基于容错的可信计算在变电站自动化系统中的应用

张其林 著

中国水利水电出版社
www.waterpub.com.cn

基于容错的可信计算在变电站自动化系统中的应用

张其林　著

中国水利水电出版社
www.waterpub.com.cn

·北京·

内 容 提 要

本书将可信计算引入变电站自动化系统，根据基于容错的可信内涵与智能电网的需求，在深入分析变电站自动化系统可信性属性的基础上，从保障系统可信性的措施——故障防止、故障容忍、故障抑制与故障预报出发，研究了构建可信变电站自动化系统的一系列问题。

本书可供信息技术、自动化、电力系统自动化等学科的研究生、教师阅读，也可供从事相关方向的研究人员参考。

图书在版编目（CIP）数据

基于容错的可信计算在变电站自动化系统中的应用 / 张其林著. -- 北京 : 中国水利水电出版社, 2018.9
ISBN 978-7-5170-6830-3

Ⅰ. ①基… Ⅱ. ①张… Ⅲ. ①容错技术－应用－变电所－自动化系统 Ⅳ. ①TM63

中国版本图书馆CIP数据核字(2018)第209166号

策划编辑：石永峰　责任编辑：张玉玲　加工编辑：孙　丹　封面设计：李　佳

书　名	基于容错的可信计算在变电站自动化系统中的应用 JIYU RONGCUO DE KEXIN JISUAN ZAI BIANDIANZHAN ZIDONGHUA XITONG ZHONG DE YINGYONG
作　者	张其林　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市兴国印务有限公司
规　格	170mm×240mm　16开本　18.75印张　290千字
版　次	2018年10月第1版　2018年10月第1次印刷
印　数	0001—2000册
定　价	75.00元

前　言

智能电网是传统电网向高效、经济、清洁、互动的现代电网的升级和跨越，代表着电网未来发展的方向。智能电网的坚强（即不脆弱）是指电网必须具有自愈性、鲁棒性、生存性等主要特征。然而，诸多事故表明，构建坚强的智能电网，需要坚强的电力自动化技术作支撑。如四川三滩水电厂“10·13”事故，控制系统与办公自动化系统的直接互联是其中的不安全因素之一；2003 年北美大停电蔓延和扩大的基本原因之一就是监控系统中 EMS 发生故障，电力系统失去可观测性和可控性，进而导致整系统陷于瘫痪瓦解；2008 年 2 月 27 日，美国中央情报局披露，犯罪者通过网络入侵计算机控制系统，切断了多个城市的电力系统网络；2015 年 12 月 23 日，乌克兰伊万诺-弗兰科夫斯克地区 7 个 110kV 变电站和 23 个 35kV 变电站出现故障，导致该地区数十万人断电，这是一起网络攻击导致的大停电事故。这一系列事故暴露出电力自动化系统与装置的以下缺陷：

（1）各种自动化系统中的偶然因素，如软件故障、硬件故障及人为的操作错误常常威胁电力系统的安全运行。

（2）电力系统中运行的各种监测控制系统并不完全值得信任。

（3）缺少对电力系统遭受到的偶然性威胁和恶意攻击进行鉴别的能力。

（4）相关的安全防御措施已不能完全抵御目前的风险威胁。

变电站是智能电网的关键节点。变电站自动化系统是通过计算机网络、现代通信技术、自动控制、传感装置等实现变电站运行状态的自动监测与控制的系统。为满足智能电网的需求，变电站自动化系统必须为电网及用户提供可信赖的服务，是一个可信的系统。

