# 第一章 绪论

随着工业化和信息化的飞速发展，工业控制系统（简称工控系统）产品与信息技术（IT）的结合日益紧密。为了适应当前工业控制的需求，提高工厂或公司运作的效率，工业控制网络（简称工控网络）通过各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制网络扩散。近年来，新的工业控制网络威胁事件不断被披露，工业控制网络安全逐渐成为学术界、工业界关注的热点。

本章将阐述工业控制系统和工业控制网络的基本概念，并简要介绍工业控制网络安全领域的现状。

## 1.1 工业控制系统概述

本节将首先介绍什么是工业控制系统，并简要介绍工业控制系统的基本架构。

### 1.1.1 工业控制系统介绍

工业控制系统（Industrial Control System, ICS），是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。工业控制系统通常指的是监视控制与数据采集系统（Supervisory Control And Data Acquisition, SCADA）、分布式控制系统（Distributed Control System, DCS）、可编程逻辑控制器（Programmable Logic Controller, PLC）以及过程控制系统（Process Control System, PCS），如图 1.1 所示


图 1.1 工业控制系统一般组成

### 1.1.2 工业控制系统架构

一个典型的工业控制系统通常由检测环节、控制环节、执行环节和显示环节组成。经历多年发展，工业控制系统在控制规模、控制技术和信息共享方面都有巨大的变化。在控制规模方面，工业控制系统由最初的小规模发展成现在的大规模；在控制技术方面，工业控制系统由最初的简单控制发展成现代复杂或者先进控制；在信息共享方面，工业控制系统由最初的封闭系统发展成现在的开放系统。

通常，企业会根据自身生产和运行流程搭建符合各自需求的、不同的工业控制系统，根据《中华人民共和国公共安全行业标准中的信息安全等级保护工业控制系统标准》，可以将通用工业企业控制系统的架构按照功能从上至下划分为 5 个逻辑层次：企业资源层、生产管理层、过程监控层、现场控制层和现场设备层。如图 1.2 所示。

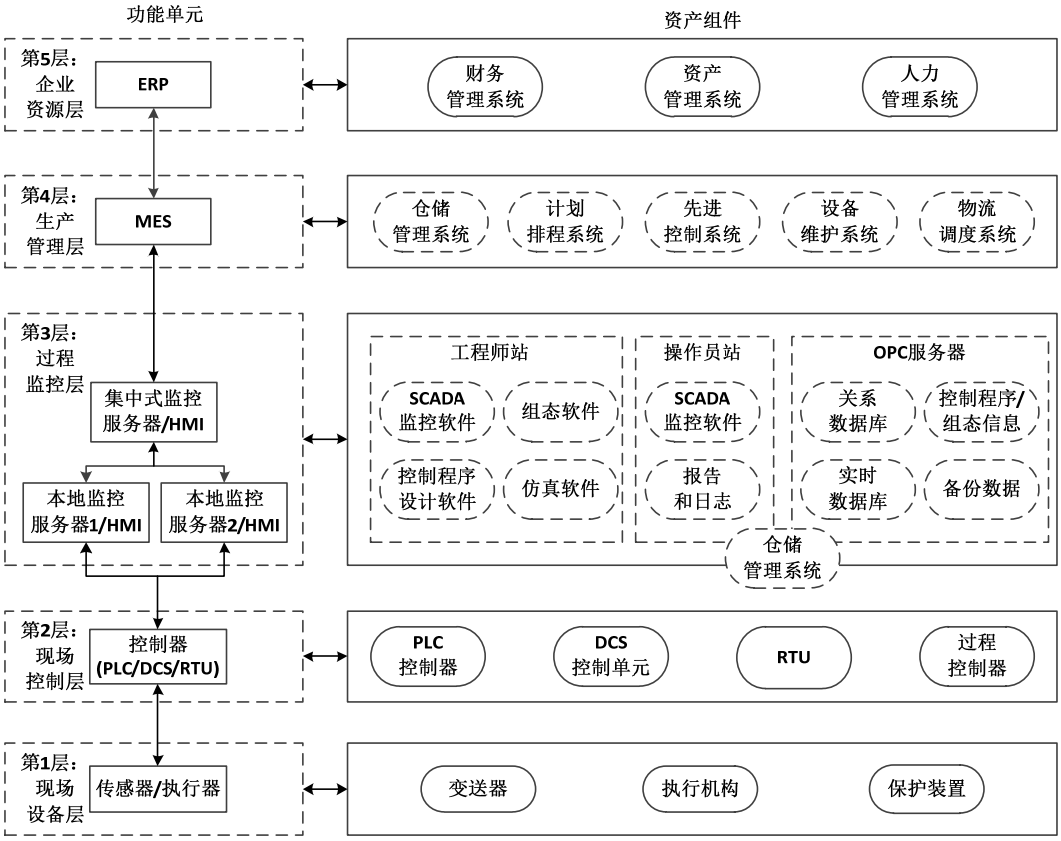


图 1.2 通用工业控制系统架构

- 企业资源层主要通过 ERP（Enterprise Resource Planning）系统为企业决策层及员工提供决策运行手段。
- 生产管理层主要通过 MES（Manufacturing Execution System）系统为企业

提供包括制造数据管理，计划排程管理、生产调度管理等管理模块。

- 过程监控层主要通过分布式 SCADA 系统采集和监控生产过程参数、并利用 HMI（Human Machine Interface）系统实现人机交互。
- 现场控制层主要通过 PLC、DCS/PCS 控制单元和 RTU（Remote Terminal Unit）等进行生产过程的控制。
- 现场设备层主要通过传感器网络对实际生产过程的数据进行采集，同时利用执行器对过程进行操作。

## 1.2 工业控制网络概述

本节将首先介绍什么是工业控制网络，并简要对比工业控制网络和传统的 IT 网络。

### 1.2.1 工业控制网络介绍

目前，对工业控制网络尚无标准定义。通常将工业控制网络定义为以具有通信能力的传感器、执行器、测控仪表作为网络节点，以现场总线或者以太网作为通信介质，连接成开放式、数字化、多节点通信，从而完成测量、控制任务的网络。

工业控制网络就是工业控制系统中的网络部分，是一个把工厂中各个生产流程和自动化控制系统通过各种通信设备组织起来的通信网络。工业控制系统包括工业控制网络和所有的工业生产设备，而工业控制网络只侧重工业控制系统中组成通信网络的元素，包括通信节点（包括上位机、控制器等）、通信网络（包括现场总线、以太网以及各类无线通信网络等）、通信协议（包括 Modbus，S7comm 等）。

工业控制网络由多个“网络节点”构成，这些网络节点是指分散在各个生产现场，具有相应数字通信能力的测量控制仪器。它采用规范、公开的通信协议，把现场总线或以太网作为连接纽带，从而是现场设备能够相互沟通，共同完成生产任务。实现测量和控制是工业控制网络的基本任务，因此保证数据传输的完整性、可靠性和实时性尤为重要，这就要求工业控制网络必须具备相应的实时通信

能力。

从发展历程来看，工业控制网络经历了从现场总线到工业以太网的道路。

现场总线技术产生于 20 世纪 80 年代，以全数字的通信代替了 4~20mA 电流的模拟传输方式，使得控制系统与现场仪表之间不仅能够传输生产过程测量与控制信息，而且能够传输现场仪表的大量非控制信息（如资产管理、自检等），使得工业企业的管理控制一体化成为可能。按照国际电工委员会（IEC）对现场总线（FieldBus）一词的定义，现场总线是一种应用于生产现场，在现场设备之间、现场设备与控制装置之间实现双向、串行、多节点数字通信的技术。现场总线目前存在以下不足：

- 标准不统一，仅国际标准 IEC 61158 就包含了 8 个类型；
- 不同总线间不能兼容，无法实现无缝集成；
- 因总线的专有性，其成本较高；
- 速度较低，支持的应用有限，不便于和信息网络集成。

工业以太网技术是普通以太网技术在工业控制网络中的延伸，是指采用与商用以太网（即 IEEE 802.3 标准）兼容的技术，选择适合工业现场环境下的产品构建的控制网络。表 1.1 对比了工业以太网络设备和商用以太网设备在性能要求方面的不同。

表 1.1 两种以太网设备的性能要求

| | **工业以太网设备** | **商用以太网设备** |
|---|---|---|
| **元器件** | 工业级 | 商用级 |
| **接插件** | 耐腐蚀、防尘、防水<br>如加固型 RJ45、DB-9 等 | 普通 RJ45 |
| **工作电压** | 24VDC | 220VAC |
| **电源冗余** | 双电源 | 一般没有 |
| **安装方式** | DIN 导轨、机架 | 桌面、机架 |
| **工作温度** | -40~85℃或-20~70℃ | 5~40℃ |
| **电磁兼容性** | 工业级 EMC | 办公室 EMC |
| **平均故障间隔时间** | 至少 10 年 | 3~5 年 |

### 1.2.2 工业控制网络与 IT 网络比较

从大体上看，工业控制网络和传统 IT 网络在网络边缘、体系结构和传输内

容三大方面存在主要的不同。

- 网络边缘不同：工业控制系统在地域上分布广阔，其边缘部分是智能程度不高的传感器和控制器，而不是 IT 系统边缘的通用计算机，两者之间在物理安全需求上差异很大，
- 体系结构不同：工业控制网络的结构纵向高度集成，主站节点和终端节点之间是主从关系；传统 IT 网络则是扁平的对等关系，两者之间在脆弱节点分布上差异很大。
- 传输内容不同：工业控制网络传输的是工业设备的遥测、遥信、遥控和遥调信息；而传统 IT 网络传输的内容则纷繁多样。

此外，两者在性能要求、软硬组件和可用性方面也存在很多不同。如表 1.2 所示。

表 1.2 工控网络与 IT 网络差异

| | **工业控制网络** | **IT 网络** |
|---|---|---|
| **建设目标** | 自动化生产、监控 | 数据共享与信息处理 |
| **包含组件** | 嵌入式智能设备（PLC、RTU）<br>TCP/IP 网络、现场总线等 | 主要是 X86 架构主机<br>网络主要是 TCP/IP 网络 |
| **操作系统** | 实时系统（VxWorks 等） | 通用操作系统（Windows 等） |
| **协议** | 通用、私有协议都存在 | 通用协议（HTTP 等） |
| **敏感性指标** | 实时性、可用性 | 保密性、完整性、可用性 |
| **系统故障影响** | 经济损失，甚至灾难 | 任务损失，甚至经济损失 |
| **链接 Internet** | 一般物理隔离 | 一般逻辑隔离 |

在安全方面，随着“两化融合”（工业化与信息化融合），IT 系统的信息安全也被融入了工业控制系统安全中。不同于传统的生产安全（Safety），工业控制网络安全（Security）的目标是防范和抵御攻击者通过恶意行为而人为制造生产事故、损害或伤亡。可以说，没有工业控制网络安全就没有工业控制系统的生产安全。只有保证了系统不遭受恶意攻击和破坏，才能有效地保证生产过程的安全。虽然工业控制网络安全问题同样是由各种恶意攻击造成的，但是工业控制网络安全的问题与传统 IT 网络的安全问题存在很大差异。

## 1.3 工业控制网络安全现状

本节首先罗列一些近年来发生的典型工业控制网络安全事件，然后简要介绍

国际、国内的工业控制系统安全标准体系。

### 1.3.1 典型工业控制网络安全事件

近年来，随着“两化融合”的深入，工业控制系统安全漏洞持续增长，针对工业控制网络的攻击行为也出现大幅增加，工业控制网络安全问题变得日益严重。

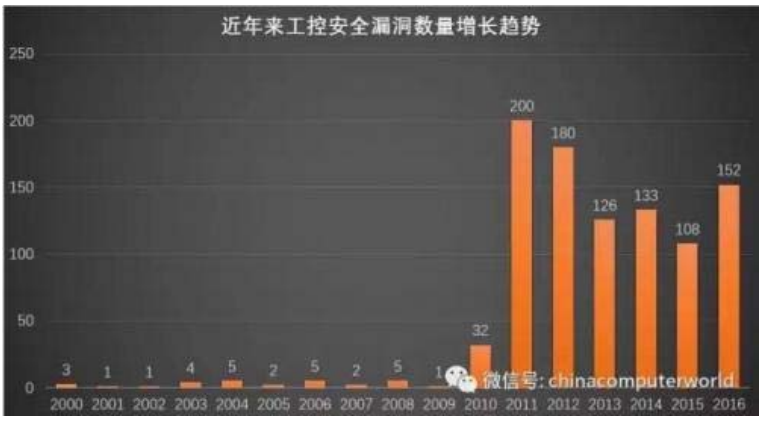


图 1.3 工业控制系统漏洞增长趋势

根据权威机构中国国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）2016 年发布的数据，工业控制系统漏洞在 2010 年之后却始终处于增长态势，如图 1.3 所示。

2014 年美国 ICS-CERT 所公布的数据中，工业控制安全事件达 632 件，而且多集中于能源行业（59%）和关键制造业（20%）。由此可见，工业控制网络正面临非常严重的安全威胁。近年来，典型工业控制网络安全问题出现在能源、水利、交通运输、生产制造等多个行业。

- 能源行业

2000 年，俄罗斯政府声称黑客成功控制了属于 GAzprom 公司的世界最大的天然气输送管道网络。

2001 年，黑客入侵了监管加州多数电力传输系统的独立运行商。

2003 年，美国俄亥俄州 Davis-Besse 的核电厂控制网络内的一台计算机被微软的 SQL Server 蠕虫所感染，导致其安全监控系统停机将近 5 小时。

2007 年，美国国土安全局的“Aurora”演习中，针对电力控制系统进行渗透测试，一台发电机在其控制系统遭到攻击后被物理损坏。

2010 年，“网络超级武器”Stuxnet 病毒针对性地侵入工业控制系统，严重

威胁到伊朗布什尔核电站核反应堆的安全运营。

2012 年，伊朗石油部和国家石油公司内部计算机网络遭受病毒攻击，为安全起见，伊朗方面暂时切断了海湾附近哈尔克岛石油设施的网络连接。

2014 年出现的 Havex 是一种专门感染 SCADA 控制系统中的控制软件的恶意软件，它先后攻击了欧、美地区的一千多家能源企业。除此之外，黑客们可通过 Havex 成功访问到能源行业的工业控制系统。

2015 年 12 月 23 日，乌克兰电力网络遭受 BlackEnergy 攻击，这是首个针对电网的成功攻击案例，导致数十万用户断电数小时。

2017 年 6 月 12 日，安全厂商 ESET 公布一款针对电力变电站系统实施恶意攻击的工控网络攻击武器 win32/Industroyer，它可以直接控制断路器，导致变电站断电。

- 水利和水处理行业

2000 年，澳大利亚一名工程师在应聘一家污水处理厂多次被拒绝后，远程侵入了该厂的污水处理控制系统，恶意造成污水处理泵站的故障，导致超过一千立方米的污水被直接排入河流，导致严重环境污染。

2001 年，澳大利亚的一家污水处理厂由于内部工程师的多次网络入侵，该厂发生了 46 次控制设备功能异常事件。

2005 年，美国水电溢坝事件。

2006 年，黑客从 Internet 攻破了美国哈里斯堡的一处污水处理厂的安全措施，在其系统内植入了能够硬性污水处理操作的恶意程序。

2007 年，攻击者侵入加拿大的一个水利 SCADA 控制系统，通过安装恶意软件破坏了用于控制从 Sacramento 河调水的控制计算机。

2011 年，黑客通过 Internet 操纵美国伊利诺伊州城市供水系统 SCADA，使得其控制的对泵遭到破坏。

- 交通运输行业

2003 年，CSX 运输公司的计算机系统被病毒感染，导致华盛顿特区的客货运输中断。

2003 年，19 岁的 Aaron Caffrey 侵入 Houston 渡口的计算机系统，导致该系统停机。

2008 年，攻击者入侵波兰某城市的地铁系统，通过电视遥控器改变轨道扳道器，导致四节车厢脱轨。

- 生产制造行业

2005 年，在 Zotob 蠕虫安全事件中，尽管在 Internet 与企业网、控制网之间部署了防火墙，还是有 13 个美国汽车厂由于被蠕虫感染而被迫关闭，5 万生产工人被迫停工，经济损失超过 140 万美元。

2010 年我国某石化厂，2011 年某炼油厂的某装置控制系统分别感染 Conficker 病毒，造成了控制系统服务器与控制器通信不同程度的中断。

2014 年，某钢铁厂遭到攻击，攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，造成重大破坏。

- 其他

2011 年，微软警告称最新发现的 Duqu 病毒可以从工业控制系统制造商那里收集情报数据。

2012 年，发现攻击多个中东国家的恶意程序 Flame 火焰病毒，他能收集各行业的敏感信息。

### 1.3.2 工业控制系统安全标准体系

国际上，研究工业控制系统安全的标准化组织有：国际电工委员会（IEC，International Electro Technical Commission）、国际自动化协会（ISA，the International Society of Automation）、美国国家标准技术研究院（NIST，National Institute of Standards and Technology），以及各个国家的标准化组织和行业协会。根据 Teodor Sommestad 等人对工业控制相关标准指南进行的总数比较以及欧洲网络和信息安全局（ENISA）的报告，将工业控制系统安全相关标准、规范、指南总结如表 1.3 所示。

表 1.3 国际相关标准

| | 组织名称 | 文件名称 | 文件类型 |
|---|---|---|---|
| 国际组织 | 国际电工委员会（IEC） | 电力系统控制和相关通信：数据和通信安全（IEC62210） | 标准 |
| | | 工业过程测量和控制的安全性-网络和系统安全（IEC62443） | 标准 |
| | 仪表系统与自动化学会（ISA） | 生产控制系统安全 | 标准&指南 |

| | | | |
|---|---|---|---|
| 美国 | 国家标准技术研究所（NIST） | 工业控制系统安全指南（NISTSP800-82）. | 指南 |
| | | 联邦信息系统和组织的安全控制建议（NISTSP800-53） | 指南 |
| | | 系统保护轮廓 - 工业控制系统（NISTIR7176） | 指南 |
| | | 中等健壮环境下的 SCADA 系统现场设备保护概况 | 指南 |
| | | 智能电网安全指南（NISTIR7628） | 指南 |
| | 北美电力可靠性委员会（NERC） | 北美大电力系统可靠性规范（NERCCIP002–009） | 规范 |
| | 美国天然气协会（AGA） | SCADA 通信的加密保护（AGAReportNo.12） | 标准 |
| | 美国石油协会（API） | 管道 SCADA 安全（API1164） | 指南 |
| | | 石油工业安全指南 | 指南 |
| | 美国能源部（DOE） | 提高 SCADA 系统网络安全 21 步 | 指南 |
| | 国土安全部（DHS） | 中小规模能源设施风险管理核查事项 | 指南 |
| | | 控制系统安全一览表：标准推荐 | 指南 |
| | | SCADA 和工业控制系统安全 | 指南 |
| | 美国核管理委员会 | 核设施网络安全措施（RegulatoryGuide5.71） | 指南 |
| 英国 | 英国国家基础设施保护中心（CPNI）和美国国土安全部（DHS）联合发布 | 工业控制系统安全评估指南 | 指南 |
| | | 工业控制系统远程访问配置管理指南 | 指南 |
| | 英国国家基础设施保护中心（CPNI） | 过程控制和 SCADA 安全指南 | 指南 |
| | | SCADA 和过程控制网络的防火墙部署 | 指南 |
| 荷兰 | 国际仪器用户协会（WIB） | 过程控制域（PCD）–供应商安全需求 | 法规 |
| 法国 | 国际大型电力系统委员会（CIGRE） | 电气设施信息安全管理 | 指南 |
| 德国 | 国际工业流程自动化用户协会（NAMUR） | 工业自动化系统的信息技术安全：制造工业中采取的约束措施（NAMURNA115） | 指南 |
| 挪威 | 挪威石油工业协会（OLF） | 过程控制、安全和支撑 ICT 系统的信息安全基线要求（OLFGuidelineNo.104） | 指南 |
| | | 工程，采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施（OLFGuidelineNo.110） | 指南 |
| 瑞典 | 瑞典民防应急局（MSB） | 工业控制系统安全加强指南 | 指南 |

## 1.112 国内标准

目前，我国从事工业控制系统信息安全标准化工作的组织有：全国信息安全标准化技术委员会（TC260）、全国电力系统管理及其信息交换标准化技术委员会（TC82）、全国工业过程测量和控制标准化技术委员会（TC124）、全国电力监管标准化技术委员会（TC296）。截止到 2013 年初，发布的标准、规范如表 1.4 所示。

表 1.4 国内相关标准

<table>
<tr><td colspan="2">全国信息安全标准化技术委员会（TC260）</td><td colspan="2">全国电力系统管理及其信息交换标准化技术委员会（TC82）</td></tr>
<tr><td rowspan="2">在编</td><td>《SCADA 系统安全控制指南》</td><td rowspan="4">发布</td><td>《数据和通信安全第 1 部分：通信网络和系统安全安全问题介绍》（GB/Z 25320.1-2010）</td></tr>
<tr><td>《安全可控信息系统（电力系统）安全指标体系》</td><td>《数据和通信安全第 3 部分：通信网络和系统安全包括 TCP/IP 的协议集》（GB/Z 25320.3-2010）</td></tr>
<tr><td rowspan="4">计划</td><td>《工业控制系统安全管理基本要求》</td><td>《数据和通信安全第 3 部分：通信网络和系统安全包括 MMS 的协议集》（GB/Z 25320.4-2010）</td></tr>
<tr><td>《工业控制系统安全检查指南》</td><td>《数据和通信安全第 3 部分：通信网络和系统安全 IEC 61850 的安全》（GB/Z 25320.6-2010）</td></tr>
<tr><td>《工业控制系统测控终端安全要求》</td><td colspan="2">全国工业过程测量和控制标准化技术委员会（TC124）</td></tr>
<tr><td>《工业控制系统安全防护技术要求和测评方法》</td><td>在编</td><td>《工业控制计算机系统通用规范第 2 部分：工业控制计算机的安全要求》</td></tr>
<tr><td>《工业控制系统安全分级指南》</td><td rowspan="4">计划</td><td>《通信网络-网络和系统安全-第 2-1 部分：建立工业自动化和控制系统信息安全程序》（等同采用 IEC 62443-2-1）</td></tr>
<tr><td colspan="2">全国电力监管标准化技术委员会（TC296）</td><td>《工业控制系统信息安全第 1 部分：评估规范》</td></tr>
<tr><td rowspan="3">在编</td><td>《电力二次系统安全防护标准》（强制）</td><td>《工业控制系统信息安全第 2 部分：验收规范》</td></tr>
<tr><td>《电力信息系统安全检查规范》（强制）</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>《电力行业信息安全水平评价指标》（推荐）</td></tr>
</table>

# 第一部分：走近工业控制系统的禁区

# 第二章 SCADA 系统和 DCS 系统

## 2.1 SCADA 系统

本节将重点介绍什么是 SCADA 系统以及 SCADA 系统的软硬件组成和系统结构。

### 2.1.1 SCADA 系统介绍

SCADA 系统指的是监视控制与数据采集系统，它是一种大规模的分布式系统，用来控制和管理地理位置广域分布的资产，这些资产一般分散在数千平方米的范围内。在工业生产过程中，中央数据采集和集中控制对整个系统运行而言非常重要，SCADA 系统通常具备这种能力，并广泛应用在供水工程、污水处理、石油和天然气管网、电力系统和轨道交通系统中。

SCADA 系统控制中心集中监视和控制远距离通信网络中的野外现场节点设备，包括告警信息和过程状态数据等。中央控制中心依靠从远程站点获取的信息，生成自动化的或者过程驱动型的监视指令并发送至远程站点，以实现对远程装置的实时控制，这类远程装置就是工业领域的对现场设备的操作，类似阀门和断路器的开启/关闭、传感器数据采集和现场环境监视报警等本地作业。

### 2.1.2 SCADA 系统架构

SCADA 系统主要由一系列远程终端单元（RTU）和中心控制主站系统组成，RTU 收集现场数据，并通过通信系统回送反馈数据给主站，主站显示这些采集到的数据并允许操作员执行过程控制任务。准确的、实时的数据可以用于优化机械设备的运行和操作工序。其他的优势包括更高效、更可靠等，最重要的还是可以确保完成各类安全操作，由此带来了比早期自动化系统更低廉的运行成本。

SCADA 系统在硬件方面基本包含五个层次或等级：

- 现场层次的测量仪器、仪表和控制装置；
- 信号分组终端和 RTU；
- 通信系统；

- 主站；
- 企业内部数据处理机构的后台计算机系统。

RTU 为分布于每一个远程现场模拟传感器或数字传感器提供了一种连接接口。

通信系统为主站系统和远程站点之间的通信提供了通道。这种通信系统可以是电力线载波、光纤、短波/超短波、电话线、微波乃至卫星通信。此外，专用协议和纠错机制被设计用来保证高效和高质的数据传输。

主站（或分布式主站）从各种 RTU 采集数据，并且大多数情况下都提供一种操作接口用来显示信息和控制远程站点。在大型遥测系统中，分布式主站从远方站点汇集信息并将这些信息中继传输给中央控制中心。

软件方面，SCADA 系统软件分为两类，即专用的商用软件和开源软件。大型企业为其自身的硬件系统定制开发专用软件，这类系统通常称为“总控键”解决方案。在工业自动控制领域，“总控键”解决方案面临的最大问题是用户对系统提供商具有巨大的依赖性和不可替代性。开源软件系统由于给整个系统带来了协同互操作性，从而得到广泛应用。协同互操作能力使得许多不同制造厂商的设备可以集成到同一个大型系统中。Citect 和 WonderWare 是在 SCADA 系统市场上普遍使用的两种开源软件包。

SCADA 系统软件的要素包括：

- 用户界面；
- 图形显示模块；
- 告警模块；
- 趋势分析模块；
- RTU 或 PLC 接口；
- 升级模块；
- 数据访问模块；
- 数据库；
- 网络模块；
- 纠错和冗余设计；
- 客户端/服务器的分布式处理流程。

最初的 SCADA 系统通过测量仪表、信号灯、条带录音机等采集数据，监视控制功能则由操作员手动控制各种球形手柄完成。这类设备至今仍然在重型机械厂、加工车间和大型发电系统中完成监视控制和数据采集功能。如图 2.1 展示了传感器使用 4~20mA 电缆连接控制面板的一种 SCADA 系统结构。虽然第一代 SCADA 系统具有结构简单，成本低廉的优点，但是也存在对人员依赖程度高，无法适应大规模系统、管理困难的突出缺陷。

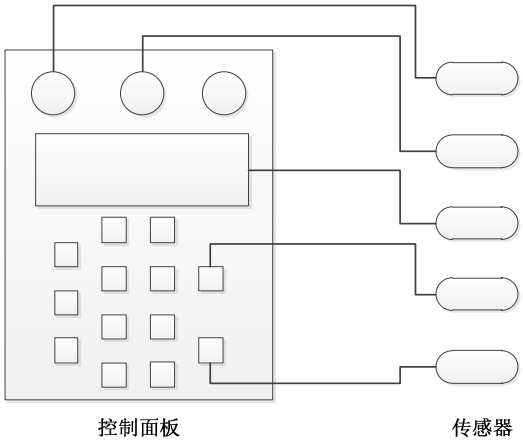


图 2.1 第一代 SCADA 系统结构

CPU 和其他电子设备的出现后，SCADA 系统制造商开始将数字电子元器件作为继电器逻辑器件的一部分。可编程逻辑控制器（PLC）是目前工业部门使用最广泛的控制器件。随着工厂车间监视和控制更多设备的需求不断增长，PLC 逐步发展为分布式系统，并且变得越来越智能化、小型化。如图 2.2 展示了计算机使用现场总线连接 PLC 和 DHC（分布式控制系统）监控传感器的 SCADA 系统结构。

