广州市科学技术协会
广州市南山自然科学学术交流基金会　资助出版
广州市合力科普基金会

网络化测控系统可信技术及应用

刘桂雄　徐钦桂　文元美　林若波　著

清华大学出版社

网络化测控系统可信技术及应用

刘桂雄 徐钦桂 文元美 林若波 著

清华大学出版社

内 容 简 介

本书主要论述网络化测控系统的可信增强与评价方法，主要内容包括可信增强网络化测控系统的总体构架与可信的形式化建模方法、完整性验证与增强方法、身份认证与访问控制方法、可信评价方法等，并介绍可信增强与可信评价方法在多个典型网络化测控系统中的应用。

本书可作为高等院校测控、物联网、信息安全、计算机等专业的博士生、硕士生和本科生的教科书，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

网络化测控系统可信技术及应用/刘桂雄等著. --北京：清华大学出版社，2014

ISBN 978-7-302-37602-6

Ⅰ. ①网…　Ⅱ. ①刘…　Ⅲ. ①计算机控制系统－安全技术－研究　Ⅳ. ①TP273

中国版本图书馆 CIP 数据核字(2014)第 186631 号

责任编辑：庄红权
封面设计：傅瑞学
责任校对：赵丽敏
责任印制：王静怡

出版发行：清华大学出版社
网　址：http://www.tup.com.cn，http://www.wqbook.com
地　址：北京清华大学学研大厦 A 座　　邮　编：100084
社总机：010-62770175　　邮　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：170mm×230mm　　印　张：10.5　　字　数：203 千字
版　　次：2014 年 10 月第 1 版　　印　次：2014 年 10 月第1 次印刷
印　　数：1～2000
定　　价：32.00 元

产品编号：056367-01

前　言
FOREWORD

遵循开放式体系标准，以仪器硬件为基础、计算机为核心、网络通信为支撑的网络化测控系统，越来越多地引入普适计算（pervasive computing）、移动计算（mobile computing）、云计算（cloud computing）等先进计算，通过软件技术实现其测控功能。但信息网络系统中存在的安全威胁不断向测控系统扩散，测控软件的开放性、复杂性等特点带来测控系统的脆弱性，降低其正确执行测控功能的可信度。因此，迫切需要专门工作来寻求网络化测控系统可信增强的基础理论创新与应用。

本书以增强网络化测控系统的可信度为主线，重点研究网络化测控系统的可信增强与评价方法。第1章主要讲述网络化测控系统可信性内涵及进展；第2章主要讲述可信网络化测控系统的总体构架设计与形式化建模方法；第3章主要讲述包括现场节点、测控应用服务器软件、操控终端软件在内的系统完整性保护分析与增强方法；第4章是身份认证与访问控制方法研究；第5章主要讲述可信评价方法；第6章为探讨可信增强与可信评价方法在网络化测控系统的应用，给出可信技术在物联网环境空气质量监测平台、高压输电线路网络监测平台、物联网LED显示集成监控平台、虚拟仪器计量技术等测控系统实际应用实际。

本书是作者长期从事网络化测控系统，特别是网络化测控系统可信性研究工作方法和应用成果总结。部分内容在《物联网技术与应用》等研究生课程中进行讲授，这些实践工作对本书的形成起到积极作用。

本书由在一线从事网络化测控系统可信研究的科研工作者完成。第1、2、3章由刘桂雄教授执笔，第4、5章由刘桂雄教授、徐钦桂教授执笔，第6章由刘桂雄教授、文元美副教授、林若波副教授

执笔。全书由刘桂雄教授策划和统稿。

本书的研究与出版工作得到了教育部新世纪优秀人才支持计划项目(NCET-08-0211)、中国博士后科学基金(2011M500130)、广东省高等学校高层次人才项目(粤教师函[2010]79号文)、广东省科技攻关重点项目(2007A060304003)、广州市科学技术协会的资助,在此表示衷心感谢!

