电力系统嵌入式设备信息安全测试技术

Information Security Testing Technology
of Embedded Equipment in Power System

胡海生　梁智强　主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

电力系统嵌入式设备信息安全测试技术

Information Security Testing Technology
of Embedded Equipment in Power System

胡海生　梁智强　主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

电力系统广泛采用各类嵌入式设备，设备的信息安全受到各种威胁，逐渐受到重视。本书阐述了电力系统嵌入式设备的安全测试技术，具体包括以下内容：嵌入式设备通信协议模糊测试、动态端口测试、操作系统安全测试、应用安全漏洞测试、配置安全测试、安全测试平台。

本书适合电力系统及其他各行业嵌入式设备的安全测试技术人员使用。

图书在版编目（CIP）数据

电力系统嵌入式设备信息安全测试技术 / 胡海生，梁智强主编 . —北京：中国电力出版社，2018.12

ISBN 978-7-5198-2540-9

Ⅰ. ①电… Ⅱ. ①胡…②梁… Ⅲ. ①电力系统—电气设备—信息安全—测试技术 Ⅳ. ①TM7

中国版本图书馆 CIP 数据核字（2018）第 243270 号

出版发行：中国电力出版社
地　　址：北京市东城区北京站西街 19 号（邮政编码 100005）
网　　址：http://www.cepp.sgcc.com.cn
责任编辑：刘　薇
责任校对：黄　蓓　闫秀英
装帧设计：张俊霞
责任印制：石　雷

印　　刷：北京九州迅驰传媒文化有限公司
版　　次：2019 年 1 月第一版
印　　次：2019 年 1 月北京第一次印刷
开　　本：787 毫米 ×1092 毫米　16 开本
印　　张：5.5
字　　数：118 千字
定　　价：26.00 元

本书编委会

主　编　胡海生　梁智强

参　编　胡春潮　林丹生　伍晓泉　高　雅

余志文　胡朝辉　曾智勇

前 言

当前，电力监控系统广泛采用各类嵌入式设备，如测控装置、保护装置、智能操作箱、远动机、站控层交换机、RTU、DTU 等。嵌入式设备大量采用通用硬件芯片、通用/开源操作系统、通用协议进行开发，各大厂商在追求设备功能、性能及易用性时，忽略了设备本体的信息安全。另外，越来越多的设备漏洞被公之于众，嵌入式设备本体的信息安全逐渐受到公众的关注，如震网病毒利用西门子 PLC 控制器设备漏洞及 SCADA 程序漏洞进行攻击事件。

随着黑客攻击技术的发展及信息安全关注点的转移，越来越多的嵌入式设备漏洞被发现，设备本体的安全给电力监控系统带来不可控的安全风险。因此，有必要对电力嵌入式设备本体的安全性进行研究和测试工作，降低设备的信息安全风险，提高系统抵御外来攻击的能力，提高系统的安全稳定运行水平。

本书作者长期从事电力系统嵌入式设备信息安全技术的研究和设备及系统的测试工作。本书将电力系统嵌入式设备的研究工作与电力生产现场测试工作进行总结，为读者展示较为全面的电力系统嵌入式设备信息安全测试技术。本书依照如下内容进行阐述：①概述；②电力系统嵌入式设备通信协议模糊测试；③电力系统嵌入式设备动态端口测试；④电力系统嵌入式设备操作系统安全漏洞测试；⑤电力工控系统固件测试技术；⑥电力系统嵌入式设备应用安全漏洞测试；⑦电力系统嵌入式设备配置安全测试；⑧电力系统嵌入式设备信息安全测试平台。

本书所涉及的内容大都具有尝试性和探索性，与此相关的许多理论和实际问题还需要进一步深入研究，限于编者水平，书中难免有疏漏和不当之处，恳请广大专家和读者批评指正。

目 录

前言

第 1 章 概述 …… 1

1.1 背景 …… 1
1.2 现状 …… 2
1.3 研究意义 …… 3

第 2 章 通信协议模糊测试 …… 4

2.1 概述 …… 4
2.2 电力系统通信协议模糊测试技术方案 …… 4
2.3 电力系统典型通信协议解析 …… 8
2.4 电力通信协议的模糊测试 …… 20

