东北石油大学

本科毕业设计（论文）

题　　目：基于 EMS 的 FDIA 电力 CPS 检测系统设计

学生专业：电气工程及其自动化

学生姓名：徐浩洋

指导教师：高新成

辅助教师：

2024 年 5 月 24 日

东北石油大学

毕业设计（论文）任务书

题目　基于 EMS 的 FDIA 电力 CPS 检测系统设计

专业　电气工程及其自动化　学号　200603140111　姓名　徐浩洋

主要内容：

使用 Matlab 对电力系统进行建模，模拟电网在遭受 FDIA 时的行为，以评估攻击对系统的影响。结合卡方算法与卡尔曼滤波器算法，设计一种新的检测算法，并通过 Matlab 仿真验证其在 FDIA 前后的性能。开发数据处理流程，建立数据库以存储和管理电力系统数据，为检测系统提供数据支持。利用 Python 编程语言，结合 Web 技术，开发一个实时监控和检测 FDIA 的在线系统，该系统将集成 EMS 数据，实现对电力系统安全的实时监控。为推动智能电网的发展提高电力系统的韧性和可恢复性提高电力系统的安全性和可靠性提供参考和指导。

基本要求：

1、利用 Matlab 进行电网 FDIA 影响模拟；

2、利用 Matlab 进行利用与检测算法的检测仿真模拟；

3、能完成建立数据库对电力系统数据的处理；

4、建立基于 Python 语言开发的 EMS 系统实现 FDIA 的检测功能；

主要参考资料：

[1] 伊娜,徐建军,陈月等.电力 CPS 多阶段低代价虚假数据注入攻击方法[J].浙江电力,2023,42(11):39-47.

[2] 吴铭辉,高文根,华峰等.基于最大似然估计的智能电网 FDIA 检测[J].四川轻化工大学学报(自然科学版),2023,36(02):38-45.

[3] Huang X ,Qin Z ,Xie M , et al.Defense of Massive False Data Injection Attack via Sparse Attack Points Considering Uncertain Topological Changes[J].Journal of Modern Power Systems and Clean Energy,2022,10(06):1588-1598.

[4] 吴壮.电力信息物理系统中的虚假数据注入攻击检测[D].兰州理工大学,2023.

[5] 杨玉泽,刘文霞,李承泽等.面向电力 SCADA 系统的 FDIA 检测方法综述[J].中国电机工程学报,2023,43(22):8602-8622.

完成期限：2023 年 12 月 11 日——2024 年 6 月 1 日 2024 年 3 月 4 日——2024 年 5 月 24 日

指导教师签名：

专业负责人签名：

2023 年 12 月 11 日

摘 要

在当今工业控制安全领域中，随着信息物理系统（Cyber-Physical Systems，CPS）在电力领域的广泛应用，电力系统的智能化和网络化水平得到了显著提升。然而，这一转型同时也带来了网络安全的新挑战，尤其是面对电网工业控制安全的虚假数据注入攻击（False Data Injection Attack,FDIA）这种攻击方式对电力系统的安全稳定运行与运维构成了严重威胁。工业控制安全是电力系统保护的关键，因为任何网络攻击的成功都可能对整个电力基础设施造成破坏，甚至影响国家安全和社会稳定。为了应对这些挑战，本文设计了基于 EMS 的电力 CPS 检测系统系统，旨在提高电力系统的安全性和可靠性，保障国家关键基础设施的安全。

基于此背景下，本文采用算法仿真模拟与 Web 开发相结合的方法，首先通过 Matlab 对智能电网中的 FDIA 进行了深入分析，揭示了其对电力系统的影响和危害。然后，设计了一种结合卡方算法与卡尔曼滤波器，设计一种新的检测算法，用于实时监测和识别潜在的 FDIA。此外，本文基于此仿真还开发了一套可集成在 EMS 的 Flask 框架的 Web 监控检测系统，实现了电力系统参数的高度可视化和实时监控，增强了跨部门协作的能力。

通过 Matlab 仿真与分析验证了该算法具有可检测 FDIA 的能力并基于此算法编写成可集成在 EMS 当中的检测系统，达成了提高电力系统对 FDIA 的检测能力，降低网络攻击的风险，增强电力系统的韧性和可恢复性，从而确保电力供应的连续性和质量。

关键词：工业控制安全；智能电网；FDIA；EMS

Abstract

In the field of industrial control security today, with the development of Cyber Physical Systems, The widespread application of CPS in the field of power has significantly improved the level of intelligence and networking in the power system. However, this transformation also brings new challenges to network security, especially in the face of false data injection attacks in the control security of the power grid industry, The FDIA attack poses a serious threat to the safe and stable operation and maintenance of the power system. Industrial control security is crucial for the protection of the power system, as any successful cyber attack may cause damage to the entire power infrastructure and even affect national security and social stability. In order to address these challenges, this article designs an EMS based power CPS detection system, aiming to improve the safety and reliability of the power system and ensure the safety of key national infrastructure.

Based on this background, this article adopts a combination of algorithm simulation and web development method. Firstly, an in-depth analysis of FDIA in the smart grid was conducted through Matlab, revealing its impact and harm to the power system. Then, a new detection algorithm was designed that combines the chi square algorithm with the Kalman filter for real-time monitoring and identification of potential FDIA. In addition, based on this simulation, this article also developed a web monitoring and detection system that can be integrated into the Flask framework of EMS, achieving high visualization and real-time monitoring of power system parameters, and enhancing the ability of cross departmental collaboration.

The ability of the algorithm to detect FDIA was verified through Matlab simulation and analysis, and a detection system that can be integrated into EMS was developed based on this algorithm. This improved the detection ability of the power system to FDIA, reduced the risk of network attacks, enhanced the resilience and recoverability of the power system, and ensured the continuity and quality of power supply.

Key words: Industrial Control Security; Smart Grid; FDIA; EMS

目 录

第 1 章　绪论

1.1 选题背景

工业控制安全是电力系统保护的关键之一，因为任何网络攻击的成功都会对整个电力基础设施造成破坏，甚至影响国家安全和社会的稳定性[1]。电力系统作为国家关键基础设施的重要组成部分，其安全性直接关系到国家能源安全和经济社会发展。且随着信息物理系统（Cyber-Physical Systems，CPS）在电力领域的广泛应用，电力系统的智能化和网络化水平得到了显著提升。这种提升带来了电力系统运行效率和智能化水平的提升，但同时也引出了新的安全挑战。特别是虚假数据注入攻击（False Data Injection Attack，FDIA），从 2009 年起作为一种新型网络攻击手段，对电力系统的安全稳定运行构成了严重威胁。FDIA 通过在电力系统的传感器和执行器中注入虚假数据，可能导致错误的决策和操作，从而对电力系统的正常运行造成破坏。因此，面向工业控制安全且针对电力系统检测系统设计，对保障电力系统的安全性和可靠性运行具有重要的实际意义和应用价值。

本文的选题背景基于此类安全网络安全问题的深入分析和理解，旨在通过研究和设计有效的检测系统，能够为电力系统的安全稳定运行提供保障，推动智能电网的健康发展，提高电力系统的韧性和可恢复性。

1.2 研究目的和意义

本研究旨在设计基于 EMS 的针对 FDIA 的电力 CPS 检测系统。通过深入研究 FDIA 危害，将开发针对这类攻击的有效的检测算法机制与 Web 检测系统，能够检测和抵御针对智能电网的 FDIA，并保护电力系统免受潜在的安全威胁。

随着电力系统的数字化转型，主要以信息物理系统的转型，电力系统的安全性面临着前所未有的挑战。虚假数据注入攻击作为一种隐蔽性强的攻击手段，可能导致电力系统受到破坏、故障甚至崩溃。为了应对这一挑战，研究电力 CPS 检测系统显得尤为重要。通过识别和抵御 FDIA，可以提高电力系统的安全性和可靠性，确保提升电网的安全基线及持续的电力供应。同时，通过开发可靠的电力检测系统，可以提高电力系统的韧性和可恢复性，使其在面对 FDIA 时能够及时检测异常数据，并采取相应的防御措施。

此外，本研究还有助于推动智能电网的发展与数字化转型。智能电网是未来

电力系统的发展方向，电力 CPS 作为其重要组成部分，结合了信息通信技术和能源系统，实现了电力系统的智能化监控和管理。其安全性对于智能电网的可持续运行和智能化管理至关重要。然而，智能电网的安全性是实现其可持续发展的关键。通过研究基于 EMS 的电力 CPS 检测系统，可以为智能电网的建设提供技术支持和指导，推动智能电网技术的创新和应用。

综上所述，本文的研究目的和意义在于应对电力系统面临的工业控制安全领域中的 FDIA 挑战，设计并实现一套基于 EMS 的电力 CPS 检测系统，以应对此类攻击。通过研究，期望能够提高电力系统对 FDIA 的检测能力，为电力系统运营商、监管机构和相关研究人员提供重要的参考和指导。希望通过分享研究成果，共同推动电力系统的安全发展，并为保障国家能源安全和社会稳定做出贡献。

1.3 当前研究与应用现状

在现代智能电网的架构中，电力系统的控制与保护系统扮演着至关重要的角色，其通过集成传感器、执行机构、控制中心和通信网络等元素，促进了电力系统的自动化与智能化。然而，随着智能电网的广泛部署，其安全问题也日益凸显，特别是针对虚假数据注入的攻击，这种攻击方式能够恶意篡改系统数据，从而对电力系统的稳定性和安全性构成严重威胁。

工业控制安全主要包括两个方面：物理安全和网络安全。网络攻击者具有破坏甚至拆除电网控制系统的能力已经成为工业控制系统用户和供应商的主要担忧问题之一，近年来发生的安全事故也验证了网络攻击的破坏力[2]。所以基于 EMS（Energy Management System）的针对 FDIA 的电力 CPS 检测系统设计，在智能电网（图 1-1）和工业自动化领域（图 1-2）具有重要的应用价值。以下是该系统在两个领域的具体使用场景：

在智能电网中，目前调控中心已具备检测大多数不良数据的能力[3]，基于 EMS 的 FDIA 检测系统的主要使用场景包括：

（1）数据监测：系统实时监测电网中的数据，确保数据的准确性和真实性。

（2）异常检测：通过分析监测到的数据，系统可以实时发现异常情况，如电压异常、电流异常等，疑似 FDIA。

（3）防御措施：当系统检测到 FDIA 时，立即采取防御措施，如隔离受攻击的设备、停止攻击数据传输等，确保电网的安全和稳定运行。

（4）攻击溯源：系统可以对攻击数据进行溯源，找出攻击源头，为后续的网络安全防护提供支持。

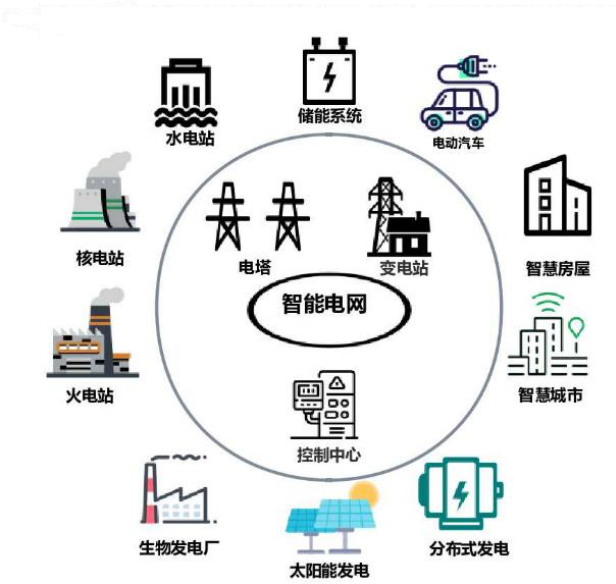

图 1-1 电力系统中智能电网的使用环境

同时，在工业中电气自动化的生产领域，工业控制系统一般采用网络边界防护手段来保护自身安全。然而，防护设备在开发过程中难以避免产生漏洞，加之工业大规模长期部署造成的相似性和静态性特点决定其难以收敛防御增益，也难以量化攻击行为恶意程度，从而难以应对未知的 APT（Advanced Persistent Threat）威胁[4]。故基于 EMS 的 FDIA 检测系统的主要使用场景涵盖：

（1）生产过程的全方位参数监控：系统可实时监测工业生产过程中的关键参数，确保生产过程的正常运行。

（2）基于数据的异常分析：通过分析监测到的异常数据，相关工作人员可以依据此系统实时发现生产过程中的设备异常运行、生产异常参数异常等情况，并由此推测是否疑似 FDIA。

（3）防御策略：当系统检测到 FDIA 时，相关工作人员立即排查并采取防御策略，如中止异常设备运行、调整生产参数等，确保生产过程的安全和稳定。

（4）溯源与告警：系统可以对异常的数据进行排查并溯源，找出攻击源头，并发出告警，为后续的能源网络安全防护和生产管理提供有力支持。

综上所述，基于 EMS 的针对 FDIA 的电力 CPS 检测系统在智能电网和工业自动化领域具有广泛的应用。通过实时监测、异常检测、防御措施和攻击溯源等功能，该系统可以有效保护电力 CPS 免受 FDIA，确保系统的安全、稳定运行。