博士生吴卓葵、吴国光、余长庚与硕士生赵大伟、袁明山、罗丽等为相关课题的研究做了大量工作。同时,本书在撰写过程中,也得到清华大学出版社的大力支持,在此表示诚挚的谢意!

由于作者水平所限,加之网络化测控系统的可信研究仍处于不断的发展和变化之中,书中错误和不足之处在所难免,恳请专家、读者指正。

作　者

2014年8月于广州

目　录

CONTENTS

第 1 章

网络化测控系统可信技术概述

1.1 网络化测控系统可信度概述

网络化测控系统越来越多通过软件技术实现其测控功能，利用各种总线将地域分散的基本功能单元（计算机、测试仪器、智能传感器、控制模块）互连起来，通过各种网络技术进行信息的传输和交换，使得测控系统功能更强、使用更灵活、性能更高[1-4]。随着普适计算（pervasive computing）、移动计算（mobile computing）、云计算（cloud computing）等先进计算模式出现，遵循开放式体系标准，以仪器硬件为基础、计算机为核心、网络通信为支撑的网络化测控系统将成为测控领域的重要发展方向[5-7]，是物联网技术的核心支撑部分。但测控软件的复杂性、开放性又容易带来测控系统的脆弱性，有时在可靠性方面不如传统硬件化测控仪器，降低其正常工作、正确执行测控功能的可信度。随着最新计算机技术、软件开发技术、网络互连技术在测控领域应用的不断深入，信息网络系统中存在的安全威胁不断向测控系统扩散。测控软件的崩溃、遭受木马攻击与异常工作，会导致军事设施瘫痪[8]、产品废品率增高甚至生产设备毁坏[9]、公众贸易结算利益受到损害[10]，甚至危及人民生命财产。开展网络化测控系统可信技术研究具有重要战略意义。

1.1.1 网络化测控系统可信度概念

网络化测控系统概念突出于测控系统工作在网络化、分布式环境下，基于测控系统层次结构分析方法，可把系统划分为数据传感、数据采集、数据传输、数据处理和数据表达等五个环节，这些环节既可集成在传统计算机及模块化硬件上，又可通过测控网络、仪器总线和外设接口连接分布在独立测控节点。