第 3 章 动态端口测试 …… 24

3.1 概述 …… 24
3.2 端口测试方法 …… 24
3.3 端口测试工具 …… 25

第 4 章 操作系统安全漏洞测试 …… 27

4.1 概述 …… 27
4.2 典型操作系统安全漏洞测试方法 …… 27
4.3 电力系统嵌入式设备操作系统安全漏洞测试 …… 29

第 5 章 电力工控系统固件测试技术 …… 32

5.1 嵌入式系统固件概述 …… 32
5.2 嵌入式固件的安全性问题 …… 33
5.3 嵌入式固件测试方法 …… 34

第 6 章 应用安全漏洞测试 …… 44

6.1 概述 …… 44
6.2 典型应用测试方法 …… 44
6.3 电力系统嵌入式设备应用安全漏洞测试 …… 46

第 7 章　配置安全测试 …… 49
7.1　概述 …… 49
7.2　电力系统配置安全检查目标与方法 …… 49
第 8 章　电力系统嵌入式设备信息安全测试平台 …… 53
8.1　测试平台概况 …… 53
8.2　系统设计原则 …… 54
8.3　测试方案及测试平台功能设计 …… 55
8.4　测试平台应用场景 …… 64
附录 A　常见 TCP 端口列表 …… 66
附录 B　工具集介绍 …… 70
附录 C　固件解包实例 …… 73
参考文献 …… 78

第1章 概 述

1.1 背景

在过去很长一段时间内，电力系统基于相对隔离的系统部署环境和多层纵深的安全防护手段能免于遭受外界的攻击，但同时也导致电力系统设备的信息安全性在整个产品生命周期中容易被忽视。然而，随着智能电网技术和现代工控系统相关技术的不断发展、开放通信协议的引入、智能终端设备的发展、与其他设备/软件连接的增加、外部连通性的增强、网络攻击事件频发等因素的增多，电力系统的安全风险日益加重。

面向电力系统的（信息）安全事件和攻击，近年来越来越多地被报道披露。2010年StuxnetWorm（震网病毒）利用西门子工控软件漏洞对伊朗核设施造成严重攻击破坏，导致该国核设施建设延迟数年；2013年5月安全检测机构NSSLabs又爆出西门子SCADA新的安全漏洞[1][2]；2015年12月23日乌克兰电力系统遭受黑客攻击导致大面积停电，该事件是世界上第一次针对电力系统的网络安全攻击，对电力行业的网络安全防护造成巨大震动。人们开始怀疑，逻辑隔离或者物理隔离的电力系统是否能够应对国家级、集团式的网络攻击；2017年5月“勒索病毒”爆发，对包括电力监控系统在内的工控系统安全防护、安全运维造成巨大震动，从业人员不得不耗费数月时间开展系统和设备的整改和加固。

上述事件不止一次地为电力系统安全敲响警钟，尽管电力一次、电力二次系统制造商和运维人员对系统进行多次加固，但是仍然不停地爆发出各种漏洞及风险。根据CVE（Common Vulnerabilities and Exposures，通用漏洞与披露）、中国国家信息安全漏洞库（CNNVD）等权威漏洞库的披露，电力系统安全漏洞广泛存在于各类电力系统设施中，如PLC（可编程控制器）、SCADA、控制服务器等。相关漏洞一旦被攻击者或者蠕虫、病毒、恶意软件等利用，电力系统中的设备及其重要控制指令将很容易被攻破，产生灾难性的后果[4]。

电力系统设备的漏洞主要包括[4][5]：

（1）通信协议漏洞。“两化”（即智能化和互联化）融合和物联网的发展使得TCP/IP协议等通用协议越来越广泛地应用在工业控制网络中，随之而来的通信协议漏洞问题也日益突出。

（2）操作系统漏洞。目前大多数工业控制系统的工程师站/操作站/HMI都是基于Windows或者Linux平台的，通常在系统开启后不会对操作系统安装任何补丁，从而埋下了安全隐患。