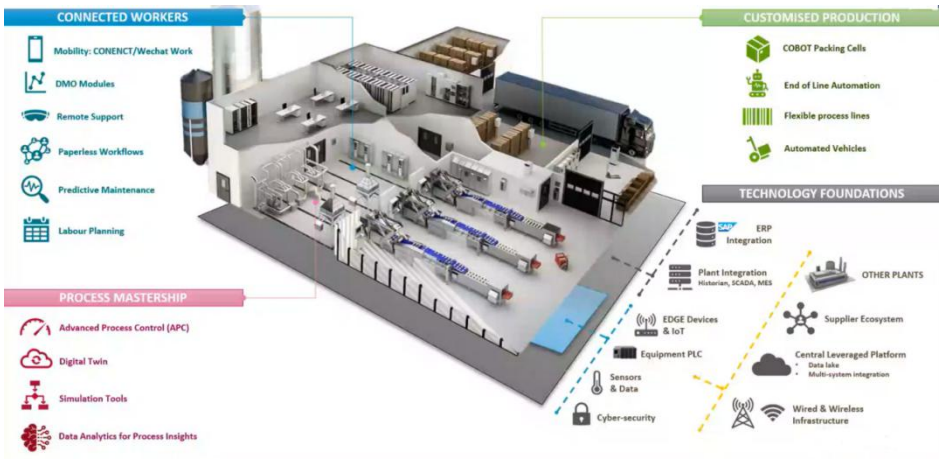

图 1-2 工业中电气工程自动化的数字化使用环境

同时，近年来，许多专家开始关注电力系统网络安全威胁，特别是针对虚假数据注入攻击。这些攻击可能影响电力市场[5]、电力系统的稳定运行，以及分布式能源的有效分配。例如，在经济层面，攻击可能导致市场状态估计错误，引发财务问题。有研究提出了一种分析攻击效果及其经济影响的方法。在电网运行方面，研究表明，通过在测量单元中注入虚假数据，可能导致电网负荷分配不均，严重威胁系统稳定性。此外，针对能源路由的攻击，可能会通过注入伪造的能源信息或链路状态信息，造成电力供需失衡，扰乱能源分配。然而，这些研究通常将网络攻击和防御视为静态过程，忽略了攻击者与防御者之间的动态互动[6]。

为了应对这一挑战，研究人员致力于开发基于电力 CPS 的检测系统，特别是在能量管理系统框架下的检测策略。EMS 是智能电网中的核心组件，主要负责监控和控制电网的运行状态，因此，将检测机制集成到 EMS 中显得尤为重要。

在 FDIA 检测技术方面，目前已有多种方法被提出并得到了研究。以为伪造测量数据进行状态估计（SE），故利用状态估计法是传统的检测手段[7]，通过对电力系统状态进行实时估计，并与实际测量值对比，来识别潜在的异常和攻击行为。数据完整性和一致性检查法则侧重于验证传感器数据的准确性和可靠性，以此来判定系统是否遭受了 FDIA。

与此同时，基于机器学习和人工智能的检测方法受到了广泛关注。这些方法通过训练模型[8]识别正常数据与异常数据之间的细微差别，从而实现对 FDIA 的有效识别。例如，支持向量机（SVM）[9]、神经网络（NN）[10]、最大似然估估计[11]、深度学习[12]等算法已被成功应用于攻击检测领域。

在检测策略方面，研究人员正在探索多种机制以处理检测到的 FDIA。动态控制策略能够根据电网的实时状态调整控制参数，以抵御攻击。自适应参数调整则能够根据电网特性和工作环境自动优化参数设置，例如调整 PMU 测量中的假数据[13]。此外，开发安全的通信协议和认证机制也是提升防御能力的关键。

协同 EMS 与 CPS 之间的互动也是研究的重点之一。有效的协同机制可以显著增强电力 CPS 的检测能力，例如，通过数据交互，信息共享实现更精确的攻

击识别和响应。

许多学者还关注了 FDIA 的经济影响，这些攻击可能导致电力市场的操纵和不正当的财务行为。因此，研究电力市场中的 FDIA 行为及其对市场运行的影响具有重要意义。

总而言之，尽管在基于 EMS 的针对 FDIA 的电力 CPS 检测系统设计方面已经取得了显著进展，但仍然需要更多的研究来进一步强化电力 CPS 的安全防护能力，确保电网的高效、安全和可靠运行。随着技术的不断进步和研究的深入，期待能够开发出更加先进有效的检测策略，以应对日益复杂的网络安全挑战。

1.4 论文组织结构

本文共分为五个章节，旨在对智能电网的检测系统进行深入研究，本文的论文架构如图 1-3 所示。

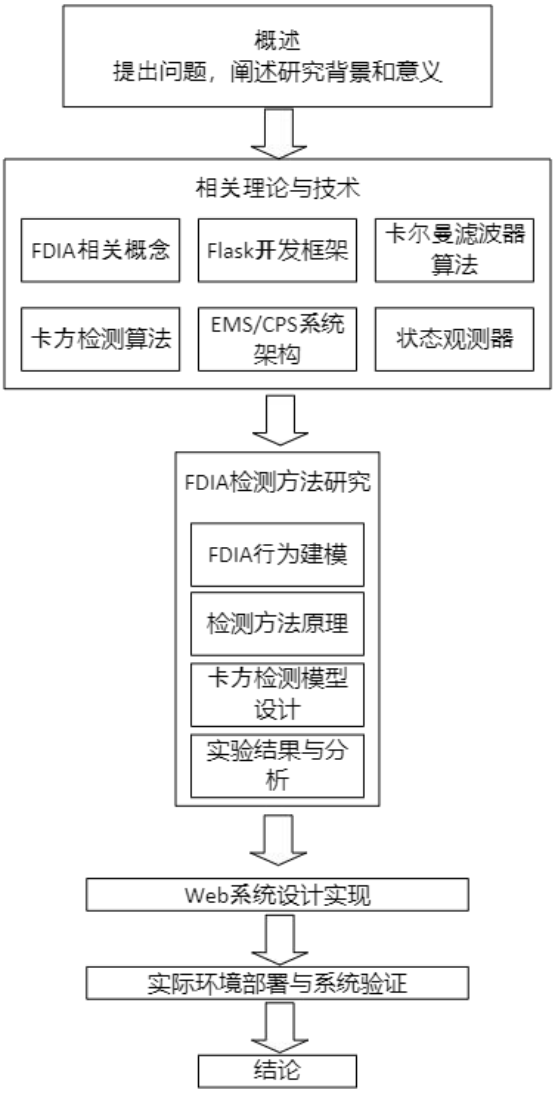

图 1-3 该论文架构

第一章以工业控制安全为背景，探讨了智能电网的检测态势感知，明确了研究目的和研究意义，并对当前国家基础设施智能电网的防御研究现状进行了梳理。

第二章着重阐述了本设计所需的理论基础与技术，为后续的研究与检测系统的搭建奠定了技术基础。第三章则开始对虚假数据注入攻击进行建模，深入探讨了其对智能电网所造成的危害。同时，本章还研究了检测算法，并进行了模型设计与实验分析。第四章从电网中工业控制安全的需求出发，设计了功能点与数据库，并逐步实现了这些功能点。第五章则开始进行系统测试与分析，包括功能点测试、性能测试、安全测试以及兼容性测试。

通过以上章节的论述，旨在为智能电网的 FDIA 检测提供一种有效的检测算法与检测系统，为我国智能电网的安全运行提供有力的保障。

第 2 章　基于 EMS 的 FDIA 电力 CPS 检测系统技术课题研究及其技术基础

2.1 FDIA 相关概念

2.1.1 FDIA 原理

虚假数据注入攻击是一类针对由网络物理信息系统控制的关键基础设施的恶意数据攻击。

FDIA 的最终目的是攻击者篡改传感器读数，以便在计算用于定义系统状态的值和变量时，包含未被检测到的损坏数据。

其传感器成为 FDIA 的关键攻击向量，如图 2-1。虚假数据注入攻击策略利用无线物联网设备通信网络的漏洞来操纵传感器数据。通过操纵传感器数据和计算，攻击者可以误导电力分配网络和控制中心。

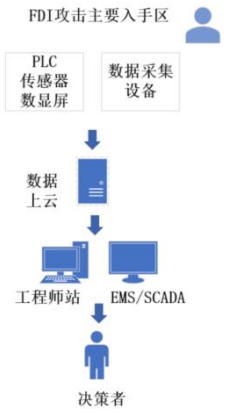

图 2-1 FDIA 原理图

在智能电网中，仪表数据由数据收集设备获取，并通过网络发送至监控与数据采集系统（SCADA）。SCADA 系统随后将这些数据转发至能量管理系统，后者对数据进行分析，以评估系统状态和识别异常。基于这些分析结果，控制中心执行诸如最优潮流分布和故障诊断等操作，并根据系统状况制定决策。最后，SCADA 系统将决策信息回传至数据收集设备，以完成指令循环。

针对状态评估的攻击方法主要包括三种：修改测量数据[14]、攻击 SCADA 系统以及侵入数据收集设备和 SCADA 系统之间的网络，图 2-2 所示。这些攻击手段均可能导致 EMS 做出错误的决策[15]。

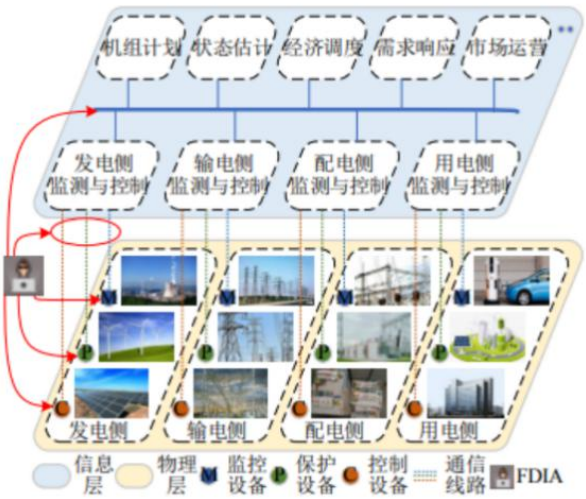

图 2-2 FDIA 在电力 SCADA 系统中的传播路径

以下是一个最为经典且成功发起的 FDIA 网络攻击的例子[16]：2015 年 12 月乌克兰大停电事件，这是公开承认的针对电力系统自动化软件的首次网络攻击之一。攻击者通过篡改或注入虚假的数据，干扰了电力系统的运行，断开了 30 个变电站的连接长达三个小时。

2.1.2 FDIA 数学模型

电力系统通常基于拓扑结构和线路参数等静态数据以及实时量测数据进行建模。系统量测方程常用交流潮流模型表示[17]：

$$z_a = h(x) + e \tag{2-1}$$

式中：$z \in R_m$为系统测量向量，包括母线电压、母线有功功率和无功功率注入，以及支路有功潮流和 无功潮流等；$x \in R_n$为系统状态变量，如节点电压复相量；$h(\cdot) \in R_m$为刻画了测量值与系统状态之间的非线性映射，通常取决于系统参数和拓扑结构；e 为均值为 0，方差为$\sigma^2 \in R_m$的量测误差向量；系统量测通常具有一定冗余度，即 $m > n$。由于高压输电网中母线电压在额定电压附近且支路电阻远小于电抗，为了简化计算、保证收敛性，系统量测方程通常采用线性化的直流潮流模型：

$$z = Hx + e \tag{2-2}$$

式中 $H \in R_{m\times n}$为线性化的量测雅可比矩阵。

攻击者构造的攻击向量有效，其电力系统数学模型可以表示为：

$$z_a = h(x) + e + a \tag{2-3}$$

其中：z_a表示被 FDIA 注入攻击向量后的测量向量，且 a 服从均值为μ_a、协方差为Σ_a的高斯分布模型。若能量管理系统使用z_a进行状态估计得出错误状态变量$\hat{x}_{bad}$，其与攻击前的状态变量$\hat{x}$的关系可以表示为：

$$\hat{x}_{bad} = \hat{x} + c \tag{2-4}$$

2.2 EMS 与 CPS 系统架构

能量管理系统是现代电力系统运行的核心（图 2-3），它通过集成先进的控制、通信、计算和人工智能技术，实现对电力系统的实时监控、分析和优化。EMS 的主要功能为数据采集与监控：EMS 首先需要收集来自电力系统各种测量设备和控制装置的实时数据，监控中心通过这些数据对电力系统的运行状态进行实时监控，确保系统的稳定性和安全性。

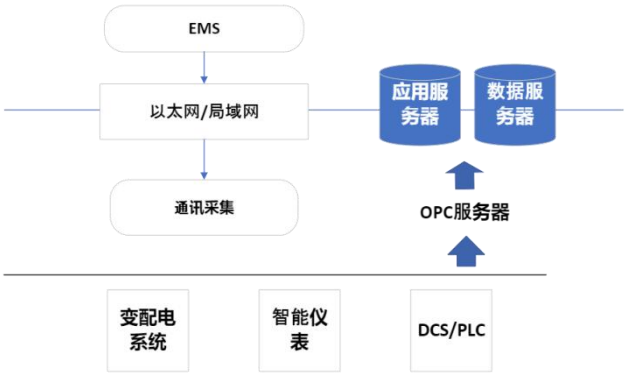

图 2-3 EMS 原理图

CPS 如图 2-4，是一种融合了物理系统和计算机科学的系统，由四个主要组成部分构成：物理实体、计算单元、通信网络和软件系统。物理实体是 CPS 中的物理设备，如传感器、执行器、机器等。计算单元负责处理和分析物理实体收集的数据，并生成控制信号。通信网络负责连接物理实体和计算单元，实现数据传输和控制指令的传递。软件系统则负责管理 CPS 的运行，包括数据采集、处理、存储、通信和控制等功能。

它在智能电网、工业自动化、医疗保健等领域具有广泛的应用。CPS 的主要特点是将虚拟的数字世界与现实的物理世界紧密结合，通过计算机系统对物理设备进行实时监控、控制和优化。

在 CPS 中，计算单元和软件系统的作用至关重要。计算单元负责对物理实体收集的数据进行实时处理和分析，包括数据清洗、特征提取、建模等。通过计算单元的处理，CPS 可以实现对物理实体的精确控制。软件系统则负责管理 CPS 的整体运行，包括初始化、配置、监控、故障检测和恢复等。此外，软件系统还负责与外部系统进行数据交换和协同工作。

