东 | 68 |
| 香港 | 60 |
| 江苏 | 48 |
| 浙江 | 42 |
| 河北 | 38 |
| 北京 | 37 |
| 河南 | 35 |

图 4-5 暴露在互联网中的工控协议数量 TOP10

## 4.4 中国范围内单个工控协议暴露在互联网中的数量

就单个协议而言，我们也对全国范围内的使用情况做了统计：

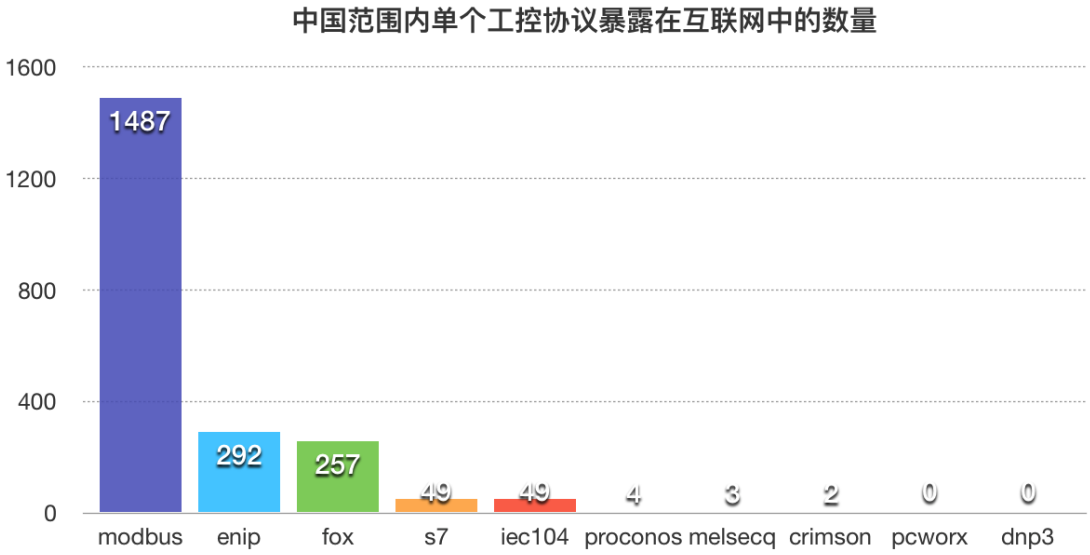


图 4-6 中国范围内单个工控协议暴露在互联网中的数量

| 协议 | 数量 |
|---|---|
| modbus | 1487 |
| enip | 292 |
| fox | 257 |
| s7 | 49 |
| iec104 | 49 |
| proconos | 4 |
| melsecq | 3 |
| crimson | 2 |
| pcworx | 0 |
| dnp3 | 0 |

图 4-7 中国范围内单个工控协议暴露在互联网中的数量

下图为全国范围内各省份使用的协议数量，未提及的及没有数字的区域为暂未监测到使用此协议的工控设备，从图中可看出中国台湾、黑龙江、山东、香港

等区域使用的工控设备较多。其中中国台湾区域使用 Modbus 协议的数量达到 954 个，使用 fox 协议的数量达到 202 个，而 proconos、melsecq、crimson 等协议均只在中国台湾监测到。