图 1-1 为网络化测控系统组成结构框图，软件系统是其重要部分，由软件实现的数据处理、数据表达环节又可细分成更多的软件层次、软件模块或软件构件，各

软硬件模块的工作可能需调用标定参数。

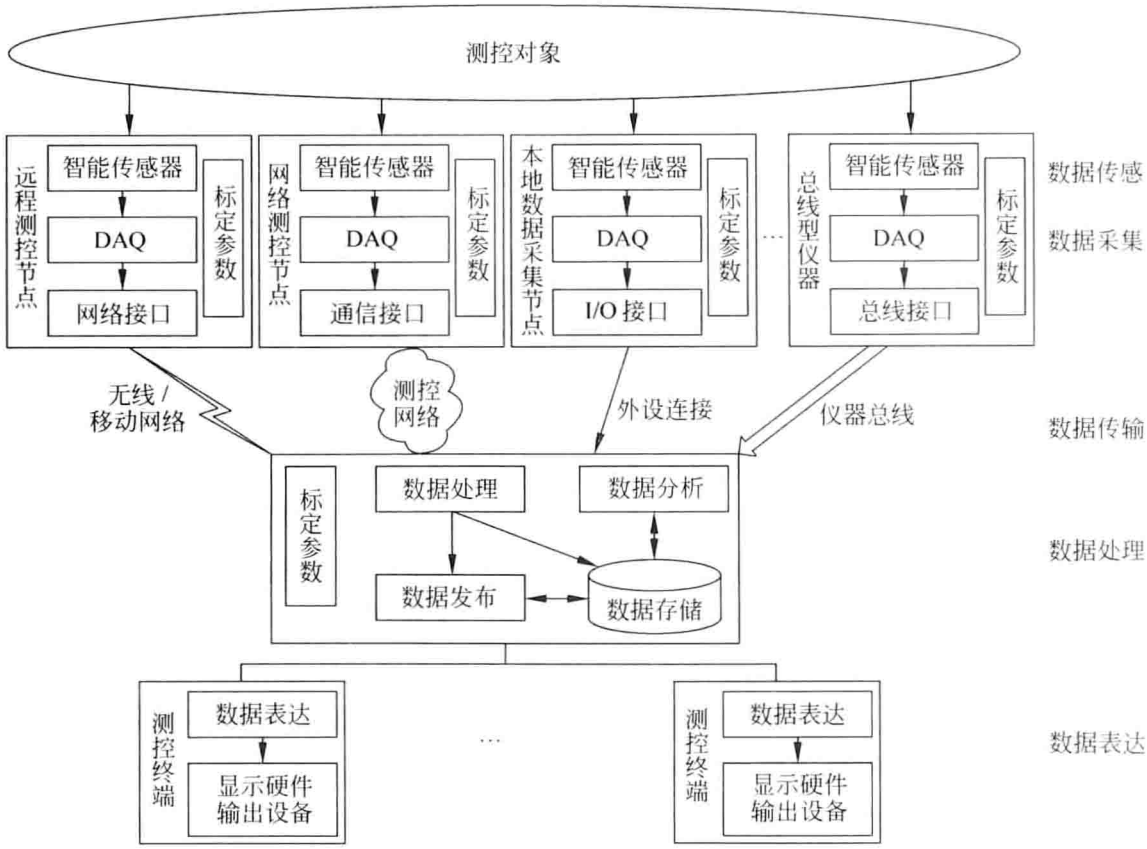

图 1-1 网络化测控系统组成结构框图

网络化测控系统可信度目前还没有明确定义，这里是指以用户、公众或监管部门期望方式工作，正确执行测量控制、系统配置、管理维护等功能，并产生可信测控结果的能力。在开放的软硬件结构、网络环境下，要使网络化测控系统给出可信测控结果，不但要求系统软硬件完整，还需要求系统工作流程正确、用户身份真实、用户操作属于其职权范围并满足系统安全。网络化测控系统应用环境还存在相当数量的系统漏洞、安全威胁，这将直接影响系统的可信度[12]。

1.1.2 脆弱性与系统可信度

图 1-2 为网络化测控系统存在脆弱性与系统可信度关系图。可以看出，如果系统存在完整性保护、身份认证、访问控制等方面脆弱性，使恶意人员、不良用户和恶意代码等通过对系统执行身份冒充、篡改软件代码、更换硬件模块、非正常操作、

篡改关键参数、测控欺诈和注入恶意程序等行为，使系统表现出操作人员身份可信、软硬件完整可信、运行环境可信、用户行为可信等多个方面可信度降低，更改系统测控逻辑，操控测控结果[13]。这也就是说，减少系统存在的脆弱性，可以减少导致可信降低行为的发生，提高系统的可信度。