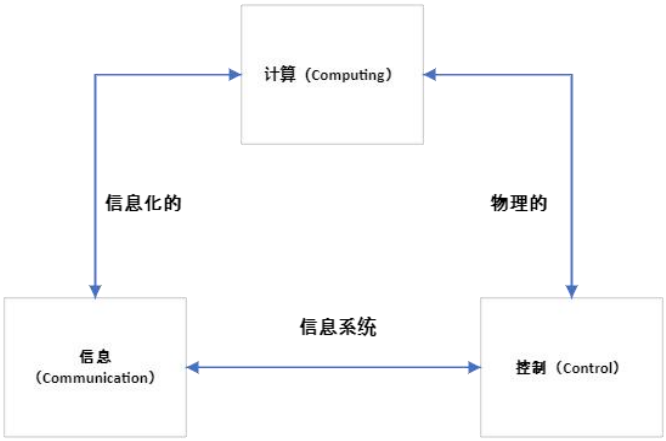

图 2-4 CPS 原理图

CPS 在智能电网[18]中（图 2-5）的应用主要体现在以下几个方面：首先，CPS 可以实现对电力系统的实时监控和控制，提高电力系统的安全性和可靠性。通过在电力系统中安装众多传感器和执行器，CPS 能够实时监测电压、电流、功率和温度等多种数据，并基于这些数据生成控制指令，以实现对电力系统的精细化管理。此外，CPS 还能提升电力系统的能源效率和经济效益。通过对系统的持续监控和分析，CPS 能够发现能源消耗的异常情况以及潜在的故障风险，并制定优化策略，确保能源的合理分配与调度。CPS 还支持电力市场的运作，通过实时收集和分析市场数据，如电价和交易量，为电力市场提供决策支持，推动市场的公平、透明和高效运营。

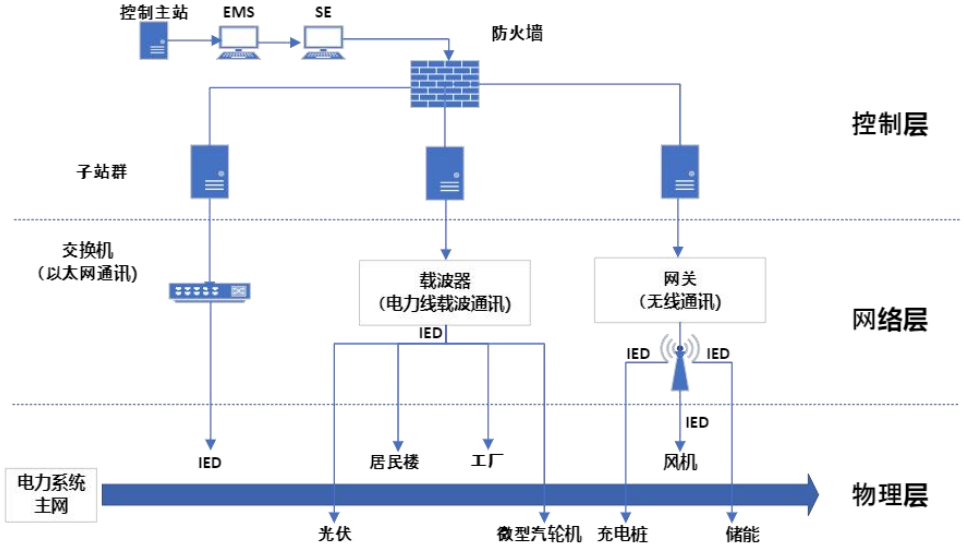

图 2-5 电网信息物理系统结构

EMS 与 CPS 之间存在着密切的联系（图 2-6）。EMS 作为电力系统运行管理的核心，负责实时监控、分析和优化电力系统的运行。而 CPS 作为一种将物理世界与数字世界结合的系统，通过计算机系统对物理设备进行实时监控、控制

和优化。在电力系统中，CPS 的物理实体、计算单元、通信网络和软件系统与 EMS 的各个功能模块相互配合，共同实现电力系统的智能化管理和优化。

具体来说，CPS 的传感器和执行器可以作为 EMS 的数据采集和控制执行单元，实时收集电力系统的运行数据，并执行 EMS 生成的控制指令。CPS 的计算单元和软件系统可以作为 EMS 的数据处理和分析平台，对收集到的数据进行实时处理和分析，为 EMS 提供决策支持。此外，CPS 的网络通信技术可以实现 EMS 与外部系统之间的数据交换和协同工作。

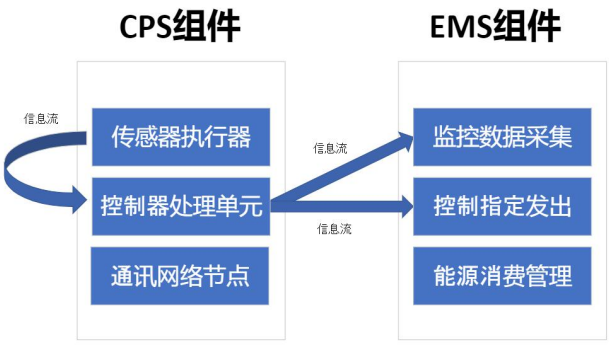

图 2-6 本文中 EMS 与 CPS 的关系

综上所述，CPS 与 EMS 之间的融合为电力系统的实时监控、控制和优化提供了强大的技术支持。通过将 CPS 的技术优势与 EMS 的管理功能相结合，可以进一步提高电力系统的安全性和可靠性，提高能源利用效率和经济效益，推动电力系统向智能化和自动化方向发展。

2.3 卡方检测算法

卡方检测是一种统计方法[19]，用于检验两个变量是否独立。其基本原理是，通过计算观察频数与期望频数的差的平方，除以期望频数的平方，然后将这些值求和，看其是否显著大于随机产生的值。如果计算出的卡方统计量显著大于在给定的自由度和显著性水平下的临界值，则认为两个变量不独立，反之则认为它们独立。

数学模型可以表示为：

$$x^2 = \sum \frac{(O-E)^2}{E} \tag{2-5}$$

O 表示观察频数，即实际数据中某个组合出现的次数。E 表示期望频数，即在假设两个变量独立的条件下，某个组合出现的次数的预期值。

期望频数通常是根据独立性假设计算得出的，对于每个可能的变量组合，期望频数通常是每个变量独立概率的乘积。

自由度是卡方检验中的一个重要参数，它与样本量和检验的类型有关。自由

度的计算公式通常是

$$(\text{行数}-1)\times(\text{列数}-1) \tag{2-6}$$

其中行数和列数分别对应于检验中的两个变量水平的数量，卡方检验的结果通常根据自由度和显著性水平通过卡方分布来解释。

2.4 状态观测器

在电气工程和控制理论中，状态观测器是一种用于估计系统状态的装置（图2-7），特别是在动态系统中。状态观测器的目的是通过系统的输出（通常是可测量的变量）来估计系统的内部状态，即使这些内部状态无法直接测量。状态观测器在自动控制、故障检测和系统监控等领域有着广泛的应用。

状态观测器的核心思想是构建一个动态系统，其输入是原始系统的输出和一些外部设计的输入，其输出则是估计的状态。通过设计这个动态系统，使其能够尽可能准确地跟踪原始系统的状态变化。

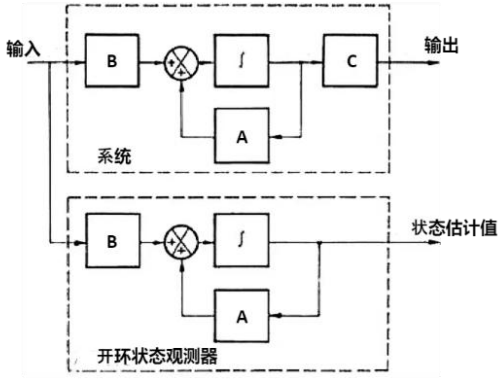

图 2-7 状态观测器方框图

状态观测器通常可以通过状态空间方程来描述。对于一个线性时不变系统，状态空间方程可以表示为：

$$\dot{X}(t) = Ax(t) + Bu(t) \tag{2-7}$$

$$\mathrm{y(t)} = \mathrm{Cx(t)} + \mathrm{Du(t)} \tag{2-8}$$

$x(t)$是系统的状态向量；$u(t)$是系统的输入向量；$y(t)$是系统的输出向量；A是系统的状态矩阵；B是系统的输入矩阵；C是系统的输出矩阵；D是系统的直接传递矩阵。

状态观测器的设计目标是找到一个观察器系统，其状态估计$\hat{x}(t)$能够准确地跟踪实际状态$x(t)$。观察器系统的状态空间方程可以表示为：

$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + \hat{B}y(t) \tag{2-9}$$

$$\hat{y}(t) = \hat{C}\hat{x}(t) \tag{2-10}$$

$\hat{A}$是观察器的状态矩阵；$\hat{B}$是观察器的输入矩阵；$\hat{C}$是观察器的输出矩阵；$\hat{y}(t)$

是观察器的输出向量，它应该尽可能地接近系统的真实输出 $y(t)$。

为了使观察器能够准确地估计状态，需要满足一定的条件，例如观察器方程应该具有完全可观测性。这意味着，通过观察器的输出$\hat{y}(t)$和足够多的初始状态估计$\hat{x}(0)$，可以唯一确定系统的状态 $x(t)$。

2.5 卡尔曼滤波器算法

卡尔曼滤波器是一种特殊类型的状态观测器，也是一种优化估计算法且用于估计系统状态的数学方法，它通过融合传感器测量值和系统模型，提供对系统当前状态的最优估计。

在本文仿真当中，卡尔曼滤波器可以在电力系统中使用。电力系统通常是由多个组件（例如发电机、变压器、线路等）组成的复杂动态系统。卡尔曼滤波器可以对电力系统状态进行估计和预测，从而实现对系统的监控、诊断和控制。在电力系统中，卡尔曼滤波器的应用于状态估计，例如卡尔曼滤波器可以通过观测到的系统输出（如电流、电压、功率等）和先验知识（如系统的动态方程）来估计系统的当前状态。这可以用于实时监测电力系统的状态，包括估计节点电压、电流、发电机转速等重要参数。还包含动态预测，例如卡尔曼滤波器可以通过系统的动态方程和先前的状态估计来预测电力系统未来的状态。这可以用于短期负荷预测、电力市场价格预测等应用。

如图 2-8 所示，在建立卡尔曼滤波处理过程的同时，也要获取数据，通过流程图可知，包括输入量、过程噪声两个输入量，输入量产生系统噪声，过程噪声设立状态参数并结合系统噪声最终传输到测量参数。这个过程会产生延时反馈给状态参数，最后得到预估值[20]。

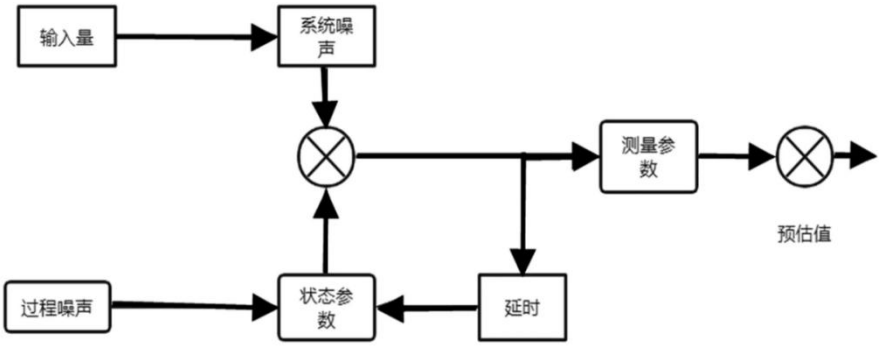

图 2-8 卡尔曼滤波器框图

卡尔曼滤波器是一种最优估计算法，它通过递归方式对系统状态进行估计。它利用系统的动态模型和观测数据，以最小化状态估计的误差协方差。卡尔曼滤波器适用于线性高斯系统，其中系统的状态转移和观测都是线性的，并且噪声都是高斯白噪声。

高斯白噪声就是指那些同时具有正态分布特征且各时间点上的值相互独立的随机变量序列。

卡尔曼滤波器的数学模型中，假设有一个线性动态系统，其状态 x 随时间变化遵循以下模型：

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{2-11}$$

x_{k+1}是下一时刻的状态。x_k是当前时刻的状态。A 是系统矩阵，描述了状态转移的动态。B 是控制矩阵，描述了控制输入u_k对状态的影响。u_k是控制输入。w_k是系统噪声，假设它是一个零均值的高斯白噪声，其协方差为Q_k。

同时，系统状态可以通过观测矩阵 H 观测到，观测模型如下：

$$z_k = Hx_k + v_k \tag{2-12}$$

z_k是观测到的数据。v_k是观测噪声，也是一个零均值的高斯白噪声，其协方差为R_k。卡尔曼滤波器算法如下：

（1）初始化：设定初始状态估计$\hat{x}_0$和状态估计误差协方差P_0。

（2）预测：计算下一状态的预测$\hat{x}_{k+1|k}$：

$$\hat{x}_{k+1|k} = Axk + Buk \tag{2-13}$$

计算预测误差协方差$P_{k+1|k}$：

$$P_{k+1|k} = AP_kAT^+Q_k \tag{2-14}$$

（3）更新：

计算卡尔曼增益 K_k：

$$K_k = P_{k+1|k}H^T\left(HP_{k+1|k}H^T + R^k\right)^{-1} \tag{2-15}$$

更新状态估计$\hat{x}_{1|1}$和误差协方差$P_{1|1}$：

$$\hat{x}_{1|1} = \hat{x}_{1|0} + K_1(z_1 - H\hat{x}_{1|0}) \tag{2-16}$$

卡尔曼滤波器能够在存在噪声的情况下，从一系列的不完全且包含随机噪声的测量中，估计动态系统的状态。

2.6 Flask 开发框架

本论文选用 Python 是因为它被广泛应用于电力系统领域且具有很多优势。在电网领域，Python 可以帮助开发人员快速构建复杂的电力系统模型、数据处理和分析工具，以及优化算法等。结合 Flask 这样的 Web 框架，开发人员可以轻松地构建基于 Python 的 Web 应用程序，用于电力系统监控[21]、管理以及数据可视化展示。Flask 提供了简洁而灵活的方式来创建 Web 应用程序，使得开发人员能够快速搭建起一个功能完善的电力系统管理平台，实现对电网数据的实时监测和追踪，并提供直观的数据分析和可视化展示。通过将 Python 和 Flask 结合运用在电力系统开发中，不仅能够提高开发效率和灵活性，还能够为电力系统领域带来更多创新和便利。