（3）应用软件漏洞。由于应用软件多种多样，很难形成统一的防护规范以应对安全问题；另外，当应用软件面向网络应用时，就必须开放其相应的端口，这也是工业控制

网络重要的攻击途径。

（4）安全策略和管理流程漏洞。追求可用性而牺牲安全性，是很多工业控制系统普遍存在的现象，缺乏完整有效的安全策略与管理流程，也给工业控制系统信息安全带来了一定的威胁。

（5）杀毒软件漏洞。为了保证工控应用软件的可用性，许多工控系统操作站通常不会安装杀毒软件，即使安装了杀毒软件，病毒库也不会定期的更新。

典型工控系统安全问题如图 1-1 所示。

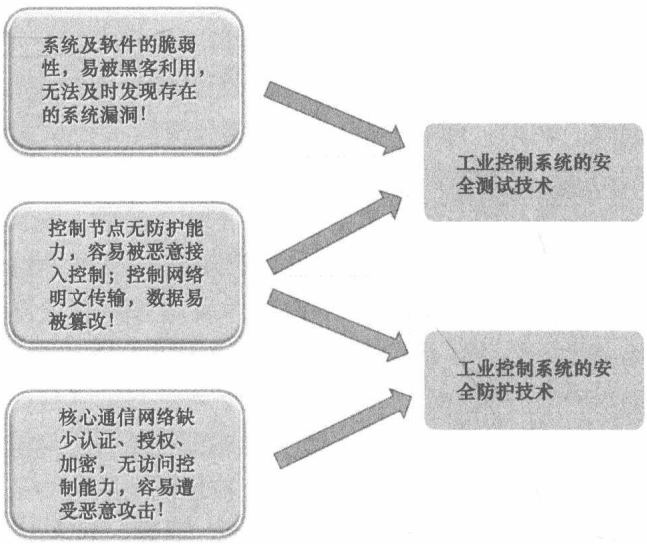

图 1-1　典型工控系统安全问题

1.2　现状

基于工业控制系统安全高度的战略意义，以及国内工业控制界与信息安全界对工业控制领域安全技术研究不足的现实，及时开展工业控制系统的安全问题分析就显得非常必要。

截至 2017 年底，行业内已经出现相关工业控制系统模糊测试工具，加拿大的 Wurldtech 已经有基于工控协议的模糊测试设备（Achilles），并在国际上得到一定的认可，同时也形成了自己完整的认证体系。众多国外的工控厂商，如西门子、施耐德等，已经陆续通过了该认证；国内的浙江中控科技（Supcon）最新的 DCS 控制器也通过了该认证。

芬兰的 CODENOMICON（科诺康）的漏洞挖掘和漏洞扫描在技术上处于领先的地位。2015 年 4 月，号称全球最大互联网漏洞——Heartbleed（心脏流血）漏洞就是科诺康发现的。Heartbleed 漏洞影响了被广泛使用的开放源代码 SSL 安全套件 OpenSSL 的加密协议。简言之，这个漏洞可以诱使服务器将其内存中的数据溢出来，从而可能让黑客掌握这一漏洞，并进一步窃取诸如信用卡和密码等之类的敏感信息。科诺康不仅在工

控领域有着深厚的技术积累，在 IT 网络上同样有着领先的技术。

自从震网病毒事件爆发，美国发布国家网络空间安全战略政策之后，工业控制系统安全才引起西方国家的高度重视，并将工业控制系统的安全问题提到了国家安全战略的高度。

与此同时，国内同样遭受着工业控制系统信息安全问题的困扰。2010 年齐鲁石化、2011 年大庆石化炼油厂某装置控制系统分别感染 Conficker 病毒，造成控制系统服务器与控制器通信不同程度地中断。这些信息安全漏洞主要集中在能源、关键制造业、交通、通信、水利、核能等领域，而且能源行业的安全事故超过了一半。

2011 年 9 月，工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451 号），强调加强工业信息安全的重要性、紧迫性，并明确了重点领域工业控制系统信息安全的管理要求。

随后，国务院又发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号），要求建立国家信息安全保障体系，提升网络与信息安全保障水平，确保重点领域信息安全，并且明确提出要保障工业控制系统安全。同时，国家发展和改革委员会等部门也开始从政策和科研层面上积极部署工业控制系统的安全保障工作。