传统的可信性（Credibility）理论是一种基于概率统计的研究具有模糊不确定现象的数学方法。随着信息技术的发展，计算机系统应用呈现出日益广泛而深入的发展态势。可信计算的含义不断地拓展，由侧重于硬件的可靠性、可用性到针对硬件平台、软件系统、服务的综合可信，适应了 Internet 上应用系统不断拓展的发展需要。基于网络的分布式计算系统及开放式网络环境增加了系统的复杂度、故障率和不安全因素，这种形势促使人们不得不对计算机系统的性能和服务质量提出严格以致苛刻的高要求，那就是高质量和低风险以致无风险的可信赖服务，而传统的“可靠性（Reliability）”已不足以描述这种性质。1985 年法国人 Jean-Claude Laprie 和美国人 Algirdas Avizienis 提出可信计算（Dependable Computing）的概念。容错专家们自 1999 年将容错计算会议改名为可信计算会议（PRDC）后，便致力

于可信计算的研究。

基于容错的可信计算更强调计算系统的可靠性、可用性和可维护性，而且强调可信的可论证性。系统必须能够抵御系统的本征故障、人为故障和恶意攻击，强调系统对攻击的抵抗能力、识别能力、恢复能力和系统的学习能力，包括可靠性、安全性、可用性、机密性、完整性以及可维护性等属性。

变电站自动化系统就是一种特殊的信息系统。为了保证提供可信赖的服务，该系统必须具备以下特点：

（!）典型的实时系统，系统在高效的网络通信支撑下，必须在规定的时间内将规定的数据送到规定的地方。

（2）系统中的部件（包括硬件、软件）必须是可靠的，保证能够 24 小时不间断地运行。

（3）必须保证从传感器（CT、VT）获取的数据的可用性、完整性和机密性，才能保证向调度中心送出的数据是可信任的。

（4）系统某个部件在面对随机或蓄意攻击时必须是鲁棒的，且因遭受攻击而出现故障后，故障的波及面尽可能小，并在可接受的时间内得到维护。

（5）具有相应的保护措施，系统的运行不应对人及物造成危害。

在上述背景下，本书将基于容错的可信计算方法引入到变电站自动化系统中，在分析变电站自动化系统可信性的基础上，分别针对故障防止、故障容忍、故障预报、故障排除等方面提出相应的解决方法，为智能电网环境下的变电站自动化设计与建设提供参考。本书的出版得到“机电汽车”湖北省优势特色学科群建设项目的资助。

鉴于作者水平有限，书中难免存在错误之处，敬请读者批评、指正。

作　者

2018 年 7 月

目　录

第 1 章　绪论

1.1　背景与意义

国家电网有限公司在 2009 年 5 月召开的特高压输电技术国际会议上宣布，中国将加快建设以特高压电网为骨干网架，各级电网协调发展，具有信息化、数字化、自动化、互动化特征的统一的坚强智能电网。

智能电网的坚强即不脆弱，就是电网必须具有自愈性、鲁棒性、生存性等主要特征。然而，诸多事故表明，构建坚强的智能电网，需要坚强的电力自动化技术作支撑。如四川二滩水电厂“10·13”事故[1]，控制系统与办公自动化系统的直接互联是其中的不安全因素之一；2003 年北美大停电蔓延和扩大的基本原因之一就是监控系统中 EMS 发生故障，电网调度人员失去对电力系统的可观测性和可控性，进而导致整系统陷于瘫痪瓦解[2]；2008 年 2 月 27 日，美国中央情报局披露，犯罪者通过网络入侵计算机控制系统，切断了多个城市的电力系统网络。这一系列事故暴露出电力自动化系统与装置的以下缺陷：

（1）各种自动化系统中的偶然因素，如软件故障、硬件故障及人为的操作错误常常威胁电力系统的安全运行。

（2）电力系统中运行的各种监测控制系统并不完全值得信任。

（3）缺少对电力系统遭受到的偶然性威胁和恶意攻击进行鉴别的能力。

（4）相关的安全防御措施已不能完全抵御目前的风险威胁。

变电站是智能电网的关键节点，承担着不同等级电压的转换，其安全、稳定地运行对整个电网的安全稳定具有极其重要的意义。变电站自动化系统是通过计算机网络、现代通信技术、传感装置等实现变电站运行状态的监测、控制自动化的系统，同样存在着上述事故中暴露出的风险，无论是信息通信系统还是监控系