Flask 是一个基于 Python 的轻量级 Web 开发框架，以其简洁的 API 和灵活的

扩展机制而著称。在本文中，选择 Flask 作为 Web 监控检测系统的开发框架，主要是因为它能够满足对系统架构、数据处理、攻击检测以及系统拓展等方面的需求。

Flask 框架的设计理念是“简洁而强大”，这使得它非常适合快速开发和迭代 Web 应用程序。其核心组件包括：

（1）WSGI 工具：提供了一种轻量级的 Web 服务接口，可以轻松地与 Web 服务器和框架集成。

（2）Jinja2 模板引擎：提供了一种动态模板生成机制，使得前端页面的设计更加灵活和高效。

（3）URL 路由器：能够根据 URL 自动匹配对应的视图函数，实现请求到响应的映射。

（4）扩展系统：Flask 提供了丰富的扩展，包括数据库集成、表单处理、验证器、测试框架等，可以方便地扩展 Flask 的功能。

本文的系统平台前端主要通过 HTML、CSS 和 JavaScript 等实现网页的设计和交互效果，后端则使用 Flask 框架搭建 Web 服务，处理来自前端的请求并将数据通过查询 MySQL 数据库进行读取。下面对该系统平台进行总体概述：系统的前端部分主要由 HTML、CSS 和 JavaScript 等组件组成，使用这些技术实现网页的设计和交互逻辑。系统的后端部分主要使用 Flask 框架搭建 Web 网络服务，处理来自前端的请求并与数据库进行交互。Flask 框架可以快速生成响应请求的程序，提供给编程者非常简便的数据库交互方式，并支持丰富扩展以便实现各种功能，Flask 系统架构图如图 2-9 所示。

图 2-9 Flask 系统架构图

Flask 框架在本文的研究中发挥了重要作用，帮助实现了基于 Python 的 Web 监控检测系统，提高了电力系统的安全性和可靠性。

2.7 Power BI 数字化平台

在实现高度可视化和数据的可操作性的选择上利用 PowerBI（Business Intelligence）商业分析工具构建数字化共享平台。首先，Power BI 提供了丰富的可视化选项，包括各种图表和仪表板，这些可视化元素能够生动地展示数据，使复杂的统计信息变得直观易懂。这种多样性使得 Power BI 能够适应不同的数据分析需求，同时 Power BI 强大的数据集成和处理能力，能够处理来自多种数据

源的大量数据。通过数据模型和透视表等功能，用户可以轻松地对数据进行清洗、转换和整合，确保了可视化结果的准确性和可靠性。最后，Power BI 注重数据的安全性，提供了多种身份验证方法和权限管理，确保只有授权用户才能访问敏感数据。这对于需要遵守严格数据保护法规的企业来说至关重要。Power BI 在数据可视化方面的优势在于其丰富的可视化选项、高度的可自定义性、交互性、数据集成和处理能力、智能化推荐、云端协作以及强大的安全性，提高了工作效率，同时挖掘数据背后的规律和趋势直观指导生产管理提升生产管理效能，这些特点使得 Power BI 成为数据分析和智能报表的可视化实现的理想选择[22]。

2.8 MySQL 数据库

在选择数据源的处理上，选择了 MySQL 数据库，其优势显而易见。首先，MySQL 具备强大的实时数据处理能力，能够有效地监控、存储和更新大规模的实时数据，满足电网系统对即时性的严格要求。其次，作为一个经过长期验证的稳定数据库系统，MySQL 保证了电网数据的可靠性和安全性，符合电网作为国家重要基础设施的特殊需求。此外，MySQL 具有良好的扩展性和性能优化能力，能够轻松处理电网系统庞大数据量和复杂查询需求，确保系统运行的高效性和稳定性。同时，MySQL 与各种编程语言和应用程序兼容性良好，便于与电网系统中的其他软件和硬件集成，实现数据的共享和交互，提升系统整体效率。综上所述，MySQL 数据库在电网领域展现出了强大的数据管理和处理能力，为电网系统的高效运行和管理提供了可靠支持。

第 3 章　FDIA 检测算法设计与仿真

3.1 电网仿真模型设计

为了设计与验证检测算法的可用性，首先是对该攻击模型的仿真模拟。图 3-1 为系统 Matlab 建模，进行了虚假数据注入攻击的模拟情况。当攻击在执行器与传感器中进行时，系统会出现不稳定的错误状态。

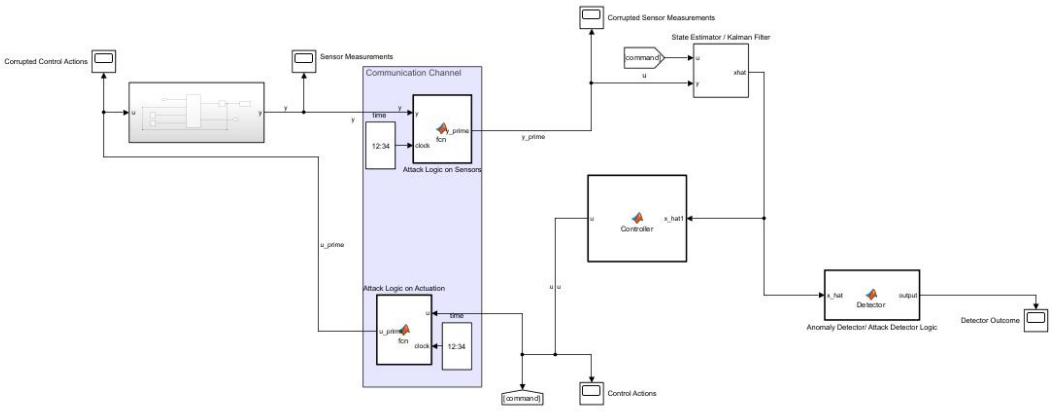

图 3-1 对 FDIA 建模

3.1.1 状态观测器设计

图 3-2 实现了一个电力系统状态观测器。实现了一个电力系统状态观测器，它通过线性状态空间方程来估计系统的当前状态和输出，即使这些状态无法通过直接测量。

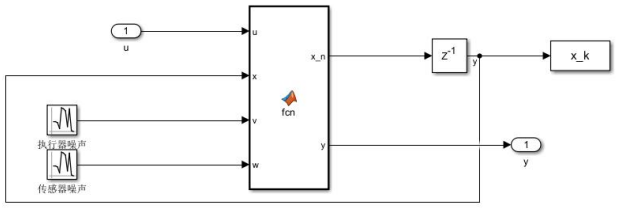

图 3-2 电力系统的状态观测器

通过定义系统矩阵：代码中定义了四个矩阵 A、B、C 和 D，这些矩阵描述

了电力系统的动态行为。矩阵 A 是状态矩阵，B 是输入矩阵，C 是输出矩阵，D 是直接传递矩阵。

接下计算下一个状态：使用线性状态空间方程计算下一个状态x_{n}。这个计算是当前状态 x、输入 u 和控制噪声 v 的线性组合，公式为

$$\mathrm{x_n} = \mathrm{Ax} + \mathrm{Bu} + \mathrm{v} \tag{3-1}$$

然后计算输出：使用线性状态空间方程计算输出 y。这个计算是当前状态 x、输入 u 和测量噪声 w 的线性组合，公式为

$$\mathrm{y} = \mathrm{Cx} + \mathrm{Du} + \mathrm{w} \tag{3-2}$$

最后返回结果：函数返回计算得到的下一个状态x_n和输出 y。

外部参数 u 作为初始值输入，执行器噪声与传感器噪声这两个同样维度的高斯噪声向量作为噪声输入，同至一个模拟不可直接被测量的离散时间系统的状态空间模型与状态方程矩阵，输出的是描述状态变量随时间如何发展，给出了每个时刻下一个状态的值。同时根据外部输入可以使用这个方程递归地计算出状态序列，同时也存在负反馈控制，保证误差的消除。

3.1.2 执行器设计

本节实现了一个 Matlab 函数 fcn，该函数模拟了攻击者在执行通道上进行虚假数据插入攻击时的控制输入修改行为，图 3-3。该函数接受原始控制输入 u 和时间变量 $clock$ 作为输入参数，并计算修改后的控制输入u_{prime}。

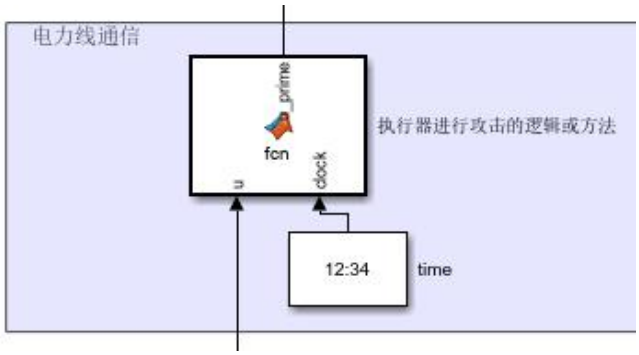

图 3-3 执行器受攻击的模块

首先，根据时间变量 $clock$ 的值，函数确定是否执行攻击以及如何修改控制输入。如果 $clock$ 的值在 0 到 40 之间（不包括 40），则不执行攻击，控制输入保持不变，即$u_{\mathrm{a}} = [0, 0]$。如果 $clock$ 的值在 40 到 50 之间（不包括 50），则执行虚假数据插入攻击，通过将$[-0.18, -0.18]$加到原始控制输入 u 上来模拟攻击。对于任何其他 clock 值，不执行攻击，控制输入同样保持不变，即$u_{\mathrm{a}} = [0, 0]$。

最后，函数通过将攻击者操作u_{a}加到原始控制输入 u 上计算修改后的控制输入u_{prime}，即$u_{\mathrm{prime}} = u + u_{\mathrm{a}}$。

3.1.3 传感器设计

用于传感器的 FDIA 场景与执行器类似，如图 3-4。

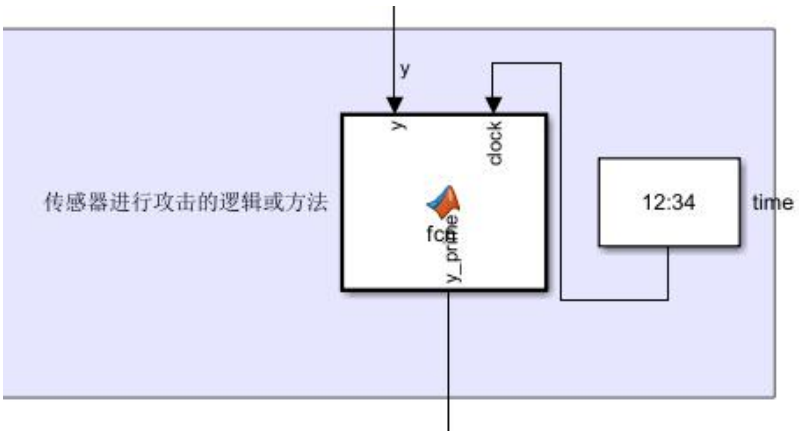

图 3-4 传感器模块

函数需要根据不同的攻击策略来修改y_{prime}的值，以模拟传感器被篡改后的输出。在此仿真模型中执行器在控制命令的虚假数据函数与传感器相同，故用于模拟传感器遭受攻击的场景。

3.1.4 无检测算法下的检测设计

在模拟攻击时，仅构建了检测框架（见图 3-5），并未包含具体的检测算法。

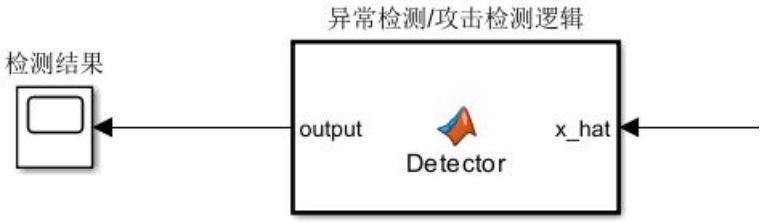

图 3-5 检测框架

图 3-6 没有加入检测逻辑所以检测结果为 0。

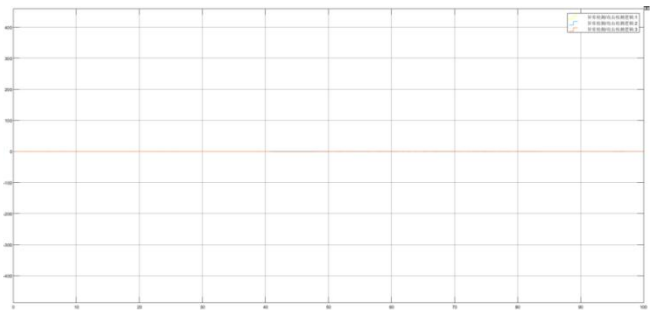

图 3-6 检测结果

3.2 电网遭受 FDIA 分析

在虚假数据注入攻击中[23]，输入信号 $u(t)$被加上一个误差信号变成$u^{'}(t)$，其中误差信号是一个与时间有关的函数，表示为$u^{a}(t)$。因此，受损指令$u^{'}(t)$可以通过原始指令 $u(t)$和误差信号$u^{a}(t)$的加法得到，即公式：

$$u^{'}(t) = u(t) + u^{a}(t) \tag{3-3}$$

其中，$u^{a}(t)$是虚假数据注入攻击生成的误差信号，它可以在实际控制系统中对输入信号进行扰动，使得控制系统行为发生改变。这种攻击可以通过恶意攻击者向控制系统中注入虚假数据来实现，从而导致控制系统失效或者误操作。这个公式就是表示当控制系统受到了虚假数据注入攻击时，输入信号会被加上一个误差信号，从而导致控制系统行为发生改变。这个误差信号可以通过恶意攻击者向控制系统中注入虚假数据来实现，从而使控制系统不再按照正常指令进行操作。

在系统信道中增加 FDIA 时，系统表现出特定的时间行为，即公式：

$$u^{a}(t) = \begin{cases} 0, & 0 \le t < 40 \\ [-0.18, -0.18]^{T}, & 40 \le t < 50 \\ 0, & t \ge 50 \end{cases} \tag{3-4}$$