所以，未来五到十年工业控制系统的信息安全建设将会成为电力、石化、冶金、交通以及市政等多领域的主要任务。增强对工业控制设备的漏洞检测能力，提高工业控制设备的安全水平，加强工业控制系统的安全防护等级迫在眉睫。

1.3 研究意义

如上所述，工业控制系统及终端智能化和互联化，增加了系统的安全风险。传统的系统安全防护只能从防御的角度减轻电力工控系统以及终端的安全风险，并未从根本上解决系统数据通信过程中遭受互联网恶意攻击的安全隐患问题。

随着黑客攻击技术的发展及信息安全关注点的转移，越来越多的嵌入式设备漏洞被发现，因此，有必要对电网嵌入式设备本体的安全性进行研究和测试工作，降低设备的信息安全风险。

第2章 通信协议模糊测试

2.1 概述

当前，电力监控系统广泛采用各类嵌入式设备，如测控装置、保护装置、智能远动机、保信装置、站控层交换机、计量装置等。嵌入式设备大量采用通用硬件芯片、通用/开源操作系统、通用协议进行开发，各大厂商在追求设备功能、性能及易用性的同时，忽略了设备本体的信息安全设计与实现。另外，越来越多的设备漏洞被利用和攻击（如震网病毒利用了西门子 PLC 控制器设备漏洞，并利用 SCADA 程序漏洞进行攻击），嵌入式设备本体的信息安全逐渐受到公众的关注。

随着黑客攻击技术的发展及信息安全关注点的转移，越来越多的嵌入式设备漏洞被发现，设备本体的安全漏洞给电力监控系统带来不可控的安全风险，因此，有必要对电网嵌入式设备本体的安全性进行研究和测试工作，降低设备的信息安全风险，提高系统抵御外来攻击的能力，提高系统的安全稳定运行水平。

2.2 电力系统通信协议模糊测试技术方案

2.2.1 技术背景

安全测试可分为安全功能测试和安全漏洞测试。传统的电力系统安全性测试主要侧重于安全功能测试，如安全接入、加密认证等。而基于通信协议层面的测试主要侧重于协议一致性测试，如 IEC61850 的一致性测试主要验证变电站智能终端设备（IED）的通信接口访问组织、帧格式、位顺序、时间同步、定时、信号形式和电平以及对错误的处理等与标准要求的一致性。

目前在电力行业中这些协议应用非常广泛，随着“两化”（智能化和互联化）融合及智能电网的建设，对协议实现的安全性和健壮性进行测试就显得非常重要。对电力行业的工控通信协议进行模糊测试是安全测试工作的重点。

明确模糊测试的目标是电网嵌入式设备的通信协议。在这里将针对电网嵌入式设备的模糊测试定义为“通过向应用提供非预期的输入并监控输出中的异常来发现被测设备的故障的方法”。模糊测试数据将通过全自动化的方式生成从而向被测设备提供非预期的输入。

2.2.2 目标

本书阐述的电力协议模糊测试面向智能远动机、保信子站、保信装置、测控装置、

PMU 装置、视频监控设备、“五防”设备、监控后台主机等电网嵌入式设备，因此，协议具备电力行业自身的特点[5][6]。通过深入了解电力系统的通信协议，对协议进行分析和建模，并采用模糊测试方法开发相关的模糊器。模糊测试协议主要针对 IEC-101 协议、IEC-102 协议、IEC-104 协议、SV 协议、IEC-103 协议、IEC 61850 协议等。针对输电网使用的智能电力设备及应用软件、主机、服务器，开发一套软硬件一体的测试设备，能够深入挖掘设备存在的安全漏洞，进行根源分析，提出专业修改意见，配备指导说明文档，能够为设备的开发、测试、运行、维护提供完整的指导流程。

本功能开发的设备是对电网工业控制设备执行测试，通过测试可以获取被测设备（DUT）的测试响应。测试结果通过图表和文本形式显示在图形用户接口（GUI）上；测试结果可以保存到文件，用于对被测设备的安全性评估。