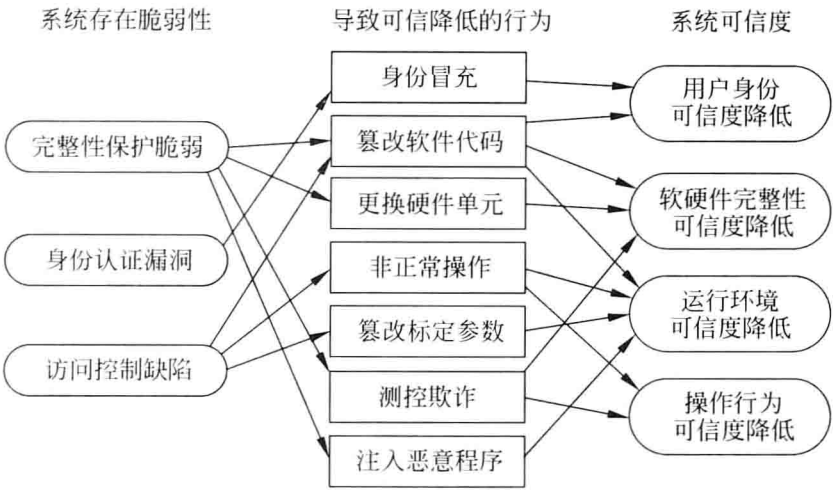

图 1-2　网络化测控系统存在脆弱性与系统可信度关系图

还可以看出，用户身份可信度降低由身份冒充行为引起，身份冒充由身份认证漏洞、完整性保护脆弱所致，要提高操作人员身份可信度，应减少或消除系统身份认证漏洞和完整性保护脆弱性；软硬件完整性可信度降低由更换硬件单元、篡改软硬件代码和测控欺诈等行为所致，使这些行为得以发生的原因是系统存在完整性保护脆弱性、访问控制缺陷，提高系统软硬件完整性可信度，必须增强系统完整性保护能力、消除访问控制保护缺陷；更换硬件单元、篡改软件代码、更改标定参数和注入恶意程序，都导致测控模块运行环境可信度降低，这些行为也需要利用系统完整性保护脆弱性、访问控制缺陷，要提高运行环境可信度也需要从完整性保护、访问控制两方面增强系统的保护能力；操作行为可信度降低是由于不良用户通过非正常操作、测控欺诈产生了不可信测控结果，非正常操作和测控欺诈行为的发生往往因为系统存在访问控制缺陷，提高操作流程可信度，需要增强系统访问控制保护能力。

因此，必须从完整性保护、身份认证、访问控制等 3 个方面研究网络化测控系统可信增强技术，来提高整个系统可信度，由于 3 个方面的脆弱性与系统 4 个可信度属性之间不是一一对应关系，因此在研究解决系统脆弱性问题可信增强方法时，需要综合考虑。

1.2 网络化测控系统可信理论国内外研究进展

近年来，围绕网络化测控系统可信理论的研究主要集中在“网络化测控系统完整性验证与增强方法”、“网络化测控系统身份认证与访问控制方法”、“网络化测控系统可信评价方法”等方面。

1.2.1 网络化测控系统完整性验证与增强方法

网络化测控系统完整性包括数据完整性、模块(包括软硬件模块)完整性，那么系统完整性保护必须保证始终保持硬件完整、信息或软件不被未授权篡改，或在篡改后能够被迅速发现，相应也可从完整性验证、完整性增强两个层次来进行。其中完整性验证是被动测试硬件、数据及软件模块的完整性状态，是被动方法；完整性增强，严防非授权操作更改硬件、数据及软件模块的内容，是主动方法。

1. 完整性验证方法

完整性验证原理是通过对硬件、数据以及模块在不同时期的不变特征值进行比较来判断模块是否已被更改[14]。基于不变特征类型，大致可划分为基于数字指纹、基于特征匹配和基于行为监控三种完整性验证方法。

1) 基于数字指纹完整性验证方法

图 1-3 是基于数字指纹的完整性验证过程，它的原理是采用一个散列函数 $h:\{0,1\}^* \rightarrow \{0,1\}^l$ 为硬件、数据以及模块 M 计算一个长度为 l 的数字指纹 g(不变特征值 P)，通过安全传输或保存，验证方重新计算待验证硬件、数据或模块的数字指纹 g'，比较 g' 与 g 是否相等来判断 M 完整性状态[15]。由 R. L. Rivest 开发的(1992)MD5 散列算法[16]能对任意长度的消息 m 采用分组、迭代、散列方法进行处理，压缩成 128bit 数字指纹 g，具有良好单向性、抗碰撞性和雪崩效应(对输入消息 m 的微小改动，算法输出的数字指纹 g 有近乎半数左右 bit 位会改变)[17]，被广泛应用于加密解密、PGP 邮件加密和文件完整性验证。为支持高安全性要求的电子商务应用，美国国家安全局(NSA)(1995)通过公开标准文件(FIPS 180-2)发布了 SHA 系列密码散列函数，其中 SHA-1 可对最大长度为 2^{64} bits 的消息计算 160bits 数字指纹，与数字签名算法 DSS(digital signature standard)联合使用[18]。SHA-1