通过这种方式，可以在执行器通道上模拟虚假数据插入攻击，并研究其对电力系统的影响，如图 3-7。

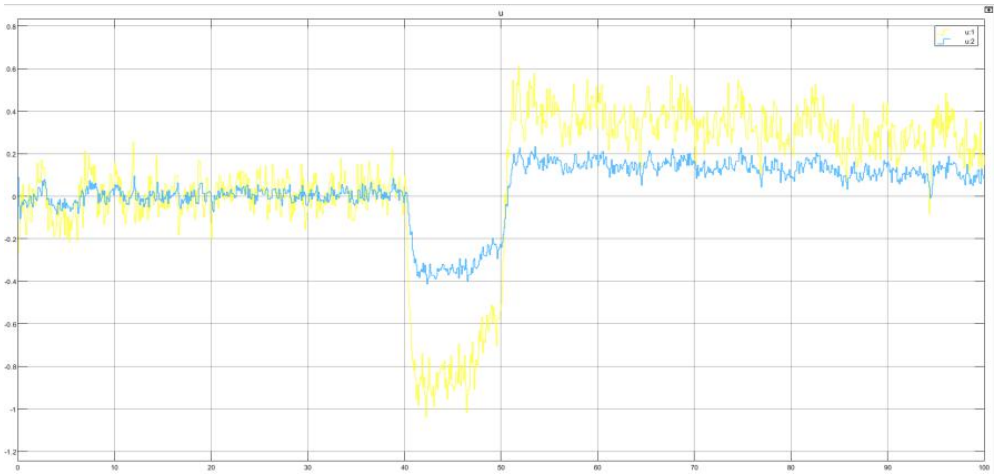

图 3-7 受到干扰的控制状态

从图中可以看出，控制状态以数据呈现，且在攻击时间部分，数值出现了显著的下降，之后又有所回升。

同时，从图 3-8 中可以看出，传感器被攻击数据在攻击时间部分，数值出现了显著的上升，之后又有所回降。

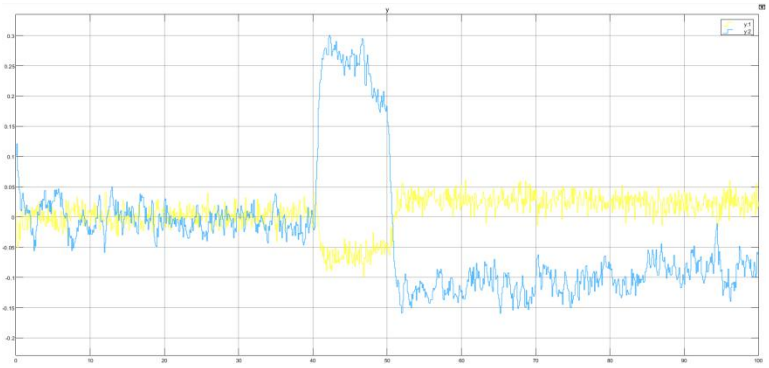

图 3-8 传感器数据状态

结合上述由此可以得出结论，在攻击下，在攻击下系统违反了电网的约束条件，因为系统在攻击期间不处于期望的平衡状态，并且影响了电网的行为。而且电网系统在攻击期间没有达到期望的平衡状态。且在攻击结束后，电网恢复了期望的平衡状态。

3.3 FDIA 检测算法设计

3.3.1 算法原理

本模拟通过结合卡方算法与卡尔曼滤波器，设计一种新的检测算法检测FDIA。其中卡方检测是一种经典的统计工具，其优点显而易见。首先，卡方检测适用性广泛，在许多领域都有应用，尤其在特征选择、异常检测等领域中得到了广泛的应用。其次，卡方检测是一种非参数方法，不需要对数据分布做出假设，因此更为灵活。此外，卡方检测原理相对简单，计算方式清晰明了，易于理解和实现，并且计算量较小，通常能够快速得出结果。另外，通过卡方值和p_{value}，可以判断变量之间是否存在显著性关系，而且卡方检测可以提供直观的结果解释，帮助理解变量之间的关联程度。综上

实现了一个基于该检测算法的异常检测函数 $Detector$，该函数接受三个输入参数：y_{prime}（修改后的测量信号），$data$（原始数据），和x_{hat}（状态估计）。该函数的主要目的是通过比较修改后的测量信号和基于状态估计的预测信号，来检测是否存在异常。

检测算法的工作原理如下：

（1）初始化：

定义输出矩阵 C，它用于从状态估计中提取与测量信号相对应的部分。

设置测量噪声协方差矩阵 R，它反映了测量过程中的不确定性。

初始化误差协方差矩阵 P，它在这里被用作输入数据。

（2）计算检测信号：

计算预测误差 r，它是修改后的测量信号 y_prime 与基于状态估计 x_hat 的预测信号之差。计算检测信号 z，它是预测误差 r 的平方与误差协方差矩阵σ的

逆的乘积。

（3）设置阈值：

选择显著性水平 *alpha*，它决定了检测的敏感度。

计算卡方分布的阈值 *tau*，它基于显著性水平和预测误差的维度。

（4）决策：

如果检测信号 z 小于或等于阈值 *tau*，则没有异常发生，函数输出 *alarm*=NO，并将 *anomaly* 设置为 0。

如果检测信号 z 大于阈值 *tau*，则表明存在异常，函数输出 *alarm*= YES，并将 *anomaly* 设置为 1。

（5）输出：

函数返回检测信号 *z* 和阈值 *tau* 作为输出参数 *output1* 和 *output2*。

可以通过修改敏感度来调整报警的敏感度，依据不同的敏感度来适应匹配各种特殊的有差异性的环境。

所述，选择卡方检测作为统计分析工具能够帮助快速而有效地进行变量相关性的推断和分析，具有广泛的应用价值。当然，在实际使用时也需要结合具体问题和数据情况来选择最适合的统计方法。

3.3.2 算法流程图

系统流程图[24]如图 3-9 所示，

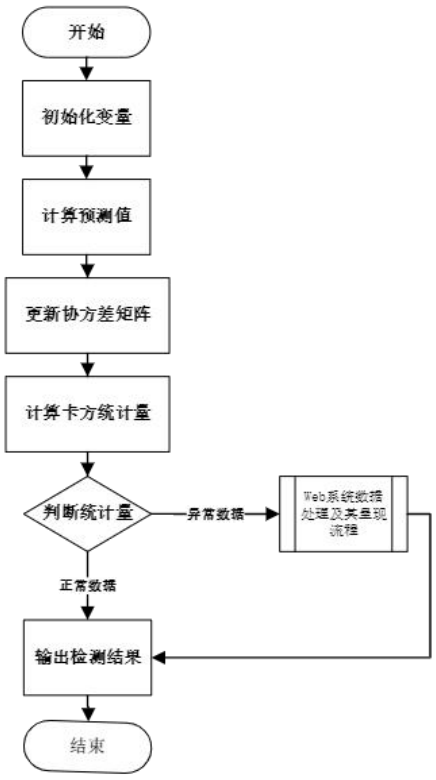

图 3-9 仿真模拟系统的程序流程图

算法开始执行后开始初始化变量：初始化状态转移矩阵（*A*）、过程噪声协方差矩阵（*Q*）、测量噪声协方差（*R*）。初始化估计值（*x_hat*）和协方差矩阵（*P*）。以及初始化异常状态位置列表（*anomaly_positions*）。之后数据遍历，对于每个时间点，执行以下操作：

（1）计算预测值：

使用状态转移矩阵（*A*）和前一个时间步的功耗消耗数据，计算当前时间点的预测值。

（2）更新协方差矩阵：

使用状态转移矩阵（*A*）和协方差矩阵（*P*），以及过程噪声协方差矩阵（*Q*），更新当前时间点的协方差矩阵。

（3）计算卡方统计量：

计算当前时间点的功耗消耗数据和预测值之间的差异，并根据测量噪声协方差（*R*）计算卡方统计量。

（4）判断异常：

如果卡方统计量超过阈值，将该时间点标记为异常状态，并将其添加到异常状态位置列表中。

（5）数据遍历结束：

如果还有更多时间点，返回到“数据遍历”步骤。

在基于 EMS 的 Web 程序子流程当中，首先利用 Plotly 库绘制功耗消耗曲线，之后根据异常状态位置列表，绘制异常标记，最后将绘制的数据转换为 JSON 格式。

3.3.3 卡尔曼滤波器设计

利用子系统实现进行卡尔曼滤波器的计算过程（图 3-10）。首先，定义了一些变量和矩阵，如卡尔曼增益矩阵 *K*、测量向量z_{k}、先验状态估计x_{priork}、先验估计误差协方差P_{priork}等。

然后，对一些矩阵进行了初始化操作，例如设置单位矩阵 *I*、过程噪声协方差矩阵 *Q*、测量噪声协方差矩阵 *R*、测量模型矩阵 *H* 以及状态转移矩阵 *F*。

接下来，根据先前的状态估计和先验估计误差协方差，使用卡尔曼滤波器的预测步骤来预测状态和协方差。然后，计算卡尔曼增益，用于调整预测的状态估计值。接着，计算测量向量z_{k}，用于校正状态估计。最后，更新估计误差协方差，并将当前状态和协方差保存为先前状态和协方差，以备下一次迭代使用。

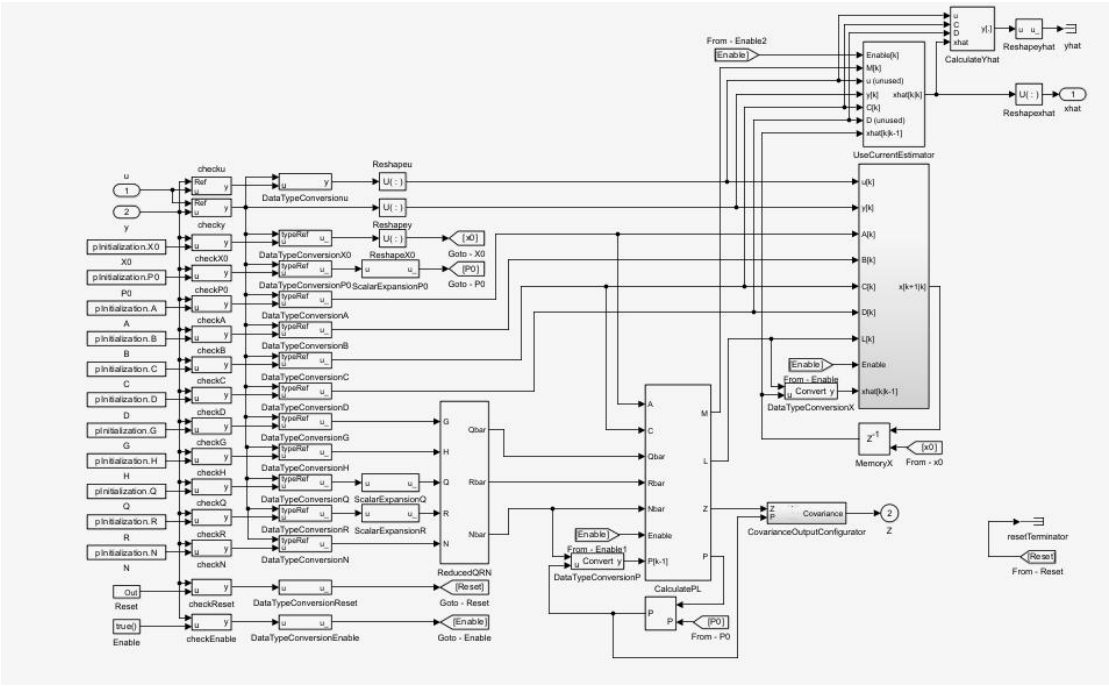

图 3-10 卡尔曼滤波器子系统

3.4 FDIA 检测算法仿真验证

本次仿真依旧采用通过定义$u^0(t)=u(t)+u^a(t)$，攻击具有以下时间行为，即公式：

$$u^a(t)=\begin{cases}0, & 0\le t<40\\ [-0.18,-0.18]^T, & 40\le t<50\\ 0, & t\ge 50\end{cases} \tag{3-5}$$