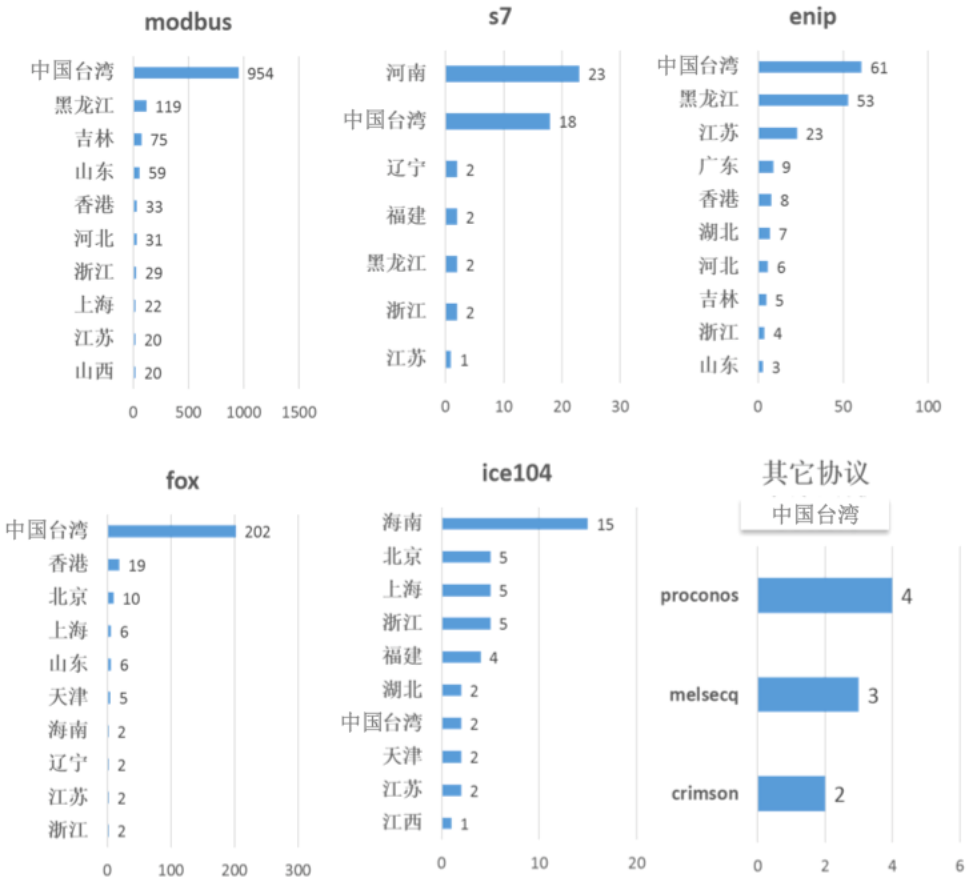


图 4-8 单个工控协议暴露在国内互联网中的数量图示

# 5. 工控设备暴露互联网中分布

## 5.1. 监控设备全球分布

下图为我国生产的主流视频监控设备在全球各区域的分布情况，其中可看到中国本土使用最为广泛，达到了 470,406 台，占比 27%，第二大区域为美国，成为了中国视频出口的大国，其次为巴西、印度等地，一定程度上代表了我国视频监控设备占据了较多海外市场。

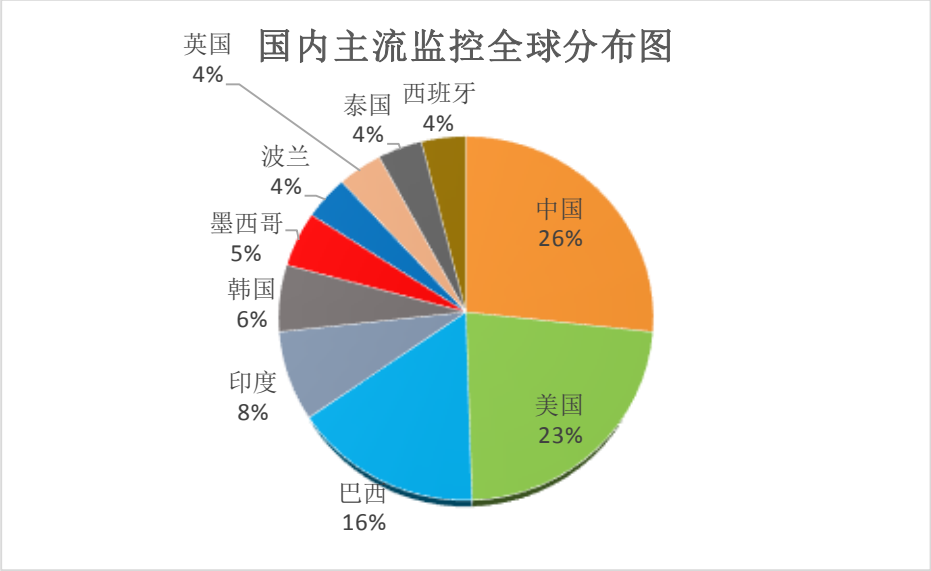


图 5-1 国内主流视频监控设备在全球各国家分布数量图

## 5.2. 监控设备境内分布

根据安恒研究院的监测结果来看，视频监控设备在国内主要分布于广东（26%）、江苏（17%）、浙江（15%）等地，其中广东区域的监控设备数量达到 89253 个，居于全国首位，这与广东区域的工业、经济等发展水平有十分紧密的联系。

| 区域 | 数量 |
|---|---|
| 广东 | 89253 |
| 江苏 | 59685 |
| 浙江 | 51540 |
| 福建 | 31198 |
| 中国台湾 | 30535 |
| 山东 | 29223 |
| 河北 | 17946 |
| 辽宁 | 14729 |
| 香港 | 12028 |
| 上海 | 11409 |