2.2.3 技术路线

模糊测试采用的方法是反复向应用程序输入非预期的数据，并在输入的同时监控输出中的异常，它对挖掘出设备、协议的未知漏洞具有决定性的意义，使得最终产品不必依赖于公开漏洞库，如 CVE/CNVD 等。模糊测试利用自动化或是半自动化的方法重复地向应用提供输入。

模糊测试可以归为两类：①“基于变异”的模糊测试器，通过在已有的数据样本上产生变异来创建测试用例；②“基于生成”的模糊测试器，使用通信协议来建模，并据此创建测试用例。

运用模糊测试的原理，设计编译测试用例，构造变异报文，检查工控协议实现的缺陷。构建完整、可扩展的动态随机分析测试框架，监控测试目标，管理测试结果，给出数据生成方法，也就是协议模型化，并且自动化生成数据，而不是简单的随机生成，同时也要考虑到被测设备容易出现的错误，通过这样的结合来生成测试数据。模糊测试结构如图 2-1 所示。

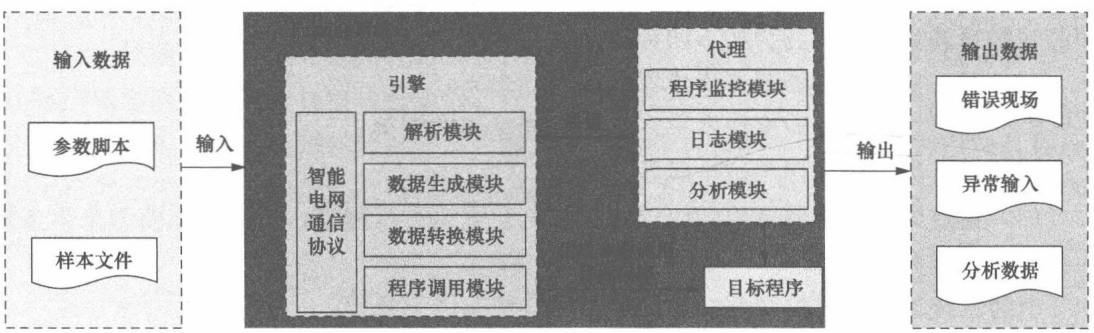

图 2-1 模糊测试结构

当对某些协议的值字段进行模糊测试时，在每个测试用例中必须计算并更新这个多字节的长度字段。否则，如果通信数据被检测为违反协议规范，测试用例就面临着被废弃的风险。大多数开源框架提供了生成伪随机数据的方法。好的框架甚至会更进一步，包含一个启发式攻击的列表。启发式攻击是一致的、会导致软件错误的数据序列。

错误检测在模糊测试中扮演着重要的角色，在最简单的层面上，如果目标应用不能接受新连接，模糊测试器能够检测到它的目标可能已经出错了。更高级的错误检测通常需要借助调试器的帮助。高级的模糊测试框架应该允许模糊测试器直接与附着在目标应用上的调试器通信，甚至是自带定制的调试器。

2.2.4 测试步骤与方法

1. 测试步骤

(1) 确定测试目标。只有有了明确的测试目标后，才能决定模糊测试工具或方法。

(2) 确定输入向量。输入向量是模糊测试的关键，如果不能预期输入值，模糊测试的作用就会受到很大的局限。

(3) 生成模糊测试数据。一旦识别出输入向量，就可以依据输入向量产生模糊测试数据。数据通过自动化过程来生成，可以使用预先确定的值、基于存在的数据通过变异生成的值或动态生成的值。

(4) 执行模糊测试数据。向被测目标发送数据包、打开文件或者执行被测应用。

(5) 监视异常。一个重要但经常容易被忽略的步骤是对异常和错误进行监控。模糊测试需要根据被测应用和所决定采用的模糊测试类型来设置各种形式的监控。

(6) 验证漏洞是否可被利用。如果在模糊测试中发现了一个错误，依据审计的目的，可能需要判定这个被发现的错误是否是一个可被利用的安全漏洞，这个过程是一个典型的手工过程。

2. 测试数据的生成方法

针对电网嵌入式设备，明确模糊测试的目标是电网嵌入式设备的通信协议。一般情况会认为模糊测试和边界值分析方法是很类似的，但不同的是模糊测试过程中不仅关注边界值，同时还关注任何能够触发未定义或者不安全行为的输入，因此针对电网中的通信协议，模糊测试的研发重点在测试方法和模糊测试数据的生成。