下面的图 3-11 为 Matlab 建模模拟用于支持上述公式。

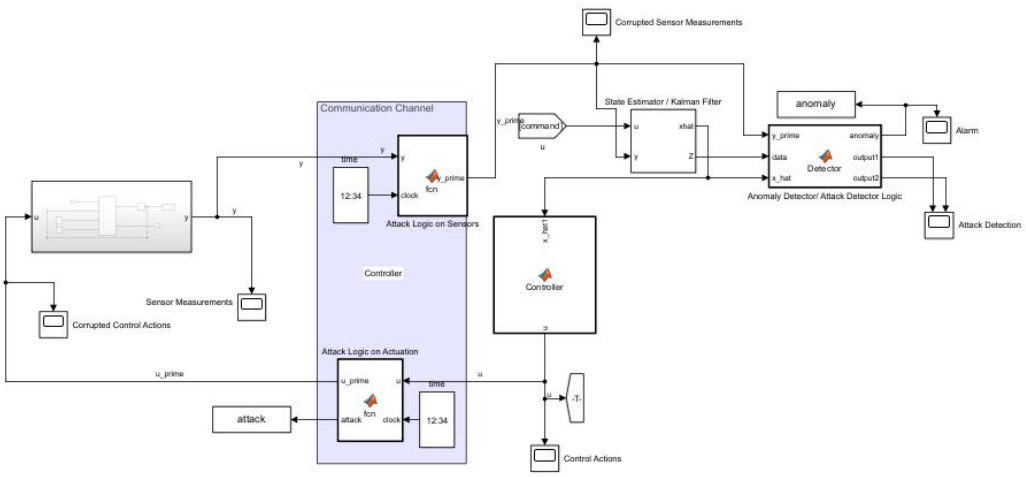

图 3-11 仿真模拟电网遭受 FDIA

3.4.1 执行器与传感器模块状态

同时为了控制变量，保证被攻击模块函数不变，观察其状态，根据本文的攻击时间，图 3-12 为执行器被攻击时的控制状态。

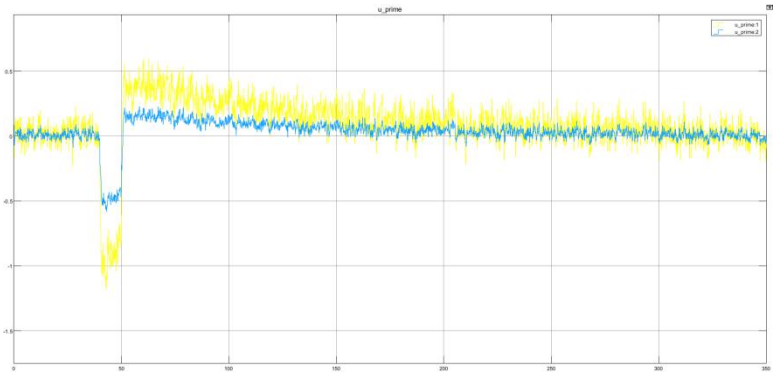

图 3-12 受损或受到干扰的控制状态

图 3-13 为执行器被攻击时传感器的接收数据状态。

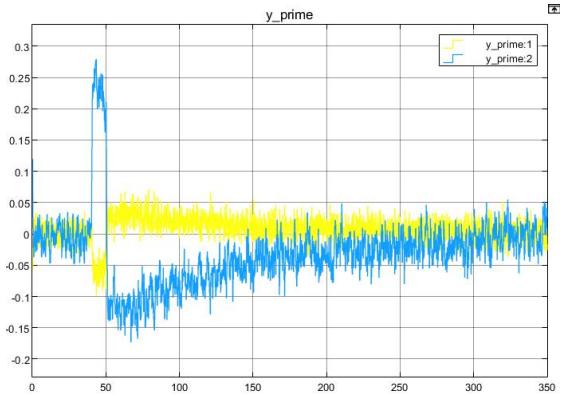

图 3-13 受攻击的传感器状态

可以根据这两个波形图的状态得出结论：无论是否加入检测模块，都保证了攻击效果的一致性。

3.4.2 检测模块与告警模块状态

检测模块是电力 CPS 检测系统中的关键组成部分，它通过比较实际测量值与正常情况下的预期值，来检测潜在的虚假数据注入攻击（FDIA）。为了适应不同的检测需求，检测模块允许通过调整α值来调整其灵敏度。α值代表了统计检测的显著性水平，较低的α值意味着更敏感的检测，较高的α值则意味着更宽松的检测标准。

在本研究中，选择了两种不同的α值设置：α=0.00001 和α=0.1，以展示算法在不同灵敏度下的表现。实验结果如图所示，其中α=0.00001（图 3-14）时的结果显示了算法在高度敏感条件下的检测能力，而α=0.1（图 3-15）时的结果则反

映了算法在较低敏感条件下的表现。

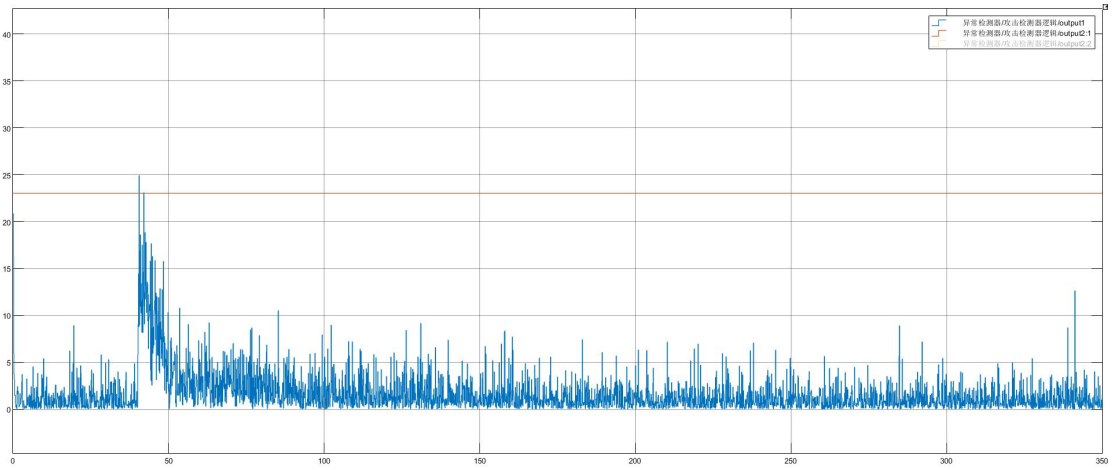

图 3-14 α=0.00001 时的异常检测

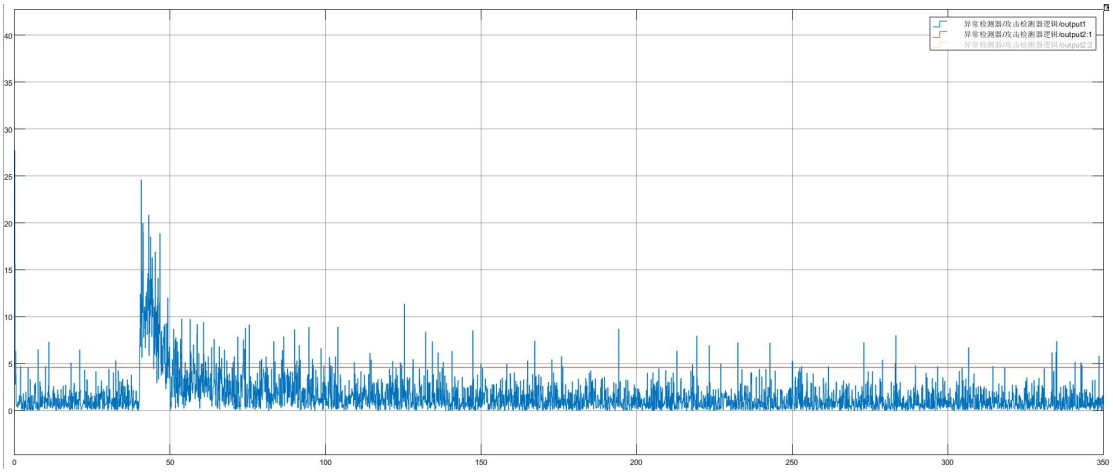

图 3-15 α=0.1 时的异常检测

通过对比分析这两种α值设置下的检测结果，可以得出以下结论：

（1）α=0.00001 时：算法对 FDIA 的检测非常敏感，能够捕捉到各种细微的异常，但这也可能导致误报率的增加。在这种情况下，系统的实时监控和告警机制需要更加精细，以确保准确性和效率。

（2）α=0.0001 时：算法的灵敏度降低，对 FDIA 的检测能力有所减弱，但误报率也相应减少。这种设置适用于对检测准确度要求较高的应用场景，可以减少不必要的警报，提高系统的稳定性和可靠性。

本设计还选取两个极端数据α=1（图 3-16）和α=0（图 3-17）。当α=1 时，默认所有数值都为异常数值。当α=0 时，默认没有异常数值。

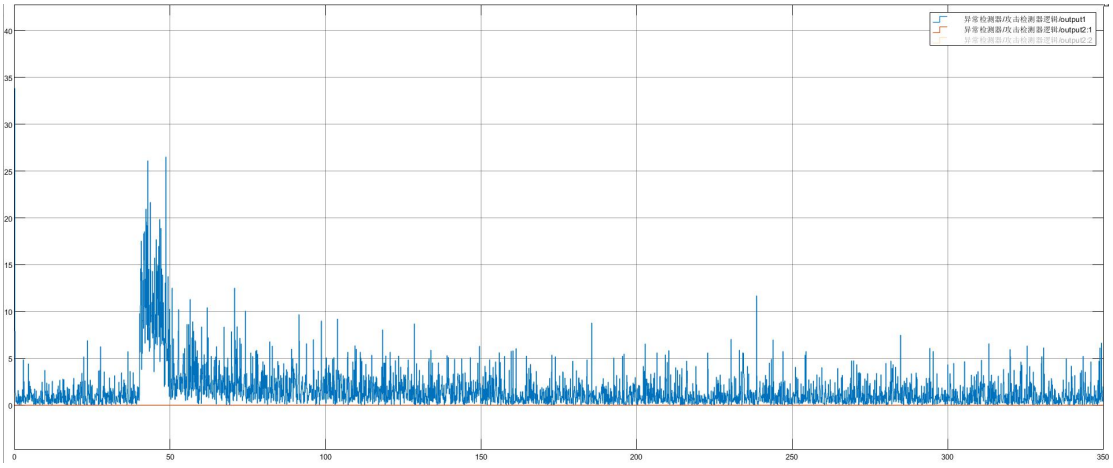

图 3-16 α=1 时的异常检测

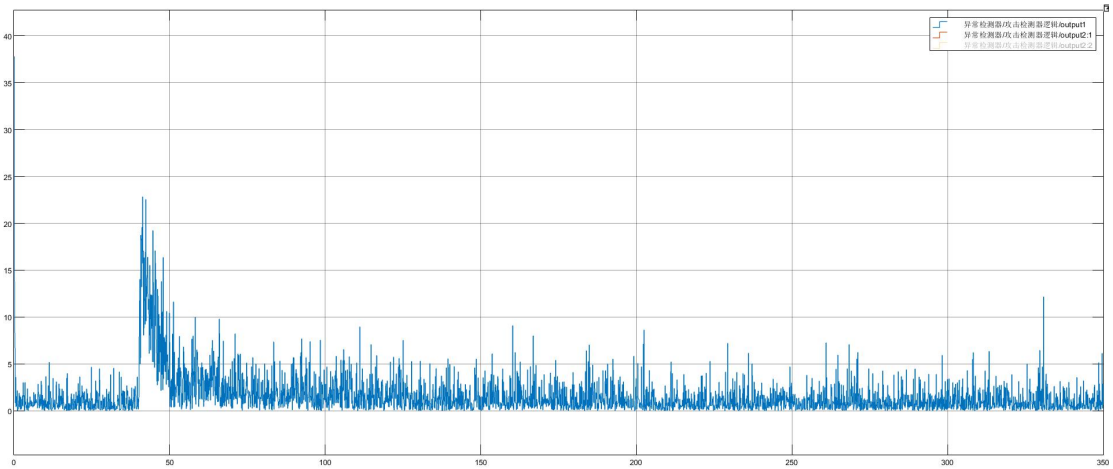

图 3-17 α=0 时的异常检测

综上所述，检测模块的α值设置是一个权衡利弊的过程，通过调整α值，可以根据实际需求和场景特点，优化算法的灵敏度和误报率，从而实现对 FDIA 的有效检测和告警。这种灵活的调整机制使得的电力 CPS 检测系统能够适应不同的安全监控需求，提高了系统的实用性和适应性。