表 5-1 国内电子监控设备区域排行 TOP10

## 5.3. 全球监控设备漏洞分布

下图为国内的视频监控设备存在的安全漏洞分布图，从图中可以看到中国、美国等区域分布的安全漏洞数量较多，其整体趋势与电子监控设备的数量保持正比关系。其中国内存在的漏洞为 147850 个，美国为 112824 个。

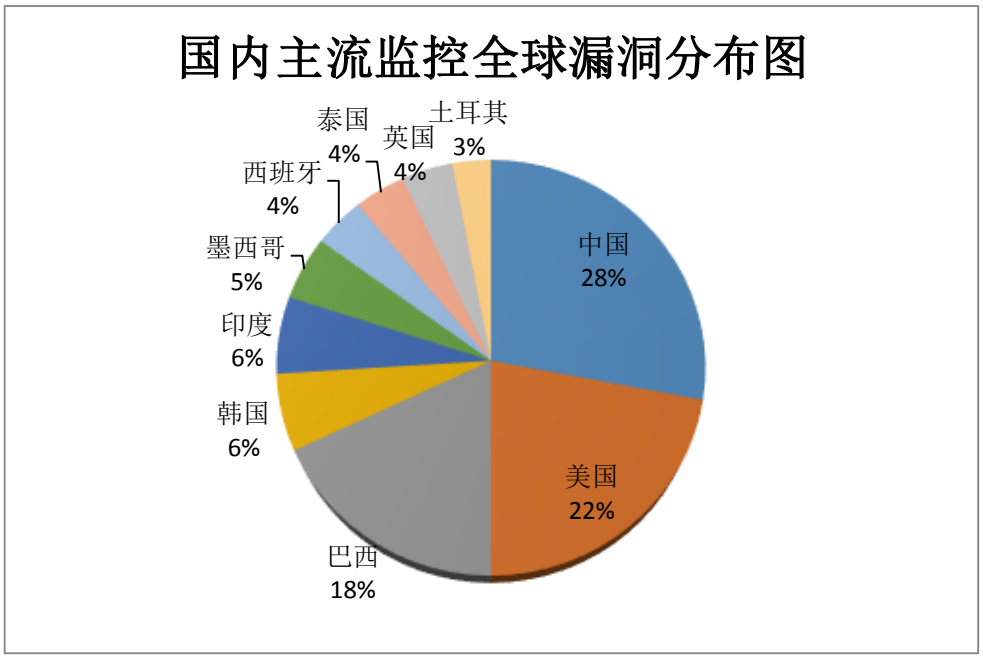


图 5-2 国内主流监控设备漏洞占比图（全球）

## 5.4. 境内监控设备漏洞分布

而国内监控设备数量较多的区域：如广东、浙江、江苏、福建等地存在的漏洞数量也较多，其中广东的漏洞达到 20743 个，浙江的漏洞数量 17125 个。

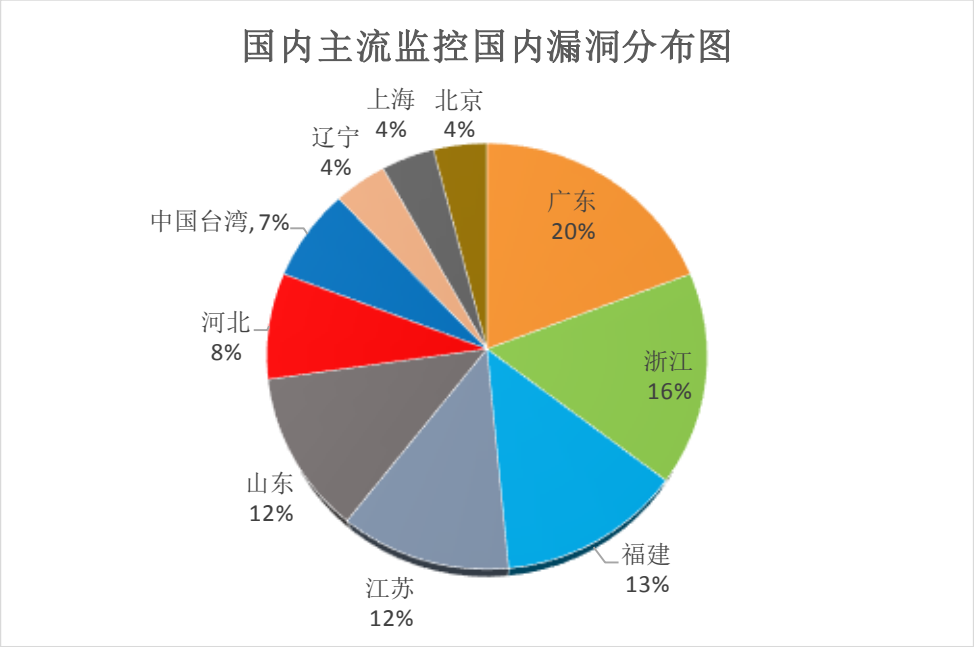


图 5-3 国内主流监控设备漏洞占比图（全国）

由此可见全国甚至全球范围内监控设备还存在大量的安全问题，尤其是弱口令漏洞，用户如直接遵从厂商设置的默认密码，黑客可直接尝试使用弱口令进入监控系统后台，获得控制监控设备的权限，以此达到黑客目的，因此工控系统安全亟需引起人们的重视。

## 5.5. 全球监控设备漏洞占比

根据对监控设备的全球漏洞百分比分析，发现中国的监控设备数量和漏洞数量都非常高，其中存在漏洞的比例达到了 31.4%，位居第一位。

国内主流监控 设备数量 漏洞数量比

| 地区 | 设备数量 | 漏洞数量 | 漏洞所占百分比 |
|---|---|---|---|
| 西班牙 | 66966 | 20,344 | 30.3795956156856% |
| 泰国 | 67340 | 20,337 | 30.2004752004752% |
| 英国 | 69924 | 19,681 | 28.1462730965048% |
| 波兰 | 72733 | 11,663 | 16.0353622152256% |
| 墨西哥 | 87829 | 25,977 | 29.5767912648442% |