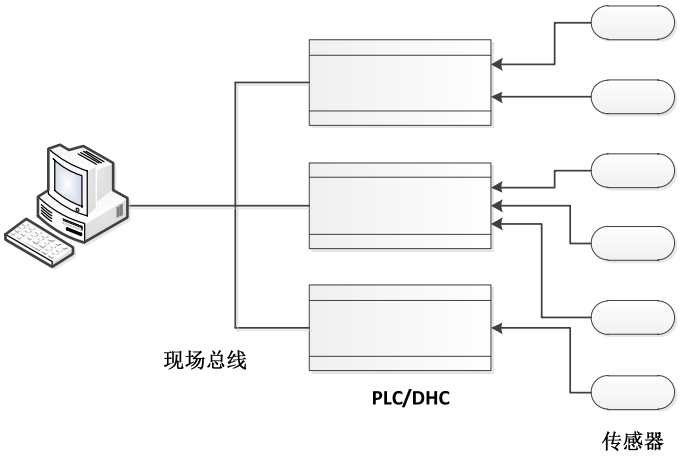


图 2.2 PLC/DCS 型 SCADA 系统结构

PLC/DCS 型 SCADA 系统的优点如下：

- 计算机可以记录并存储海量数据；

- 数据可以根据用户需求的任何形式显示；
- 地理空间分布很广的成千上万只传感器能够被连接到统一系统中；
- 操作人员可以在系统中进行实时数据模拟；
- 多种类型的数据可以通过 RTU 进行收集；
- 数据可以在任何地方查看，不限于工业现场。

PLC/DCS 型 SCADA 系统的缺点包括：

- PLC/DCS 型 SCADA 系统相对于第一代控制面板型 SCADA 系统更加复杂；
- 开发 PLC/DCS 型 SCADA 系统需要多种不同的技术人员，如系统分析人员和程序开发人员；
- 如果连接成千上万个传感器，仍然需要很多线缆，管理困难；
- 操作人员只能看到 PLC 层次的内容；

随着工业界对小型化、智能化系统需求的不断增长，新型传感器越来越多地使用智能 PLC 和 DCS。这些设备被称为智能电子装置（Intelligent Electronic Device, IED）。IED 通过 Profibus、DeviceNet 或 Foundation Fieldbus 等现场总线与 PC 连接，如图 2.3 所示。这种智能电子装置具有足够的智能处理能力来获取数据，与其他设备通信并具有独立的程序模块。每一台智能传感装置的硬件主板上具有不止一种传感器。典型的 IED 装置可以将模拟输入传感器、模拟输出传感器、比例-积分-微分（Proportion-Integral-Differential, PID）控制器、通信系统和程序存储器集成在同一个设备中。

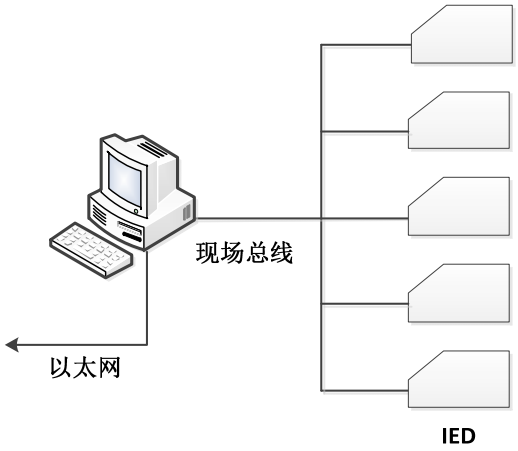


图 2.3 IED 型 SCADA 系统结构

IED 型 SCADA 系统的优势如下：

- 所需的连接线缆最少；

- 操作人员可以直接观测到传感器层次的底层信息；
- 从 IED 获取的数据将包括类似串口数量、模型数量等现场设备自身配置参数；
- 所有装置支持即插即用，因此安装和更换零件更加容易；
- 更小型化的装置意味着将为数据采集系统节省更多空间。

IED 型 SCADA 系统的缺点则包括：

- 更加先进的系统需要具备更多专业知识的用户；
- 传感器自身成本提高；
- IED 的可靠性更多依赖通信系统。

## 2.2 DCS 系统

本节主要介绍分布式控制系统的相关知识，包括基本概念，组成和系统架构。

### 2.2.1 DCS 系统介绍

DCS 是指分布式控制系统，也被称为集散式控制系统，是工业控制系统的重要组成部分。DCS 是一个由过程控制级和过程监控级组成的以通信网络为纽带的多级计算机系统，综合了计算机、通信、终端显示和控制技术发展起来的新型控制系统。其基本思想是分散控制、集中操作、分级管理、配置灵活以及组态便捷。它满足了大型工业生产和日益复杂的过程控制需求，从综合自动化的角度出发，按功能分散、管理集中的原则构思，采用了多层分级、合作自治的结构形式。

DCS 网络是 DCS 的基础和核心，它对 DCS 的实时性、可靠性和可扩展性起着决定性作用。因此，对于 DCS 网络而言，它必须满足实时性的要求，即在确定的时间限度内完成信息的传输。这里所说的“确定”的时间限度，是指无论在任何情况下，信息传送都能在这个时间限度内完成，而这个时间限度则是根据被控制过程的实时性确定的。所以衡量系统网络性能的指标不是网络的速率，即通常所说的每秒比特数（bit/s），而是系统网络的实时性，即能在多长的时间内确保所需信息的传输得以完成。

DCS 具有如下特点。

- 高可靠性

DCS 采用容错设计，当某一台计算机出现故障时并不会导致系统丧失其他功能。此外，由于系统中各台计算机所承担的任务比较单一，因此可以针对需要实现的功能采用具有特定结构和软件的专用计算机，从而提高系统中每台计算机的可靠性。

- 开放性

DCS 采用开放式、标准化、模块化和系列化设计，系统中各台计算机采用局域网方式通信，实现信息传输，当需要改变或者扩充功能时，可将新增加计算机方便地连入系统通信网络或从网络中卸下，几乎不影响系统其它计算机的工作。

- 灵活性

通过组态软件根据不同的流程应用对象进行软硬件组态，即确定测量与控制信号及相互间连接关系，从控制算法库选择适用的控制规律以及从图形库调用基本图形组成所需的各种监控和报警画面，从而方便地构成所需的控制系统。

- 易于维护

功能单一的小型或微型专用计算机，具有维护简单、方面的特点，当某一局部或某个计算机出现故障时，可以在不影响整个系统运行的情况下在线更换，迅速排除故障。

- 协调性

各工作站之间通过通信网络传送各种数据，整个系统信息共享，协调工作，以完成控制系统的总体功能和优化处理。

- 控制功能齐全

控制算法丰富，集连续控制、顺序控制和批处理控制于一体，可实现串级、前馈、解耦、自适应和预测控制等先进控制，并可方面地加入所需的特殊控制算法。

### 2.2.2 DCS 系统架构

DCS 是以微处理器和网络作为基础的集中分散型控制系统。它包括操作员站、工程师站、监控计算机、现场控制站、数据采集站。通信系统。DCS 的基本构成如图 2.4 所示。

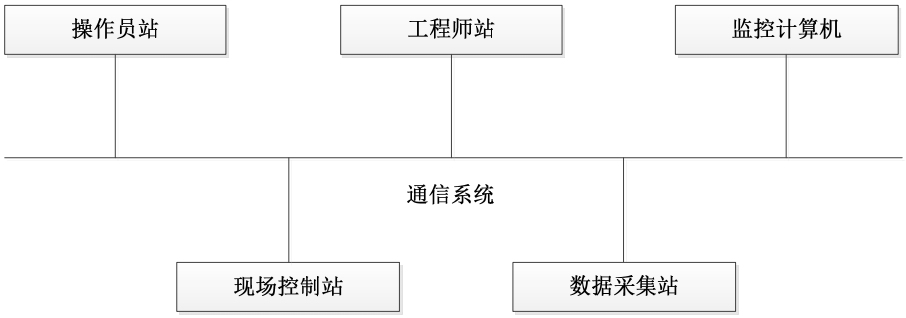


图 2.4 DCS 的基本构成

- 操作员站

操作员站是操作人员对生产过程进行显示、监视、操作控制和管理的主要设备。操作员站提供了良好的人机交互界面，用以实现集中监视、操作和信息管理等功能。在一些小型 DCS 系统中，操作员站兼具工程师站的功能，在操作员站上也可以进行系统组态和维护的部分或者全部工作。

- 工程师站

工程师站用于对 DCS 进行离线的组态工作和在线系统监督、控制与维护。工程师能够借助于组态软件对系统进行离线组态，并在 DCS 在线运行时，可以实时地监视通信网络上各工作站的运行情况。

- 监控计算机

监控计算机通过网络收集系统中各个单元的数据信息，根据数学模型和优化控制指标进行后台计算，优化控制等，他还用于全系统信息的综合管理。

- 现场控制站

现场控制站通过现场仪表直接与生产过程相连接，采集过程变量信息，并进行转换和运算等处理，产生控制信号来驱动现场的执行机构，最终实现对生产过程的控制。现场控制站可以控制多个回路，具有极强的运算和控制功能，能够自主地完成回路控制任务，实现反馈控制、逻辑控制、顺序控制和批量控制等功能。

- 数据采集站

数据采集站与生产过程相连接，对过程非控制变量进行数据采集和预处理，并对实时数据进一步加工；为操作员站提供数据，实现对过程的监视和信息存储，为控制回路的运算提供辅助数据和信息。

- 通信系统

通信系统连接 DCS 的各种操作员站、工程师站、监控计算机、现场控制站、

数据采集站等部分，传递各工作站之间的数据、指令及其他信息，使整个系统协调一致地工作，从而实现数据和信息资源的共享。

DCS 自下而上通常分为控制级、监控级和管理级，每级之间分别由控制网络（Control Net, Cnet）、监控网络（Supervision Net, Snet）、管理网络（Management Net, Mnet）把相应的设备连接在一起，进行数据和命令的传输。DCS 的系统结构如图 2.5 所示。

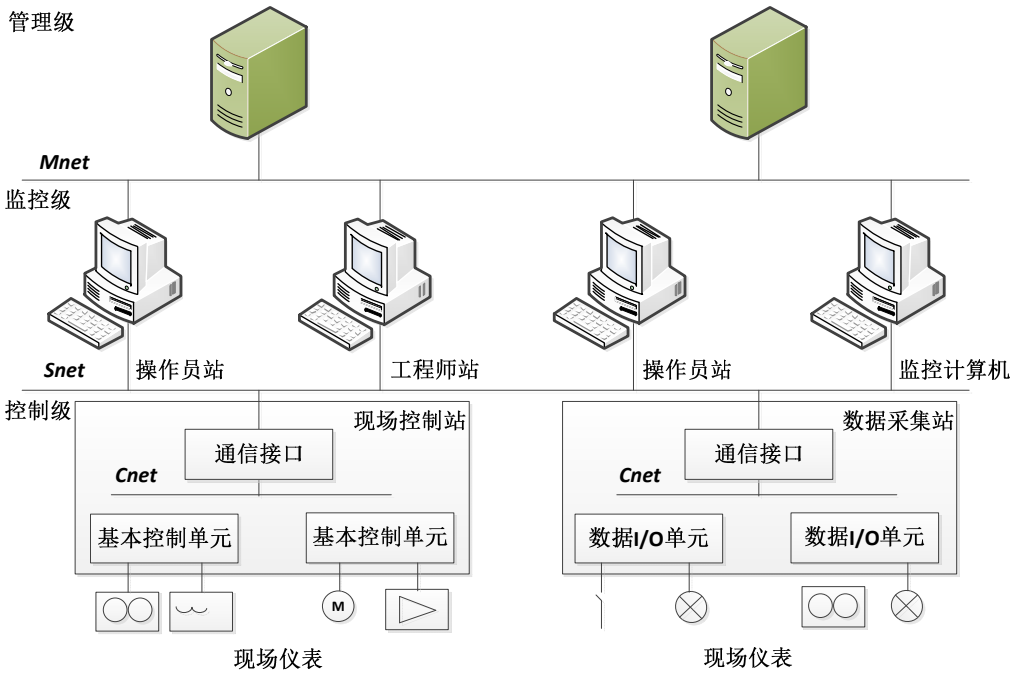


图 2.5 DCS 的系统结构

# 第三章 PLC 设备技术原理

控制器（Controller）是指按照预定顺序通过改变主电路或控制电路的接线和改变电路中电阻值来控制电动机的启动、调速、制动和反向的主令装置，是发布命令的“决策机构”，完成协调和指挥整个计算机系统的操作。在工业控制系统中，常见的控制器有可编程逻辑控制器（PLC）、可编程自动化控制器（PAC）、远程终端单元（RTU）等。

本章将重点介绍 PLC 设备，包括其基本组成和工作原理，以及其通信技术。

## 3.1 PLC 设备介绍

在 PLC 问世之前，继电器控制在工业领域占主导地位。继电器控制系统采用固定接线的硬件实现控制逻辑，如果生产任务生产任务或者工艺发生变化，就必须重新设计和改变硬件结构，这样就会造成时间和资金的浪费。另外，大型控制系统用继电器、接触器控制，使用的继电器数量多、体积大、功耗大，且继电器触电为机械触点，工作频率较低，在频繁动作情况下寿命较短，容易造成系统故障，系统的可用性差。

1968 年，美国最大的汽车制造商通用汽车公司（GM 公司）为了适应汽车型号不断翻新的需求，以求在激烈竞争中占得优势地位，提出以一种新型的控制器装置取代继电器、接触器控制装置，并且对未来的新型控制装置做出了具体的设想——利用计算机的完备功能，以及灵活性、通用性好等优点，要求新的控制装置编程简单，即使不熟悉计算机的人员也能够很快掌握它的使用技术。为此还拟定了以下公开招标的 10 条技术要求：

- 编程简单方便，可在现场修改程序。
- 硬件维护方便，采用插件式结构。
- 可靠性高于继电器、接触器控制装置。
- 体积小于继电器、接触器控制装置。
- 可将数据直接送入计算机。
- 用户程序存储器容量至少可以扩展到 4KB。
- 输入可以是交流 115V。

- 输出为交流 115V，能直接驱动电磁阀、交流接触器等。
- 通用性强，扩展方便。
- 成本上可以与继电器、接触器控制系统竞争。

美国数字设备公司（Digital Equipment Corporation, DEC）根据 GM 公司的招标技术要求，于 1969 年研制出世界上第一台可编程控制器，并在 GM 公司汽车自动装配生产线上使用且取得成功。其后，日本、德国相继引入这项新技术，可编程控制器由此迅速发展起来。

PLC 综合了继电器、接触器控制以及计算机灵活、方便的优点而设计、制造和发展的，因此与其他控制器相比，PLC 具有以下 8 个方面的优点。

- 高可靠性

PLC 所有的 I/O 接口电路均采用光电隔离，使工业现场的外电与 PLC 内部电路之间电气隔离。PLC 各个输入端均采用 R-C 滤波器，其滤波时间常数一般为 10~20ms。PLC 各模块均采用屏蔽措施，以防止辐射干扰。PLC 还采用了良好的开关电源，并对所有元器件进行严格的筛选。此外，PLC 还有良好的自诊断功能，一旦电源或其他软、硬件发生异常情况，CPU 立即采用有效措施，以防止故障扩大。大型 PLC 还可以采用由双 CPU 构成冗余系统或者由三 CPU 构成表决系统，使得可靠性进一步提高。

- 通用性强，方便使用

PLC 产品已经系列化和模块化，PLC 的开发制造商为用户提供了品种齐全的 I/O 模块和配套部件。用户在进行控制系统设计时，不需要自己设计和制作硬件装置，只需要根据控制要求进行模块的配置。用户所做的工作只是设计满足控制对象控制要求的应用程序。对于一个控制系统，当控制要求改变时，只需要修改程序就能变更控制功能

- 采用模块化结构，系统组合灵活方便

为了适应各种工业控制，需要除了单元式的小型 PLC 以外的绝大多数 PLC 均采用模块化结构。PLC 的各种部件包括 CPU、电源、I/O 等均采用模块化设计，由机架以及电缆将各模块连接起来，系统的规模和功能可根据用户的需要自行组合。

- 编程语言简单易学，便于掌握

PLC 是由继电器、接触器控制系统发展而来的一种新型的工业自动化控制装置，其主要使用对象是广大的电气技术人员。为使工程技术人员方便学习和掌握 PLC 的编程，PLC 的开发制造商采用了与继电器、接触器控制原理相似的梯形图语言。

- 系统设计周期短

系统硬件的设计任务仅仅是根据对象的控制要求配置适当的模块，而不是去设计具体的接口电路，这样大大缩短了整个设计所花费的时间，加快了整个工程的进度。

- 对生产工艺改变适应性强

PLC 的核心部件是微处理器，它实际是一种工业控制计算机，其控制功能是通过软件编程来实现的。当生产工艺发生变化时，不必改变 PLC 硬件设备，只需改变 PLC 中的程序，这对现代化的小批量、多品种的生产尤其合适。

- 安装简单，调试方便，维护工作量小

PLC 控制系统的安装接线工作量比继电器、接触器控制系统少得多，只需要将现场的各种设备与 PLC 相应的 I/O 端相连。PLC 软件设计和调试大多可在实验室进行，用模拟实验开关代替输入信号，其输出状态可观察 PLC 上相应的发光二极管，也可以另接模拟实验板。模拟调试好后，再将 PLC 控制系统安装到现场，进行联机调试，这样既节省时间又很方便。PLC 本身的可靠性高，又有完善的自诊断功能，一旦发生故障，可以根据报警信息，迅速查明原因。如果 PLC 本身发生故障，则可用更换模块的方法排除故障。这样提高了维护的工作效率，以保证生产的正常进行。

- I/O 接口模块丰富

PLC 针对不同的工业现场信号（如交流和直流、开关量和模拟量、电压和电流、脉冲或电位和强电或弱电等）有相应的 I/O 模块与工业现场的器件或设备（如按钮、行程开关、接近开关、传感器及送变器、电磁线圈和控制阀）直接连接。另外为了提高操作性能，它还有多种人机对话的接口模块；为了组成工业局部网络，它还有多种通信联网的接口模块，等等。

随着大规模集成电路技术的迅猛发展，功能更强大、规模不断扩大而价格日趋低廉的元器件不断涌现，促成 PLC 产品亦随之功能大增但成本下降。目前 PLC

的应用已经远远超越了早期仅用于开关量控制的局面，其应用领域主要包括以下5个方面。

- 开关量逻辑控制

这是PLC最广泛的应用。开关量逻辑控制已经逐步取代传统的继电器逻辑控制装置，被应用于单机或者多机控制系统以及自动生产线上。PLC控制开关量的能力非常强，所以控制的入、出点数有时可多达几万点。由于可以联网，所以点数几乎不受限制。所控制的如组合的、时序的、要考虑延时的、需要进行高速计数等的逻辑问题都可以解决。

- 运动控制

目前许多厂商已经开发出大量的运动控制模块，且功能是给步进电动机或者伺服电动机等提供单轴或多轴的位置控制，并在控制中满足适当的速度和加速度，以保证运动的平滑水准。

- 过程控制

当前PLC产品中，还有一大类是针对生产过程参数，如温度、流量、压力、速度等的检测和控制而设计的。常用的有模拟量I/O模块，通过这些模块不仅可以实现A/D和D/A转换，还可以进一步构成闭环，实现PID一类的生产过程调节。而针对PID闭环调节，又有专门的模块，可以更方便地实施。这些产品往往还引入了智能控制。

- 数据处理

现代的PLC已具有数据传送、排序、查表搜索、位操作以及逻辑运算、函数运算、矩阵运算等多种数据采集、分析、处理功能。目前还有不少公司，将PLC的数据处理功能与计算机数值控制（CNC）设备的功能紧密结合在一起，开发了用于CNC的PLC产品。

- 通信

随着网络的发展和计算机集散控制系统的逐步普及，PLC的网络化通信产品也在大量被推出。这些产品解决了PLC之间、PLC与其扩展部分之间、PLC与上级计算机之间或其他网络间的通信问题。

需要注意的是，并非所有PLC都具有上述全部功能，越小型的PLC其功能相应也越少。

## 3.2 PLC 设备基本组成和工作原理

本节将介绍 PLC 设备的基本组成和工作原理。

### 3.2.1 基本组成

典型 PLC 的组成如图 3.1 所示，分别是中央处理单元（CPU）、存储器、输入/输入（I/O）模块、电源和编程器，下面将对其进行详细介绍。

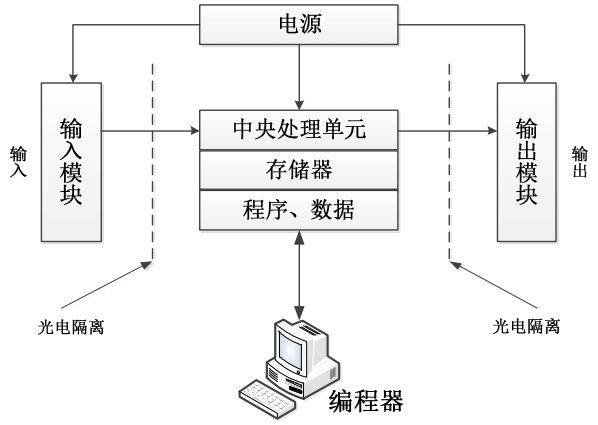


图 3.1 PLC 的组成结构示意图

- 中央处理单元

中央处理单元是 PLC 的控制中枢。它按照 PLC 系统程序赋予的功能接收并存储从编程器键入的用户程序和数据：检查电源、存储器、I/O 以及警戒定时器的状态，并能诊断用户程序中的语法错误，当 PLC 投入运行时，首先它以扫描的方式接收现场各输入装置的状态和数据，并分别存入 I/O 映像区，然后从用户程序存储器中逐条读取用户程序，经过命令解释后将按照指令规定执行的逻辑或算数运算结果送入 I/O 映像区或数据寄存器内。等所有的用户程序执行完毕之后，最后将 I/O 映像区的各种输出状态或输出寄存器内的数据传送到相应的输出装置，如此循环运行，直到停止运行。

为了进一步提高 PLC 的可靠性，近年来对大型 PLC 还采用双 CPU 构成的冗余系统，或者采用三 CPU 的表决式系统。这样，即使某个 CPU 出现故障，整个系统仍能正常运行。

- 存储器

存放系统软件的存储器成为系统程序存储器，存放应用程序软件的存储器称

为用户程序存储器。

PLC 常见的存储器类型主要有 RAM、EPROM 和 EEPROM。RAM（Random Access Memory）是一种读/写存储器（随机存储器）。用户可以用编程器读出 RAM 中的内容，也可以将用户程序写入 RAM。它是易失性的存储器，将它的电源断开后存储器的信息将会丢失。EPROM（Erasable Programmable Read Only Memory），是一种可擦除的只读存储器，在断电情况下存储器内的所有内容保持不变（在紫外线连续照射下可以擦除存储器内容）。EEPROM（Electronic Erasable Programmable Read Only Memory），是一种电可擦除的只读存储器。使用编程器就能够很容易地对其所存储的内容进行修改。

关于 PLC 的存储空间分配，虽然各种 PLC 的 CPU 的最大寻址空间各不相同，但是根据 PLC 的工作原理其存储空间一般包括以下 3 个区域：系统程序存储区、系统 RAM 存储区（包括系统 I/O 映像区和系统软设备区）和用户程序存储区。

系统程序存储区中存放着相当于计算机操作系统的系统程序，包括监控程序、管理程序、命令解释程序、功能子程序、系统诊断子程序等。这些都被制造厂商固化在 EPROM 中，用户不能直接存取。它们和硬件一起决定了该 PLC 的性能。

系统 RAM 存储区包括系统 I/O 映像区和系统中各类软设备（如逻辑线圈、数据寄存器、计数器、计时器、变址寄存器、累加器等存储器存储区）。

由于 PLC 投入运行后，只是在输入采样阶段才依次读入各输入状态和数据，在输出刷新阶段才将输出状态和数据送至相应的外设。因此，它需要一定数量的存储单元（RAM）以存放 I/O 的状态和数据，这些单元即被称作 I/O 映像区。一个开关量 I/O 占用存储单元中的一个位（bit），一个模拟量 I/O 占用存储单元中的一个字（16bit）。因此整个 I/O 映像区可看作由两个部分组成：开关量 I/O 映像区和模拟量 I/O 映像区。

除了 I/O 映像区以外，系统 RAM 存储区还包括 PLC 内部各类软设备的存储区。该存储区又分为具有失电保持的存储区域和无失电保持的存储区域。前者在 PLC 断电时由内部的锂电池供电，数据不会丢失；后者当 PLC 断电时，数据被清零。与开关输出一样，每个逻辑线圈占用系统 RAM 存储区中的一位，但不能直接驱动外设，只供用户在编程中使用，其作用类似于电器控制线路中的继电器。另外，不同的 PLC 还提供数量不等的特殊逻辑线圈，具有不同的功能。与模拟量

I/O 一样，每个数据寄存器占用系统 RAM 存储区中的一个字（16bit）。另外，PLC 还提供数量不等的特殊数据寄存器，具有不同的功能。

用户程序存储区的区别在于它是用来存放用户编制的用户程序。不同类型的 PLC 其存储容量各不相同。

- 电源模块

电源模块为机架上的其他模块提供直流电源。PLC 的电源在整个系统中起着十分重要的作用。如果没有一个良好的、可靠的电源系统是无法正常工作的，因此 PLC 的制造商对电源的设计和制造也十分重视。一般交流电压波动在正负 10%或正负 15%范围内，可以不采用其他措施而将 PLC 直接连接在交流电网上。

### 3.2.2 工作原理

最初研制生产的 PLC 主要用于代替继电器、接触器构成的传统控制装置，但这两者的运行方式并不是相同的。继电器控制装置采用硬逻辑并行运行的方式，即如果这个继电器的线圈通电或断电，该继电器所有的触点（包括其常开或常闭触点）无论在继电器控制线路的哪个位置上都会立即同时动作。PLC 的 CPU 则采用顺序逻辑扫描用户程序的运行方式，即如果一个输出线圈或逻辑线圈被接通或断开，该线圈的所有触点（包括其常开或常闭触点）不会立即动作，必须等扫描到该触点时才会动作。

为了消除二者之间由于运行方式不同而造成的差异，考虑继电器控制装置各类触点的动作时间一般在 100ms 以上，而 PLC 扫描用户程序的时间一般均小于 100ms，因此，PLC 采用了一种不同于一般微型计算机的运行方式——扫描技术。这样，对于 I/O 响应要求不高的场合，PLC 与继电器控制装置的处理结果就没有什么区别了。