统中的任何一个元部件发生故障，都可能导致灾难性的事故发生。因此，变电站自动化系统必须为电网的安全、稳定运行提供可信赖的服务，即变电站自动化系统必须是一个可信的系统。从系统的性能角度看，可信系统必须能够抵御系统的本征故障、人为故障和恶意攻击，强调系统对攻击的抵抗能力、识别能力、恢复能力以及系统的学习能力。

传统的可信性理论是一种基于概率统计的研究具有模糊不确定现象的数学方法。随着信息技术的发展，计算机系统应用呈现出日益广泛而深入的发展态势，政治、经济、商业运作和各类事务处理越来越严重地依赖于计算机的应用，在国防军事、核反应堆控制、飞机航行控制、火控及化学反应控制等关键应用和医疗、金融、交通、通讯、气象、电力、石油化工、Web 服务、联机事务处理、科学计算等重要应用中尤其如此。与此同时，基于网络的分布式计算系统及开放式网络环境增加了系统的复杂度、故障率和不安全因素，这种形势促使人们不得不对计算机系统的性能和服务质量提出严格甚至苛刻的高要求，那就是高质量和低风险以致无风险的可信赖服务，而传统的“可靠性”已不足以描述这种性质。Avizienis 提出了表达计算机系统信任属性的可信性概念[3]，表示这种信任属性放在系统递交的服务上是合理的[4]。可信是人机之间的信任关系，也是系统之间的信任关系，一直是信息技术研究者关注的热点。

变电站自动化系统就是一种特殊的信息系统。为了保证提供可信赖的服务，该系统必须具备以下特点：

（1）典型的实时系统，系统必须在规定的时间将规定的数据送到规定的地方。

（2）系统中的部件（包括硬件、软件）必须是可靠的，保证能 24 小时不间断地运行。

（3）必须保证从传感器（CT、VT）获取的数据的可用性、完整性和机密性，才能保证向调度中心送出的数据是可信任的。

（4）系统某个部件在面对随机或蓄意攻击时必须是健壮的，且在遭受攻击出现故障后，故障的波及面尽可能小，并在可接受的时间内得到维护。

（5）具有相应的保护措施，系统的运行不应对人及物造成危害。

变电站自动化系统的这些特性基本可以用Avizienis提出的计算机系统信任属性的可信性（Dependability）概念[3]来表达，包括可靠性（Reliability）、安全性（Safety）、可用性（Availability）、机密性（Confidentiality）、完整性（Integrity）以及可维护性（Maintainability）等属性，但必须结合变电站自动化系统的特点经过必要的扩充，以求更加准确。目前，单独研究变电站自动化系统可靠性或者信息安全的文献较多，但将它们综合考虑研究其可信性的文献尚不多见。然而，智能电网的发展又迫切需要整体考虑系统的可信性，研究它包含的各属性之间的关系、对系统的各种安全威胁、系统组件故障或者失效的规律以及如何采取有效的措施尽可能地防止系统组件的故障，以保证变电站自动化系统为电网及用户提供可信的服务，具有重要的理论与现实意义。