而告警模块则是更加直观地显示在什么时间点数据超过阈值，并显示。

当α=0.00001 时如图 3-17 所示。

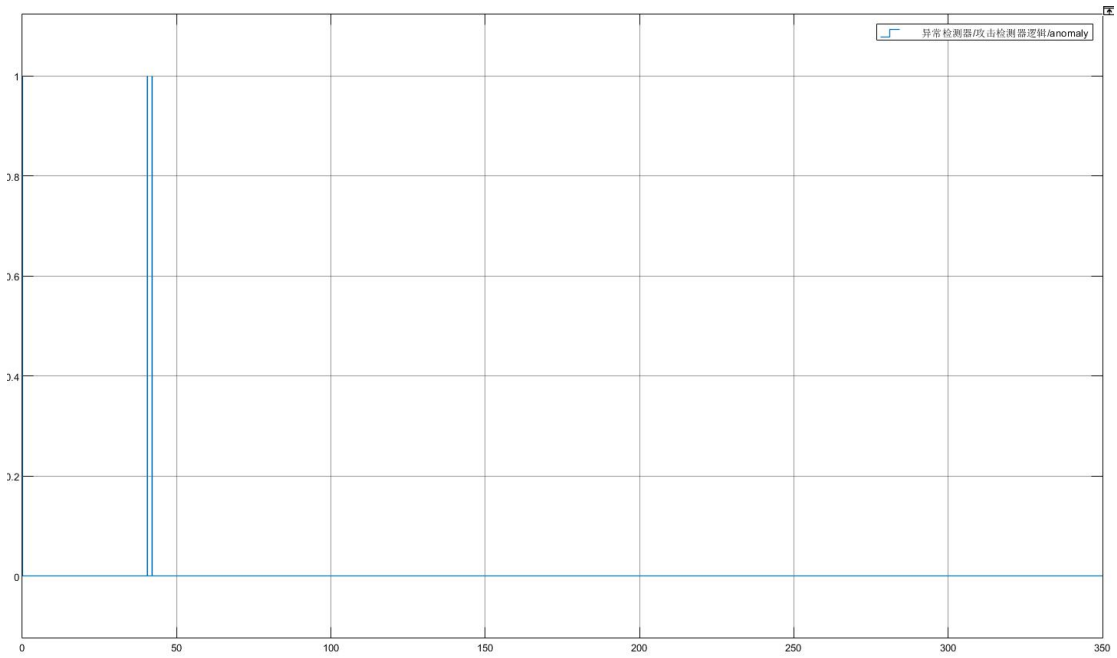

图 3-17 报警唯一值

当α=0.1 时如图 3-18 所示。

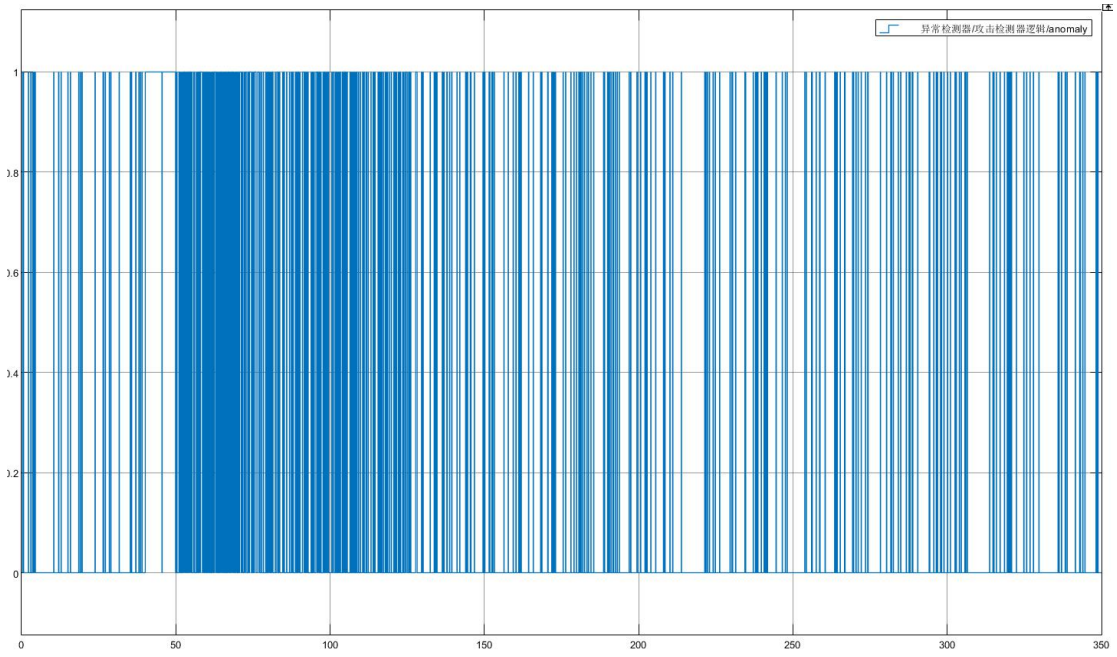

图 3-18 报警次数增多

当α=1 时，这意味着完全接受所有报警，如图 3-19 所示。

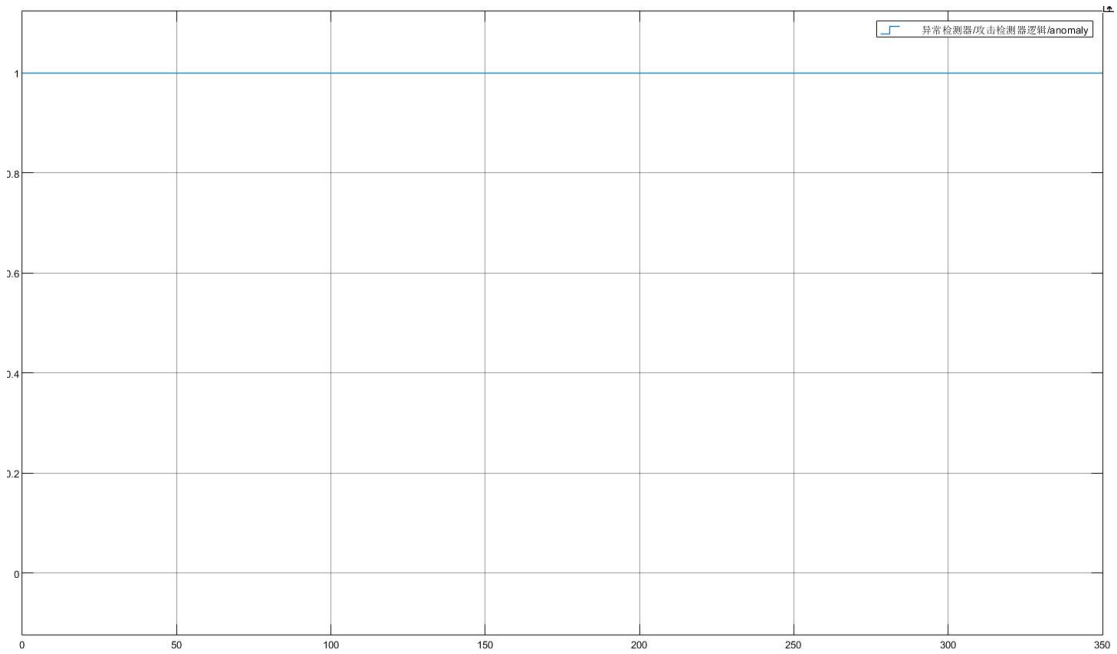

图 3-19 全部数据为报警

当α=0 时，这意味着完全不接受所有报警，如图 3-20 所示。

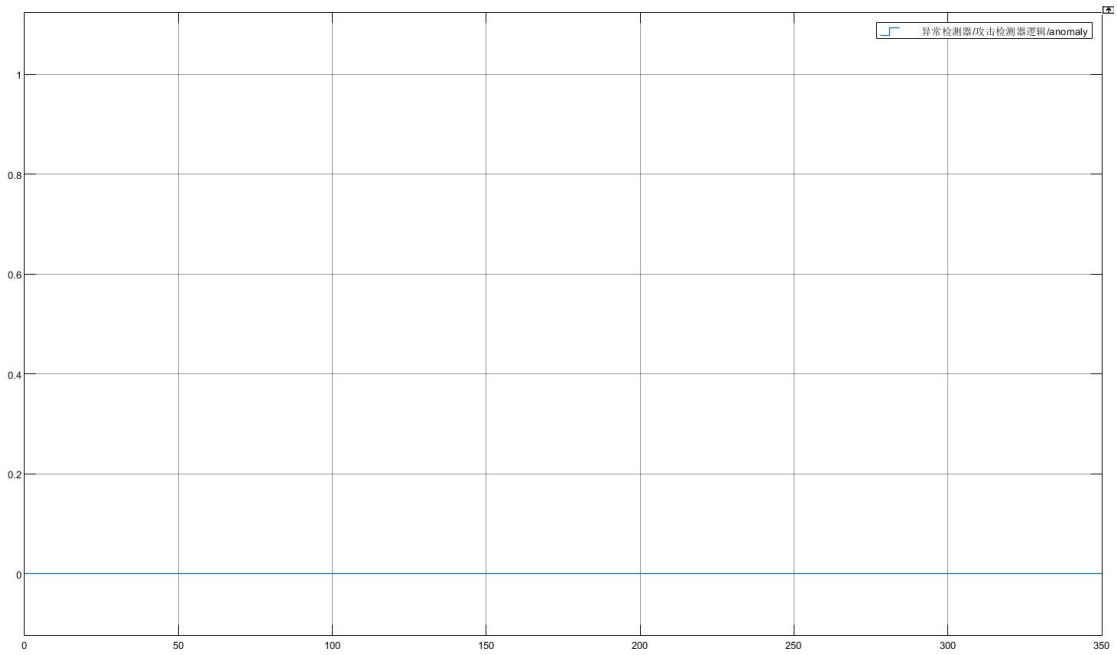

图 3-20 全部数据不报警

在攻击期间，电网不稳定运行。且从图表上可以观察到，电网中途达到了平衡状态。同时由于系统具有弹性，在攻击结束后，系统达到了稳定的平衡状态。

在本章中，将通过两次仿真实验来评估基于 EMS 的 FDIA 电力 CPS 检测系统的有效性。第一次实验是在没有检测算法的情况下进行的，以展示系统在未添加任何检测措施时的表现。第二次实验是在加入了检测算法的情况下进行的，以

验证该检测算法对系统检测效果的提升。

在第一次仿真实验中，模拟了一个未添加检测算法的电力 CPS 系统。结果显示，系统在面对 FDIA 时，由于缺乏有效的检测机制，无法检测到异常数据，导致系统产生了错误的决策和操作。这表明，在未添加检测算法的情况下，系统对 FDIA 的检测效果非常有限，甚至没有检测效果。

在第二次仿真实验中，在系统中加入了检测算法。结果显示，系统在面对 FDIA 时，能够有效检测到异常数据，并及时发出告警。这表明，该检测算法能够提高系统对 FDIA 的检测能力，从而提高系统的检测效果。

通过对比两次仿真结果，可以得出以下结论：

（1）对比结果：在第一次仿真实验中，系统未添加检测算法，对 FDIA 的检测效果非常有限。而在第二次仿真实验中，系统加入了检测算法，能够有效检测到 FDIA，提高了系统的检测效果。

（2）检测算法的作用：检测算法能够提高系统对 FDIA 的检测能力，从而提高系统的检测效果。这表明，该检测算法能在电力 CPS 检测系统中起到一定的作用，能够有效提升系统的安全性和可靠性。

通过这种方式，该检测算法能够有效地识别电力系统中的异常情况，为系统的安全运行和及时维护提供重要支持。

第 4 章 基于 EMS 的 FDIA 电力 CPS 检测系统的设计与实现

4.1 基于 EMS 的 FDIA 电力 CPS 检测系统需求分析

在工业控制安全领域中，随着信息物理系统在电力领域的广泛应用，电力系统的安全性面临着新的挑战。特别是虚假数据注入攻击对电力系统的安全稳定运行构成了严重威胁。因此，基于 EMS 的电力 CPS 检测系统的设计具有重要意义。

该系统的主要核心需求可以分为六个方面：检测 FDIA、实时监控、本地知识库机器人、远程电气端控制、集成 EMS/CPS、跨部门协作，检测 FDIA 则是指对虚假数据注入攻击进行实时检测和预警，以防止攻击对电力系统造成破坏；实时监控指的是对电力系统数据的实时采集和分析，以便及时发现异常情况时为可靠的分析做支撑；本地知识库机器人是保证智能电网遭受 FDIA 或其他电气故障时可以为电网运维人员做出可靠的知识帮助；远程电气端控制是远程电气端控制是指通过远程操作来控制电网设备，以便在检测到 FDIA 或其他电气故障时，可以迅速采取措施，如隔离受影响的设备或调整系统运行参数，以减少潜在的损害；集成 EMS/CPS 是指将该检测系统与能量管理系统集成，使该系统具有良好适应性；跨部门协作是指不同部门之间共享信息，以便更有效地应对 FDIA 和其他电网安全问题。这包括与 IT 部门合作，以确保网络安全；与运维部门合作，以便快速响应电网问题；以及与规划部门合作，以便更好地预测和防止未来的电网问题。

4.2 基于 EMS 的 FDIA 电力 CPS 检测系统总体设计

根据前文 Matlab 对于 FDIA 与其卡方算法检测算法模型仿真的分析，监控平台功能需求和架构设计，且考虑到安全性，稳定性，可靠性，数据安全性的基本要求与因素，结合实际的生产与电力环境，同时结合前文的基础技术点，系统的整体设计主题包含以下方面：

（1）登录功能

为了严格实施数据保护法规，在中国的《网络安全法》中，要求企业对用户数据进行保护，登录框是实现这些要求的基本措施之一。同时登录框确保只有经过验证的用户才能访问存储在系统中的敏感数据。如果没有登录机制，任何人都

可能访问到其他用户的数据，增加数据泄露的风险。

（2）调节报警敏感度

为了实现系统的可兼容性和可调整性，预留调整卡方值的功能，用户可基于其实际生产环境调试与部署，保证了系统的可持续发展与降低劳动成本。

（3）告警功能

如果采集到的消耗功率超出卡尔曼滤波器的预期那么该数据标记，为橙色，同时在系统网页下方提示该系统可能存在 FDIA。

（4）消除告警功能

如果存在误报，可以手动消除系统网站下方的告警提示，但保留问题，以备后续翻阅查看。

（5）高度可视化

为保障系统的可持续化与可用性，采用数据库连接的其他字段，如：地点、电压、频率、相角等进行美观且直观地展示。

（6）知识库机器人[25]

引用第三方 ChatGLM3 大模型 AI 机器人，保证使用者遇到专业知识问题可以快速自主解决。

（7）使用手册

保证使用者可以快速进行系统学习，降低学习成本。

（8）更多关键基础设置参数配置

随着系统所接入的关键基础设施增多，需要进行更快捷方便的手段进行管理。

（9）多部门协作

当遇到问题的时候，需要系统使用者快速进行跨部门合作，联合行动等动作。

（10）导航

在实际的电网以及大型工业系统中，很多的系统都是由各个服务组成，此功能保证了快速访问，增强机动性。

（11）远程控制与自动化：实现对电力系统设备的远程控制和自动化操作，以提高系统的响应速度和效率。

（12）保证检查时数据可操作性与高度关联性

利用开发平台的特性，进行全数据关联，方便核查，提升工作效率，降低人力成本。

（13）EMS 集成：确保 Web 监控检测系统与 EMS 紧密集成，实现数据的实时同步和共享，以便系统能够基于实时数据进行分析和决策。

（14）历史数据查询：允许用户查询和分析历史数据，以便对电力系统的长期趋势进行分析和预测。

由此结合本论文的 Matlab 仿真，根据系统的总体设计，结合实际情况与系统开发的基本要求，设计出来一套基于 EMS 的针对电网 CPS 的 FDIA 的检测

Web 微系统[26]，该系统包含 5 个大的模块与 16 个小的功能模块，具体的系统功能模块设计如图 4-2 所示。

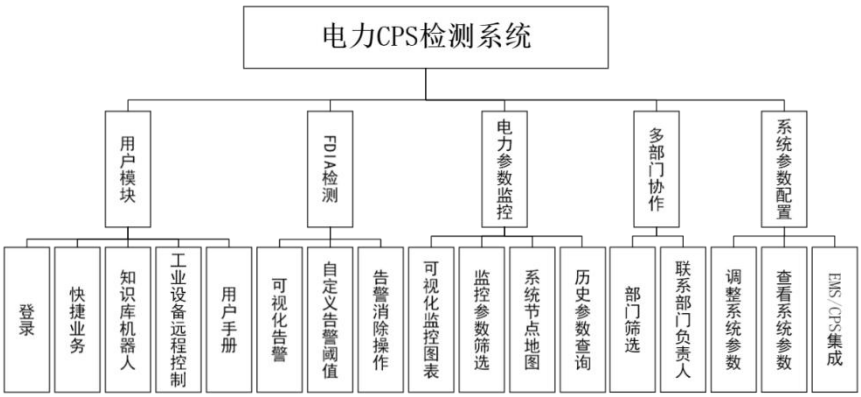

图 4-2 系统功能模块图

在智能电网系统中，FDIA 可能对不同类型的电力设备进行攻击，但主要以从部署在各个关键节点的传感器，如输电线路、变电站、发电站以及用户端，实时监测电力系统的运行状态。这些传感器收集的数据是 SCADA 或 EMS 系统等高级控制系统进行决策的基础。然而，这些传感器也可能成为 FDIA 的切入点，攻击者可以通过篡改传感器数据，向系统中注入虚假信息，从而引发一系列问题。