- 扫描技术

当 PLC 投入运行后，其工作过程一般分为 3 个阶段，即输入采样、用户程序执行和输出刷新 3 个阶段。完成上述 3 个阶段称作一个扫描周期。在整个运行期间，PLC 的 CPU 以一定的扫描速度重复执行上述 3 个阶段。

在输入采样阶段，PLC 以扫描方式依次读入所有输入状态和数据，并将它们存入 I/O 映像区中的相应单元内。输入采样结束后，转入用户程序执行和输出刷

新阶段。在这两个阶段中，即使输入状态和数据发生变化，I/O 映像区中的相应单元的状态和数据也不会改变。因此，如果输入是脉冲信号，则该脉冲信号的宽度必须大于一个扫描周期，才能保证在任何情况下该输入均能被读入。

在用户程序执行阶段，PLC 总是按由上而下的顺序依次扫描用户程序（梯形图）。在扫描每一条梯形图时，又总是先扫描梯形图左边的由各触点构成的控制线路，并按先左后右、先上后下的顺序对由触点构成的控制线路进行逻辑运算，然后根据逻辑运算的结果，刷新该逻辑线圈在系统 RAM 存储区中对应位的状态；或者刷新该输出线圈在 I/O 映像区中的对应位的状态；或者确定是否要执行该梯形图所规定的特殊功能指令。

也就是说，在用户程序执行过程中，只有输入点在 I/O 映像区内的状态和数据不会发生变化，而其他输出点和软设备在 I/O 映像区或系统 RAM 存储区内的状态和数据都有可能发生变化，而且排在上面的梯形图，其程序执行结果会对排在下面的凡是用到这些线圈或数据的梯形图起作用；相反，排在下面的梯形图，其被刷新的逻辑线圈的状态或数据只能到下一个扫描周期才能对排在其上面的程序起作用。

当扫描用户程序结束后，PLC 就进入输出刷新阶段。在此期间，CPU 按照 I/O 映像区内对应的状态和数据刷新所有的输出锁存电路，再经输出电路驱动相应的外设，这时才是 PLC 的真正输出。

一般来说，PLC 的扫描周期包括自动诊断、通信等，如图 3.2 所示，一个扫描周期等于自诊断、通信、输入采样、用户程序执行、输出刷新等所有时间的总和。

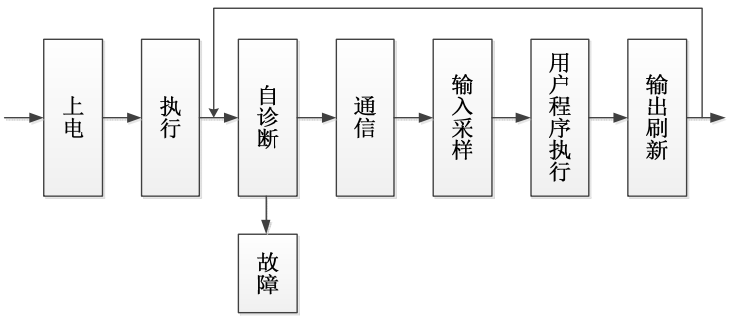


图 3.2 PLC 的扫描周期

- PLC 的 I/O 响应时间

为了增强 PLC 的抗干扰能力，提高其可靠性，PLC 的每个开关量输入端都采

用光电隔离等技术。

为了能实现继电器控制线路的硬逻辑并行控制，PLC 采用了不同于一般微型计算机的运行方式，即扫描技术。

上述两个主要原因，使得 PLC 的 I/O 响应比一般微型计算机构成的工业控制系统慢得多，其响应时间至少等于一个扫描周期，一般均大于一个扫描周期甚至更长。

所谓 I/O 响应时间指从 PLC 的某一输入信号变化开始到系统有关输出端信号的改变所需的时间。其最短的 I/O 响应时间与最长的 I/O 响应时间如图 3.3 和 3.4 所示。

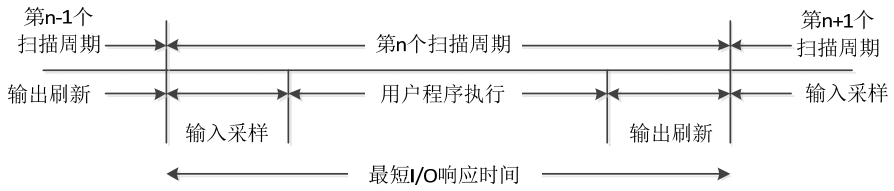


图 3.3 最短 I/O 响应时间

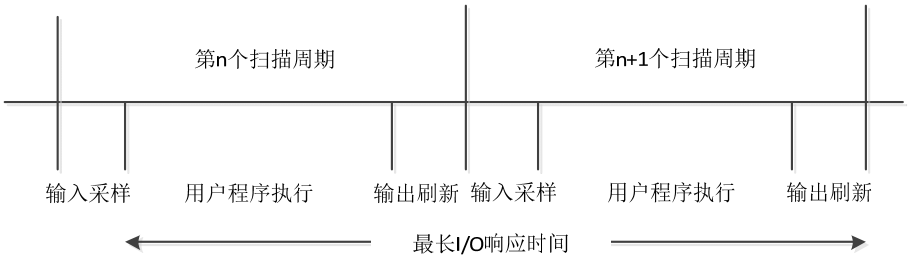


图 3.4 最长 I/O 响应时间

## 3.3 PLC 设备通信技术

PLC 设备的串行通信采用半双工异步传输模式，支持 CCM（Communications Control Module）通信协议，并具有以下功能：

- 上位通信功能
- 主站功能
- 一对一功能
- 无协议串行通信功能

这些功能可以实现 PLC 的寄存器和内部继电器的读入和写出、传送状态的跟踪等。由于 CCM 协议采用主从通信方式，所以通信过程中由主站保持主动权，

向子站发出呼叫，并通过向子站发送命令帧来控制数据传送的方向、格式和内容；子站对得到的主站呼叫做出响应，并根据命令帧要求进行数据传输。

数据传输过程以主站向子站写入数据为例，如图 3.5 所示，通信从主站向子站提出呼叫开始，子站做出应答从而建立连接，主站接到应答后，向子站发送首标，子站将依据首标各项要求与主站进行数据传输，在子站在此做出应答后，主站开始发送数据，数据以固定长度的分组方式进行传输，最后主站发送 EOF（End Of File）信息号结束本次通信。其中，首标作为命令帧，规定了数据传送方向、数据操作起始地址以及数据传输量等。

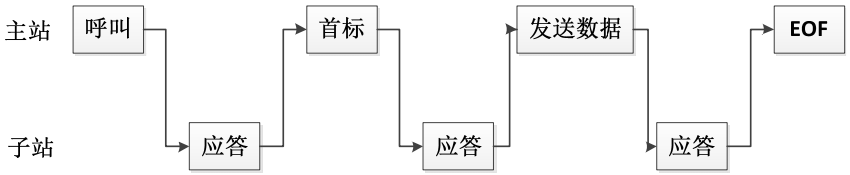


图 3.5 数据传输过程

在进行数据通信时，通信应答时间决定了系统读写速度，而作为主站的计算机通信时间因上位计算机类型、PC 扫描时间、PLC 数据通信模块应答延迟时间设定值、波特率、数据传送量的不同而不同。其中，PC 扫描时间与应答延迟时间对通信时间的影响为，当 PC 扫描时间比应答延迟时间短时，前者对通信时间没有影响；反之，当 PC 扫描时间比应答延迟时间长时，在计算总通信时间时，采用 PC 扫描时间，计算公式如下：

总通信时间=A+B+C+D

其中，A 为呼叫发送/应答时间，B 为首标发送/应答时间，C 为数据发送/应答时间，D 为通信结束应答时间。

以数据发送时间为例：

数据发送时间=数据传送字符数*通信时间/字符+PC 扫描时间

数据通信中，数据传送量因采用的传送方式不同而不同。传送方式支持 ASCII 码和二进制两种。其中 ASCII 码是用 8 位表示数字、字母等，因此采用它来进行数据通信时，一字节二进制数要由两字节 ASCII 码来表示，实际传输量就是采用二级制数据通信的两倍。而在某些要求较高的可靠性和实时性的系统中，为提高通信速率和更好的实现实时监控，应选用二进制传输方式，波特率选用 9600bit/s，并采用奇校验，通信时间/字符为 1ms/字符。

# 第四章 典型工业控制系统通信协议

通信协议是指双方实体完成通信或服务所必须遵循的规则和约定，协议定义了信息单元使用的格式、信息单元应该包含的信息与含义、连接方式、信息发送和接收的时序，从而确保网络中数据顺利地传送到确定的地方。工业控制系统通信协议是指应用于生产、生活的控制系统协议，其应用领域可以分为程序自动化、工业控制、智能建筑、输配电通讯协定、智能电表、车用通讯等。常用的工业控制系统通信协议有 Modbus、S7、BACnet、DNP3、IEC 104 等。

## 4.1 Modbus 协议

### 4.1.1 Modbus 协议介绍

Modbus 是一种串行工业协议标准，是 Modicon（现为施耐德电气子公司）在 1979 年为使用 PLC 而发表的，现已成为工业领域通信协议的业界标准，并且是工业电子设备之间相当常用的连接方式。

Modbus 协议被定义成一个 master/slave（主/从）协议，主设备操作一个或多个从设备，从设备不能主动提供信息，必须等待主设备问询。主设备可以根据从设备的寄存器地址或者索引，对从设备的寄存器中的数据进行读和写。

如图 4.1 所示，Modbus 协议使用请求/响应模式，只适用三种不同协议数据单元：Modbus 请求、Modbus 应答、Modbus 异常应答。每个使用 Modbus 进行通信的设备都必须指定唯一的地址，每个命令都制定了目的地址，虽然其他设备也可能接收到命令消息，但只有地址匹配的设备才会响应。

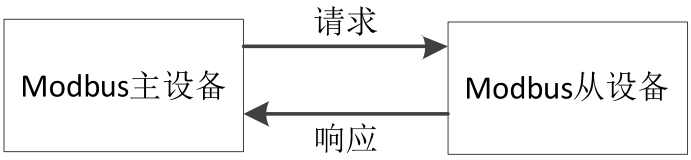


图 4.1 Modbus 协议请求/响应模式

在 Modbus 发展过程中，产生了几个适应特定需求的衍生协议：

- Modbus ASCII 和 Modbus RTU

- Modbus TCP
- Modbus Plus

Modbus ASCII 和 Modbus RTU 是比较简单的串行协议，使用 EIA-232 或 EIA-485 传输数据包，协议定义了功能码和用于传输数据的编码方案，基础数据包按照 Modbus ASCII，RTU 或 TCP 协议进行封装。modbus RTU（基于 TCP 的 modbus RTU）协议的消息格式如图 4.2 所示。

| Unit/Slave ID 1字节 | Function Code 1字节 | Data N字节 | CRC 2字节 |
|---|---|---|---|

图 4.2 Modbus RTU 消息格式

Modbus 协议的 TCP 版本遵循 OSI 网络参考模型，定义了 OSI 模型中的表示层和应用层，使用 TCP/IP 协议在网络上传输 Modbus 命令和消息。

Modbus Plus 协议是一种异步半双工通讯的对等网络协议，物理接口是 RS485，波特率 1Mbps，采用的是令牌总线访问协议。通讯介质采用屏蔽双绞线或光纤，不使用其它附加设备最大支持 32 个接点，双绞线最远传输距离 450m，光纤 3km，如果采用中继器、桥等设备双绞线最远传输距离 1800m，光纤 12km，最大接点数 64 个。Modbus Plus 协议提供了 3 种连接:主控计算机（人机接口上位计算机）、现场控制器（PLC 系统）、现场设备（变频器等）。

### 4.1.2 Modbus/TCP 协议规范

Modbus/TCP 协议的消息格式如图 4.3 所示。

| Transaction ID 2字节 | Protocol ID 2字节 | Length 2字节 | Unit/Slave ID 1字节 | Function Code 1字节 | Data N字节 |
|---|---|---|---|---|---|

图 4.3 Modbus/TCP 消息格式

由于可以依赖 TCP/IP 协议的校验，modbus/TCP 协议省去了 CRC 校验，不过现阶段某些 Modbus 协议又保留了 CRC 校验。

Modbus/TCP 协议的 master/slave（主/从）的区分不太明显，因为以太网允许点对点通信，客户端和服务端都是已知的网络实体，在这种情况下，从设备变成服务端，主设备变成客户端，这里允许多个客户端从同一个服务端获取数据，这就意味着可以存在多个主设备和多个从设备，而不是基于硬件给物理设备定义

主从，这里需要系统设计者为主从功能之间创造逻辑关联。

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），由功能码向服务器指示将执行哪种操作，功能码由 1 字节表示，有效范围为 0~255（128~255 为异常响应保留），一些功能码加入子功能码来定义多项操作。

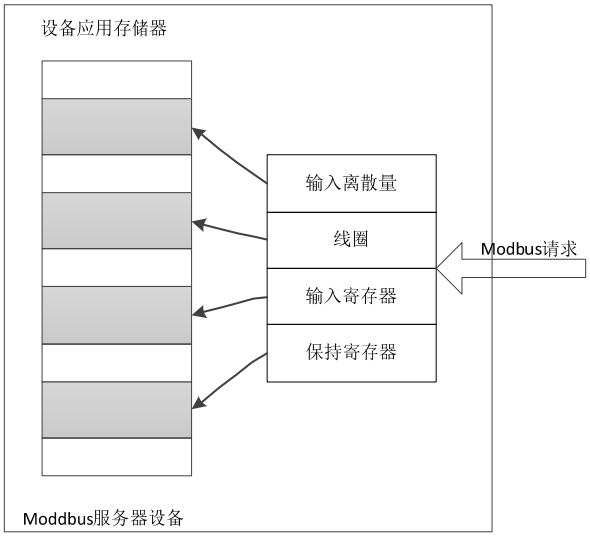


图 4.4 Modbus 协议数据块

Modbus 定义了 4 个不同的数据块，如图 4.4 所示，每个数据块都有地址或者寄存器号码，因此，准确的找到一个数据需要功能码（或寄存器类型）和地址（或寄存器号码）。表 4.1 对寄存器种类进行了说明。

表 4.1 Modbus 寄存器种类说明

| 寄存器种类 | 说明 | PLC 类比 | 举例说明 |
|---|---|---|---|
| 线圈状态 | 输出端口。可设定端口的输出状态，也可以读取该位的输出状态。可分为两种不同的执行状态，例如保持型或边沿触发型。 | DO<br>数字量输出 | 电磁阀输出，MOSFET 输出，LED 显示等。 |
| 离散输入状态 | 输入端口。通过外部设定改变输入状态，可读但不可写。 | DI<br>数字量输入 | 拨码开关，接近开关等。 |
| 输入寄存器 | 输入参数。控制器运行时从外部设备获得的参数。可读但不可写。 | AI<br>模拟量输入 | 模拟量输入 |
| 保持寄存器 | 输出参数或保持参数，控制器运行时被设定的某些参数。可读可写。 | AO<br>模拟量输出 | 模拟量输出设定值，PID 运行参数，变量阀输出大小，传感器报警上限下限。 |

Modbus 协议有三类功能码，如图 4.5 所示。

- 公共功能码

- 用户定义的功能码
- 保留功能码

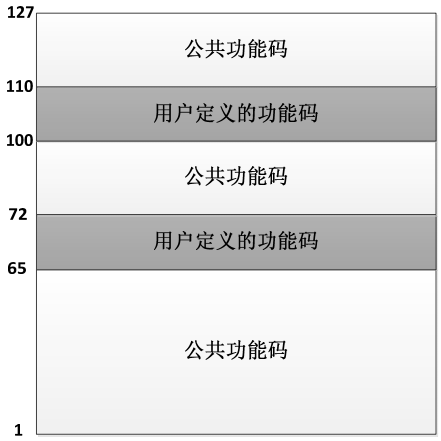


图 4.5 Modbus 功能码类型

Modbus 设备最常用的功能码如表 4.2 所示，这只是所有功能码的一部分。

表 4.2 Modbus 部分功能码

| 功能码 | 寄存器类型 | 描述 |
|---|---|---|
| 1 | READ_COILS | 读线圈 |
| 2 | READ_DISCRETE_INPUTS | 读离散输入 |
| 3 | READ_HOLDING_REGS | 读多个保持寄存器 |
| 4 | READ_INPUT_REGS | 读输入寄存器 |
| 5 | WRITE_SINGLE_COIL | 写单个线圈 |
| 6 | WRITE_SINGLE_REG | 写单个保持寄存器 |
| 7 | READ_EXCEPT_STAT | 读不正常状态 |
| 8 | DIAGNOSTICS | 诊断 |
| 9 | PROGRAM | 程序（484） |
| 10 | | 查询（484） |
| 11 | GET_COMM_EVENT_CTRS | 获得通信事件计数器 |
| 12 | GET_COMM_EVENT_LOG | 获得通信事件记录 |
| 13 | PROGRAM | 程序（184/384/484/584） |
| 14 | | 查询（184/384/484/584） |
| 15 | WRITE_MULT_COILS | 写多个线圈 |
| 16 | WRITE_MULT_REGS | 写多个保持寄存器 |
| 17 | REPORT_SLAVE_ID | 报告从设备 ID |
| 18 | PROGRAM | 程序（884 和 MICRO84） |
| 19 | COMM_LINK_RESET | 通信链路复位 |
| 20 | READ_FILE_RECORD | 读文件记录 |
| 21 | WRITE_FILE_RECORD | 写文件记录 |
| 22 | MASK_WRITE_REG | 屏蔽写寄存器 |
| 23 | READ_WRITE_REG | 读/写多个寄存器 |

| | | |
|---|---|---|
| 24 | READ_FIFO_QUEUE | 读 FIFO 队列 |
| 43 | ENCAP_INTERFACE_TRANSP | 封装接口传输 |
| 90 | UNITY_SCHNEIDER | |

常用的功能码是 01H、02H、03H、04H、05H、06H、0FH、10H。功能码可以分为位操作和字操作两类，位操作的最小单位实比特，字操作的最小单位是两个字节。位操作指令：读线圈状态 01H，读离散输入状态 02H，写单个线圈 05H 和写多个线圈 0FH。字操作指令：读保持寄存器 03H，写单个寄存器 06H，写多个保持寄存器 10H。

## 4.2 S7 协议

### 4.2.1 S7 协议介绍

S7 是西门子公司专有协议，在西门子 S7-300、400、1200、1500 系列的可编程逻辑控制器（PLC）之间运行。以太网、PROFIBUS 和 MPI 网络中都可使用 S7 协议进行通信。

以太网中 S7 协议利用 TCP 102 端口传输，如图 4.6 所示，S7 协议数据包先使用 COTP 协议封装，再采用 TPKT 协议封装进行 TCP 连接。

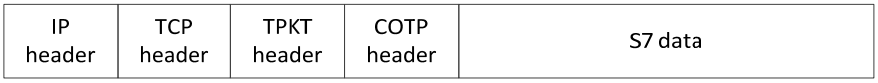


图 4.6 S7 协议数据包封装方式

如图 4.7 所示，S7 协议通信分为三个阶段，第一阶段是建立 COTP 连接，第二阶段是 S7 通信设置，第三阶段是功能码请求与响应。

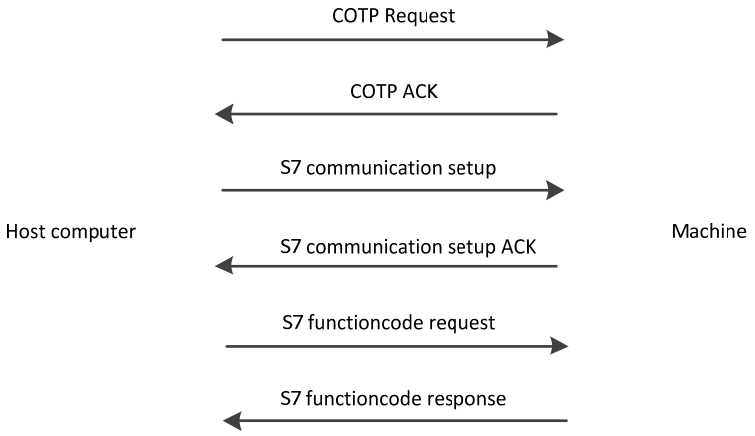


图 4.7 S7 协议通信过程

### 4.2.2 S7 协议规范

S7 协议数据 Magic 标识固定为 0x32，包含字段 S7 type，data unit ref，parameters length，data length，result info，paremters，data，如图 4.8 所示

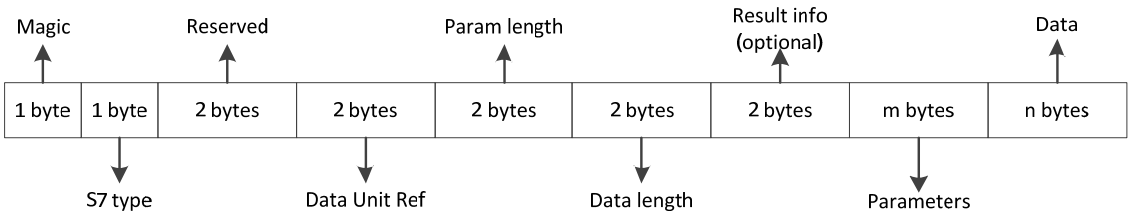


图 4.8 S7 协议数据格式

Parameters 字段的第一字节为 S7 的功能码，S7 的功能码及对应的功能如表 4.3 所示。其中 Communication Setup 用于建立 S7 协议连接，Read 用于上位机从下位机中读取数据，Write 用于上位机向下位机中写入数据，Request Download，Download Block，Download End，Download Start，Upload，Upload End 用于 download 或者 upload block。PLC Stop 用于关闭 PLC 设备，PLC Control 包含 Hot Run 和 Cool Run，用于启动 PLC。

表 4.3 S7 协议功能码

| Code | Fuctions |
|---|---|
| 0x00 | Sytem Functions |
| 0x04 | Read |
| 0x05 | Write |
| 0x1a | Request Download |
| 0x1b | Download Block |
| 0x1c | Download End |
| 0x1d | Download Start |
| 0x1e | Upload |
| 0x1f | Upload End |
| 0x28 | PLC Control |
| 0x29 | PLC Stop |
| 0xf0 | Communication Setup |

当功能码为 0x00 时，表示 system functions，system functions 是对用于系统设置与状态查看一类功能码的统称，在 parameters 字段中通过 4bits 的 function group 和 1byte 的 subfunciton 来区分，如图 4.9 所示。

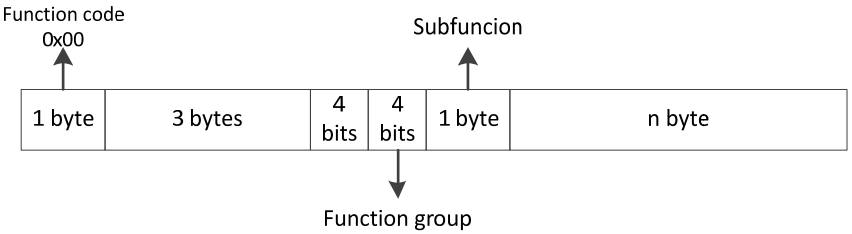


图 4.9 S7 协议数据格式

Systems Functions 分为 7 类 group，如表 4.4 所示。其中 block function 用于读取 block 信息，time function 用于查看和设置系统时间。

表 4.4 S7 协议 System 功能码与子功能码

| fuction group code | function | subfunction code | subfunctions |
|---|---|---|---|
| 1 | Programmer commands | 1 | Request diag data |
| | | 2 | VarTab |
| 2 | Cyclic data | 1 | Memory |
| 3 | block function | 1 | List blocks |
| | | 2 | List blocks of type |
| | | 3 | Get block info |
| 4 | CPU function | 1 | Read SZL |
| | | 2 | Message service |
| 5 | Security | 1 | PLC password |
| 6 | PBC BSEND/BRECV | None | None |
| 7 | time function | 1 | Read clock |
| | | 2,4 | Set clock |
| | | 3 | Read clock （following） |

## 4.3 BACnet 协议

### 4.3.1 BACnet 协议介绍

BACnet（Building Automation and Control Network）是一种为楼宇自动控制网络所指定的数据通信协议，由美国采暖、制冷与空调工程师协会资助的标准项目委员会于 1995 年 6 月制定，1995 年 12 月称为美国标准，2003 年 1 月正式成为国际标准，也是智能建筑楼宇自动控制领域中唯一的国际标准。BACnet 标准产生的背景是用户对楼宇自动控制设备互操作性的广泛要求，即将不同厂家的设备

组成一个一致的自控系统。

BACnet 标准对 ISO/OSI-RM 进行了精简和压缩，其目的是为了解决楼宇自控网络信息通信和互操作性的基本问题，在体系结构上可以划分为通信功能和互操作性两大部分，并且这两大功能部分即相互独立，又相互联系。

### 4.3.2 BACnet 协议规范

BACnet 协议通信功能由物理层、数据链路层和网络层三个协议层进行定义，如图 4.10 所示，互操作功能由应用层单独定义。其传输层采用 UDP 协议，设备默认开放 47808 端口监听。BACnet 协议的数据流称为协议数据单元（PDU），由应用层产生的数据流称为应用层协议数据单元（APDU）。

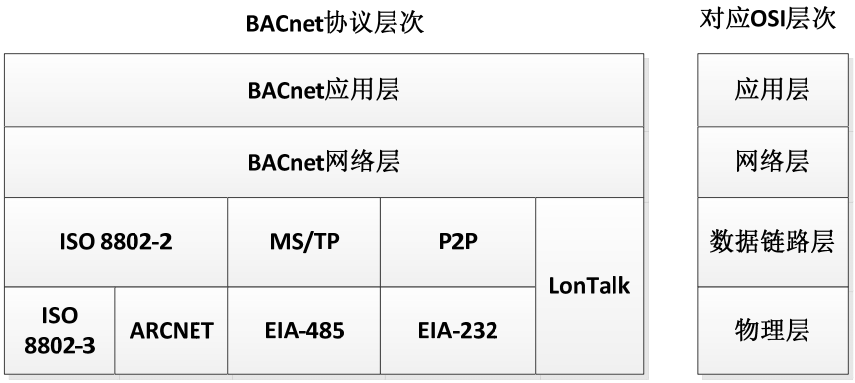


图 4.10 BACnet 协议对应通信协议层

BACnet 应用层协议数据单元（APDU）的第 1 字节的第 2-4 比特表示 APDU 类型，如图 4.11 所示。


图 4.11 BACnet 协议 APDU 数据格式

APDU 共有 8 种类型，如表 4.5 所示：

表 4.5 APDU 类型

| Code | APDU type |
|---|---|
| 0 | ConfirmedRequestPDU |
| 1 | UnconfirmedRequestPDU |
| 2 | SimpleAckPDU |
| 3 | ComplexAckPDU |

| | |
|---|---|
| 4 | SegmentAckPDU |
| 5 | ErrorPDU |
| 6 | RejectPDU |
| 7 | AbortPDU |