| 韩国 | 102676 | 32,878 | 32.0211149635747% |
| 印度 | 141592 | 31,748 | 22.4221707441098% |
| 巴西 | 273440 | 92,453 | 33.8110737273259% |
| 美国 | 408262 | 112,824 | 27.6351950463183% |
| 中国 | 470406 | 147,850 | 31.430296382274% |

图 5-4 全球监控设备漏洞占比图

根据监控设备国内漏洞数量百分比，中国的漏洞比大约 31%，说明每 100 台设备中就有大约 31 台存在安全问题。

## 5.6. 境内监控设备漏洞占比

通过分析得知在福建地区存在的漏洞比例情况最为严重达到 46%，也说明大约每 100 台设备中就有 46 台存在安全问题。

国内主流监控 设备数量 漏洞数量比

| 地区 | 设备数量 | 漏洞数量 | 漏洞所占百分比 |
|---|---|---|---|
| 上海 | 11,409 | 4,387 | 38.4520992199141% |
| 香港 | 12,028 | 3,887 | 32.3162620552045% |
| 辽宁 | 14,729 | 4,793 | 32.5412451626044% |
| 河北 | 17,946 | 8,309 | 46.3000111445447% |
| 山东 | 29,223 | 12,716 | 43.5136707388016% |
| 中国台湾 | 30,535 | 7,856 | 25.7278532831177% |
| 福建 | 31,198 | 14,522 | 46.5478556317713% |
| 浙江 | 51,540 | 17,125 | 33.2266201008925% |
| 江苏 | 59,685 | 13,114 | 21.9720197704616% |
| 广东 | 89,253 | 20,743 | 23.2406753834605% |

图 5-5 境内监控设备漏洞占比图