算法产生 160bits 数字指纹，对穷举攻击能力更强，MD-5 的碰撞攻击对 SHA 无效[19]，理论上破解运算量达 2^{80} 次，用每秒十万亿次速度计算机破解需要 5000 年，但还是有学者找到将 SHA-1 碰撞消息算法复杂度降低为 2^{69} 的方法[20]。美国马萨诸塞州 RSA 实验室 Michael Szydlo 等(2006)采用消息扩充函数对输入消息进行预处理方法，进一步增强 MD5 和 SHA-1 抗冲突性能，但并未增加理论上的破解难度[21]。文献[22](2010)研究一种输出长度为 160bits 的动态散列函数构造方案，对 MD 结构进行改进，提高了散列函数抵抗部分消息碰撞攻击的能力。

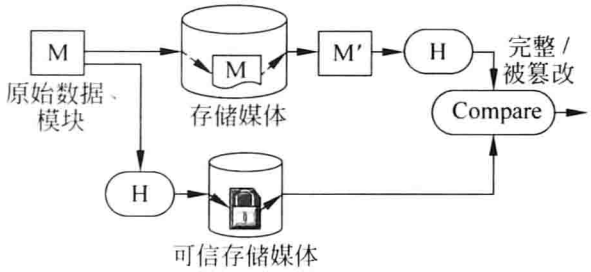

图 1-3　基于数字指纹的完整性验证过程

2) 基于特征匹配完整性验证方法

图 1-4 是特征匹配完整性验证过程，它将计算机病毒、网络蠕虫、特洛伊木马、后门代码、rootkit 等恶意代码的二进制特征码、检测规则分别建立成特征库和规则库，按照匹配规则用每个特征码去匹配待验证模块二进制串，一旦发现某个特征码匹配，则认为模块 M 已被相应恶意代码篡改，完整性遭到破坏[23]。基于特征匹配验证方法关键是特征库的全面性、特征匹配算法的验证能力与效率。Vienna 大学 C. Kruegel 等(2004)以 rootkit 恶意代码的执行序列为特征，采用非形式化方法描述这些特征并建立特征库，对被检程序二进制代码进行静态分析或符号执行，获得指令执行序列，然后进行特征码匹配，实验结果获得了 100%的 rootkit 识别率和零误报率[24]。C. Wysopal 等(2008)研究特殊凭证、隐藏功能、安全关键参数控制、

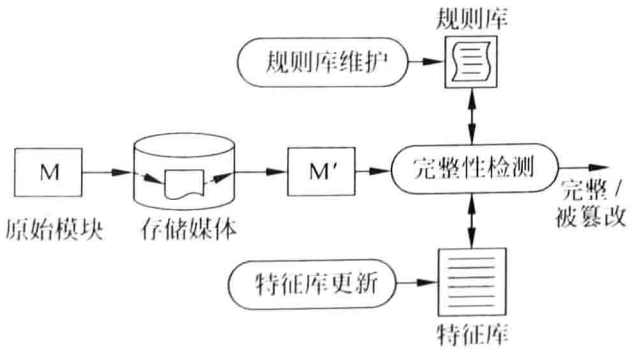

图 1-4　基于特征匹配的完整性验证

植入 Shell 命令、逻辑炸弹、类 Rootkit 行为、自修改代码、代码或数据异常等应用级后门程序代码的特征码，提出基于源程序、二进制形式模块的静态检测方法，在 Symantec 病毒防护系统中得到应用，但不能检测未知后门代码和恶意代码[25]。文献[26](2010)年提出一种基于规则优化与排序的恶意代码匹配检测方法，将面向协议特征变换为面向内容特征进行搜索匹配，精简特征库中规则条数，采用规则匹配成功的频繁度对规则排序，提高恶意代码检测能力和检测速度。