## 4.4 DNP3 协议

### 4.4.1 DNP3 协议介绍

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。DNP 协议标准由 IEEE 提出，参考了 IEC 870-5、以及其他一些 IEC 协议，主要为了解决 SCADA 行业中，协议混杂、没有公认标准的问题。DNP 协议有一定的可靠性，这种可靠性可以用来对抗恶劣环境中产生的电磁干扰、元件老化等信号失真现象，但不保证在黑客的攻击下、或者恶意破坏控制系统的情况下的可靠性。

DNP3.0 规约采用 EPA 模型，分为三层结构：数据链路层，伪传输层和应用层。数据链路层负责通信链路的建立、数据的接收、发送和初步处理；伪传输层负责应用数据的分包和组包；应用层实现真正的信息处理。

### 4.4.2 DNP3 协议规范

DNP3 可通过 TCP/UDP 进行封装，以便在以太网上运行，支持 DNP3 协议的从设备默认会开放 TCP 的 20000 端口用于通信。

DNP3.0 规约多采用问询—应答方式，但也允许从站主动上送信息。

一个典型的 DNP 应答处理过程一般如下所示。

主站：

- 应用层组织好信息后交给伪传输层；
- 传输层把应用层报文分帧，每帧前加上一个 TH 报头，然后交给链路层；
- 链路层则把每帧报文分块，每块最多 16 字节，每个块后加一个 16 位的 CRC 校验码，同时链路层有一个固定长度的报头，包含有地址、长度等

信息；主站链路层发送报文，并且在规定时间内，在未收到对方确认时进行重发（如果要求）。

从站：

- 链路层接收完一帧报文后，进行 CRC、地址、长度等合法性检查，如对方链路层要求确认，则回答 ACK 或 NACK 报文，然后把接收正确的报文去掉报头和每块的 CRC 后交给传输层；
- 传输层检查 TH 报头，并在多帧报文时按顺序把报文组成一个完整的应用层数据包，然后交给应用层；
- 应用层收到报文后，如对方应用层要求确认，先回答一个 Confirm 报文，然后对信息进行处理，再组织回答报文（回答过程类似主站）。

DNP3.0 的数据链路层采用一种可变帧长格式：FT3。

如图 4.12 所示，一个 FT3 帧被定义为一个固定长度的报头，随后是可选的数据块，每个数据块附有一个 16 位的 CRC 校验码。固定的报头含有 2 个字节的起始字，一个字节的长度（LENGTH），一个字节的链路层控制字（CONTROL），一个 16 位的目的地址，一个 16 位的源地址和一个 16 位的 CRC 校验码。

| 定长的报头 | | | | | | 主体 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 起始字节<br>0x0564 | 长度 | 链路层<br>控制字 | 目的地址 | 原地址 | CRC<br>校验码 | 用户数据 | CRC<br>校验码 | …… | 用户数据 | CRC<br>校验码 |

图 4.12 DNP3.0 数据格式

DNP 的传输层是一个伪传输层。伪传输层功能专门设计用于传送超出链路规约数据单元（LPDU）定义长度的信息。其格式如图 4.13。

| TH（传输层报头） | 数据块 |
|---|---|

图 4.13 数据单元定义

传输层报头 TH：传输控制字，1 个字节。数据块：应用层用户数据 1-249 个字节。由于数据链路层的 FT3 帧格式中长度字的最大限制为 255，因此传输层数据块的最大长度为：255-5（链路层控制字+源地址+目的地址）-1（TH）=249。当应用层用户数据长度大于 249 字节时，传输层将以多帧报文方式传送，并每帧前加 TH 控制字。如 1234=249+249+249+249+238，分 5 帧传送。

DNP 的应用层负责真正的信息处理。其报文分为请求报文和响应报文两类。在 DNP 中，只有指定的主站能够发送应用层的请求报文，而从站则只能发送应

用层的响应报文。报文格式如图 4.14 所示。

- 请求（响应）报头：标识报文的目的，包含应用规约控制信息（ACPI）；
- 对象标题：标识随后的数据对象；
- 数据：在对象标题内指定的数据对象。


图 4.14 DNP 报文格式

## 4.5 IEC60870-5-104 协议

### 4.5.1 IEC60870-5-104 协议介绍

IEC60870-5-104 网络传输规约是国际标准规约，主要应用于电力系统变电站计算机监控系统或 RTU 与主站 SCADA 系统之间的数据通信。主站与从站之间的网络通信底层采用 TCP/IP 协议，应用层协议采用 IEC60870-5-104 传输规约。其协议基本参数如下：

- 最大帧长 255 字节
- 帧时间间隔 50ms
- TCP 网络端口号 2404
- 采用平衡传输，每个节点（包括主站、从站）均可启动报文发送

### 4.5.2 IEC60870-5-104 协议规范

IEC60870-5-104 协议应用层产生的数据流称为应用层协议数据单元（APDU）。一个 APDU 由应用协议控制信息：APCI（Application protocol control information）和应用服务数据单元：ASDU（Application service data unit）两部分组成，如图 4.15 所示。


图 4.15 IEC60870-5-104 数据格式

每个 APCI 包含下列的定界元素：一个启动字符，ASDU 的长度，以及控制域。可以传输一个完整的 APDU（或者处于控制目的，APDU 中仅包含 APCI 域）。

起始字节 0x68 定义了一帧数据的起始。APDU 长度定了 APDU 体的整个长度，包括了 APCI 的四个控制域和 ASDU 的长度。ASDU 的最大长度限制在 249（减去 4 字节的控制域）以内，因为 APDU 域的最大长度是 253（255 减去起始和长度字节）。控制域定义了保护报文不致丢失和重复传送的控制信息、报文传输启动、停止、以及传输连接的监控等控制信息。

APCI 分为 I 类帧、S 类帧和 U 类帧：

I 类帧的控制域包含发送序号和接收序列号，两个序列号在每个 APDU 和每个方向上都应按顺序加一，两个序列号都在 0~32767 之间的循环。发送方增加发送序列号，接收方增加接收序号，接收方可连续确认多个 APDU。如果只在一个方向上进行较长的数据传输，则另一方使用 S 帧确认这些 APDU。I 类帧一般用于双方都需确认的情况，在一个 TCP 连接创建后，发送和接收序号均被置 0。

S 类帧具有计数的监视功能，其为短帧，长度固定为 6 个字节。接收方收到Ⅰ类帧发送的数据，但自身没有数据要发送的情况下，S 帧用于确认收到对方的帧。

U 类帧具有不计数的控制功能，长度固定为 6 字节，用于控制报文。

IEC60870-5-3 描述了远程系统传输帧中的基本应用数据单元，并定义了配套系统中的应用服务数据单元（ASDU），其基本结构如图 4.16 所示。

<table>
<tr><td>类型标识</td><td rowspan="6">数据单元标识符</td><td rowspan="7">ASDU</td></tr>
<tr><td>可变结构限定词</td></tr>
<tr><td>传输原因Low-Byte</td></tr>
<tr><td>传输原因High-Byte</td></tr>
<tr><td>公共体地址Low-Byte</td></tr>
<tr><td>公共体地址High-Byte</td></tr>
<tr><td>IEC104定义的一个或多个信息对象</td><td>信息对象</td></tr>
</table>

图 4.16 ASDU 结构

ASDU 由数据单元标识符和一个或多个信息对象组成。数据单元标识符在所有 ASDU 中具有相同的结构，而一个 ASDU 中的信息对象也常有相同的结构、类型和格式，它们的结构、类型和格式由类型标识域所定义。应用服务数据单位元

公共体地址的八位位组是由系统参数所决定，公共体地址是站地址，可以去寻址整个站或者仅仅是站的特定部分。

时标（如果出现的话）它属于单个信息对象。信息对象由一个信息对象标识符（如果出现的话），一组信息元素和一个信息对象时标（如果出现的话）组成。

信息对象标识符仅由信息对象地址组成，大多数情况下，在一个特定系统中，应用服务数据单元公共体地址连同信息对象地址一起可以区分全部信息元素集，在每一个系统中这两个地址结合在一起将是明确的，类型标识不是公共体地址也不是信息对象地址。

一组信息元素集可以是单个信息元素，一组综合元素或者一个顺序元素。

## 4.6 其他工业控制系统通信协议

还有许多其他工业协议，本文难以一一描述，仅选择下面三种作简单介绍。

### 4.6.1 Ethernet/Industrial Protocol 协议

Ethernet/Industrial Protocol（EtherNet/IP）是由洛克威尔自动化公司开发的工业以太网通讯协定，由开放 DeviceNet 厂商协会（ODVA）管理，是一个高级的工业应用层协议，可应用在程序控制及其他自动化的应用中，是通用工业协定（CIP）中的一部分。

EIP 采用和 DevieNet 以及 ControlNet 相同的应用层协 CIP（Control and Information Protoco1），可以理解为通过以太网传输的 CIP 协议即为 EIP。EIP 和 CIP 技术的主要管理者为 ODVA（OpenDeviceNet Vendor Association）组织，ODVA 组织成立于 1995 年，由超过 300 个来自世界的领先工业自动化产品供应商组成。在上世纪 90 年代工作于 ControlNetInternationalLtd.（CI）的技术团队开发了 EIP，在 2000 年 ODVA 和 CI 联合形成一个组织 JTA（JointTechnology Aggreement）进行 EIP 协议开发，在 2009 年，JTA 组织终结，最终 EIP 成为 ODVA 组织的一个成员，直至今日 EIP 技术主要的控制方也是 ODVA。其主要技术细节如下。

- 传输基本的 I/O 信息通过 UDP 协议，叫做隐性信息。
- 上传和下载参数，设置信息等通过 TCP 协议传输，叫做显性信息。

- 轮询，循环数据和设备状态改变检测通过 UDP。
- 一对一（单播），一对多（多播），一对所有（广播）通信通过 IP 方式。
- 通常显性信息（TCP）使用 44818 端口，隐性信息（UDP）使用 2222 端口。

### 4.6.2 Profibus 协议

Profibus 协议是一种 20 世纪 80 年代末由德国电器工业中心协会开发的现场总线协议。它包括几种变体，如 Profibus-DP（分散性外围），与 Profibus-PA（过程自动化）。其中标准化变体 Profibus-DP 本身又有 V0、V1 和 V2 三种常见的变体。而 Profibus 通信也有异步、同步和以太网三种类型，以太网上的 Profibus 也成为 Profinet。

### 4.6.3 EtherCAT 协议

EtherCAT 是一个实时以太网现场总线协议，它使用以太类型 0x88A4 在标准以太网络上传输控制系统信息。由于以太网帧载荷较大（46-1500 Bytes），而分布式过程数据较小，一版每周期仅有几字节数据，为了最大限度地提高通信效率，EtherCAT 将多个分布式过程数据封装到单个以太网帧中传输，这样一个完整周期只需要一个或两个以太网帧。从节点一次加入响应消息后将帧传给其他从节点，知道最后一个从节点返回完整的回应帧。

### 4.6.4 SERCOS III 协议

串行实时通信系统（Serial Real-time Communications System，SER-COS）是一种专门为数字运动控制设计得现场总线。SERCOS III 是一种用于在 PLC 与 IED 之间进行高速闭环串行通信的实时以太网通信协议。

# 第二部分：揭开工业控制网络安全的面纱

# 第五章 工业控制络基础

前边主要介绍了工业控制系统的相关概念和知识，本章则重点介绍工业控制网络的基本知识。

## 5.1 工业控制网络概述

工业控制网络是工业控制系统（ICS）的网络部分，涵盖多种类型的控制系统中的组件，包括监控和数据采集（SCADA）系统，分布式控制系统（DCS）等控制系统，而大多数实际应用的工业控制系统往往是两者混合的控制系统。对于工业控制网络逻辑结构和关键组件的理解，是工业控制网络安全研究的一个基础前提。

在工业控制网络结构方面，美国 NIST SP 800-82 分别给出了 SCADA 系统、DCS 系统以及混合控制系统的实际应用场景和典型拓扑结构；ANSI/ISA-99 发布的标准则明确了工业控制网络的结构模型，将工业控制系统分为 5 层，分别为：企业网络层、监控执行层、数据采集层、监控层以及物理过程层，明确将工业控制系统划分为控制组件和网络组件，并分别详细介绍了每个组建的功能。Michael Berg 等人则根据发电厂的应用场景，分析了控制自动化系统（Control and Automation Systems）中的网络结构，将工业控制网络结构模型分为：基础设施设备层（Infrastructure Equipment）、SCADA 现场设备层（SCADA Field Equipment）、控制中心层（Control Center）和自动监管层（Automation Oversight），并将数据和设备作为控制自动化系统的组件分别进行介绍，并运用对象角色建模（ORM）的方法，阐述了组件之间的关系。

### 5.1.1 工业控制网络体系结构

工业控制网络的体系结构随着对应工业控制系统的具体工艺流程、生产环境、控制技术等因素的不同，会产生较大的差异。但是，忽略不同系统间的个性差异差异（如 SCADA 与 DCS 系统间的差异）。依据工业控制系统普遍实现的控制功能，则工业控制网络参考模型如图 5.1 所示。

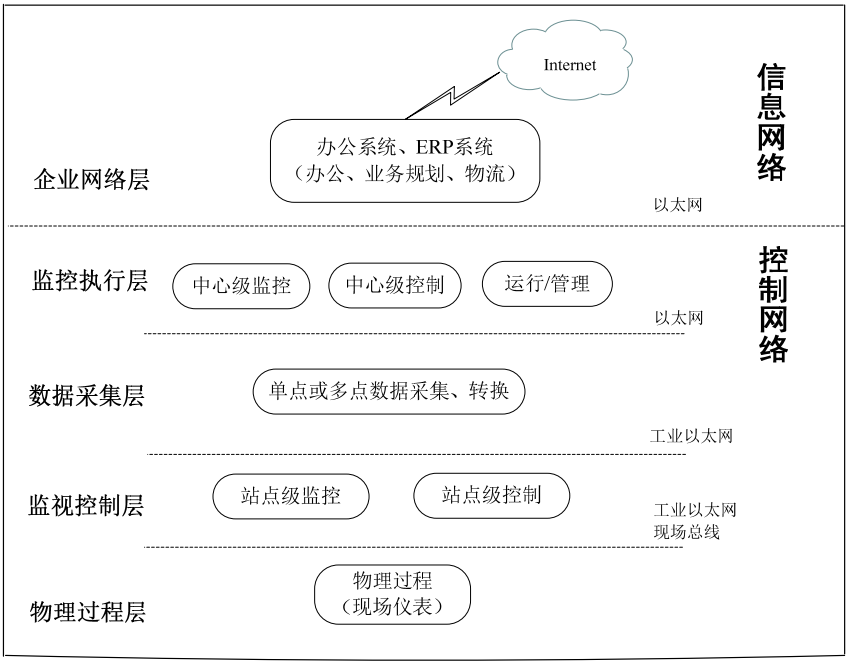


图 5.1 工业控制系统网络功能分层参考模型

如图 5.1 所示，工业控制系统网络一般分为企业网络层、监控执行层、数据采集层、监视控制层以及物理过程层等 5 个层次，具体如下。

- 企业网络层：办公网络，主要进行商业计划、人力资源、物流管理等。
- 监控执行层：生产执行网络，主要进行管理中心级别的生产工艺整体监控，以及生产计划制定等。
- 数据采集层：数据采集网络，主要对控制设备进行单点或者多点的过程数据采集或转换。
- 监视控制层：控制网络，主要进行站级的生产工艺局部监控，以及逻辑修改、下发等。
- 物理过程层：现场过程网络，主要执行各种物理过程。

其中，企业网络层为信息网络，监控执行层、数据采集层、操作控制层和物理过程层为控制网络。

### 5.1.2 工业控制网络关键组件

不同工业控制网络中所包含的组件类型根据工艺过程和生产环境，会有一定差异，但是总体上可以分为 PC 类型智能组件、嵌入式类型智能组件以及非智能组件。具体如图 5.2 所示。

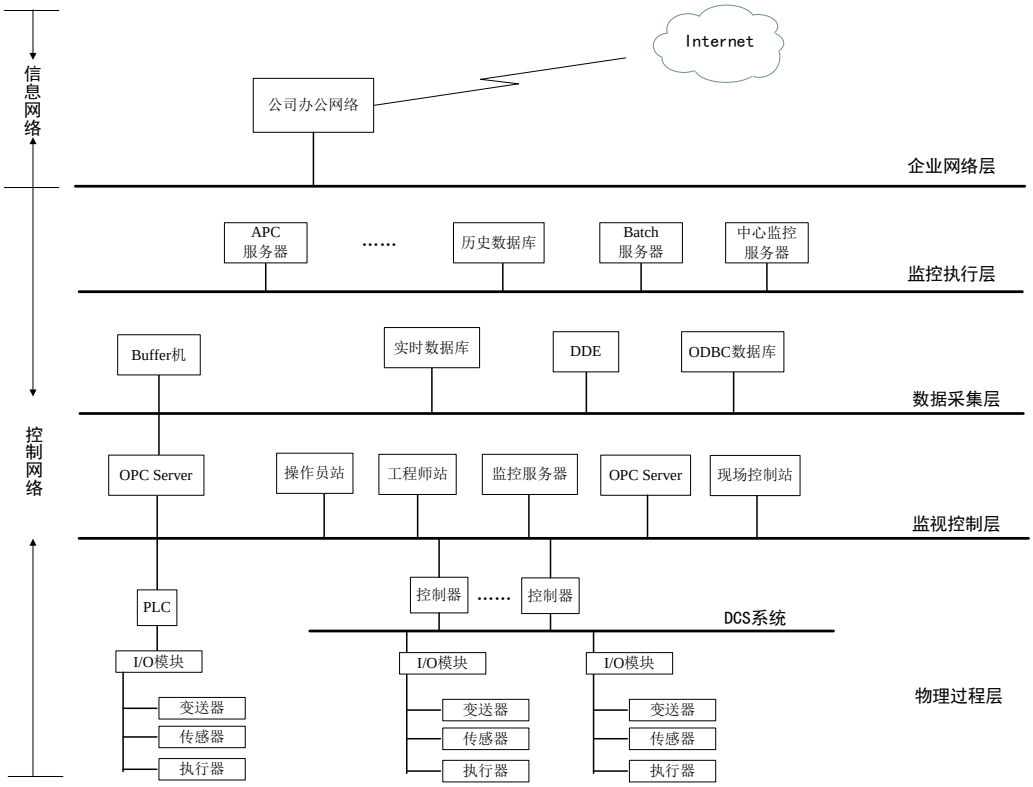


图 5.2 工业控制系统组件间体系结构

如图 5.2 所示，工业控制系统中除物理过程层外所包含组件基本都为 PC 类型智能组件，物理过程层包含嵌入式类型智能组件（如 PLC、RTU、智能仪表等），以及非智能组件（如电动调节阀、液位变送器等）。具体如下。

- 企业网络层：传统办公 PC，服务器等。
- 监控执行层：APC 服务器、历史数据库、Batch 服务器、中心监控服务器。
- 数据采集层：Buffer 机（OPC Client）、实时数据库、DDE、ODBC 数据库。
- 监视控制层：OPC Server、操作员站、工程师占、监控服务器、现场控制站、PLC、RTU 以及各种控制器。
- 物理过程层：I/O 模块、智能仪表和非智能仪表等。

### 5.1.3 工业控制网络与 IT 网络的集成

工业控制网络一般包含处理工业控制系统管理与决策信息的信息网络和处理控制现场实时测控信息的控制网络两部分。信息网络位于企业中上层，处理大量、变化、多样的信息，具有高速、综合的特征；控制网络位于企业中下层，处

理实时、现场的信息，具有实时性强，安全性强（这里专指物理安全，即 Safety）。信息网络和控制网络的集成，可以通过以下几种方式实现。

- 采用硬件实现

硬件设备可以是一台专门的计算机，依靠其中运行的软件完成数据包的识别、解释和转换；可以是一块智能接口卡，完成现场总线设备与以太网中监控计算机之间的数据通信。这种集成方式功能较强，但实时性较差。

- 采用 DDE 技术实现

当控制网络和信息网络之间有一个共享工作站或通信处理机时，可采用动态数据交换技术（Dynamic Data Exchange，DDE）方式实现两者的集成。这种方式具有较强的实时性，而且比较容易实现，可以采用 Windows 技术，但是协议转换较复杂，软件开销比较大，只适合配置简单的小型系统。

- 采用统一的协议标准实现

这是解决网络集成最好的办法，不过这需要设计控制网络的协议以提高其传输速度，从而更好的与信息网络相融合。如目前比较流行的工业以太网，它是在以太网技术和 TCP/IP 技术的基础上开发出来的一种控制网络（包含 Profinet、HES、Ethernet/IP、ModbusTCP 等）。

- 采用数据库访问技术实现

当控制网络采用工业以太网时，可以通过在控制网络部署数据库，通过 TCP/IP 将数据库内容发布到控制网络的方式实现控制网络和信息网络的集成。

- 采用 OPC 技术实现

OPC（OLE for Process Control）技术基于 Windows 的 DCOM 技术，由大部分的自动化公司合作开发的一套数据交换工业标准。OPC 技术的主要特点是“即插即用”，它采用标准方式配置硬件和软件接口，一个设备可以很容易地加入现有系统并立即使用。

## 5.2 典型工业领域的工业控制网络

本节将重点介绍一些典型工业领域的工控网络。

### 5.2.1 钢铁行业的工业控制网络

钢铁行业的工业控制以太网一般采用环网结构，为实时控制网、动作控制器、操作员站、工程师站之间的过程控制数据提供实时传输。网络上所有操作员站、数据采集站以及 PLC 都使用以太网接口并设置为同一网段的 IP 地址，网络中远距离传输介质为光缆，本地传输介质为普通网线（如 PLC 与操作员站之间）。生产监控主机利用双网卡结构与管理网相连。图 5.3 是典型钢铁厂网络拓扑图。

- 网络垂直划分为互联网层、办公网层、监控层、控制层及现场层（仪表）。
- 网络水平则划分为不同功能区域（烧结、炼铁、炼钢、轧钢等）。

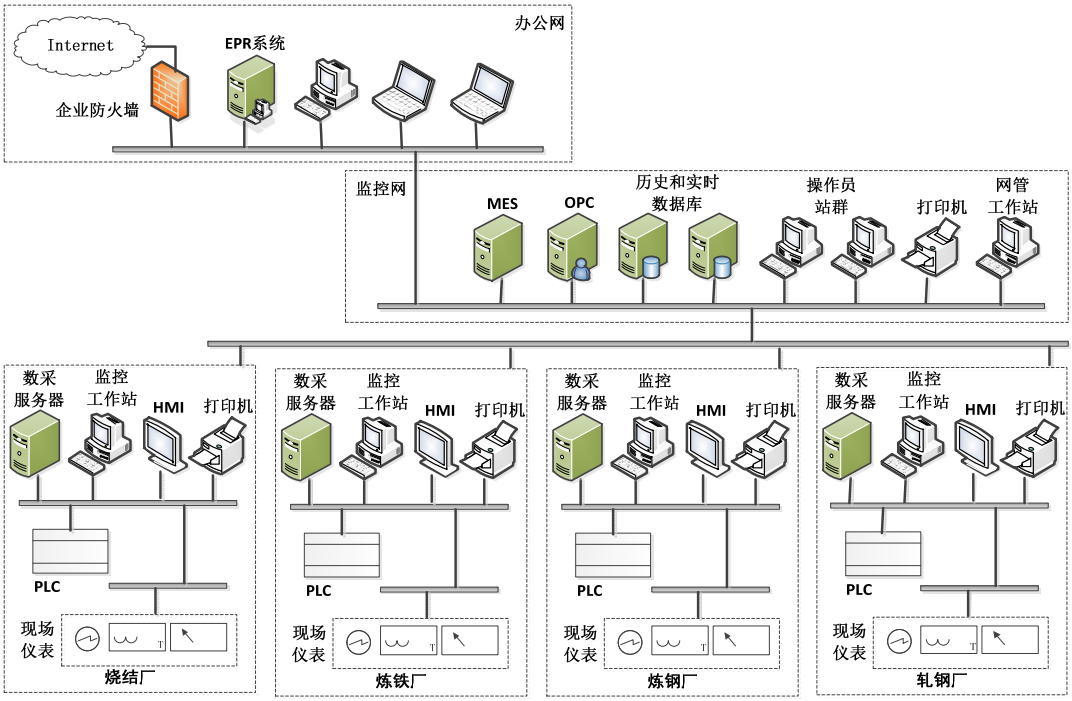


图 5.3 典型钢铁厂网络拓扑结构图

### 5.2.2 石化行业的工业控制网络

典型情形下，现有的炼化厂生产控制系统的网络拓扑如图 5.4 所示。大型石油化工生产控制系统庞大，安全要求高，现场由多个控制系统完成控制功能。大型石油化工工程全厂 DCS 采用大型局域网架构，网络架构较为复杂。现场的主要控制功能都是由 DCS 来完成的，其他系统集中控制在某种程度上可以完全由 DCS 监控。DCS 含有大量的数据接口，是构建企业信息化的数据来源和执行机构。除 DCS 外的其他系统一般对外并没有数据接口（无生产数据），且相对独立，网络

结构简单。

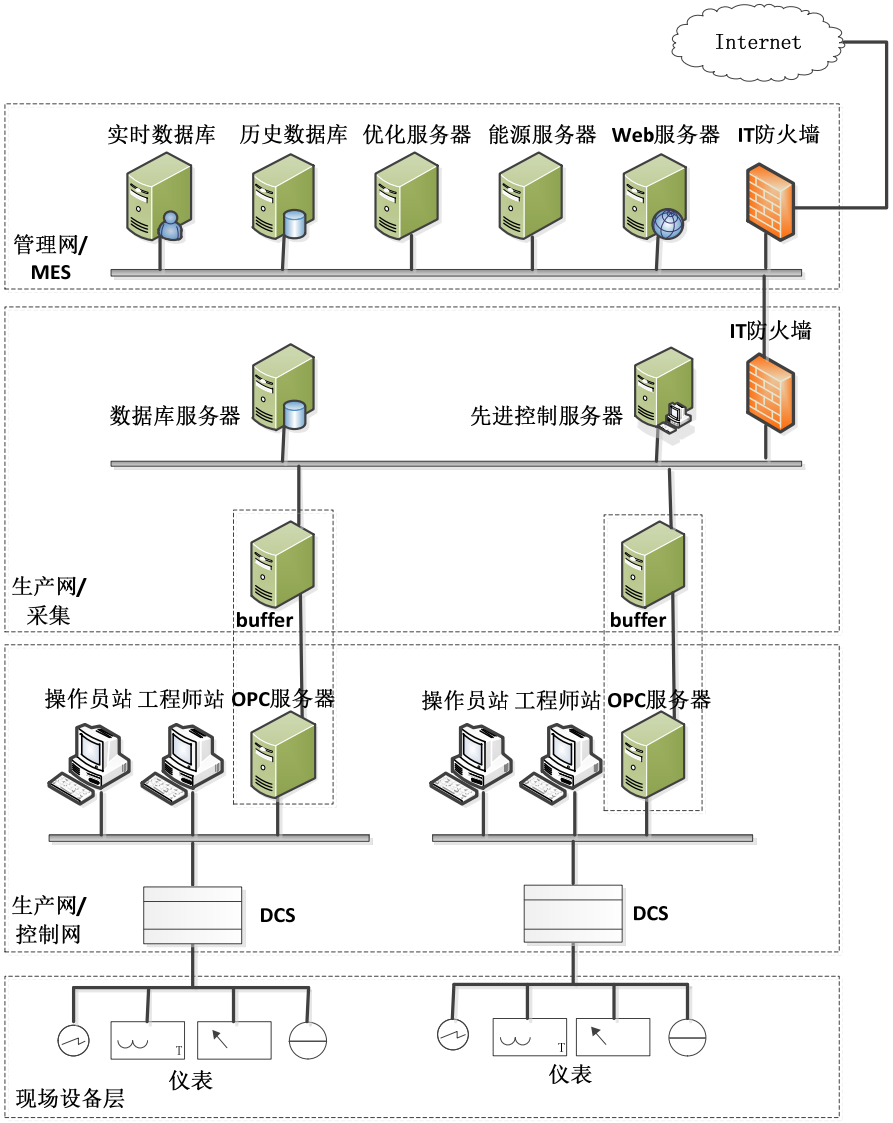


图 5.4 典型炼化厂网络拓扑图

主要控制系统的功能如下所示。

- 分布式控制系统（DCS）

DCS 完成生产装置的基本过程控制、操作、监视、管理、顺序控制、工艺联锁，部分先进控制也在 DCS 中完成。大型石油化工工程全厂 DCS 采用大型局域网架构。根据生产需求，系统规模和总图布置划分为若干独立的局域网，确保每套生产装置独立开停车和正常运行。