1.2 国内外研究现状

文献[5]将系统的可信性看成是一个全局性、综合性的概念，包含特征属性、可信性威胁、可信性方法，如图1.1所示。

图1.1 可信性的概念

研究可信计算在变电站自动化系统中的应用，将以图1.1的线索，从系统属

性、系统面临的威胁、威胁的预防等几个方面展开。1.2.1 将阐述可信计算的相关研究现状；本书的研究对象是变电站自动化系统，1.2.2 将介绍变电站自动化系统在可靠性与信息安全方面的研究现状，特别是基于 IEC 61850 标准的变电站自动化系统的特点；可信性包含多个属性，不同的系统对这些属性有不同的要求，且侧重点也各有差异。如机械加工系统侧重于可靠性，网络系统侧重于信息的安全，电力系统则除了考虑可靠性还要考虑可维护性。因此，变电站自动化系统在这些属性上必定存在特殊的需求，还有可能需要其他的属性来描述，下面将在 1.2.3 介绍可信性需求方面的研究现状；针对系统中的故障，首先必须防止系统缺陷的产生，这就要求采用合适的设计方法，保证系统运行逻辑的正确性，1.2.4 综述各种设计方法的研究现状；当系统中组件发生故障时，故障以何种规律在系统中传播是一个关键问题，1.2.5 将介绍连锁故障的研究现状；变电站自动化系统就是对变电站一次设备进行监测与控制的信息系统，系统的信息均来自安装在一次设备上的传感器，即电流互感器、电压互感器。保证系统信息来源的可信是变电站自动化系统运行的基础，1.2.6 将介绍基于数据驱动的故障诊断研究现状。

1.2.1 可信计算与可信系统

可信计算源于容错计算，以 IEEE 国际容错计算会议为标志。可信计算有三个来源：可信计算（Dependable Computing）、可信赖计算（Trusted Computing）和高信度计算（Trustworthy Computing）。

因构成器件不可靠，早期的计算机采用了一些实用技术以提高部件及系统的可靠性，如差错控制、复式比较、三模冗余等。随后，J. Von Neumann、E. F. Moore 和 C. E. Shannon 等提出了冗余理论，采用多个冗余器件屏蔽器件的缺陷[4]。1985 年第 15 届国际容错计算会议上，J. C. Laprie 代表 IFIP WG10.4 和 IEEE CS 容错计算技术专业委员会，提出了可信计算概念[6]。可信被定义为计算机系统的一个信任属性，该信任放在系统递交的服务上是合理的，指系统在规定时间与环境内交付可信赖的服务的能力。这种能力在不同场合有不同的表现。例如，在办公室文字处理系统中，可信表现为系统能提供服务的时间对全部运行时间的百分比；在

生产过程管理系统中，可信表现为控制系统故障每年引起生产停顿的次数；在事务处理系统中，可信表现为在指定时间内能成功地完成任务的可能性；在电力系统中，可信表现为在一定时间内发生停电事故的次数。

可信赖计算的概念源于美国军方。19 世纪 70 年代，美国政府意识到信息安全关系到国家安全与国家利益，开展了信息安全评测认证的研究，制定了美国计算机系统安全评价系统标准——“彩虹”系列：可信计算机系统评测标准（Trusted Computer System Evaluation Criteria，TCSEC）、可信赖网络诠释（TNI）、可信赖数据库管理系统诠释（TDI）等[7]。近年来，这一标准已扩展到公共管理领域，为了从结构上解决 PC 机的不安全，推行可信计算技术。1999 年由 COMPAQ、HP、IBM、Intel 和 Microsoft 组织了 TCPA（Trusted Computing Platform Alliance），于 2001 年发布了标准规范 V1.1，目的是在计算和通信系统中广泛使用基于硬件安全模块支持的可信赖计算平台，提高整体的安全性。可信赖计算包括以下几方面的含义：用户的身份认证、平台软硬件配置的正确性、应用程序的完整性和合法性。2003 年，TCPA 中的 AMD、HP、IBM、Intel 和 Microsoft 宣布，将 TCPA 更名为 TCG（Trusted Computing Group），继续使用 TCPA 制定的“Trusted Computing Platform Specifications”，并制定符合 Palladium 的 TPM 1.2 技术规范。

高信度计算机是由 Microsoft 创始人比尔·盖茨于 2002 年 1 月发给 Microsoft 公司员工的一封电子邮件中提出的，随后在 Microsoft 内部发行的白皮书中对此概念进行了系统的阐述。Microsoft 的高信度计算的战略目标是增强计算平台的安全性，具体包括安全性（Security）、私密性（Privacy）、可靠性（Reliability）和商业完整性（Business Integrity）。它涵盖了软件的设计、使用、服务和整个产业，一经推出，在 IT 界就产生了广泛的影响，产生了 Microsoft 的 Palladium、IBM 的嵌入式安全子系统（Embedded Security Subsystem，ESS）笔记本电脑、Intel 支持 Palladium 的 LaGrande 技术、Microsoft 的 Vista 等高信度计算机的产品。