3) 基于行为监控的完整性验证方法

图 1-5 是基于行为监控的完整性验证方法框架，它由可信监控模块对处于运行过程的模块行为进行跟踪，设置监控规则，进行行为特征匹配，识别程序异常状态，判断恶意代码的存在性与模块的完整性状态[27]。行为监控、捕捉和特征码提取方法是关键技术。Carnegie Mellon 大学 Newsome 等(2005)提出商用软件恶意代码检测模型 TaintCheck，自动检测、分析堆栈覆盖攻击代码，利用语义分析产生攻击特征码，可有效识别多态蠕虫代码，但算法开销较大[28]；EunYoung Kim 等(2006)提出一种启发式恶意代码实时检测系统，通过监测进程操作、注册表访问和网络行为生成程序轮廓，将偏离正常轮廓的行为视为非正常代码，对未知恶意代码检测准确率达 93%，但恶意代码可通过反检测措施逃避监测[29]。Jochen(2008)在维持代码语义不变条件下在移动代码中嵌入篡改检测标记，实现移动代码完整性验证，但不具有通用性[30]。

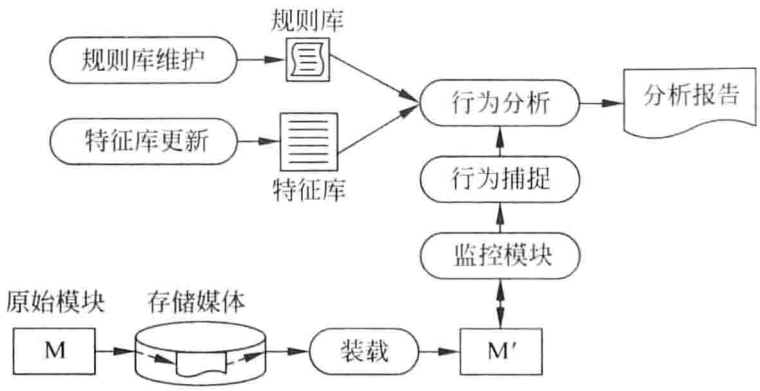

图 1-5 基于行为监控的完整性验证方法框架

表 1-1 为 3 种完整性验证方法特性对比表。可以看出：①基于数字指纹的验证方法可对任何硬件、数据、模块实施完整性验证，但依赖于数字指纹可信度、散列算法安全性；②基于特征码匹配验证方法根据代码特征可检测已知恶意代码，但依赖于代码特征可靠度，可能存在误判；③基于行为监控完整性验证方法可检测未知恶意代码，但恶意行为特征提取难度大，3 类完整性验证方法各有特点，可根

据应用场合灵活应用、改进。

表 1-1　3 种完整性验证方法特性对比表

所述类别	验证方法	适用应用	安全性能	不足
基于数字指纹完整性验证方法	MD5 数字指纹	任何硬件、数据、模块的完整性验证	找到碰撞的理论试验数 2^{64} 次，最短个案破解时间 <10min[18]	需要采用可靠手段存储数字指纹
基于特征码匹配完整性验证方法	C. Kruegel 的 rootkit 扫描器	被植入已知恶意代码的软件模块	100% rootkit 识别率和零误报率[24]	依赖于恶意代码特征可靠度，可能存在误判
基于行为监控完整性验证方法	EunYoung Kim 恶意代码行为实时检测系统	被植入代码特征不明显恶意代码的软件模块	检测未知恶意代码的测试准确率达到 93%[29]	恶意代码行为特征提取难度大

2. 完整性增强方法

完整性增强是指采用硬件或软件手段加固模块、系统，阻止破坏系统完整性的数据流，隔离被篡改软硬件模块，使测控操作由可信测控软件在可信软硬件环境下执行完成。与网络化测控系统可信有关的完整性增强方法主要有完整性增强的信任链传递方法、完整性增强的信息流控制方法、计量规范完整性保护方法等。

1）完整性增强的信任链传递方法

图 1-6 描述了计算机系统信任链传递过程，其基本思想是以防篡改、防伪造的可信平台模块 TPM（一个含有密码运算部件和存储部件的小型 SoC 片上系统）和 BIOS Boot Block 作为可信根源，系统上电时，首先获得 CPU 控制权，对 BIOS 执行完整性度量和验证，若通过验证则将 BIOS 加入可信模块集（Trusted Modules Set，TMS）并将控制转移到给它，此后，BIOS 对 Bootloader、Bootloader 对 OS、OS

