1.1 国内外研究现状

1.1.1 智能变电站信息安全标准概述

为推进智能变电站发展，规范其建设模式，国内外研究机构和组织制定了一系列相关标准。2004年，国际电工委会（IEC）制定了IEC61850系列标准，该标准基于IEC60870系列标准和UCA标准，同时吸收了很多先进技术，对智能变电站的发展产生了深远的影响。

智能变电站相关研究随着IEC 61850的提出进入高速发展期，随着研究的进一步深入，变电站信息安全问题受到人们的关注。2005年，IEC制定了IEC 62351标准。该标准根据电力系统的特殊要求，运用已经被广泛使用的通信安全机制确保电力行业网络安全。随后，还有定义了变电站IED设备的基本安全要求和特征的IEEE 1686-2007标准，以及在智能变电站信息安全管理和安全性评估方面应用广泛的ISO/IEC 15408标准。

我国尚未发布专门的电力工业信息安全标准，仅在二次系统防护方面，国家电监会发布《电力二次系统安全防护规定》，该规定作为行政令规范了包括智能变电站在内的各电力企业二次系统的安全防护工作。

1.1.2 智能变电站信息安全防护研究现状

目前，国内外在智能变电站工业控制系统上，尚未有完整的安全防护体系研究，主要原因是早些年企业将生产安全问题放在重要位置，而对信息安全问题却并不重视，但随着乌克兰事件等由于工控系统导致的安全事件发生、“震网”病毒等，国内外都开始注重工业控制系统的信息安全，也开始逐渐加大对变电站工业控制系统的信息安全防护力度。

学术界主要从三个方向研究智能变电站的信息安全相关问题：（1）从信息安全管理的角度对智能变电站信息安全进一步研究，旨在在人员管理、设备管理、资产管理等方面制定一系列规范和要求，从宏观上保障智能变电站信息安全[1]；（2）从风险评估的角度研究智能变电站信息安全，旨在建立变电站企业风险评估体系，进而评估其安全等级[2]；（3）从安全防护角度研究智能变电站信息安全，旨在运用各种信息安全技术确保智能变电站信息安全[3]。当前，研究人员越来越把从安全防护的角度来研究智能变电站的信息安全作为主要研究方向。

研究人员普遍认为，由于智能变电站的特殊性，不能将IT网络中应用成熟的信息安全技术简单叠加来解决其网络安全问题。文献[4]全面分析了变电站网络面临的信息安全威胁，并提出了相应的信息安全防护措施；文献[5]对智能变电站安全防护技术进行了深入的研究，其安全防护技术可成功拦截非授权控制命令，可有效抵抗服务拒绝权利、利用型攻击等，具有较高的防护能力；文献[6]研究了面向智能变电站的安全防护技术，提高了变电站内设备的互操作性和互换性，也对变电站的信息可靠性和安全性提出了新的挑战；文献[7]提出了将分布式防护墙技术应用于变电站中，研究了分布式防火墙应用于SCADA系统时的拓扑类型和过滤规则；文献[8]研究了智能变电站网络和报文安全防护、实施安全方案的的报文实时性、智能变电站密匙管理等。

综上，研究人员围绕智能变电站信息安全需求，开展了很多研究，也取得了一定成果，但仍旧有一定的缺陷性，智能变电站综合自动化系统工业信息安全领域还未形成完整的工业安全防护体系，因此还需要进一步的研究。

参考文献：

[1]刘婷. 智能变电站信息安全管理方法研究 2013-06-01

[2]曲朝阳，杨琴，杨杰明等. 基于贝叶斯网络的智能变电站风险关联模型 2016-01-25

[3]刘劼，徐超，徐声龙等. 智能变电站工控系统安全防护技术研究 2017-12

[4]朱学雄. 数字化变电站信息网络安全研究 2011

[5]翟峰，岑炜，赵兵等. 智能变电站系统安全防护技术研究 2015-03-15

[6]赵清林，丁伟. 面向智能变电站的安全防护技术研究 2017-01-25

[7] SS Wu ，CC Liu. Distributed specification-based firewalls for power grid substations 2014

[8]崔秀帅 智能变电站报文安全及其实时性研究