- 安全仪表系统（SIS）

SIS 设置在现场机柜室，与 DCS 独立设置，以确保人员及生产装置、重要机组和关键设备的安全。SIS 按照故障安全型设计，与 DCS 实时数据通信，在 DCS

操作员站上显示。大型石油化工工程全厂 SIS 采用局域网架构。根据生产需求、系统规模和总图布置划分为若干独立的局域网，确保采用 SIS 的生产装置独立开停车和安全运行。

- 可燃/有毒气体检测系统（GDS）

生产装置、公用工程及辅助设施内可能泄漏或聚集可燃、有毒气体的地方分别设有可燃、有毒气体检测器，并将信号接至 GDS。

- 压缩机控制系统（CCS）

压缩机控制系统完成压缩机组的调速控制、防喘振控制、负荷控制及安全联锁保护等功能，并与装置的 DCS 进行通信，操作人员能够在 DCS 操作员站上对机组进行监视和操作。

- 转动设备监视系统（MMS）

MMS 主要用于透平机、压缩机和泵等转动泵等转动设备参数的在线监视，同时对转动设备的性能进行分析和诊断，对转动设备的故障预测维护进行有力的支持。

- 可编程逻辑控制器（PLC）

操作控制相对比较独立或特殊的设备的控制监视和安全保护功能原则上采用独立的 PLC 控制系统。与 DCS 进行数据通信，操作人员能够在 DCS 操作员站上对设备的独立运行进行监视和操作。

- 在线分析仪系统（PAS）

在线分析仪（工业色谱仪、红外线分析仪等）应包括采样单元、采用预处理单元、分析器单元、回收或放空单元、微处理器单元、通信接口（网络与串行）、显示器（LCD）单元和打印机等。

### 5.2.3 电力行业的工业控制网络

大型电厂全厂 DCS 采用大型局域网架构，网络架构较为复杂。以下是 DCS 网络的架构说明。

- L1 基础控制层

该层网络完成控制生产过程的功能，主要由工业控制器、数据采集卡件，以及各种过程输入输出仪表组成，也包括现场所有的系统间通信。可以本地实现连

续控制调节和顺序控制、设备检测和系统测试与自诊断、过程数据采集、信号转换、协议转换等功能。

- L2 监控层

该层包含各个分装置的工程师站以及操作员站，可以对生产过程进行生产过程的监控、系统组态的维护、现场智能仪表的管理。事实上，由 L1 和 L2 层就能进行产品的正常生产，但是在大型电厂中，为了实现生产管理智能化以及信息化，通常都会设置 L3 及以上的网络层。

- L3 操作管理层（集控 CCR）

DCS 管理层网络通过 L3 级交换机汇聚各分区 L2 层的 LAN。设置全局工程师站可以对分区内所有装置的组态进行维护，查看网络内各装置的监控画面、趋势和报警。L3 层设置的中心 OPC 服务器，可以实现对各装置实时数据的采集。

- L4 调度管理层（厂级 SIS）

SIS 是实行生产过程综合优化服务的实时管理和监控系统，它将全厂 DCS、PLC 其他计算机过程控制系统汇集在一起，并与管理信息系统（Management Information System，MIS）有机结合，在整个电厂内实现资源共用、信息共享，做到管控一体化。

典型情形下，现有的火电厂生产控制系统的网络拓扑图如图 5.5 所示。

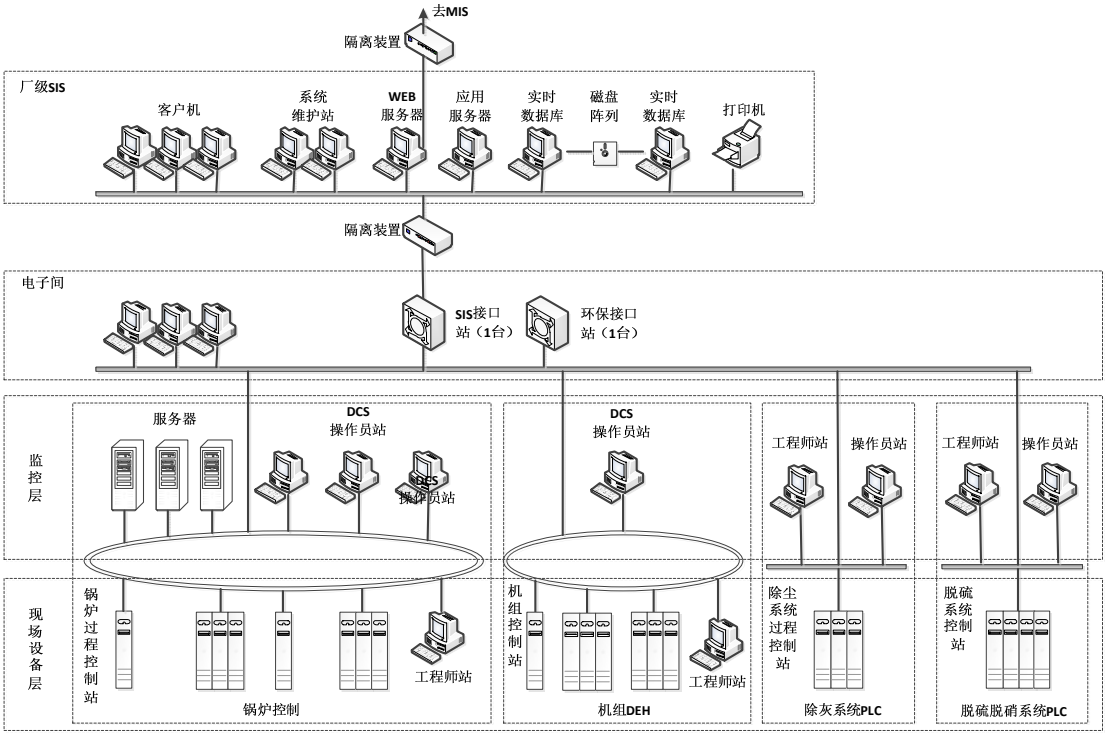


图 5.5 现有的火电厂生产控制系统的网络拓扑图

### 5.2.4 市政交通行业的工业控制网络

地铁综合监控系统的总体架构如图 5.6 所示。它由中央综合监控系统、车站综合监控系统（包括车辆段综合监控系统）以及将它们连接的综合监控系统骨干网组成。

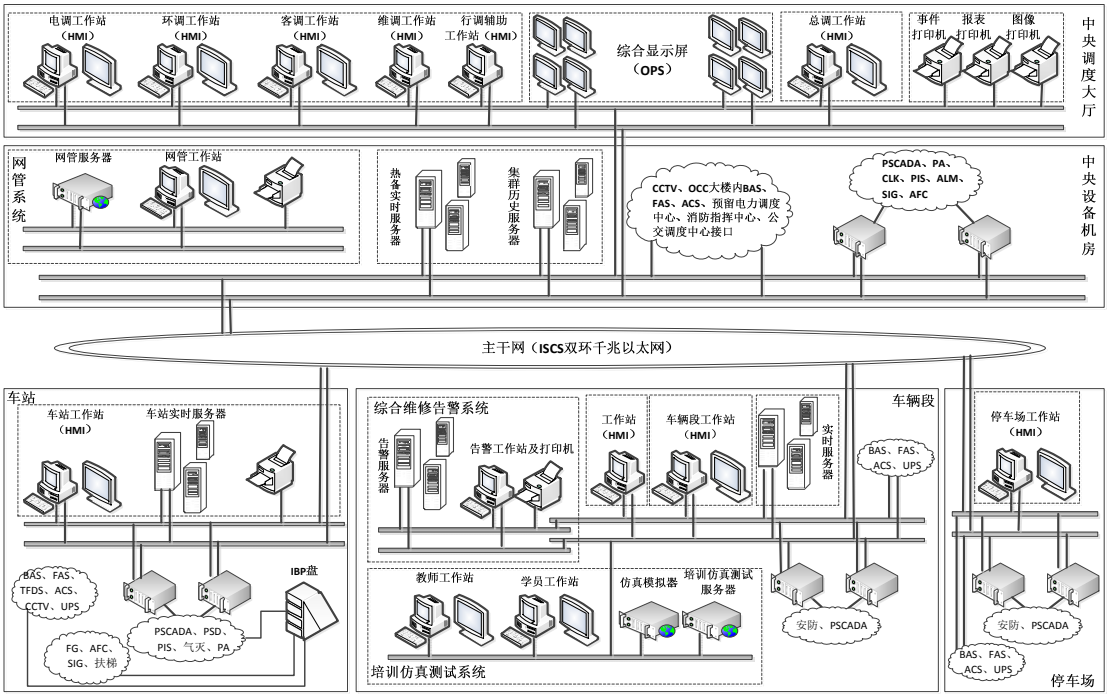


图 5.6 典型的交通综合监控系统网络架构

- 中央综合监控系统

中央综合监控系统安装在线路监控中心，用于监视全线各个车站（包括车辆段）的各个子系统的运行状态，完成中心级的操作控制功能。中央综合监控系统由中央监控网、OCC（Operating Control Center，运行控制中心）实时服务器、历史和事件服务器、磁盘阵列、磁带记录装置、各类操作员工作站、中心互联系统、UPS 打印机、机柜和附件等部分组成。此外，还有全系统的网络管理系统（NMS）、大屏幕系统（OPS）。

- 车站综合监控系统

车站级监控网为双冗余高速交换式以太网，数据传输率为 100Mbit/s 或 1000Mbit/s，遵循 IEEE802.3 标准、使用 TCP/IP 协议，网络交换机为冗余配置。

- 综合监控系统骨干网

综合监控系统骨干网（MBN）可采用地铁工程通信骨干网的传输信道，也可

单独组建骨干网。地铁综合监控系统是一个地理分散的大型 SCADA 系统。它构建在分布于方圆几十千米的广域网上。

# 第六章 工业控制网络威胁分析

“维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险”，为了保护网络免受攻击，了解攻击者如何接近工业网络、获准访问并最终取得控制权是很重要的。在经典的 Internet 网络环境（TCP/IP）中，黑客的手法和技术通常可以概括为“识别、探测及渗透”，然而，在工业控制网络中，黑客的手法虽然相同，但技术方面有着细微差别。在对系统进行有效保护之前，应对工业控制网络的脆弱性，安全问题的根源，以及系统、设备和协议的漏洞进行深入了解。

## 6.1 工业控制网络的脆弱性

现在使用的工业控制网络大多数都很陈旧，很多是在公共和私有网络、桌面计算和互联网普及之前，基于性能、可靠性、功能安全和灵活性的需求进行开发的。在很多场合，这些工业控制网络通过物理隔离与其他网络分开，并使用专用软件、硬件和缺乏网络安全功能的通信协议。而随着技术的革新，硬件、软件和网络技术的发展成果也被大量用在了工业控制网络中，使得工业控制网络与外界的隔离程度变得越来越低，其中一个负面影响就是迫切需要对其进行网络安全防护。工业控制网络的安全，一方面面临着通用 IT 技术方面的问题，另一方面也面临自己独有的难题。

工业控制网络与传统计算机网络有很多性质上的不同，包括不同的风险和特性；工业控制网络对性能和安全有着不同的要求，并使用典型 IT 人员不熟悉的操作系统和应用软件；在控制系统的设计和操作中，成产功能安全和网络安全防护往往是相互矛盾的；表 6.1 给出了工业控制网络与传统计算机网络不同点的总结。

表 6.1 IT 系统与 ICS 系统区别

| 分类 | IT 系统 | ICS 系统 |
| --- | --- | --- |
| 不可预料的后果 | 安全解决方案都是围绕典型的 IT 系统 | 安全工具必须进行测试，以确保它们不会危及 ICS 的正常操作 |
| 对时间要求严格的相互作用 | 不太重要的紧急互动；严格限制的访问控制可以必要程度的 | 对人员和其他紧急相互作用的响应是至关重要的；访问 ICS 的应严格控制， |

| | | |
|---|---|---|
| | 实现； | 但不能妨碍人机交互。 |
| 系统操作 | 系统是为典型操作系统的使用而设计的；升级可直接由自动部署工具完成； | 不同的、定制的操作系统没有安全功能；因为特殊的控制算法可能涉及修改硬件和软件的功能，软件更新必须精心完成，通常由软件供应商负责。 |
| 资源约束 | 系统指定有足够的资源，以支持诸如安全解决方案等第三方应用软件的加入； | 系统的设计旨在支持预期工业生产过程，使用最少的存储和计算资源以支持增加的安全技术。 |
| 通信 | 标准通信协议；典型 IT 网络实践； | 许多专有和标准的通信协议，多种类型的通信媒介，包括使用专用线和无线；网络是复杂的，有时需要专业的控制工程师。 |
| 变更管理 | 因存在一个良好的安全计划和程序，软件应用更改时及时进行的，这些程序通常是自动完成的； | 软件更改必须对整个系统进行彻底测试和部署，以确保控制系统的完整性；ICS 的中断往往必须提前数天或周进行规划。 |
| 管理的支持 | 允许多元化的支持方式； | 服务支持通常是通过一个单一的供应商。 |
| 组件寿命 | 3-5 年生命周期； | 15-20 年生命周期 |
| 访问组件 | 组件通常是在本地的，易于访问； | 组件是孤立的，偏远的，需要大量的实际工作量来获得它们。 |

- ICS 与 IT 系统之间的操作和风险差异加大了部署网络安全和操作策略的复杂度，针对 ICS 的特殊性，ICS 网络安全防御面临以下问题：
- ICS 一般都是实时性要求很高，它不允许延迟，因此部署工业控制网络安全防御必须考虑对系统实时性的影响。
- ICS 过程很多在本质上是连续的，它不允许中断，如果中断要提前进行安排，因此工业控制网络安全防御不应对 ICS 的生产连续性有影响。
- ICS 首先考虑的是人员、设备、产品等的安全问题，因此工业控制网络安全防御要协调好功能安全与网络安全之间的矛盾关系。
- ICS 的集中控制器和分布控制器如 PLC 等在网络安全中都很重要，因此工业控制网络安全防御步进要放在集中控制器上，还应考虑分布控制器。
- ICS 系统与物理过程有很复杂的联系，因此在部署工业控制网络安全防御时必须测试其与现在的 ICS 的兼容性。
- ICS 中，系统自动响应和对人际互动的时间有严格的要求，例如 HMI 上的口

令验证不应阻碍控制系统的紧急执行命令。

- ICS 的操作系统和应用软件不能兼容 IT 方面的成果，ICS 网络更复杂，应用软件和硬件很难升级，这对部署工业控制网络安全防御有更高的要求。
- ICS 环境下的控制系统用于现场设备的通信协议与 IT 环境下是不同的，部署 ICS 安全防御要考虑到实际的通信协议。
- ICS 预计的常使用寿命另外增加了两个类型的挑战：如何确保目前传统系统的运作以及现在如何设计系统，可以很容易适应未来的安全威胁和技术。
- 自动化设备缺乏基本的安全功能，例如，定义用户账号或支持安全通信协议的能力。

大多数目前使用的工业控制通信协议都没有或只有简单的安全功能，此安全功能主要是涉及到数据的访问控制项，这主要是为了防止意外操作失误，但不能抵御专门的攻击。一些在 ISO/OSI 模型不同层次的传统加密算法和协议可用于帮助解决一些安全问题，但是加密不能解决所有安全问题。总之，工业控制网络大量采用了 IT 上开放的网络协议，增加了工业控制网络的互联性，IT 很多的技术可以用到工业控制网络上，但他们之间的差异性也对工业控制网络安全防御提出了更多的挑战。

工业控制网络由工艺设备、过程控制硬件、网络设备和工业计算机等组成，是一个非常复杂的系统，远远超越了计算机系统的范畴，但是目前业界并没有专门为工业控制网络定义属于该领域的脆弱性概念，而是大部分沿袭了信息领域的定义。下面从系统策略、平台和网络上对工业控制网络脆弱性的概念进行总结定义。

第一，在工业控制网络安全中，存在于控制系统安全政策、实现指南、安全培训、安全架构、配置管理等事件中的，能够被威胁主体渗透以获取对工业控制信息的未授权访问或者扰乱关键步骤的弱点。

第二，在工业控制网络安全中，存在于控制系统硬件、操作系统、应用程序等平台中的，能够被渗透从而对工业控制系统或组件造成损害的缺陷、误配置以及不良维护等弱点。

第三，在工业控制网络安全中，存在工业控制网络以及与其它网络连接中的，能够被渗透从而对工业控制网络组件或行为造成损害的缺陷、误配置以及不良维

护等弱点。

简单而言，工业控制网络的脆弱性就是工业控制网络在硬件、软件、协议的具体实现或系统策略上存在的与网络安全相关的缺陷或不足，对该缺陷的渗透可获得工业控制网络的额外控制权限，从而获得更多的工业控制网络资源，或产生对工业控制网络更大地破坏。

## 6.2 工业控制网络信息安全问题根源

工业控制网络安全问题的根源就是缺乏本质安全。工业控制网络在设计之初，由于资源受限、物理隔离等原因，为保证实时性和可用性，系统各层普遍缺乏安全性设计。尽管目前已有工控产品提供商开始对旧系统进行加固升级，研发新一代的安全工控产品，但是由于市场、技术、使用环境等方面的制约，工控产品生产商普遍缺乏主动进行安全加固的动力。

信息系统中的主要组成单元是计算机，而网络上的计算机是被攻击和入侵的主要对象。黑客经常利用计算机软件或配置上存在的脆弱性，进行无授权访问、特权提升、DDoS 攻击等。信息系统的网络安全本质上讲就是网络上的信息安全，攻击者的攻击目的一般是为了获取计算机上的信患资产。一旦攻击成功后，被攻击计算机一般遭受的是信患破坏，严重一点是处于瘫痪状态。而工业控制网络中的组件有操作员站、工程师站、控制器、操作服务器、监控计算机、OPC 服务器、实时数据库和 PLC 等，这些控制组件一旦遭到网络攻击，往往造成的是关键数据、生产工艺与流程的破坏，甚至会引起人员伤亡、设备损坏、环境污染等重大事故。同时，这些组件所控制的系统资源重要程度是不一致的，而工业控制网络中的攻击往往具有很强的目的性，攻击者的一般目的是攻击那些能够引起最大生产损失的核心组件。同时，攻击者在工业控制网络中的攻击发起点往往不是那些核心组件，他们需要利用工业控制网络中的脆弱性来找到所关心的攻击目标并展开攻击。

### 6.2.1 工业控制网络脆弱性主要来源

整体上来看，工业控制网络脆弱性主要来自于安全策略与管理流程、工控平台和工业控制网络。具体而言，工业控制网络脆弱性主要来自于以下方面：

- 集成在 ICS 中的未打补丁的第三方应用程序；
- ICS 组件上未打补丁的操作系统；
- 不必要的服务造成的组件暴露；
- 不安全的 ICS 代码；
- 易于受到欺骗和中间人攻击的远程访问协议和工业通讯协议；
- ICS 通讯和数据传输中脆弱的服务器应用；
- 数据库脆弱性，Web 脆弱性；
- 认证绕过问题和证书管理；
- 未能保证 ICS 组件环境的安全；
- 不安全的网络设计，不良的防火墙规则；
- 未能保证网络设备的安全，无效的网络监控。

### 6.2.2 工业控制网络脆弱性分布

在工业控制网络中，网络设备与协议、操作系统、工业控制软件以及其它运行在工业控制网络组件上的脆弱性使得攻击者能够发起对工业控制网络进行信息收集、破坏和操纵等攻击行为。从整体上而言，工业控制网络脆弱性主要分布在产品、组件和网络上。与产品中的脆弱性相比，组件和网络中的脆弱性要少很多，产品中存在着大量的脆弱性，大约占到整个工业控制网络脆弱性的 70％左右。

这一现象并不足为奇，因为大多数的工业控制网络产品在设计和开发过程中缺少安全规范，工业控制网络协议和相关服务器应用都易受到中间人数据查看和篡改。安全意识的缺乏导致了低质量代码，网络协议的实现表现为脆弱的认证机制和 Web 应用，由此会造成信息暴露和系统攻陷。工业控制网络产品通常采用第三方的应用产品（如 Web 服务器、远程服务和加密服务）。很多过时的且脆弱的第三方软件产品和服务被集成到新的 ICS 产品中。ICS 产品、组件和网络上的脆弱性根据功能进行细分，得到的详细脆弱性分类和分布情况如图 6.1 所示。

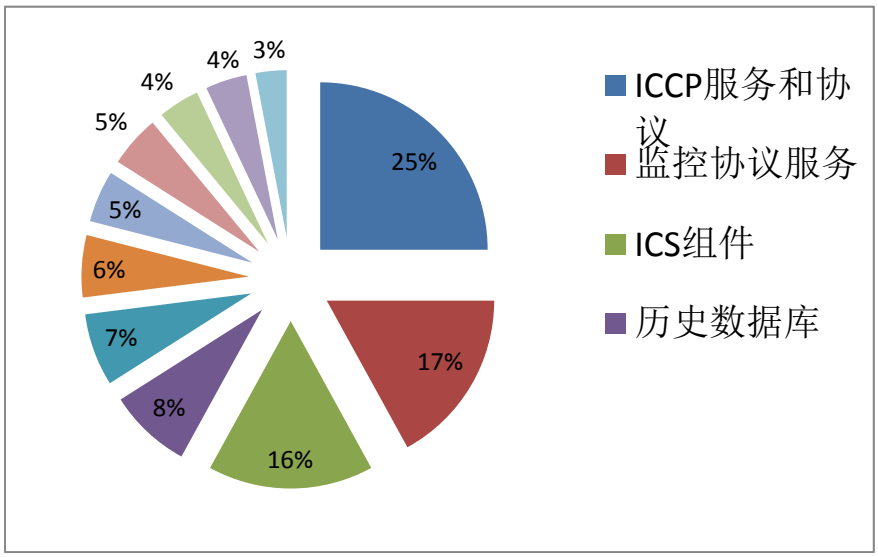


图 6.1 根据组件功能对脆弱性进行详细分类

## 6.3 工业控制网络漏洞分析

除了认识工业控制网络信息安全问题的根源，了解工业控制网络的漏洞会给防御者带来优势。许多漏洞都源于应用程序或网络协议栈的软件缺陷，而其他漏洞则源于薄弱的安全策略、糟糕的网络设计和其因素。

### 6.3.1 工业控制网络漏洞种类

NIST SP 800-82 中列举了常见的工业控制网络漏洞，该漏洞列表的范围较广，包括不充足的安全策略导致的程序漏洞（如缺乏培训、安全意识和规范化的安全过程等）、平台配置漏洞（即未打补丁的系统、使用默认配置和弱口令等）、软件漏洞（固有的缺陷，如缓冲区溢出；脆弱的协议或服务，如 DCOM 等）、缺乏足够的恶意软件、网络配置不当（薄弱的网络安全控制、未加密、无访问控制、无冗余设计等）、低级的网络认证和边界防护、无完整性检测。

表 6.2 常见的工业控制网络漏洞

| 漏洞类型 | 常见漏洞 | 推荐措施 |
|---|---|---|
| **策略和程序的漏洞** | 不安全的体系结构设计 | 识别功能组，并且使用合适的安全措施分离到安全区域中 |
| | 在 ICS 中没有和很少安全审计 | 实现集中的日志和事件收集报告机制 |
| | 缺少针对 ICS 的专门的配置变化管理 | 使用历史数据或引入历史数据系统到 |

| | | |
|---|---|---|
| | | 安全工具中，监管控制过程的变化 |
| **平台配置漏洞** | 操作系统和供应商软件补丁可能直到明显的安全漏洞被公布后才会开发；<br>操作系统和应用程序安全补丁没有进行维护；<br>操作系统和应用程序安全补丁没有进行充分测试； | 执行常规漏洞评估扫描以及遵循漏洞管理措施 |
| **默认配置漏洞** | 缺乏安全的口令策略<br>没有使用口令；<br>口令泄露；<br>口令猜测。 | 在漏洞评估过程中检查弱口令或长期不更换的口令 |
| **平台软件漏洞** | 缓冲区溢出；<br>没有安装默认的安全功能；<br>未定义、定义不明确或非法条件等误处理。 | 执行常规漏洞评估扫描以及遵循漏洞管理措施 |
| | 用于过程控制的 OLE 依赖于远程过程调用以及分布式组件对象模型；<br>使用了不安全的 ICS 协议。 | 对定义的区域外的 SCSDA 和 DCS 进行监控 |
| | 运行了不必要的服务 | 漏洞扫描能够识别主机上开放的端口和服务，同时网络流量监控能识别网络正在使用的服务 |
| | 入侵检测、防御软件未安装 | 实现基于主机或者是基于网络的入侵检测。主机 IDS 至少要在所有的关键资产中使用，网络 IDS 应该要在所有的区域边界使用。 |
| | 没有维护日志 | 所有日志应使用日志管理系统或者是 SIEM 系统集中收集和使用。对于不能产生日志的设备，应采取补救措施，比如，采用被动的网络监控以生产代理日志，或使用历史数据系统。 |
| | 事件未检测 | 实现事件关联和集中分析系统，检测潜在的事件并将其归档。 |
| **平台恶意软件防护漏洞** | 恶意程序防护软件没有安装 | 安装主机或网络防恶意程序软件 |
| | 恶意程序防护软件及其数据库不是最新的 | 在基于白名单而不是基于签名检测的基础上考虑主机及网络防恶意程序软件的解决方案 |
| | 恶意程序防护软件没有进行充分的测试 | 进行充分的测试 |

| | | |
|---|---|---|
| **网络配置漏洞** | 脆弱的网络安全体系结构 | 识别功能组，并且使用合适的安全措施分离到安全区域中 |
| | 没有部署数据流控制 | 实现防火墙、路由器或者 ACL 控制强制进行数据流控制。<br>使用网络管理系统、网络异常行为检测系统或其他工具监管违规的数据流。 |
| **网络边界漏洞** | 安全边界没有定义<br>没有防火墙或者没有正确的配置防火墙 | 识别功能组，并且使用合适的安全措施分离到安全区域中 |
| | 用于非受控流量的控制网络 | 在控制网络区域中对非 DCS 流量使用监控。在其他边界采取异常规则检测以防止来自控制网络的非受控流量。 |
| | 不在控制网络之中的控制网络服务 | 对各个区域的外部监控 SCADA 和 DCS，拒绝这些来自安全边界区域边界的流量 |
| | 没有足够的防火墙和路由器日志<br>在 ICS 网络中没有安全监管 | 允许登录所有的网络设备，并且实现集中收集和分析日志 |
| | | 在控制系统网络中实现具有 SCSDA 和 DCS 功能的网络入侵检测系统或其他威胁感知系统，将其作为被动的 ICS 安全监管设备 |
| | | 在理想情况下使用这些设备作为一个更大的安全信息监管解决方案的一部分 |
| **通信漏洞** | 用户、数据或设备的认证低于标准或者就是根本没有认证 | 实现集中式的认证管理。在理想情况下，使用身份认证管理环境的监管工具监测管理用户活动 |
| | 对通信数据缺乏完整性检查 | 实施白名单策略技术，以确保只有经过认证的通信才能经过应用层内容检测设备或类似的技术来验证所有的通信数据的完整性，以确保“认证过的”应用程序和协议没有在线上被修改 |
| **无线连接漏洞** | 在客户和访问点之间缺乏足够的认证 | 通过隔离区域，保护所有无线、拨号和其他远程访问方法的接入点 |
| 注：本表格仅为 NIST 所确定的 ICS 漏洞的一个子集，完整列表请参见最新版本的 NIST 800-82，http://csrc.nost.gov/publications/PubsSPs.html | | |