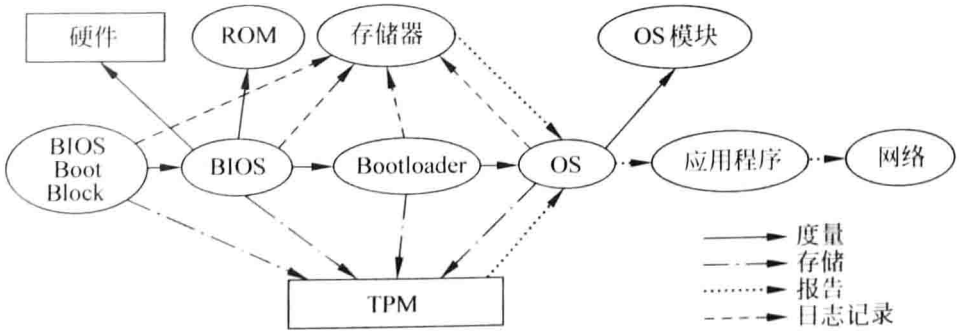

图 1-6　计算机系统信任链传递过程

对 OS 模块与应用程序依次执行同样的完整性度量、验证、控制转移操作，将通过验证的模块加入 TMS，最终将信任边界扩展到系统启动路径上所有模块[31]。Joshua Guttman 等(2008)基于 TCG 规范，建立可信软件栈，实现远程完整性验证功能，验证时间满足实时性要求[32]；还有学者(2010)提出基于可信计算技术软件运行时的可信证据收集机制，在操作系统层引入一个可信证据收集代理，收集目标应用程序运行时的可信证据，实现基于 TPM 的应用程序完整性保护方案，但软件模块数字指纹的安全存储仍然是一个薄弱环节[33]。

2) 完整性增强的信息流控制方法

基于信息流控制完整性增强方法由 Kenneth J. Biba(1977)首次提出，图 1-7 描述了其工作原理，系统为每个受保护的数据、模块绑定一个完整级标签，将系统保持完整性定义为系统中未曾发生完整级高的信息被完整级低的信息所污染时所处的状态，系统通过安全策略监控所有受保护数据访问请求，若本次访问可导致低完整级信息直接或间接流向高完整级的信息，则阻止该次数据访问[34]。美国国防部(1985)《可信计算机系统评价准则》(trusted computer system evaluation criteria，TCSEC)规定安全等级在 B1 级及以上计算机和信息系统都要进行信息流控制，以增强对恶意代码的免疫保护能力[35]。美国国家安全局(national security agency，NSA) Loscocco 和 NAI 公司 Smalley 将 Biba 完整性保护模型集成进 Linux 内核，使通用操作系统获得基于信息流控制的完整性保护特性[36]。孙玉芳等(2005)在基于 Linux 的安全操作系统 RFSOS 中实现一种动态完整性实施方案，对系统整体效率影响小于 1%[37]。Jafarian 等(2009)提出根据上下文动态调整完整性标签方法，将基于信息流控制完整性增强方法推广到普适计算环境，但存在从低完整级到高完整级合法数据流被误拒问题[38]。