国内方面，从 20 世纪 80 年代中期开始，武汉大学、中国科学院软件研究所等高校和科研机构开展了可信计算的研究。武汉大学与武汉瑞达公司合作研制出了国内第一款可信计算机[8]；沈昌祥院士在可信计算的多方面进行了深入研究[9]；林闯教授对可信网络相关技术进行了探索研究，使可信网络的相关属性有了统一

的认识[10]。文献[11]认为："Dependability 应翻译成可信性，它是由容错计算的研究扩充至可信计算的一个综合性概念。"不同的学者从不同的角度和层次对可信性的相关概念和可信计算的发展进行了阐述。文献[12]从可信硬件、软件、系统和网络等方面介绍了可信计算的概念与发展。文献[13]全面总结了可信计算的不同发展阶段，对当前网络环境下可信计算的研究内容进行了分析和点评。文献[14]从密码学、可信计算、网络安全和信息隐藏等方面综述了信息安全技术的研究进展，将可信计算看作解决安全问题的一个新方案。陈火旺院士指出形式化设计方法对保证软件可信性有重要的意义，尽管目前形式化方法对软件开发的支持还不够，但将成为未来的趋势[15]。北京大学梅宏教授在自愈技术的基础上提出了一个通过可信结构和反射中间件来实现自恢复系统的方法，并开发出一个基于反射式 J2EE 应用服务器模型 PKUAS[16]。北京航空航天大学的金茂忠等对基于目标的软件可靠性需求规约方法进行了研究，在非功能需求规约框架基础上，利用 B 抽象机理论，结合面向目标的规约方法，建立了一种可信需求分析方法，为可信性需求模型的定理化证明奠定了基础[17]。熊光泽等基于安全关键领域对软件可信性的可靠性与防危性进行了研究[18]。此外，还出现了一些相关的产品，如联想公司的"恒智"芯片与可信计算机、兆日公司的 TPM 芯片、卫士通公司的终端可信控制系统以及鼎普公司的可信存储系统。

通过上述分析可知，可信计算大致分为两种思路：一种是以 J. C. Laprie 为代表的容错计算思路；另一种是以信任根为基础的信息安全思路。这两种思路的目标是一致的，即希望通过一定的手段，使系统提供可信赖的服务。但是对于不同的应用场合，这两种概念的适应性不同，容错的概念更加适用于分布式系统的描述。变电站自动化系统是典型的分布式系统，因此，本书中的可信计算以 Dependable Computing 为基础，后文将以 Avizienis 提出的概念为基础展开研究。

1.2.2 变电站自动化系统

变电站自动化系统是利用自动控制技术、计算机技术、通信技术和信号处理技术等，对变电站二次设备（包括测量仪器仪表、信号处理系统、继电保护装置、自动控制装置、远动装置）进行功能的重新组合和优化设计，实现对变电站的主

要设备和线路进行自动监视、测量、控制和保护的一种综合性的信息集成自动化系统。变电站二次系统的发展分传统变电站二次系统、独立自动化装置、变电站综合自动化和基于 IEC 61850 标准的变电站自动化系统等几个阶段。其中，独立自动化装置阶段的系统存在功能重叠、数据重复、灵活性差、维修费用高等缺陷，变电站综合自动化应运而生。