### 6.3.2 工业控制网络漏洞态势

工控网络已经成为信息安全人员关注的新焦点，一些恶意的攻击者不断扫描工控系统的漏洞，并使用针对工控系统的专用黑客工具发动网络攻击。今年来漏洞数量呈爆发式增长的趋势，主流的工业控制系统也普遍存在安全漏洞，且多为能够造成远程攻击、越权执行的严重威胁类漏洞。此外，工业控制网络通信协议种类繁多、系统软件难以及时升级、设备使用周期长，以及系统补丁兼容性差、发布周期长等现实问题，造成了工业控制系统的补丁管理困难，难以及时处理严重威胁的漏洞。因此，及早发现工控系统中的漏洞是保护工业控制系统的关键。

2015 年，随着“互联网+”、“中国制造 2025”等国家战略方针的出台，国内工业控制系统的网络化、智能化水平快速提高，但国内工控系统安全问题突出，系统网络普遍脆弱，整体安全形式面临严峻挑战。截至 2015 年年底，根据中国国家信息安全漏洞共享平台所发布的 2015 年新增漏洞信息，共整理出新增的工业控制网络相关的漏洞 108 个。从图 6.2 可以看出，出了 2011 年爆发式增长外，每年公开发布的新增漏洞数量都呈下降趋势。

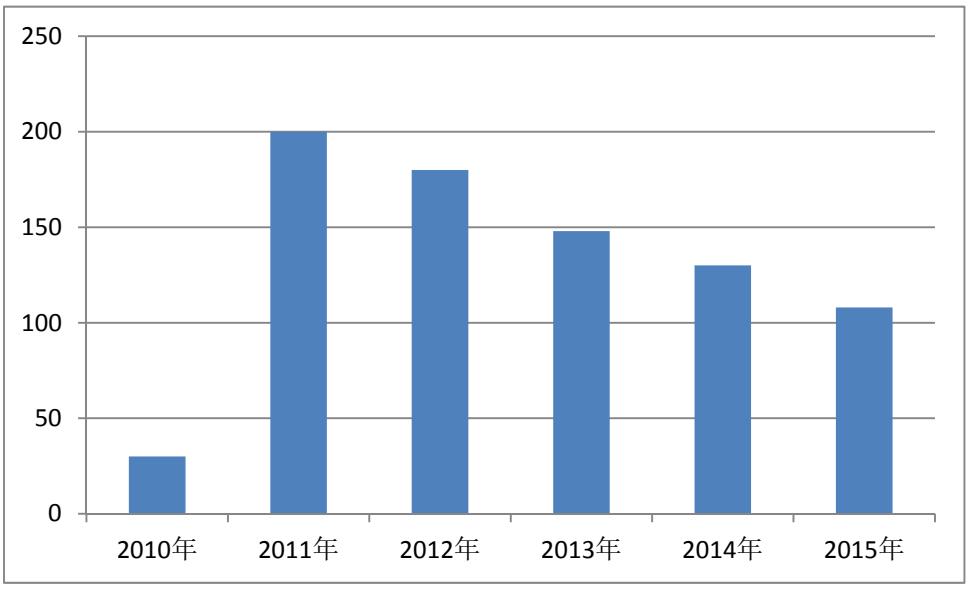


图 6.2 工控行业每年新增漏洞统计

造成这一趋势的原因如下：

一方面，工控系统的主要厂商意识到其产品在安全方面的脆弱性并加强自身产品的安全性设计和开发，是漏洞挖掘的难度增加。

另一方面，由于政治、军事等因素的影响，作为国家基础设计建设的工控系

统已经成为信息战场的必争之地，导致部分漏洞信息可能被限制公开或转为地下交易。从美国 ICS-CERT 每年发布的安全事件数量可以佐证这一推论，如图 6.3 所示。虽然每年公开的新增漏洞数量在下降，但工控安全事件数量却呈明显的上升趋势。

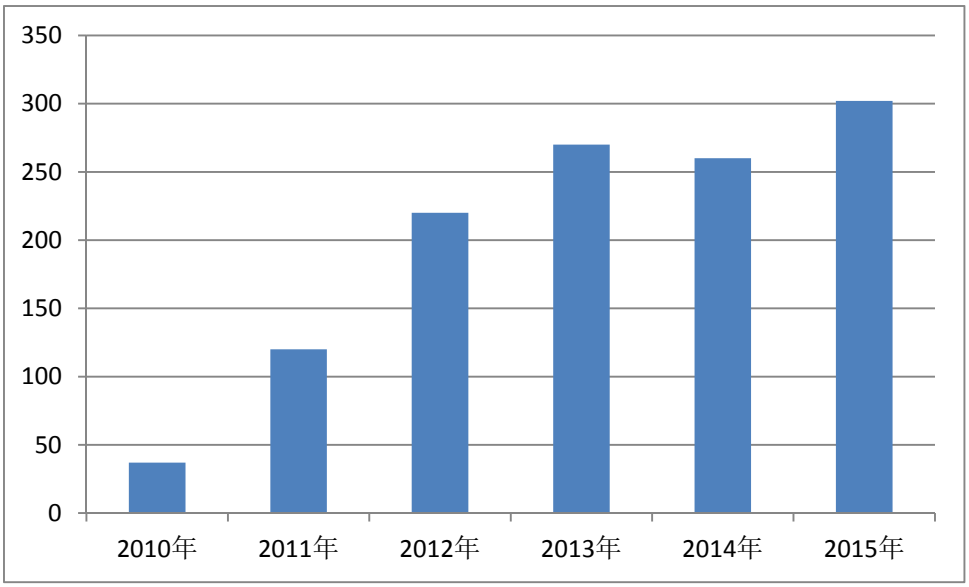


图 6.3 工控行业每年安全事件数量统计

目前，工控安全厂商和国家安全组织仍在不遗余力第收集、挖掘工控安全漏洞信息，并寻求解决方案，以帮助工控企业提高系统安全防护能力，抬高攻击者门槛和攻击成本。

# 第七章 工业控制网络安全防护技术

工业领域的安全通常可分为物理安全（Physical Safty）、功能安全（Functional Safty）和信息安全（Security）三类。

物理安全是减少由于电击、着火、辐射、机械危险、化学危险等因素造成的危害。

功能安全是为了实现设备和工厂安全功能，受保护的安全相关部分和控制设备的安全相关部分必须正确执行其功能。当失效或者故障发生时，设备或系统必须仍能保持安全条件或进入安全状态。

信息安全的范围较广，大到国家军事政治等机密安全，小到防范企业机密的泄露、个人信息的泄漏等。在 ISO/IEC 27002 中，信息安全的定义是“保持信息的保密性、完整性、可用性，另外也可包括真实性、可核查性、不可否认性和可靠性等。”

工业控制网络安全防护的核心是建立以安全管理为中心，附以符合工控网络特殊性的安全技术，进行有目的、有针对性的防御。本章将首先介绍工业控制网络安全的含义，然后针对已知安全威胁和未知安全威胁的处理方法，分别阐述如何实现工业控制网络的基础软硬件安全、设备与主机安全、行为安全和结构安全。

## 7.1 工业控制网络安全的内涵和外延

工业控制网络安全是工业领域安全的一个分支，是近年来学术界和产业界共同关注的热点。工业控制网络安全与传统的信息网络安全有一定的共性，在很多方面都存下交集，但也存在许多显著区别，取决于工业控制网络的架构。

工业控制网络的安全是针对工控网络中的设施和信息保护而言的，涉及一下三个方面的基本需求。

- 可用性

工业控制网络安全必须确保所有必须确保工业控制系统中的各个部件可用，运行正常以及功能正常。

工业控制系统的工作过程是连续的，不能接受意外中断，如果需要人为中断，必须提前计划和安排，即使如此，在具体实施前开展测试也是必须的，以确保工

业控制系统的高可用性。针对意外中断，许多工业控制系统为了保证生产的连续性，不允许随意启动和停止设备。在某些情况下，生产的产品或者使用的设备比信息中断增加重要。因此，如果简单采用典型信息网络的安全策略，如重新启动某个组件，通常在工业控制网络安全中是无法接受的，将会对工业控制系统的可用性、可靠性和可维护性产生不利影响。在某些工业控制系统中包含许多冗余部件，它们并行运行，在主部件出现故障后可以切换到备份部件，从而提高系统的工作连续性。

- 完整性

工业控制网络安全必须确保工业控制系统中的各种信息的完整性和一致性。主要涵盖一下两个方面：数据完整性，即数据未被篡改或者破坏；系统完整性，即系统未被非法操作，按既定的目标运行。

- 保密性

工业控制网络安全必须确保对工业控制系统中各个部件和信息的授权访问，防止系统中盗用和盗取事件的发生。

和传统信息网络相比，工业控制网络对上述三个需求的优先级存在明显区别，如图 7.1 所示。

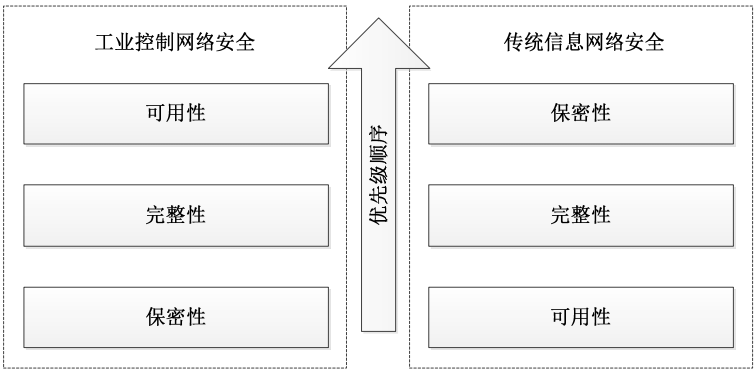


图 7.1 工业控制网络与信息网络安全需求对比

## 7.2 已知安全威胁的防护技术

本节将介绍针对关键基础设施安全基准来解决安全架构的设计针对已知威胁的防御技术。

### 7.2.1 结构安全

结构安全性即基础设施建设过程中网络拓扑结构、以及区域、层次的划分是否满足安全需求。通过隔离、过滤、认证、加密等技术，实现合理的安全区域划分、安全层级划分，实现纵深防御能力。对于新装系统，应实现结构安全同步建设;对于再装系统,应进行结构安全改造;对于因条件限制无法进行改造的系统，应建立安全补偿机制。所以结构安全最为重要,结构安全解决了大部分安全问题。结构安全可以从两个部分考虑,分别为网络结构的优化与防护技术和设备的部署。

- 结构优化

结构主要指的是网络的结构，但是也包括生产的布局结构。它与入侵容忍度是紧密相关的。当安全事件发生的时候，必须有相应的结构，这样才能保证工业控制系统中的其他部分不受影响。本质上这就是“分区隔离”的概念，它会将危害限制在一个尽量小的可控范围之内,如国家电网采用的“横向隔离、纵向认证”策略。

结构安全中所谓的隔离并不一定是物理隔离,因为工业控制系统中很多部分需要互联，甚至是互联网的接入，因此引入了访问控制技术。新装系统的结构安全性问题和在装系统的结构安全性改造问题大多数时候就是将部分行为安全中安全管理的内容条理化，转变为结构安全问题。

但是结构安全在最新的应用场景下也暴露出了新的问题,这就是无线网络的应用。例如，传输线路采用光纤和无线互为备份，因为无线是开放的，所以就带来了结构安全性问题。如果此时想要保证结构安全性，既可以对网络进行调整，也可以增加新的技术、设备措施。

- 访问控制

结构安全的根本所在就是通过控制如何访问目标资源来防范资源泄露或未经授权的修改。访问控制的实现手段在本质上都处于技术性、物理性或行政管理性的层面。基于策略的文档、软件和技术、网络设计和物理安全组件都需要实施这些控制方法。工业控制网络的接口处是最应该实施安全控制的一个地方，毕竟这是通向关键资产的入口，需要层层防御来实施访问控制。

访问控制本身是一种安全手段,他控制用户和系统如何与其他系统和资源进行通信和交互。访问控制能够保护系统和资源免受未经授权的访问，并在身份认

证过程成功结束后确定授权访问的等级如图 7.2 所示模型，在访问控制环境中，正确理解主体和客体的概念是非常重要的。

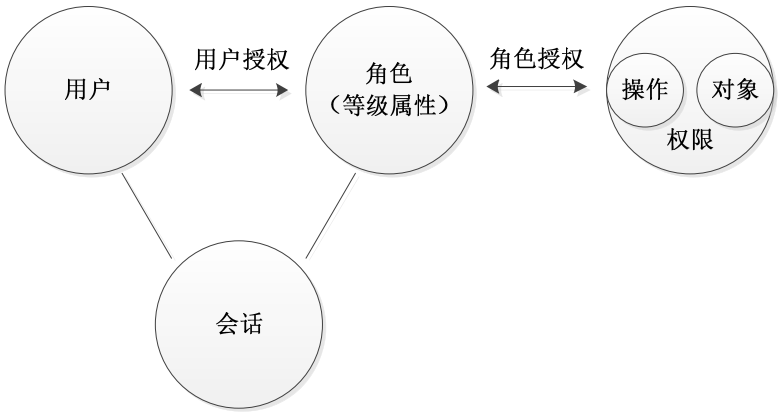


图 7.2 主体-客体角色约束模型

访问是在主体和客体之间进行的信息流动。主体是一个主动的实体，它请求对客体或者客体内的数据进行访问，主体可以是通过访问客体以完成某种任务的用户、程序或进程。当程序访问文件时，程序是主体，而文件是客体。客体是包含被访问信息或者所需功能的被动实体。在工业控制网络中，客体可以是某个系统、PLC、传感器、计算机、数据库、文件、应用程序、目录或数据库中某个表内包含的字段。

访问控制包含的范围很广，它涵盖了几种对计算机系统、网络和信息资源进行访问控制的不同机制。因为访问控制是防范计算机系统和资源被未授权访问的第一道防线，所以地位非常重要。用户的访问权限主要基于其身份、许可等级和组成员资格。访问控制给予组织机构控制、限制、监控以及保护资源可用性、完整性和机密性的能力。

- 防火墙技术

防火墙用于限制从另一个网对特定网络的访问。防火墙设备支持和实施企业的网络安全访问策略。有组织的安全访问策略可以提供高层次、可接受和不可接受的操作的提示，从而维持整体的边界安全性，所以防火墙技术本身也是结构安全层面最为重要的安全技术手段，是实现结构安全的基础。防火墙具有定义更详细和更细粒度的安全策略的能力，从而规范工业控制网络中哪些地址、哪些端口、哪些服务或者协议允许或者被禁止访问哪些区域。一般情况下，防火墙提供以下四种主要服务：

1) 服务控制：确定可以访问的网络服务；

2) 方向控制：决定在哪个方向上的服务请求可以被发起并通过防火墙；

3) 用户控制：内部用户、外部用户所需的某种形式的认证机制；

4) 行为控制：控制一个具体的服务怎样被实现。

防火墙的实现形式包括搭载防火墙软件产品的服务器或者其他特殊硬件设备，防火墙会将经过它的数据包进行分析过滤，可能丢弃、重新打包、重定向或者直接放行。通常在工业控制网络结构优化设计阶段，会使用防火墙在工业企业内部不同安全级别和业务需求的区域之间部署防火墙产品和策略，实现彼此之间互相访问资源的时候可以有严格的安全策略进行过滤和控制。

### 7.2.2 设备与主机安全

设备与主机安全即工控环境中各种设备自身的安全性。例如，智能设备在基础设施建设中广泛使用，包括感知设备、网络设备、监控设备等，这些设备普遍存在漏洞、后门等安全隐患。保证工业控制系统中的设备与主机的安全性赢首先具备标准化的监测工具，这些智能设备在出厂时需要做充分监测从而保证设备的离线安全、在项目建设过程中进行入网安全监测、在项目运行过程中进行实时的在线监测，从而全方位保证设备的自身安全性。

设备与主机的安全很重要的一点就是设备本身的安全性。大量工控厂商会混淆稳定性和安全性的概念，例如双备份系统，一定程度上增强了系统的稳定性，但如果两个系统都存在同样的安全缺陷，双备份系统并不会增强安全性。对于实际使用这些系统的工业企业而言，也很难发现和解决这些安全缺陷。

- 漏洞发现与补丁

工业企业自身即使发现漏洞并打好补丁的可能性比较小，而且还存在一个时间窗口。而工业控制设备厂商的版本发布周期长达一年甚至更长，发现问题后一般无法即使修改代码。因此，信息网络中普遍使用的打补丁方法，在先天缺乏安全基因的工业控制领域显然难以适用。因此就必须依赖漏洞扫描和漏洞挖掘技术发现系统漏洞，它们是系统管理员保障工业控制系统安全的有效工具。

漏洞扫描技术的对象包括工业网络控制设备、工业网络工控系统、工业网络安全设备和工业网络传输设备等。进行漏洞扫描时，首先探测目标的存活性，然后对存活设备进行端口和协议扫描，确定目标开发的端口和运行协议，同时根据

协议指纹识别技术判别目标的系统类型和版本，最后根据上述信息，调用漏洞资料库中的各种漏洞注意进行检测，通过对响应数据包的分析判断目标对象是否存在漏洞。漏洞扫描技术主要针对已知漏洞，而漏洞挖掘技术则侧重发现工业控制系统中未知的安全威胁。现阶段，安全研究人员对于工业控制设备的内部结构了解不足，对工业控制设备的逆向技术处于起步阶段，又很难获得工业控制系统的源代码和目标文件，无法采用白盒和灰盒测试方法，因此采用模糊测试来挖掘工业控制设备漏洞的方法较为常见。

- 补偿性措施

当某个特定数据包会导致工业控制系统崩溃或者引发进一步的安全问题时，保护设备可以拦截该数据包，这样就不用修改工业控制系统代码或者安装补丁了。类似此类保护设备实现的功能称之为补偿性措施。

保护设备放置在需要保护的工业控制设备或者系统的前端。如果用户已知某个漏洞风险很大，一定导致某些危害，并且已经曾经发生过，那么这样的补偿性措施对用户而言就尤为必要，并且这类补偿性措施的升级比工业控制系统本身的升级和打补丁的风险要低得多。

此外，设备与主机的安全性问题也可能被意外触发（非恶意攻击）。例如，不同厂商的工业控制设备部署在同一系统中，可能存在相互干扰，即使非恶意使用也会导致恶意结果。对于工业企业而言，有效管理这部分威胁对于提高设备和主机的安全性也非常重要。

### 7.2.3 行为安全

行为安全包括两部分，即系统内部发起的行为是否具有安全隐患，系统外部发起的行为是否具有安全威胁。行为安全性防护首先应具备感知能力，在云端通过大数据分析感知威胁和安全态势，通过本地端通过靶场、蜜罐、审计、溯源等技术，对网络流量、文件传输、访问记录等进行综合分析与数据挖掘，实现对已知威胁和未知威胁的感知，以及对全局和局部安全态势的感知，并与其它安全技术联动，对不安全行为及时进行处理。除了行为分析技术外，在工业控制网络中，行为安全的管理技术也非常重要。行为安全管理不仅针对恶意的，也包括非恶意的，例如操作员错误发出一个指令，可能导致整个系统停机。此外行为安全管理

还包括许多日常管理，如 USB 设备管理、定期操作审查等。

改善系统中行为安全的最常见的技术为入侵检测技术。它是对入侵行为的发觉，通过从网络或特定系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测软件和硬件的组合便是入侵检测系统，其对系统的运行状态进行监视，发现各种攻击企图、攻击行为或者攻击结果，以保证系统资源的机密性、完整性和可用性。

### 7.2.4 基础软硬件安全

基础软硬件安全性即工业控制系统使用的 CPU、存储器、操作系统内核、基本安全算法与协议以及各种其他核心软硬件的完全可信、自主可控。有条件的工业企业，应实现对自有系统与设备的基础软硬的安全性改造，以及对进口系统与设备的基础性软硬件安全性加固。不具备条件的工业企业，也应增加安全补偿机制。

基础软硬件安全的概念非常宽泛，它的核心概念在于免疫性安全，即设备自身具有排除破坏、攻击、篡改的能力。基础软硬件安全技术中相对具有代表性的是可信网络和可信计算。

可信网络架构不是一个具体的安全产品或一套针对性的安全解决体系，而是一个有机的网络安全全方位的架构体系化解决方案，它强调实现各厂商的安全产品横向关联和纵向管理。可信网络的一般性架构主要包括可信安全管理系统、网关可信代理、网络可信代理和端点可信代理四个部分，从而确保安全管理系统、安全产品、网络设备和端点用户 4 个安全环节的安全性与可信性。它旨在实现用户网络资源的有效整合、管理与监管，实现用户网络的可信扩展以及完善的信息安全保护；解决用户的现实需求，达到有效提升用户网络安全防御能力的目的。

可信计算是一项由可信计算组织推动和开发的技术。该技术的拥护者称它将会使计算机更加安全，更加不易被病毒和恶意软件侵害，因此从最终用户角度来看也更加可靠。而反对者则认为可信计算背后的那些公司并不那么值得信任，这项技术给系统和软件的设计者过多的控制权和控制。从广义的角度，可信计算旨在为网络用户提供一个更为宽广的安全环境，它从安全体系的角度来描述安全问题，确保用户的安全执行环境，突破被动防御打补丁的方式。

## 7.3 未知安全威胁的防护技术

防火墙、IDS 和防病毒等技术措施都是针对已知安全威胁，本节将讨论如何发现和防御工业控制网络中新型的、未知的安全威胁。

### 7.3.1 纵深防御技术

按照传统的纵深防御技术针对工业控制网络的结构进行全面部署之后，至少应该具备类似传统信息网络中防火墙、入侵检测系统、入侵防御系统、防病毒和应用程序监控等安全设备的能力。纵深防御技术除了可以解决结构安全和提供对已知威胁的防御能力之外，如果应用巧妙也可以发现和防御很多未知威胁的攻击。

防火墙和 IDS 设备的特定策略都可以用来评估各种行为，匹配策略的不同条件对应的不同行为可以区分所有数据的情况，虽然防护的结果是“是非判断”的结论，但是通过分析大量看似安全的行为和事件同样可以发现可疑的潜在威胁。使用数据挖掘的方法分析数据和日志信息，将它们建立相互关联，就能够覆盖防护区域内的通信状态、用户访问、运行状态和控制管理等。例如，在工业控制网络内部通信的源地址不可能出现无法识别的非内网网段地址。

### 7.3.2 异常行为检测

有时即使一个非威胁行为也可能违背预设的安全策略，通过与已知的正常参数进行比较和分析就可以了解到这些异常事件的具体原因。这种比较可以采用人工方式也可以使用程序自动化分析处理，其最大的意义在于实际的业务运转过程中必然会有大量的数据或者事件产生，其中一部分可能是没有意义“脏数据”，但还有可能是目前未知的新的攻击方法产生的数据，后者是攻击者为实施某一攻击目的所做的铺垫行为。

发现这些异常的情况并分析出潜在的恶性后果是异常行为检测的最终目的，为了实现这些目的必须首先定义一些固定的衡量标准和算法，这些衡量标准被称为衡量参量。参量就包括正常参量和异常参量，这是进一步进行异常行为检测和分析的基础。通过一个或者多个参量可以将某个异常行为完全确定下来。

异常参量作为异常行为检测的最小分析单元，需要通过一个特定的衡量标准

进行制定，在不同行业的工业控制系统中可能有较大差别。但是因为所有的正常和异常行为特性都必然在同一个时空轴中进行，所以不同行业中众多的异常参量中会有一个共有的固定参量，即时间参量。每一参量都是基于固定时间的运行平均值，这个特性为现有业务行为之间的比较提供了基础。异常参量不仅在比较过去和现在的行为方面行之有效，在衡量工控控制系统中的程序处理能力、业务指标等方面也非常有效。通过分析参量的过去情况可以预测未来行为的延续性趋势。

通过对比异常参量可以发现偏离正常范围的一些异常情况，但是单一的异常参量并不一定可以确定一个异常事件或是威胁。那么，对于有些具有时间规律的业务就可以引入时间参数取解决这个问题，生产一个非线性基线图作为参量。例如，为管理员一周时间内登录系统的次数绘制基线图，那么可能周一的频次会较多，而周末则偏少。时间相关的基准是非常有用的，因为大量的业务规律都随着时间变化呈现一定的规律性。针对不同的业务场景和系统情况，可能 1 小时为一个周期、1 天为一个周期，甚至 1 个月、1 个季度为一个周期。每个工业控制系统都可能有数百个这种基于不同时间规律的基线。通过对这些基线的异常参量，就可以发现一些可疑的异常行为。

由于无需依赖检测标志，异常行为检测是一种非常实用的未知威胁检测技术。相比于一般的信息系统，工业控制系统中的业务的规律性和稳定性更强，通过时间参量进行建模之后，随着时间推移能够检测分析出大多数场景中的异常行为。

### 7.3.3 白名单技术

结构安全中使用的访问控制功能本质上就是白名单技术的应用，人工培植的每一条访问控制安全策略就是每一个访问路径的白名单规则。白名单的防御技术是一种与黑名单思路截然相反的安全防御方式，它本身不需要分析和检测未知威胁，只需要关心哪些不是威胁即可达到安全防护的效果。常见的白名单技术有以下几类。