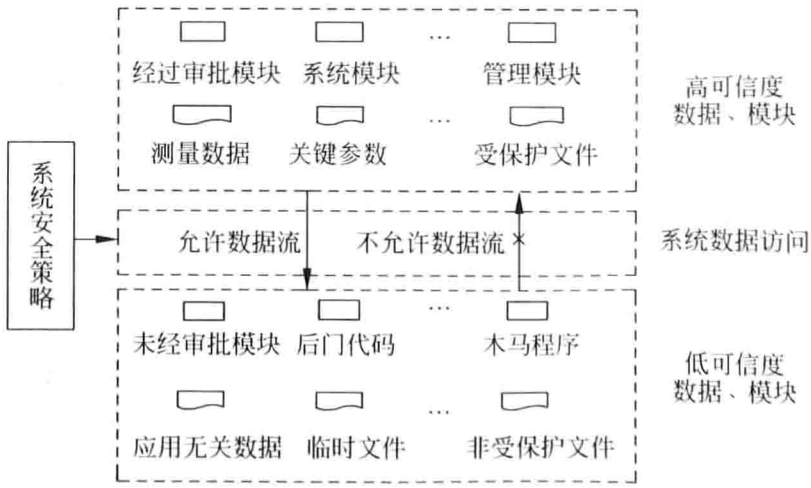

图 1-7 基于信息流控制完整性增强过程

3）计量规范完整性保护方法

计量规范完整性保护方法近年来得到国内外计量部门的关注和重视，国际法定计量组织、欧洲国家法定计量服务组织和中国国家技术监督总局等计量组织(2004—2008)相继发布了“计量器具软件通用要求(OIML D-SW)”[39]、“欧洲计量器具法规(WELMEC 7.2)”[40]和“计量器具软件测评指南(JJF 1182—2007)”[41]，规定可能影响到测控结果的软件模块都应经过管理部门审批，以保证基于软件计量器具给出测量结果可信。图 1-8 描述了计量规范软件完整性保护结构。系统首先应采用硬件锁、铅封和电子封缄等硬件方法使攻击者无法更改测控仪器硬件单元和其中软件代码，若强行更改将留下明显印记，对于部署与存储设备中的测控功能模块，根据重要程度不同封装成独立的库文件或可执行文件，利用系统访问控制机制实施保护；软件升级过程有检验人员在场监督，或在一个可信的监控管理模块(trusted supervising module，TSM)控制下，严格按照装载、完整性检查、来源鉴别、安装、激活五个步骤执行，以保证载入和安装的升级模块经过了审批并保持完整性；软件升级和用户操作事件写入日志文件以便进行事后安全审计[39-41]。德国时钟同步负载电表项目(tLZ)组(2007)发布同步模块化电表规范，提出遵循 WELMEC 7.2 规范智能电表软件远程升级流程[42]，Fraunhofer 安全信息技术研究所 Andreas Fuchs 和 Siegen 大学 Donatus Weber (2011)对升级过程安全性进行形式化分析和证明[43]。

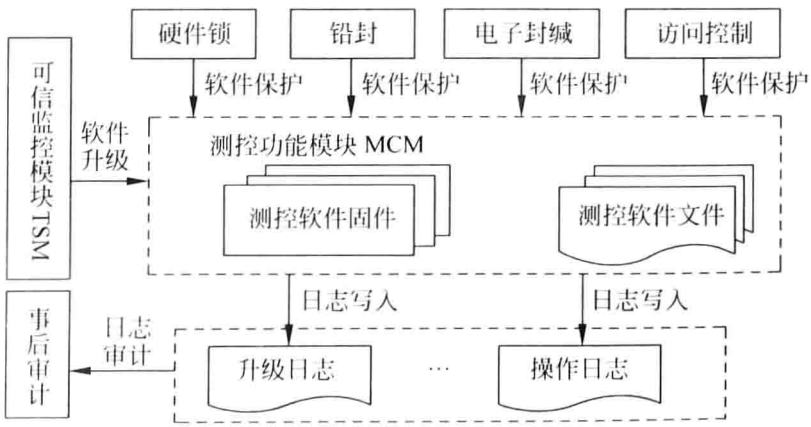

图 1-8　基于计量规范软件完整性保护结构

表 1-2 是 3 种完整性增强方法特性对比表。可以看出：①完整性增强的信任链传递方法可从系统启动模块开始实施完整性保护，可信度高，但数字指纹安全存储是一个薄弱环节；②完整性增强的信息流控制方法允许以合法方式更新受保护信息，但需按具体应用需求进行构造、配置和改进；③计量规范完整性保护方法反映测控计量领域对软件完整性的要求，但需根据应用需要确定适合的实现方案。