模糊测试数据将通过全自动化的方式生成，从而向被测设备提供非预期的输入。模糊测试数据的生成方法分为如下四种：

(1) 基于变异的模糊测试生成器；

(2) 通过对已有的数据样本进行变异来创建测试用例；

(3) 基于生成的模糊测试生成器；

(4) 通过为被测设备使用的协议格式和交互逻辑进行建模，从而用此模型来生成输入并据此创建测试用例。

电力系统通信协议模糊测试数据的生成方法有以下几种：

(1) 随机生成输入。随机方法是最低效的方法，但是这种方式可以被用来快速地识别目标应用中是否有非常糟糕的代码。随机方法简单地向目标应用发送伪随机数据，希望得到最好或者最坏的结果。

(2) 手工协议变异测试。手工协议测试比随机生成输入的方法在技术方面更加初级。手工协议变异测试不需要自动化模糊测试器。实际上，在手工测试中，测试者就是模糊测试器。在加载了目标应用后，测试者仅仅通过输入不正确的数据，试图使服务器

崩溃，或是诱发一些不正常的行为。这种方法的优点在于，分析者能够在安全审计中充分发挥自己过去的经验。

（3）强制性测试。强制性测试是指模糊测试器从一个有效的协议样本或者数据格式样本开始，持续不断的打乱数据包中的每个字节（byte）、字（word）、双字（dword）或者字符串（String）。这是一种有效的早期模糊测试方法，因为这种方式几乎不要求对应用进行研究，而且，实现一个基础的强制性模糊测试器也是相对直接的。基本上强制性模糊测试器只需要修改数据并将其发送给被测应用。当然除了发送数据外，也可以在强制性模糊测试器中加入更多的错误检测手段、日志手段等。这样一个工具通常能够在短时间内被创建出来。

强制性测试方法相对比较低效，因为许多 CPU 周期会被浪费在生成完全不可解析的数据上。然而，该方法具有以下优点能够抵消这个不足：

1）整个强制性模糊测试的过程可以被完全自动化。

2）使用强制模糊测试方法代码覆盖依赖于一致的合法数据包。

3）大多数协议规约都是相对复杂的，因此即使要达到较低的覆盖率，也需要大量的样本。

（4）自动协议生成测试。自动协议生成测试是一种更高级的强制性测试方法。在这种方式中，首先要做的是对被测应用进行研究、理解和解释协议规约。这种方法首先要创建一个描述协议规约如何工作的语法。

采用这种方式，测试者可以识别出数据包中的静态部分和动态部分，动态部分就可以被模糊化变量替代。随后模糊测试器动态分析包含了静态和动态部分的模板，生成模糊测试数据，将结果数据包发送给被测应用。

这种方法是否能够成功取决于测试者的能力，测试者需要能够指出规约中最容易导致目标应用在解析时发生故障的部分。

（5）启发式技术。启发式指自我发现的能力或运用某种方式或方法判定事物的知识和技能。启发式技术能够提升模糊测试的自动化程度和性能。

（6）代理模糊测试。在典型的基于网络的客户端—服务器模型中，代理模糊测试可在客户端和服务器之间直接进行通信。代理模糊测试器在客户端和服务器之间的连接中充当中继。为了有效地完成这一任务，客户端和服务器必须被手工配置为指向代理服务器。也就是说，客户端把代理当作服务器，而服务器把代理当作客户端。代理模糊测试架构如图 2-2 所示。

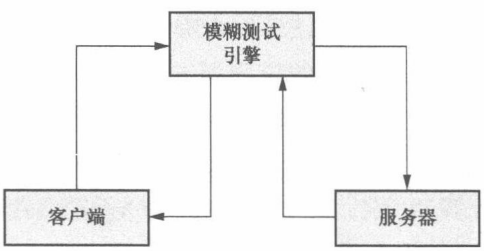

图 2-2 代理模糊测试架构

（7）改进的代理模糊测试。对代理模糊测试的改进是为了让其更“聪明”，使用启发式规则辅助进行自动字段检测和数据变异是其中一种方法。可以应用启发式规则将识别出来的数据进行进一步的处理。