- 应用程序白名单

应用程序白名单是用来防止未认证的应用程序运行的一种措施，只有规则允许的应用程序才能被运行。在特定的工业应用场景下，需要针对场景中为了实现业务系统的正常运转所需使用的所有软件和应用程序进行统计，然后对其进行充

分的代码审计、安全测试和分析，结合完整性检查方法的应用，一般为散列法，确保该应用程序是已经认证安全通过的。

- 用户白名单

为了发现一些潜在威胁，针对一般用户活动和管理员行为的分析是非常必要的。大量的渗透攻击都是通过拿到一定权限的用户或管理员账号后实施下一步恶意行为的。用户白名单的技术措施独立于系统自身的用户管理措施，但不同于结构安全中的基本访问控制功能，其自身还针对用户所拥有的权限进行白名单管理，实现了部分审计功能的自动化。

- 资产白名单

许多针对工业控制系统的攻击和误伤行为，都是由于在工业控制网中非法接入了其他设备造成的。可以借助成熟的自动化网络扫描工具，快速获得工业控制网络中的资产清单。结构安全中基于边界的各种安全策略通过白名单技术可以落实到每一个设备上。一旦恶意设备或地址接入到工业控制系统中，基于资产白名单技术，通过结构安全方法仍然能快速检测到该威胁源。

- 行为白名单

同资产白名单一样，应用程序的每一个行为都可以被记录为白名单，并且行为白名单也需要先进行明确的定义，从而将应用程序的正常业务行为和其他恶意或无关行为区分开。相比于应用程序白名单和资产白名单，行为白名单要以更细粒度、更加贴合业务的方式定义和实现。

### 7.3.4 关联分析技术

- 智能列表

智能列表的概念在“2010 欧洲 SCADA 与过程控制峰会”上首次提出，它将智能分析引入到白名单的概念中，从而相结合催生出智能列表概念。通常黑名单技术阻断恶意行为，白名单技术只允许合法的行为，而智能列表则基于白名单和时间轴线，动态定义黑名单的内容。智能列表本质上是一种基于多种白名单技术和关联比对能力，可以动态调整黑名单安全机制的新型控制方式。这种方式可以在新出现的威胁爆发的时候，第一时间对其进行发现和识别。

- 事件关联

事件关联是利用大量离散的事件数据并将其作为一个整体，结合时间和实际的场景等客观因素进行综合分析，找到需要立即引起注意的重要模式和事故，从而提高威胁监测方法和手段的能力，发现一些隐藏在正常时间数据背后的异常事件。从某种意义上而言，事件关联的灵感其实多来自于人工分析安全问题的方式，目前事件关联技术的发展程度虽然还没有达到可以完全替代人工的程度，但是已经可以给人工的安全评估工作提供许多便利，解决一些人工难以处理的问题。

### 7.3.5 蜜罐技术

蜜罐是一种引诱攻击者，主动吸引扫描、攻击流量，并监视、检测和分析攻击的技术。蜜罐的价值在于可以捕获、发现新的攻击手段及攻击方法，是针对未知威胁最有效的发现工具。由于蜜罐技术的目的性强，捕获的数据价值高，误报和漏报的情况极少，对于大多数应用场景都适用。典型的工业控制系统蜜罐为模拟某种工业控制设备，并将它与互联网相连或者与本地真实的工业控制网络相连。

蜜罐技术的核心主要有三个部分：数据捕获技术、数据控制技术以及数据分析技术。蜜罐根据系统功能的区别可以分为产品型蜜罐和研究型蜜罐；根据交互程度的区别可以分为低交互蜜罐和高交互蜜罐。

蜜罐技术具有误报率和漏报率低的优势，拉近了攻防双方的距离，使得安全防护的一方不再完全被动。入侵检测、防火墙、认证加密等技术都存在缺陷性，它们与蜜罐技术紧密结合，将成为未知威胁检测最有利的武器。

# 第三部分：数据驱动的工业控制网络安全

# 第八章 工业控制设备扫描识别

无论是网络系统安全性评估还是黑客发起网络攻击，网络扫描都是不可或缺的重要手段。通过网络扫描能够发现网络中各种设备开放的端口、服务、硬件型号、软件版本，甚至内存中的数值以及这些服务存在的安全漏洞。

## 8.1 工控设备扫描识别技术

### 8.1.1 工控设备扫描识别技术介绍

工控设备扫描识别是利用不同信息描述运行于网络中的工业控制设备或者软件的一种技术。我们了解最多的是工控设备指纹，被用来远程识别工控设备的硬件，操作系统，运行软件（及其相关的版本号，配置参数）等信息。

指纹提取方法主要分为两类：主动式（active）和被动式（passive）。主动式指纹提取要求工具去主动扫描网络系统获取信息，被动式指纹提取方法则是通过尽可能少的网络侵扰（less intrusive），被动式的监听网络获取信息。通常，主动式指纹识别成功识别系统的概率更大些。这是因为主动式识别意味着收集所有生成 fingerprint 所需要的信息，而被动式识别只能收集会话通道信息。但主动式识别并不是任何时候都能够起作用，探测扫描更易造成网络繁忙，且易被检测。例如，在 SCADA 系统中，主动式扫描可能造成系统过载。主动调试会使设备处理的 frame 数量增长，PLCs 和 RTUs 无法支持超出的流量，从而导致正常请求无法响应。而被动式监听网络由于收集信息复杂则存在指纹准确性问题。

指纹识别技术应用于 ICS 领域的过程中，在相对传统网络有可利用的优势同时也伴随着挑战。ICS 系统组件相对于常规互联网和公司局域网有着其固有的特性和缺陷。一方面，相较于传统 IT 系统，ICS 系统中工控设备具有长生命周期，稳定的网络拓扑和会话；另一方面，信息采集方式面临着主动式或是被动式方法选择问题，设备多样化，长时间 TCP 会话连接等问题。设备供应商协议定制则是一把双刃剑,协议允许检测者对 ICS 系统进行定位（公开协议）或者识别特定设备（私有协议），而相对私有协议做报文分析因无文档而显得很困难。

在 ICS 环境中，我们总是更倾向于只使用被动式监控，最小化潜在的风险。

目前已有些比较成熟的被动式识别工具（如 ettercap, p0f, Satori and NetworkMiner）,它们基于 TCP/IP 协议栈监听分析网络。但研究者们更倾向于采用透明的，无深度包检查的方式来识别 ICS 网络行为。

### 8.1.2 工控设备扫描识别工具

Nmap （网络映射器）是一个开源工具，它使网络探测和安全审计得以专业化。最初由 Gordon “Fyodor” Lyon 发布。官网官方网站是 http://nmap.org。Nmap 采用一种新颖的方式利用原始 IP 包来决定网络上是什么样的主机，这些主机提供什么样的服务（应用程序名和版本），它们运行着什么样的操作系统（操作系统版本）它们使用什么类型的过滤器/防火墙以及许多其他的特征。它虽然被设计用来快速扫描大型网络，但是在单个主机上也会工作的非常好。Nmap 可以运行在所有的主流计算机操作系统上，Linux，Windows，Mac OS X 都可以找到官方的安装包。Nmap 脚本引擎 （NSE） 是 Nmap 最有力灵活的的一个特性，它允许用户撰写和分享一些简单的脚本来一些较大的网络进行扫描任务，这些脚本是用 Lua 编程语言来完成的。Nmap 脚本库中包含一些工业设备发现的脚本，如 s7-info.nse、modbus-discover.nse 等，我们可以利用这些脚本进行工控设备探测识别，也可以根据工业协议自己开发脚本进行探测。


图 8.1 Nmap

Zmap 是美国密歇根大学研究者开发出一款工具。在第 22 届 USENIX 安全研讨会，以超过 nmap 1300 倍的扫描速度声名鹊起。相比大名鼎鼎的 nmap 全网扫描速度是他最大的亮点。在千兆网卡状态下，45 分钟内扫描全网络 IPv4 地址。ZMap 则是一种“无状态”的工具；也就是说，这种工具会向服务器发出请求，然后就“忘记”这些请求。ZMap 不会保留未获回复请求的清单，而是在传出的数据包中对识别信息进行编码，这样一来该工具就能对回复进行鉴别。这种方法拥有巨大的优势，意味着 Zmap 输出数据包的速度比 Nmap 高出 1000 倍以上。因此，用 Nmap 对整个互联网进行扫描需要花费几个星期时间，而使用 ZMap 这

种工具则只需要 44 分钟。在拥有这种工具以后，人们将可迅速扫描整个互联网，而且费用也不高，这就为针对整个互联网的研究工作开辟了一些令人深深着迷的新可能性。Zmap 项目组也发布了开源的工控设备探测组件 Zgrab，我们可以利用该组件结合 Zmap 进行工控设备高效探测。

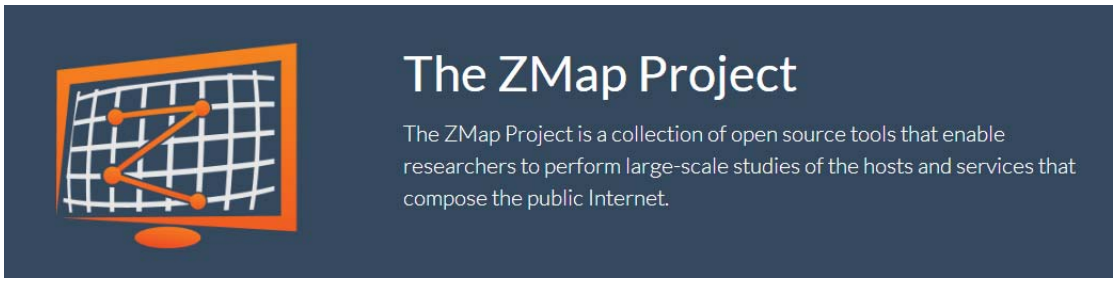


图 8.2 The Zmap Project

### 8.1.3 工控设备扫描识别技术应用场景

网络空间搜索：Shodan 是目前最流行的网络空间搜索引擎，它扫描 HTTP, FTP, SSH, Telnet, SNMP and SIP 等协议，通过分析客户端与服务端交互过程中的信息，识别全网设备。目前较流行的威胁感知系统也是利用 fingerprint devices 技术探测网络空间设备。

资产管理：现实中，系统管理员很少了解资产的全部信息，或者了解到的是错误信息。导致这种现状出现可能是因为信息未能及时更新，或者是系统维护交由外包管理，或者是设备供应商提供了错误的配置信息。因此，ICS 系统有必要提供信息保证高效的现场检查（site-inspection），系统管理员能够准确的了解系统的相关配置信息。

入侵检测：攻击者理论上可以通过注入命令或者假数据来侵扰 ICS 网络，如造成大面积停电等灾难性后果。一些设备由于老旧无法升级，甚者一些设备供应商不提供线上升级打补丁。安全工作人员能够及早的发现入侵行为显得尤为重要。

## 8.2 网络空间搜索引擎

Google、baidu、bing 等搜索引擎已经索引了整个虚拟世界，然而它们尚未成功地将自己的触角延伸到现实世界当中。区别于传统的基于内容的搜索引擎，网络空间搜索引擎是面向物联网的崭新的搜索引擎，它搜索的不是与某个字段相

关联的内容，而是每时每刻都在寻找着所有和互联网关联的物理设备，包括服务器、摄像头、打印机、路由器、工业控制设备等等，从而有效的索引现实世界。著名的网络空间搜索引擎有 Shodan、censys 和 Zoomeye。

### 8.2.1 Shodan

2004 年，John Matherly 在大学期间开发了世界上首个网络空间搜索引擎 Shodan，虽然目前人们都认为谷歌是最强劲的搜索引擎，但 Shodan 才是互联网上最可怕的搜索引擎。与谷歌不同的是，Shodan 不是在网上搜索网址，而是直接进入互联网的背后通道。Shodan 可以说是一款“黑暗”谷歌，一刻不停的在寻找着所有和互联网关联的服务器、摄像头、打印机、路由器等等。每个月 Shodan 都会在大约 5 亿个服务器上日夜不停地搜集信息。

图 8.1 Shodan 作者 John Matherly

Shodan 所搜集到的信息是极其惊人的。凡是链接到互联网的红绿灯、安全摄像头、家庭自动化设备以及加热系统等等都会被轻易的搜索到。Shodan 的使用者曾发现过一个水上公园的控制系统，一个加油站，甚至一个酒店的葡萄酒冷却器。而网站的研究者也曾使用 Shodan 定位到了核电站的指挥和控制系统及一个粒子回旋加速器。


图 8.4 Shodan 页面 1

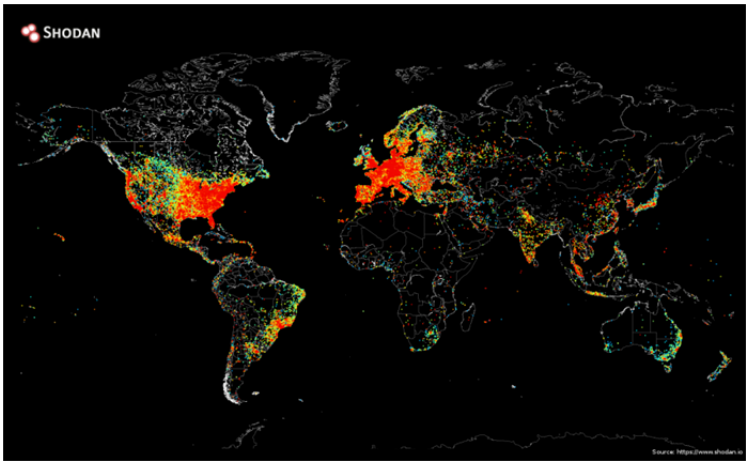


图 8.5 Shodan 页面 2

由于 2008 年开始，美国土安全部（DHS）利用 Shodan 展开 SHINE 计划，使得 Shodan 具备了深刻的政府背景。Shodan 上能找到的设备包括但不限于服务器、路由器、交换机、公共 IP 地址的打印机、网络摄像头、加油站的泵、VOIP 电话、SCADA 系统等等。

使用 Shodan 需要注册账号，搜索服务免费，但并不能查看所有搜索结果。目前 Shodan 支持免费查看 20 条搜索结果，查看其他的或者批量导出结果需要付费。在主页的搜索框中输入想要搜索的内容即可，例如搜索“PLC”：

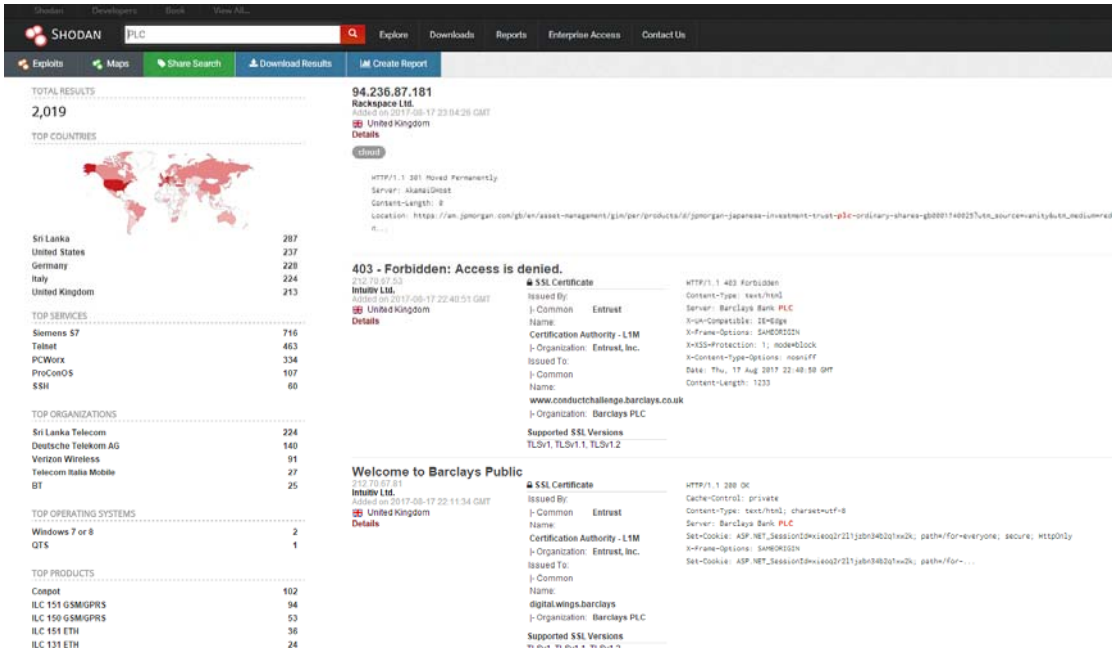


图 8.6 Shodan 查询结果

图 8.6 显示的搜索结果包含两个部分，左侧是大量的汇总数据包括：

- Results map – 搜索结果展示地图
- Top services （Ports） – 使用最多的服务/端口
- Top organizations （ISPs） – 使用最多的组织/ISP
- Top operating systems – 使用最多的操作系统
- Top products （Software name） – 使用最多的产品/软件名称

随后，在中间的主页面我们可以看到包含如下的搜索结果：

- IP 地址
- 主机名
- ISP
- 该条目的收录收录时间
- 该主机位于的国家
- Banner 信息

想要了解每个条目的具体信息，只需要点击每个条目下方的 details 按钮即可。此时，URL 会变成这种格式 https://www.shodan.io/host/[IP]，所以我们也可以通过直接访问指定的 IP 来查看详细信息。

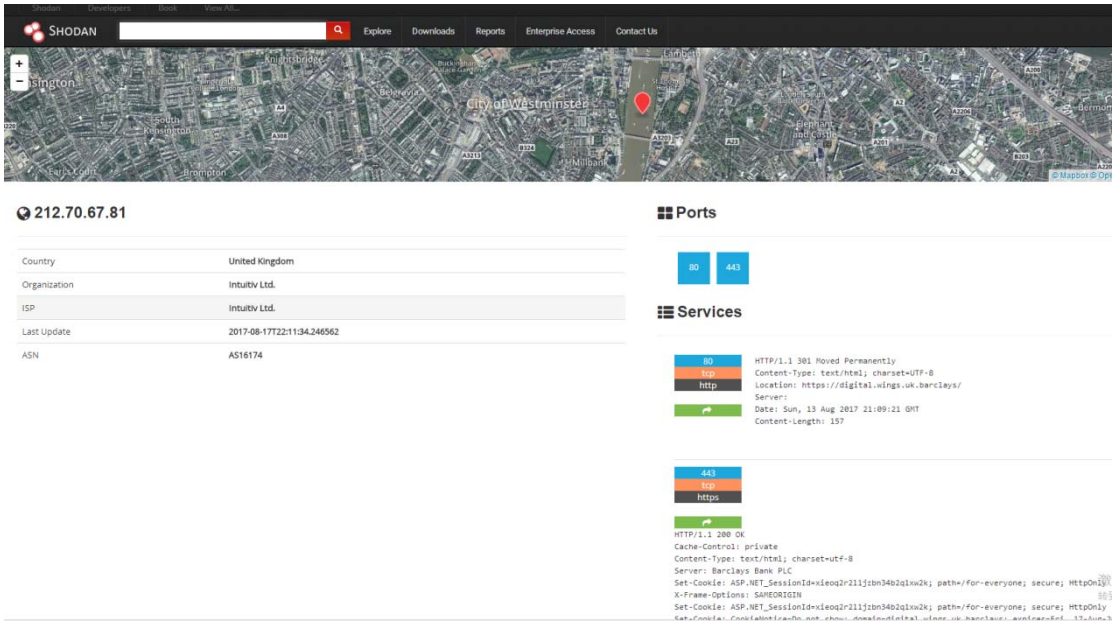


图 8.7 Shodan 查询结果

图 8.7 中我们可以从顶部在地图中看到主机的物理地址，从左侧了解到主机的相关信息，右侧则包含目标主机的端口列表及其详细信息。

如果像前面单纯只使用关键字直接进行搜索，搜索结果可能不尽人意，那么此时我们就需要使用一些特定的命令对搜索结果进行过滤，常见用的过滤命令如下所示：

hostname：搜索指定的主机或域名，例如 hostname:"google"

port：搜索指定的端口或服务，例如 port:"102"

country：搜索指定的国家，例如 country:"CN"

city：搜索指定的城市，例如 city:"BeiJing"

org：搜索指定的组织或公司，例如 org:"google"

isp：搜索指定的 ISP 供应商，例如 isp:"China Telecom"

product：搜索指定的操作系统/软件/平台，例如 product:"Apache httpd"

version：搜索指定的软件版本，例如 version:"1.6.2"

geo：搜索指定的地理位置，参数为经纬度，例如 geo:"31.8639, 117.2808"

before/after：搜索指定收录时间前后的数据，格式为 dd-mm-yy，例如 before:"11-11-15"

net：搜索指定的 IP 地址或子网，例如 net:"210.45.240.0/24"

此外，Shodan 还为研究者提供了 API 开发接口，支持各种主流编程语言，

研究者可以利用 API 更加方便的进行信息检索。

### 8.2.2 Censys

Censys 是由密歇根大学的科研人员发布的一款网络空间搜索引擎，它允许计算机科学家了解组成互联网的设备和网络。Censys 由因特网范围扫描驱动，它使得研究人员能够找到特定的主机，并能够针将设备、网站和证书的配置和部署信息创建到一个总体报告中。


图 8.8 Censys

与 Shodan 不同的是，Censys 所有搜索结果都能免费提供，但通过 Web 页面只提供前 10000 条结果，多于 10000 条需要通过调用 API 的方式获取。更为令人兴奋的是，Censys 还免费提供原始扫描结果数据下载，如图 8.9 所示。如果感兴趣的话，甚至可以在网上找到 Censys 的扫描源代码。

| Name | Port | Protocol | Subprotocol | Destination | Last Scan |
|---|---|---|---|---|---|
| 0-icmp-echo_request-full_ipv4 | | icmp | echo request | full ipv4 | 2017-10-13 23:00:53 |
| 21-ftp-banner-full_ipv4 | 21 | ftp | banner | full ipv4 | 2017-10-16 22:31:45 |
| 22-ssh-v2-full_ipv4 | 22 | ssh | v2 | full ipv4 | 2017-10-18 00:19:02 |
| 23-telnet-banner-full_ipv4 | 23 | telnet | banner | full ipv4 | 2017-10-18 00:01:27 |
| 25-smtp-dhe_export-1%_sample_ipv4 | 25 | smtp | dhe export | 1% sample ipv4 | 2017-10-18 14:15:23 |
| 25-smtp-starttls-alexa_top1mil | 25 | smtp | starttls | alexa top1mil | 2017-10-18 12:44:29 |
| 25-smtp-starttls-full_ipv4 | 25 | smtp | starttls | full ipv4 | 2017-10-15 00:13:20 |
| 53-dns-lookup-full_ipv4 | 53 | dns | lookup | full ipv4 | 2017-10-15 23:05:54 |
| 80-http-get-alexa_top1mil | 80 | http | get | alexa top1mil | 2017-10-18 13:11:57 |
| 80-http-get-full_ipv4 | 80 | http | get | full ipv4 | 2017-10-12 07:04:56 |
| 102-s7-szl-full_ipv4 | 102 | s7 | szl | full ipv4 | 2017-10-18 12:33:07 |
| 110-pop3-starttls-full_ipv4 | 110 | pop3 | starttls | full ipv4 | 2017-10-15 00:18:28 |
| 143-imap-starttls-full_ipv4 | 143 | imap | starttls | full ipv4 | 2017-10-15 22:45:51 |
| 443-https-dhe-alexa_top1mil | 443 | https | dhe | alexa top1mil | 2017-10-18 12:38:19 |
| 443-https-dhe-full_ipv4 | 443 | https | dhe | full ipv4 | 2017-10-15 23:15:39 |
| 443-https-dhe_export-1%_sample_ipv4 | 443 | https | dhe export | 1% sample ipv4 | 2017-10-18 04:14:59 |
| 443-https-dhe_export-alexa_top1mil | 443 | https | dhe export | alexa top1mil | 2017-10-18 11:08:23 |
| 443-https-dhe_export-full_ipv4 | 443 | https | dhe export | full ipv4 | 2017-10-12 22:38:03 |
| 443-https-heartbleed-alexa_top1mil | 443 | https | heartbleed | alexa top1mil | 2017-10-18 14:14:34 |
| 443-https-heartbleed-full_ipv4 | 443 | https | heartbleed | full ipv4 | 2017-10-18 00:26:36 |
| 443-https-rsa_export-1%_sample_ipv4 | 443 | https | rsa export | 1% sample ipv4 | 2017-10-18 04:18:34 |
| 443-https-rsa_export-alexa_top1mil | 443 | https | rsa export | alexa top1mil | 2017-10-18 14:08:26 |
| 443-https-rsa_export-full_ipv4 | 443 | https | rsa export | full ipv4 | 2017-10-12 22:38:08 |
| 443-https-ssl_3-alexa_top1mil | 443 | https | ssl 3 | alexa top1mil | 2017-10-18 15:14:05 |
| 443-https-ssl_3-full_ipv4 | 443 | https | ssl 3 | full ipv4 | 2017-10-11 22:53:19 |
| 443-https-tls-alexa_top1mil | 443 | https | tls | alexa top1mil | 2017-10-18 10:30:42 |
| 443-https-tls-full_ipv4 | 443 | https | tls | full ipv4 | 2017-10-13 09:06:44 |
| 443-https_www-tls-alexa_top1mil | 443 | https_www | tls | alexa top1mil | 2017-10-18 11:30:57 |
| 445-smb-banner-full_ipv4 | 445 | smb | banner | full ipv4 | 2017-10-18 21:01:20 |
| 465-smtps-tls-full_ipv4 | 465 | smtps | tls | full ipv4 | 2017-10-17 22:51:58 |
| 502-modbus-device_id-full_ipv4 | 502 | modbus | device id | full ipv4 | 2017-10-15 08:01:19 |
| 993-imaps-dhe_export-full_ipv4 | 993 | imaps | dhe export | full ipv4 | 2017-10-18 04:14:56 |
| 993-imaps-tls-full_ipv4 | 993 | imaps | tls | full ipv4 | 2017-10-12 00:20:48 |
| 995-pop3s-tls-full_ipv4 | 995 | pop3s | tls | full ipv4 | 2017-10-14 00:14:49 |
| 1900-upnp-discovery-full_ipv4 | 1900 | upnp | discovery | full ipv4 | 2017-10-16 02:13:41 |