在变电站综合自动化兴起的初期，由于各电气设备厂商的变电站自动化系统的应用条件和需求不同，因此系统功能和使用的通信标准也存在差异，如 RS-232、RS-485 等通信协议和 LonWorks、PROFIBUS、CAN 等现场总线标准都被广泛应用。不统一的通信标准使得不同厂商的设备接入同一变电站自动化系统时难度较大，变电站自动化集成和扩展的成本较高。为了改善这种状况，IEC 在《远动设备及系统　第 5 部分　传输规约》（IEC 60870-5）各部分的基础上，于 1997 年发布了《继电保护设备信息接口配套标准》（IEC 60870-5-103），用于变电站自动化系统内部通信，并在世界范围内取得了较为广泛的应用[19]。但是，IEC 60870-5-103 的不足之处在于：标准仅适用于两个具有固定连接通路的设备间的通信，且仅定义了间隔层设备和变电站层设备之间的通信，没有涉及过程层设备之间的通信以及过程层设备与变电站层、间隔层设备的通信；此外，标准在语义和语法定义上有一定的缺陷，使得基于 IEC 60870-5-103 标准的设备虽然可以互联，但需要人工配置才能实现设备的互操作[20, 21]。

因此，IEC 又制定了《变电站通信网络和系统标准》（IEC 61850），其最终目标是实现变电站内不同电气设备厂商的智能电子设备（IED）之间的互操作。IEC 61850 标准把“变电站自动化系统”定义为“在变电站内提供包括通信基础设施在内的自动化”[22-28]。本书研究的对象就是基于 IEC 61850 标准的变电站自动化系统。

基于 IEC 61850 标准的变电站自动化系统正迅速发展，其可靠性、安全性方面的研究引起了诸多学者的关注。文献[29]针对数字化继电保护系统，对不同的冗余方式，使用可靠性框图分析了保护不拒动可靠性，并分析了组成保护系统各元件的重要度；文献[30]评估了 IEC 61850-9-2 用于过程总线后的变电站自动化系统可靠性；文献[31]采用可靠性框图分析方法，对基于 IE C61850 标准的变电站自

动化系统结构的可靠性和可用性进行了评估；文献[32]指出数字化变电站自动化系统可靠性的本质是功能可靠性，采用分布式程序可靠性及分布式系统可靠性相关理论，提出了基于图论和离散时间马尔可夫链的数字化变电站自动化系统可靠性模型。

在变电站自动化系统安全方面，Upeka Premaratne 等[33]对基于 IEC 61850 标准的变电站自动化系统进行了安全分析，提出了一种 IED 的安全度量方法。在文献[34]中，他们还提出了一种基于 IEC 61850 标准的变电站自动化的入侵检测系统，以应对来自外界对变电站 IED 的攻击。段斌等[35]设计了基于可信计算的变电站自动化远程安全通信体系，主要考虑变电站远程控制的安全需求。文献[36]研究了 IEC 61850 标准的安全通信机制以及基于此标准的变电站智能电子设备 IED 的可信设计。Tarlochan S.Sidhu 等[37]利用网络仿真工具 OPNET 对基于 IEC 61850 标准的变电站通信系统进行了仿真评估，为变电站自动化系统的设计提供了一定的参考依据。Hachidaiito 等[38]通过网络设备的冗余来提高变电站自动化系统的可信性，并比较了不同情况下系统的可用性。在电力保护方面，ECT 公司在 1995 年推出了初具可信概念的中高压保护系统产品。美国伊利诺伊大学的 Hassan Khorashadi-Zadeh 和 Zuyi Li[39]、意大利的 Sergio Bruno 等[40]、Luca Ferrarini 等[41]、Vincenzo Fazio 等[42]就可信保护系统和设备的研究作了许多卓有成效的工作。文献[43]对将来的可信家用电器设备展开了研究。在自动化领域，日本的 Yoshiki Kinoshita 等[44]就将来的嵌入式系统的可信标准展开研究；Toshihiro Hanawa 等[45]研究了可信嵌入式系统的通信机制。Andrea Bondavalli 等[46]就分布式系统的可信测量展开研究，推出了相应的工具。

已有文献只是研究了变电站自动化系统的某一方面的属性，不足以描述系统的特征，特别是在智能电网开放的网络环境下，更加需要完全地表述系统的属性。然而，将变电站自动化系统的可信性作为一个整体、全局的概念来考虑，并研究保障系统可信性相关措施的相关研究文献较少。

1.2.3 信息系统可信性分析

随着计算机及相关技术的发展，计算机被广泛地应用于科学研究、经济、文