（8）汇编/反汇编启发式技术。应用汇编/反汇编层面的启发式技术来辅助进行更为有效的模糊测试是一个可行的概念，但目前还没有任何公开可用的模糊测试工具或是框架应用这个概念。在进行模糊测试时，使用插装工具监视被测目标上的代码执行。在调试中，寻找静态字符串和证书进行比较操作。然后，将这些信息传回给模糊测试器，为以后生成测试用例提供参考。

（9）生物信息学。该技术利用应用数据、信息学、统计学和计算机科学的方法研究生物学的问题。从本质上来说，生物信息学给出了一些用来发现复杂但结构化的数据序列中的模式的技术。网络协议也可以被看作是由结构化数据组成的长序列，但网络协议能够包含截然不同的消息类型，利用 PI 框架来分析不同的消息类型，PI 框架的目标是通过分析大量观察到的数据，自动推断协议的字段边界，PI 框架应用了 SW 本地序列对齐算法、NW 全局序列对齐算法、相似矩阵和进化树方法。

（10）遗传算法。遗传算法是模拟进化软件使用的一种近似搜索技术。通常需要定义以下三方面的内容：

1）表示方法：解决方案（个体）的表示方法。

2）适应度函数：用来评估得到的方案（个体）对环境适应度的函数。

3）生产函数：复杂变异和让两个方案（个体）交配的函数。

本书将结合（3）和（4）进行模糊测试数据的生成。针对模糊测试，对数据结构了解得越多，就越能够在模糊测试中关注那些易引发异常的协议部分，所以分析的数据确定集中在网络协议与工控协议。必须要了解电力通信协议的组成与规范，才能生成一个更好的模糊测试数据。

2.3 电力系统典型通信协议解析

2.3.1 IEC 104 协议解析

1. 概述

IEC 60870-5-104 协议（以下简称 IEC 104 协议）适用于具有串行比特数据编码传输的远动设备和系统，用于对地理广域过程的监视和控制。制定远动配套标准的目的是使兼容的远动设备之间达到互操作。IEC 104 协议利用了 IEC 60870—5 的系列文件。IEC 104 协议规定了 IEC 60870-5-101 的应用层与 TCP/IP 提供的传输功能的结合。在 TCP/IP 框架内，可以运用不同的网络类型，包括 X.25、FR（帧中继）、ATM（异步传输模式）和 ISDN（综合服务数据网络）。根据相同的定义，不同的 ASDU，包括 IEC 60870—5 全部配套标准（例如 IEC 60870-5-102）所定义的 ASDU，可以与 TCP/IP 相结合，不过这些在 IEC 104 协议中没有进一步说明。

IEC—104 规约是由 IEC—101 规约演化而来的，一般采用网络 TCP 通道，标准的

端口号为 2404，有 IANA-互联网数字分为授权定义和确认，也可根据需要自行确定。

IEC 60870—5 系列通信协议包含如下几个部分：

IEC 60870-5-1：传输帧格式；

IEC 60870-5-2：链路传输规则；

IEC 60870-5-3：应用数据的一般结构；

IEC 60870-5-4：应用信息元素的定义和编码；

IEC 60870-5-5：基本应用功能；

IEC 60870-5-101：基本远动任务配套标准；

IEC 60870-5-102：电力系统电能累积量传输配套标准；

IEC 60870-5-103：继电保护信息接口套餐标准；

IEC 60870-5-104：采用标准传输协议子集的 IEC 60870-5-101 网络访问。

2. 应用范围

电力仪表、RTU 等。

3. 通信模型

IEC 104 通信模型如图 2-3 所示。

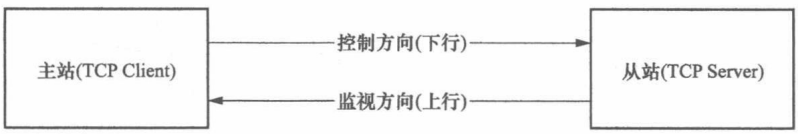

图 2-3 IEC 104 通信模型

4. “四遥”