图 8.9 Censys 扫描数据

利用 Censys 搜索 protocols: "102/s7" Siemens，如图 8.10 所示。

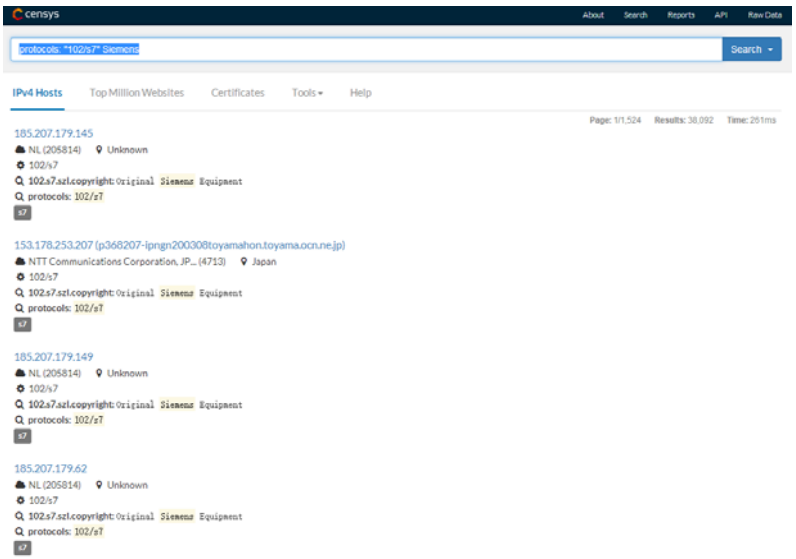


图 8.10 Censys 查询结果 1

共搜索到 38092 个结果。

点击 153.178.253.207，得到结果如图 8.11 所示。

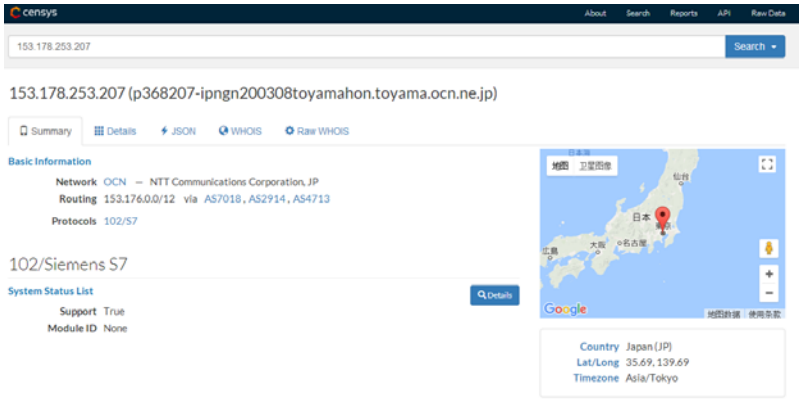


图 8.11 Censys 查询结果 2

点击 Details 得到结果如图 8.12 所示。

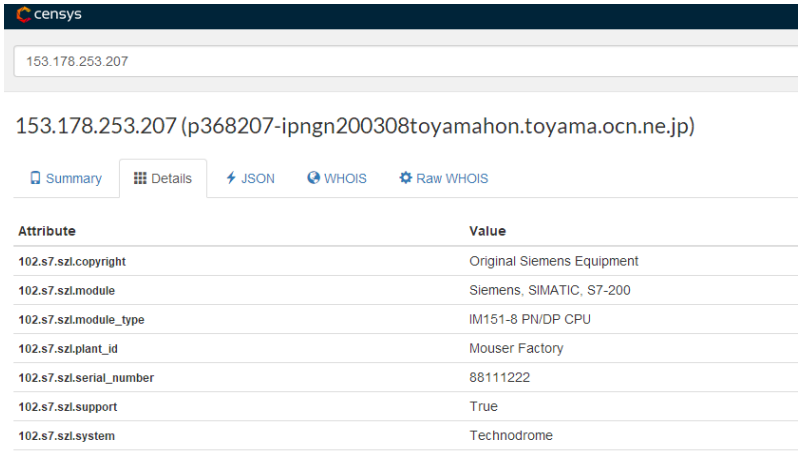


图 8.12 Censys 查询结果 3

### 8.2.3 ZoomEye

ZoomEye 是一款针对网络空间的搜索引擎，收录了互联网空间中的设备、网站及其使用的服务或组件等信息。ZoomEye 拥有两大探测引擎：Xmap 和 Wmap，分别针对网络空间中的设备及网站，通过 24 小时不间断的探测、识别，标识出互联网设备及网站所使用的服务及组件。研究人员可以通过 ZoomEye 方便的了解组件的普及率及漏洞的危害范围等信息。虽然被称为“黑客友好”的搜索引擎，但 ZoomEye 并不会主动对网络设备、网站发起攻击，收录的数据也仅用于安全研究。ZoomEye 更像是互联网空间的一张航海图。

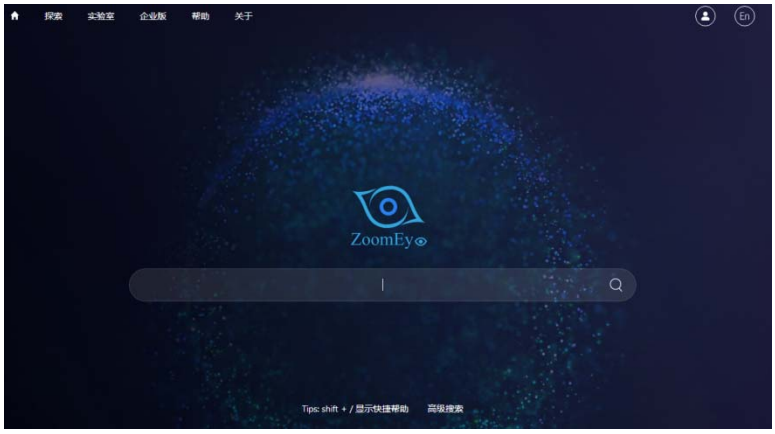


图 8.13 Zoomeye

ZoomEye 和 Shodan 的区别是 ZoomEye 目前侧重于 Web 层面的资产发现而 Shodan 则侧重于主机层面，目前 ZoomEye 共收录了 132,122,600 个站点，400,000,000 个设备，7,942 个组件。

比如我们以当前使用量世界第一的 Blog 应用 Wordpress 作为关键字分别进行搜索。使用 Shodan 搜索到了 3 万多条记录，而使用 ZoomEye 搜索到了 30 多 W 条记录且结果吻合度非常高。除了最普通的关键词搜索，ZoomEye 目前还支持对 Web 应用指定版本号，比如我们想搜索使用 wordpress 3.5.1 版本的网站，输入搜索短语 wordpress:3.5.1 即可。同样我们还可以对国家和城市进行限定，比如输入 wordpress:3.5.1 country:cn city:beijing 能够搜索到主机位于中国北京且使用 wordpress 3.5.1 版本的网站。

该搜索引擎目前正在逐步完善，更多功能也在逐步添加当中，目前已经整合了全球 4100 万网站的网站组件指纹库，数据量相对可观，后期会继续扩充。在搜索框中可以搜索你关心的网站组件，比如 discuz、dedecms，比如 nginx、apache，甚至你搜 hacked by 也能得到一些亮点。

### 8.2.4 其他网络空间搜索引擎

傻蛋联网设备搜索是一款监测互联网基础设施安全威胁并评估其安全状况的产品，它能自动发现网络设备、服务器设备、工业控制设备等所有互联网基础设施，识别和收集这些设施的指纹信息，检测其是否存在安全威胁，评估其安全状况；一旦出现新安全事件，可基于大数据处理技术，重新计算和评估基础设施的安全性，并预测新漏洞的影响范围。产品布署在互联网上，为互联网用户提供

网络安全威胁搜索、网络安全监测、网络安全加固等网络安全服务。


图 8.14 Shadan

东北大学计算机学院姚羽教授组织学生编写研发——谛听（ditecting）网络空间工控设备搜索引擎，取谛听辨识万物之意，意在搜寻暴露在互联网上的工业控制系统联网设备，帮助安全厂家维护工控系统安全、循迹恶意企图人士。通过谛听，你可以定位工控设备位置，捕捉开放端口，发现安全漏洞。通过谛听，你可以直观感受全球工控安全形势，关注你身边的工控系统安全。谛听旨在为工控安全提供开放自由的研究环境，善用谛听，关注工控系统安全，促进工控安全发展。

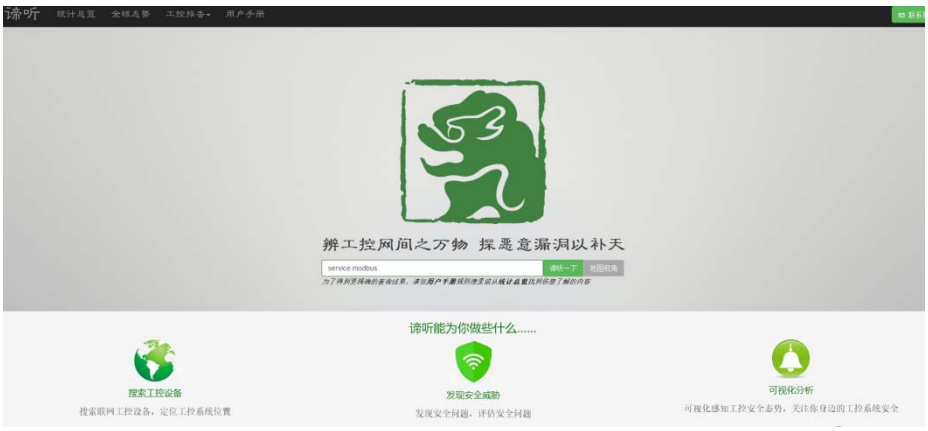


图 8.15 谛听

# 第九章 工业控制网络威胁数据采集

互联网从诞生以来，一直遭受着网络攻击与恶意代码的威胁。随着攻击技术的不断发展，新形态的安全威胁不断涌现并在持续进化，而防御技术并不能及时跟上安全威胁的变化步伐，这使得互联网的安全状况日益恶化。究其根源，会发现攻击方与防御方之间在进行着一场不对称的技术博弈：攻击方可以在夜深人静时只要找到攻击目标的一个漏洞就能够攻破系统，而防御方必须确保系统不存在任何可被攻击者利用的漏洞，并拥有全天候的监控机制，才能确保系统的安全；攻击方可以利用扫描、查点等一系列技术手段，全面获取攻击目标的信息，而防御方即使在被攻陷后仍然很难了解到攻击的来源、方法和动机；一旦博弈失败，由于安全响应技术与协调机制的欠缺，在很多情况下，攻击方不会遭受任何损失，而防御方却通常将面临系统与信息被破坏或窃取的风险。

要想扭转这种信息不对称的局面，网络防御方必须采取措施，主动采集网络威胁数据，利用数据来对网络攻击者进行分析和监测。

## 9.1 工业控制蜜罐

蜜罐（honeypot）就是一项用来采集攻击数据的主动防御技术，它定义为一类安全资源，没有任何业务上的用途，其价值就是吸引攻击方对它进行非法使用。蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

20 世纪 80 年代末蜜罐技术在网络安全管理实践活动中诞生以来，就赢得了安全社区的持续关注，并得到了长足发展与广泛应用。针对不同类型的网络安全威胁形态，出现了丰富多样的蜜罐软件工具。在网络安全威胁监测研究与实际网络安全管理实践中，利用蜜罐采集的网络威胁数据大量应用于网络入侵与恶意代码检测、恶意代码样本捕获、攻击特征提取、取证分析、追踪溯源等多种用途。

工业控制系统蜜罐通过模拟工业控制通信协议伪装成真实的工业控制系统，

能够记录入侵者对工业控制系统的网络探测与攻击数据。

Conpot 是一个低交互蜜罐工业控制系统蜜罐，它模拟具有 Modbus 和 S7comm 协议连接的西门子 SIMATIC S7-200 PLC。它的默认设置能够延伸到模拟其他使用专有 S7comm 协议的西门子 PLC。但是 S7comm 协议的实现是相当不完整的，它只能读取系统状态列表（SSL）的条目。默认配置下，Conpot 添加了两项标识了西门子 PLC 的型号和版本的条目，一个真正的西门子 PLC 有差不多 1000 个这些条目，缺失的那些使对手很容易识别 Conpot。

CryPLH 模拟了一个 S7-300，作者认为 CryPLH 是一个高交互蜜罐，其明确目的是提高交互性、可配置性和不可区分性。CryPLH 再现了一个看起来与真实界面完全相同的 PLCWeb 界面的静态副本。登录被禁用以便对手无法访问状态信息。CryPLH 提供 SNMP 服务，标识为 PLC 并提供从主机操作系统获取网络统计信息的功能。对手甚至可以使用西门子的 SIMATIC STEP 7 软件连接到 CryPLH。但是，CryPLH 模拟 S7-300 PLC 的最高保护级别，并且拒绝任何提交的密码。因此，CryPLH 阻止了对手的进一步探索。由于对手既不能观察也不能修改 PLC 应该运行的程序，CryPLH 在我们的分类方案中仍然被归类为低交互。然而，通过 Nmap 获取的 TCP/IP 操作系统指纹与真正的 PLC 不同，这使得 CryPLH 可以容易地被对手识别为蜜罐。

灯塔实验室运营人员显然有 PLC 蜜罐。由于他们没有发布他们的蜜罐配置或其功能描述，我们只能从他们发布的蜜罐日志做出推论。他们的日志类似于 Snap7 输出，并在 SSL 中显示许多对标识条目的请求，其中大多数请求源自 Shodan 和 Censys。一个连接查询其他 SSL 条目和一些程序及数据块，工程工作站可能被使用了，另一个查询单个配置数据块和一些不寻常的 SSL 条目。他们提到三次尝试的攻击：对手试图停止程序执行，修改内存区域和调整系统时钟。总的来说，灯塔实验室的蜜罐似乎比我们之前讨论过的两种蜜罐允许更大的交互性，但是仍然不支持与模拟 PLC 程序的交互。基于这个有限的信息，我们将他们的蜜罐分类为低交互。

DT 实验室的 DemonTrace 是一款工业控制系统高交互蜜罐，它支持 S7comm、Modbus、BACnet、IEC104、DNP3、HTTP、kamstrup 协议。不同于 Conpot，DemonTrace 支持与攻击者进行深度交互，能够模拟真实 PLC 回复攻击者的每一次数据请求，逐步诱导攻击者由低级别的扫描探测到发起高级别的网路攻击。

## 9.2 其他采集技术

### 9.2.1 Snort

1998 年，Marty Roesch 用 C 语言开发了开放源代码的入侵检测系统 Snort。到今天，Snort 已发展成为一个多平台实时流量分析，网络 IP 数据包记录等特性的强大的网络入侵检测/防御系统。Snort 有三种工作模式：嗅探器、数据包记录器、网络入侵检测系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网络入侵检测模式是最复杂的，而且是可配置的。我们可以让 snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

Snort 能够对网络上的数据包进行抓包分析，但区别于其它嗅探器的是，它能根据所定义的规则进行响应及处理。Snort 通过对获取的数据包，进行各规则的分析后，根据规则链，可采取 Activation（报警并启动另外一个动态规则链）、Dynamic（由其它的规则包调用）、Alert（报警），Pass（忽略），Log（不报警但记录网络流量）五种响应的机制。

Snort 有数据包嗅探，数据包分析，数据包检测，响应处理等多种功能，每个模块实现不同的功能，各模块都是用插件的方式和 Snort 相结合，功能扩展方便。例如，预处理插件的功能就是在规则匹配误用检测之前运行，完成 TIP 碎片重组，http 解码，telnet 解码等功能，处理插件完成检查协议各字段，关闭连接，攻击响应等功能，输出插件将得理后的各种情况以日志或警告的方式输出。

### 9.2.2 p0f

p0f 是一款远程操作系统被动判别工具，能够通过捕获并分析目标主机发出的数据包来对主机上的操作系统进行鉴别。它支持：

- 反连 SYN 模式
- 正连 SYN+ACK 模式
- 空连 RST+ 模式
- 碎片 ACK 模式

p0f 比较有特色的是它还可以探测：

- 是否运行于防火墙之后
- 是否运行于 NAT 模式
- 是否运行于负载均衡模式
- 远程系统已启动时间
- 远程系统的 DSL 和 ISP 信息等

## 9.3 工业控制网络威胁数据应用

### 9.3.1 工业控制网络恶意代码检测

恶意代码攻击是信息战、网络战最重要的入侵手段之一，震网事件就是恶意代码的一次典型案例，恶意代码问题无论从政治上、经济上，还是军事上，都成为工控系统网络安全面临的首要问题。利用工业控制网络威胁数据可有效开展网恶意代码检测，主要方法可以归结为两种：基于特征码的检测方法和基于行为的检测方法。

基于特征码的检测方法取决于模式识别，该方法不考虑恶意代码的指令意义，而是分析指令的统计特性、代码的结构特性等。比如在某个特定的恶意代码中，这些静态特征数据会在数据的特定位置出现，所以完全可以使用这些静态特征和其在数据中出现的位置作为描述恶意代码的特征。

工作原理如下：提取数据包的固定字节序列，并与特征库中的信息字节码进行比较，如果该模式与苦衷相匹配，就会被认为是恶意代码。这种方法很容易通过代码变换技术绕过，但是同一恶意代码变换后都具有一定的同源性，可以利用数据挖掘和机器学习等大数据和人工只能方法来检测恶意代码的同源性。

新的恶意代码每天都在产生，基于特征码的检测方法无法有效防御新的或未知的恶意代码，从而要求特征库要保持更新，而很多恶意代码的定义都需要人工来完成。

基于行为的检测方法是通过监视恶意代码是如何运行，如果发现有异常行为，就标记为恶意代码。但是工业生产环境要求无损，绝不可能让不确定的代码在工业控制系统中运行。工业控制系统中的行为检测要求不运行恶意代码本身，而是

考虑构成恶意代码的工业控制协议功能码的含义，通过理解功能码含义建立恶意代码的流程图和功能框图，进一步分析恶意代码的功能结构。在该技术的分析过程中首先参照工业控制协议对数据包进行解读，通过这种技术可以得到恶意代码的所有功能特征，如收发网络数据、响应每个触发事件、文件读写操作等，根据这些行为可以判断该代码是否是恶意的。

### 9.3.2 工业控制网络攻击特征提取

网络攻击都具有一定的特征，工业控制网络攻击也不例外，根据网络攻击特征可以有效检测并阻止网络攻击。常见的工业控制网络攻击特征有：基于时间序列的特征、基于端口序列的特征、基于功能码序列的特征、基于参数序列的特征等。

基于时间序列的特征：事件序列也称为动态序列，由一组随时间变化的观测量组成，描述事物随时间变化的过程。

基于端口序列的特征：端口序列指的是工业控制系统中开放网络端口的有序列表，例如，一个攻击者尝试连接到 80 端口，然后连接到 8080 和 1080 端口，则该攻击会话的端口序列特征就是 80-8080-1080。

基于功能码序列的特征：功能码序列是指同一攻击会话所使用的工业控制协议中的功能码按照时间先后顺序组成的序列。

基于参数序列的特征：参数序列是指同一攻击会话所使用的工业控制协议中的参数值按照时间先后顺序组成的序列。

其他特征：如流量特征、数据包载荷特征、操作系统指纹特征等，均可以作为辅助特征参与网络攻击检测。

### 9.3.3 工业控制网络安全威胁追踪与分析

网络攻击都包含很多步骤，例如，许多攻击者都是从扫描开始，接着是枚举，但后针对枚举的账户尝试进行认证，或者开始检测系统能够中是否存在漏洞。网络安全威胁追踪与分析就是将上述步骤产生的大量的离散时间数据关联成一个整体进行分析，前面讨论的检测技术在单独使用时都会分析提供有价值的证据。

常用的安全追踪方法有 IP 地址地理位置查询，IP 地址绑定域名查询，域名 whois 信息查询，域名绑定邮箱查询与同一邮箱其他域名信息查询，操作系统检测，软件同源性检测等。

IP 地址地理位置信息查询可以使用 GEOIP 库，该库免费版可以到网站 https://www.maxmind.com/en/geoip-demo 下载，通过该数据库能够定位到国家、城市、经纬度等地理位置信息。国内的 IPIP.net 以一个基于 BGP/ASN 数据分析处理而得来的 IP 库，相对于 GEOIP 库，IPIP 能提供更加准确的地理位置信息，但是需要付费查询。

Whois 是用来查询域名的 IP 以及所有者等信息的传输协议。简单说，whois 就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、邮箱、地址、联系电话、域名注册商）。有些注册商，对国际域名的 whois 信息是屏蔽的，如果要查询只能联系对应的注册商。这种保护机制是防止有人恶意利用这种 whois 信息的联系方式，暴露客户的隐私信息。国内提供 whois 信息查询的网站有站长之家，万网等。

### 9.3.4 工业控制网络安全态势感知

“态势感知（Situation Awareness，SA）”是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、相应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地应用。“态势感知”最早在 20 世纪 80 年代被美国空军提出，覆盖感知、理解和预测三个层次。90 年代，概念开始被广泛接受，并随着互联网的兴起而升级为“网络空间态势感知（CyberspaceSituation Awareness，CSA）”，是指在大规模网络环境中能够引起网络态势发生变化的安全要素进行获取、理解、显示，以及趋势预测分析从而支撑决策的系列活动。近年来，随着大数据技术的兴起，态势感知技术也正逐渐成为信息安全技术中的一个新的门类。

工业控制网络的态势感知技术是态势感知技术在工业控制系统中的落地。如前文所述，工业控制网络与传统信息网络不论是在软硬件架构，还是安全性需求方面都存在较大差异，而态势感知技术本身又属于新兴的技术门类，因此将态势感知应用于工业控制网络这样一个全新业务领域，必然会产生一些独特的特点和

规律。

承载着关键信息基础设施的工业企业网络，一般会划分为信息管理网络和生产控制网络两部分，该两部分网络具有：彼此严格隔离和协议类型完全不同（传信息网络协议、工业以太网协议）的特点。这就造成了工控安全态势感知技术的如下关键特征。

- 生产控制网络与信息管理网络独立信息采集

由于工业企业信息管理网络与生产控制网络严格隔离，所以信息采集工作须从该两个网络分别着手。对于生产控制网络而言，应着重考虑内部资产（如 PLC、DCS、RTU 等）的品牌类型、软硬件版本等，以及内部恶意行为等信息的采集工作；对于信息管理网络来说，应着重考虑外部恶意行为，以及内部资产非法外联等信息的采集工作。

- 工业协议数据采集

工控网络态势安全态势感知技术应该主要用于监测工业控制网络安全状况和变化趋势，并支撑相应应急响应机制建设。这就要求该技术主要基于工业协议（如 Siemens S7、Modbus、Bacnet、Ethernet/IP 等）来开展各种维度的监测、分析等工作。

- 主被动采集手段相结合

由于工业控制网络安全等级要求很高，一旦操作不当可能会操作物理伤害，所以不同于传统信息网络，在信息的采集过程中要首要考虑采集会否影响工业生产系统本身安全性，所以建议使用主被动结合采集□手段，并且优先使用被动采集手段。

- 工业控制网络安全知识库为核心

知识库作为工业控制网络安全态势感知技术的核心模块，应该主要包含工业控制设备（如各品牌 PLC、RTU、IED 等）指纹库、工业控制网络恶意行为指纹库（比如，支持 Siemens S7、Modbus、Bacnet、Ethernet/IP 等协议）、工业控制网络恶意组织指纹库、工业控制网络漏洞库等专业知识库。

- 信息采集重点与行业特点相关性很强

不同行业的工业企业的生产控制网络结构差异化较大，在进行基础采集探针部署阶段，要进行针对性的调整。比如，电网、燃气等应用 SCADA 较多的行业，

可重点考虑工业设备非法外联监测和外部威胁监测；石油炼化、先进制造等应用 DCS 较多的行业，则可重点考虑外部威胁监测和内部威胁监测。

一个典型工业控制网络安全态势感知系统整体架构如下图 9.1 所示，由五个层□面的功能构成。

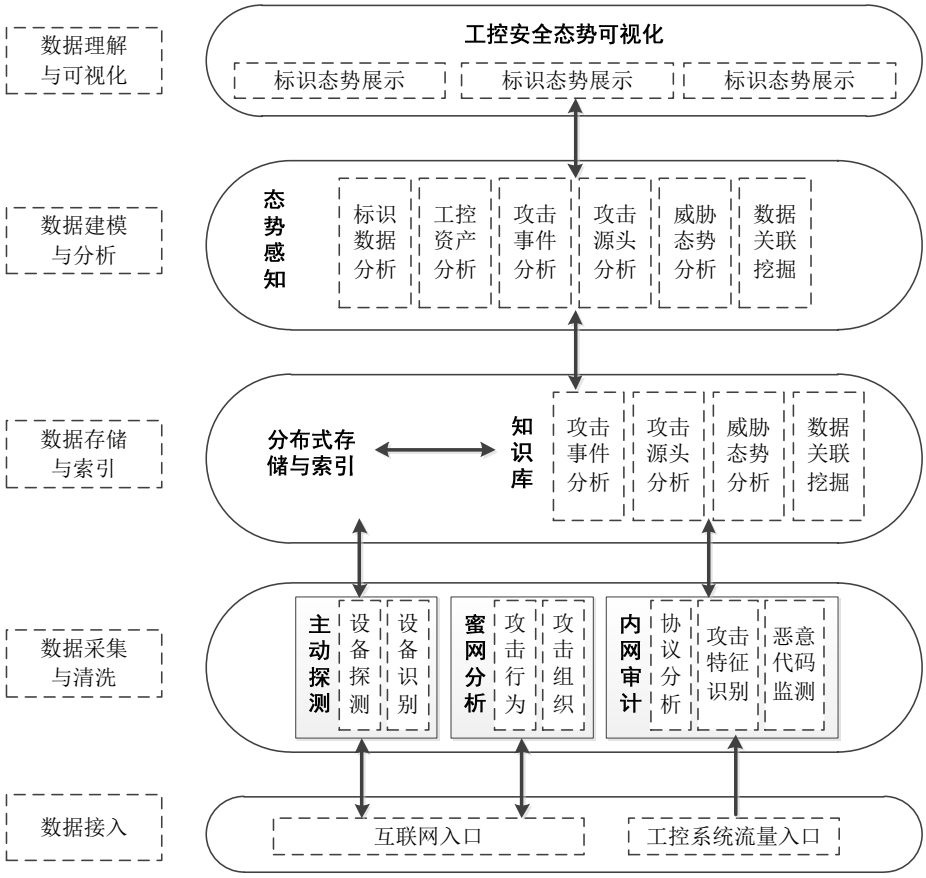


图 9.1 工业控制网络安全态势感知系统整体架构

数据接入层：实现数据的接入功能，通过开放的互联网资源接入到开放联网的工业控制系统；基于企业工业控制系统流量入口的数据采集系统，通过镜像接获取局域网通信流量数据。

数据采集与清洗层：实现工业控制设备及企业工业控制网络入口流量数据的采集与清洗功能，通过主动探测对工业控制设备进行识别。

数据存储与索引层：实现探测数据、监测数据及知识库资源的数据汇聚、存储及索引功能，提供开放接口供数据建模层进行数据获取。

数据建模与分析层：实现数据的关联分析，深入分析工业控制网络标识信息、工业控制系统资产信息、攻击事件和攻击源头信息，进行威胁态势展示和数据关联挖掘。

数据理解与可视化层：对标识态势、攻击源、攻击事件和工控资产的态势进

行可视化展示，并通过可视化界面进行数据关联查询。

工业控制网络安全态势感知服务必须根据工业企业不同业务特征和需求进行定制，提供针对其生产控制网络的威胁、脆弱性信息，并根据知识库的各种工业指纹库，进行综合分析处理，形成针对目标工业控制网络的整体安全状况以及变化趋势，支撑响应工业企业安全保障机制建设。