电力系统的“四遥”包括遥信、遥控、遥测、遥调。“四遥”信号如表 2-1 所示。

表 2-1 “四遥”信号

数据访问	PLC、仪表	Modbus（数据模型）	IEC 104（命令类型）
数字量	离散输入	离散输入	遥信
	离散输出（或内部变量）	线圈	遥信、遥控
模拟量	模拟量输入	输入寄存器	遥测
	模拟量输出（或内部变量）	保持寄存器	遥测、遥调

5. 协议格式

IEC 104 协议格式如图 2-4 所示。

类型标识为一个字节，可变结构限定词为一个字节，传输原因可以为一个或两个字节，公共地址可以为一个或两个字节，信息体地址可以为一个、两个或三个字节，具体采用几个字节表示需要遵照通信双方的约定。ASDU 的详细内容请参考有关的 IEC 60870-5-101 规约。

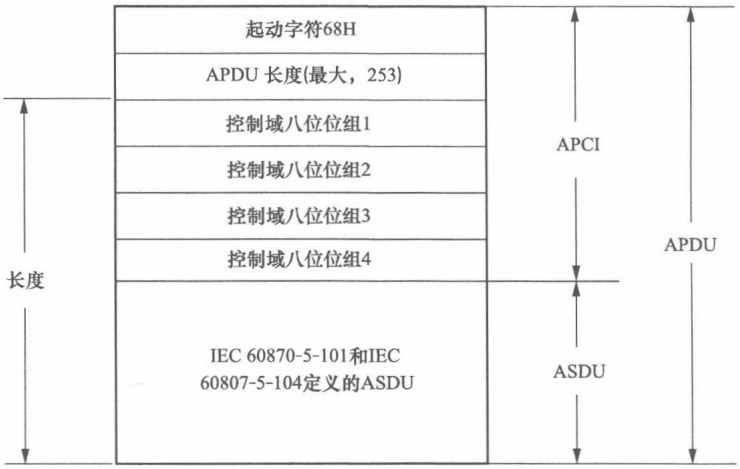

图 2-4　IEC 104 协议格式

2.3.2　MMS 协议解析

1. 概述

制造报文规范 MMS 是 ISO/IEC 9506 标准所定义的一套用于工业控制系统的通信协议。MMS 规范了工业领域具有通信能力的智能传感器、智能电子设备（IED）、智能控制设备的通信行为，使出自不同制造商的设备之间具有互操作性（Interoperation）。

MMS 是一种实时通信机制，IEC 61850 MMS 和 GOOSE 报文通信是基于 IEC 61850 数字化变电站的通信基础。

MMS 的目的是为了规范工业领域具有通信能力的智能传感器、智能电子设备（IED）、智能控制设备的通信行为，使出自不同制造商的设备之间具有互操作性（interoperation），使系统集成变得简单、方便。MMS 规范分为五部分，即服务规范、通信协议、工业机器人通信规范、过程控制通信规范、数字控制通信规范。MMS 的特点是通过使用 MMS 使工业系统具有互操作性和独立性。其中互操作性是制定 MMS 的初衷，即为设备和应用定义一套标准通信机制，使其在此通信体制下具有高度互操作性。独立性是指 MMS 不同于很多只适用于特定产品的专用通信系统，它是一个通用的、独立于专用设备的国际标准体系，即它为用户提供了一个独立于所完成功能的通用通信环境。MMS 提供了通过网络进行对等（peer-to-peer）实时通信的一套服务集。MMS 作为通用通信协议可以用于多种通用工业控制设备，如可编程控制器和工业机器人等。MMS 可以支持多种通信方式，包括以太网、令牌总线、RS-232C、OSI、TCP/IP、MiniMAP 等，

MMS 也可通过网桥、路由器或网关连接到其他系统上。在国外，MMS 技术广泛用于工业过程控制、工业机器人等领域。目前，MMS 在电力系统远动通信协议中的应用越来越广泛。国际电工委员会第 57 技术委员会（IEC TC57）新近推出的 IEC 60870—6TASE. 2 系列标准定义了 EMS 和 SCADA 等电力控制中心之间的通信协议，