这种攻击可能导致电力负荷数据、电压数据、电流数据、功率因数、相角和事件记录等关键参数遭到篡改，从而影响系统的正常运行和决策过程。

故，建立和设计一个合理的数据库来存储必要的数据是一项重要任务。在设计数据库时，需要考虑数据的类型、存储方式以及数据之间的关系。以下是数据库表的详细设计说明：

（1）电气相关生产参数表（ami）存放电气生产相关参数时间（Time）、地点（Locate）、消耗功率（PowerConsumption）、电压值（U）、频率（HZ）、相角（degree），如表 4-1 所示：

表 4-1 数据库表

列名	数据类型	长度	描述
Time	varchar(255)	8	数据采集的时间，格式为年月日时分秒
Locate	datetime	255	数据采集的地点，默认值为大庆地区
PowerConsumption	float	20	数据采集点的瞬时消耗功率，单位为 MW
U	float	20	电压值，单位为 U
HZ	float	20	频率值，单位为 Hz
degree	float	20	相角值，单位为度

（2）账户表（user）存放用户信息，用户名（username）、密码（pwd），

如表 4-2 所示：

表 4-2 数据库表

列名	数据类型	长度	描述
username	varchar(255)	255	用户账号
pwd	varchar(255)	255	用户密码

（3）设备表（device）包括设备 ID（Id）、设备 IP（IP）、设备名（Devicename），设备表如表 4-3 所示：

表 4-3 数据库表

列名	数据类型	长度	描述
Id	varchar(255)	255	设备代号
IP	varchar(255)	255	被控制设备 IP
Devicename	varchar(255)	255	设备名称

（4）跨部门协作的协作信息（worker）包括接收人（Receive）、电话号（Tel）、部门（Part）如表 4-4 所示：

表 4-4 数据库表

列名	数据类型	长度	描述
Receive	varchar(255)	255	设备代号
Tel	varchar(255)	255	被控制设备 IP
Part	varchar(255)	255	设备名称

4.3 基于 EMS 的 FDIA 电力 CPS 检测系统系统功能实现

4.3.1 登录页面与系统主页面

这部分是需要智能电网或大型智慧工厂运维或网络安全人员在系统上的登录，需要输入账号密码点击登录会进入此系统，进行观察数据，保证了数据隐私的安全性，用户登陆页面如图 4-3 所示，且当智能电网或大型智慧工厂运维或网络安全人员在系统上的登录后，显示选择页面，进行选择多种功能。

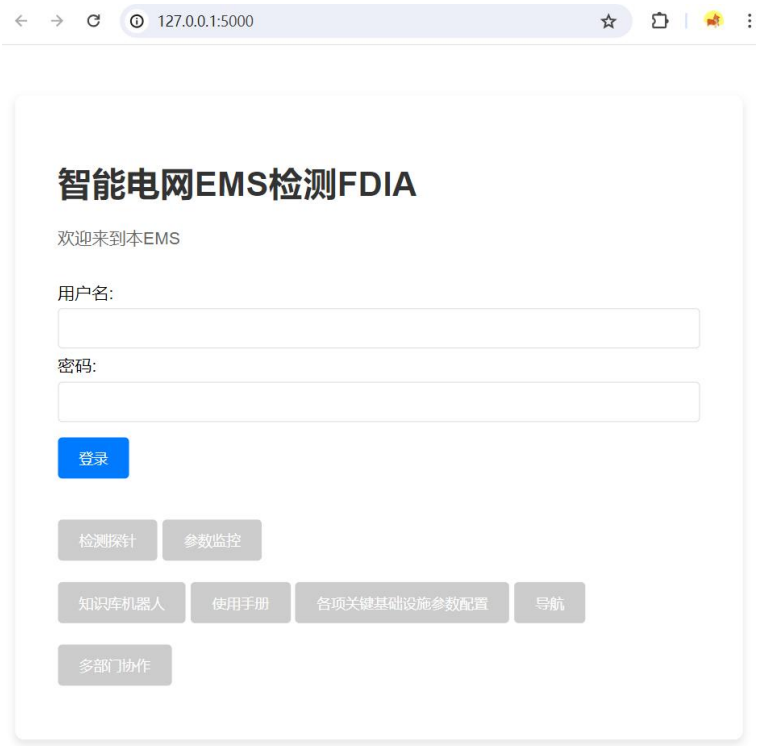

图 4-3 登录页面

4.3.2 FDIA 检测页面

在本 Web 设计中，采用了 Flask 框架作为开发框架，以确保系统的稳定性和可扩展性。监控检测页面作为系统的重要组成部分，实现了对电力系统实时监测和异常检测的关键功能。

图 4-4 展示了监控检测页面的实现[27]，该页面通过折线图的形式直观地展示了电力系统的实时运行数据[28]。通过突出显示非正常数据，用户能够快速识别和定位异常点，从而及时发现和处理潜在的问题。

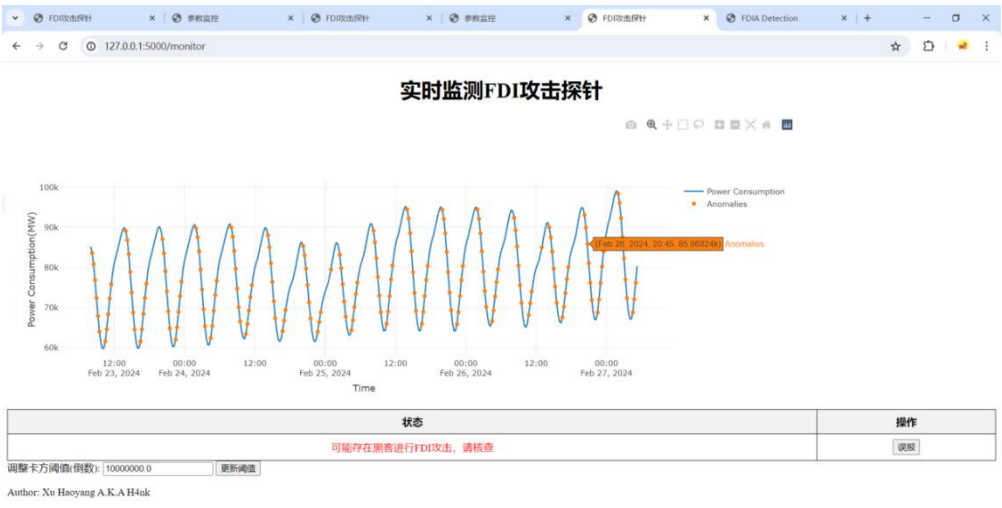

图 4-4 实时监测 FDIA 功能实现

在监控检测页面中，实现了基于异常数据的报警功能，当检测到异常数据时，系统会自动发出告警，提醒用户进行关注和处理。同时，系统还提供了消除误报的功能，用户可以根据实际情况手动消除误报，以避免不必要的干扰。

此外，监控检测页面还允许用户调整卡方的值，以实现对报警敏感度的自定义设置。通过可调节的敏感报警值，用户可以根据实际需求调整报警的灵敏度，以适应不同的监控场景和需求。

通过监控检测页面的设计，旨在为用户提供一个强大的工具，以实时监控电力系统的运行状态，及时发现和处理异常情况。这种高交互性的设计确保了用户能够有效地利用系统提供的数据，从而提高电力系统的安全性和可靠性。

4.3.3 参数监控页面

在全参数监控页面中，旨在为用户提供一个全面且直观的视角，以便在存在问题数据时能够准确判断系统中的告警点是否出现问题。此系统通过整合来自不同传感器[29]的数据，为用户提供了一个丰富的、多维度的电力系统状态视图。

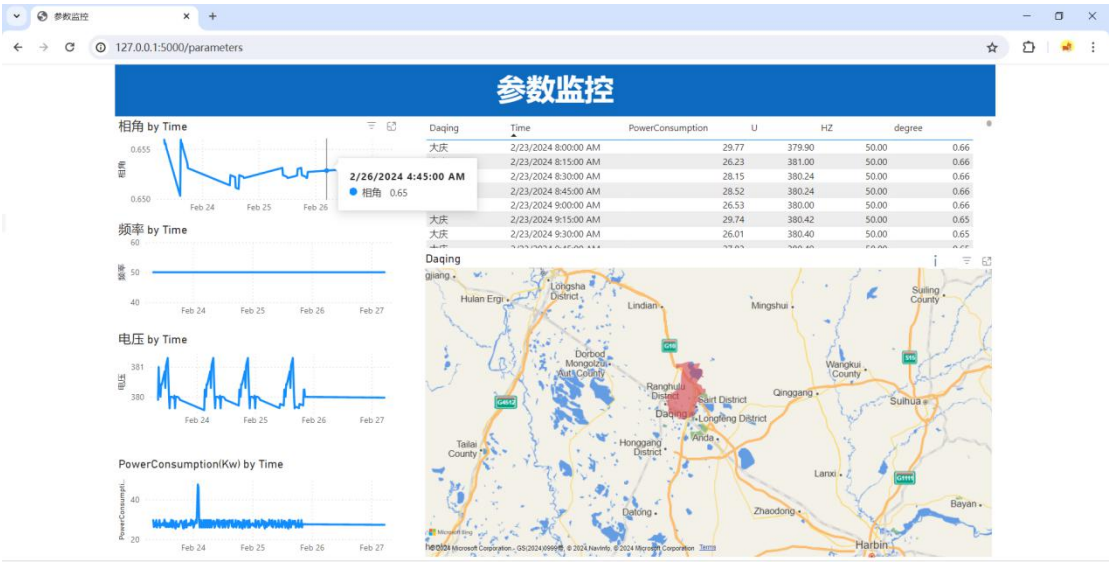

图 4-5 全参数监控页面实现

图 4-5 展示了全参数监控页面的实现，它通过清晰的图表和数据展示，使得用户能够清楚地了解电力系统的实时运行状况。此外，该页面还提供了高交互功能，允许用户进行自定义视图、数据筛选和图表分析，以实现精准分析的目的。

在全参数监控页面的开发过程中，采用了 Power BI 作为数据可视化工具，通过数据清洗和数据关联技术，确保了数据的准确性和一致性。数据清洗技术用于去除噪声数据和异常值，而数据关联技术则用于将不同来源的数据进行关联分析，以提供更全面的数据洞察。

通过全参数监控页面的设计，旨在为用户提供一个强大的工具，以监控和分析电力系统的运行状态。这种高交互性的设计确保了用户能够有效地利用系统提

供的数据，从而提高电力系统的安全性和可靠性。

4.3.4 知识库机器人页面实现

在本页面的模块中，引入了第三方知识库机器人，如图 4-6 所示，以实现电力系统智能问答服务。以实现电力系统智能问答服务。为了达到这一目标，选择了本地部署基于 ChatGLM3 大模型作为本地知识库机器人。ChatGLM3 大模型是一个基于大规模语言模型的人工智能助手，能够处理自然语言输入并生成相应的回答。它拥有强大的本地知识库解析功能，能够理解并回答围绕知识库的问题。在电力系统领域，ChatGLM3 大模型能够提供关于电力设备、电网运行、故障诊断等方面的知识。

图 4-6 基于 ChatGLM3 大模型的问答机器人

ChatGLM3 的算法集成了自然语言处理（NLP）技术和机器学习算法，以理解和生成语言。它基于预训练的大型语言模型，通过在大规模文本数据上进行训练，学习语言的语法和语义结构。ChatGLM3 的算法还包括自然语言理解（NLU）部分，用于解析用户的输入查询，涉及分词、词性标注、命名实体识别等步骤，以确定输入文本中的关键信息。此外，它还包括知识检索部分，用于从本地知识库中检索与用户查询相关的信息，通常涉及到索引和搜索技术。ChatGLM3 的算法还包括多轮对话管理部分，用于处理连续的对话交互，包括对话状态跟踪、意

图识别、情感分析等步骤。自然语言生成（NLG）部分用于生成与用户查询相关的回答，涉及文本生成和语言润色技术。此外，ChatGLM3 的算法还包括持续学习和优化部分，用于根据用户反馈和交互数据不断改进模型的性能，通常涉及使用机器学习技术来调整模型参数和优化模型结构。

通过将 ChatGLM3 本地知识库机器人集成到基于 EMS 的电力 CPS 检测系统中，成功地提供了一个智能化的问答服务。这不仅提高了用户查询电力系统相关知识的效率，还增强了系统的实用性和用户体验。ChatGLM3 的集成展示了其在电力系统领域的应用潜力，为未来的系统升级和功能扩展提供了可能性，同时保证了问题的快速解决。

4.3.5 多部门协作功能实现

在本系统中，引入了多部门协作功能，旨在促进不同部门之间的沟通与协作，提高工作效率和项目透明度，减少信息孤岛，优化资源分配，增强团队间的知识共享，从而提升整体的业务流程和决策质量。

图 4-7 展示了多部门协作功能的实现，通过该功能，用户可以方便地选择并定位到特定部门，进而获取当前部门的人员姓名及其电话号码，如图 4-8 所示。详细展示了部门人员详情信息，包括个人基本信息、职责范围等。

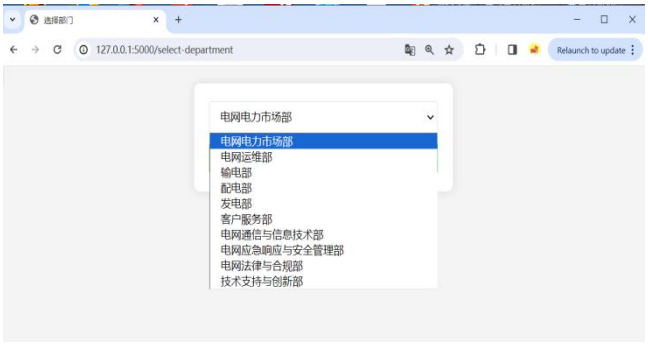

图 4-7 选择部门模块

图 4-8 部门人员详情信息

通过多部门协作功能的实现，为用户提供了便捷的沟通与协作平台，使得不同部门之间能够高效地共享信息、协调资源，共同推进项目进展。这种功能的设

计不仅提升了团队间的协作效率，也为项目的成功实施提供了有力支持。

4.3.6 EMS/CPS 集成实现

基于 EMS 与 CPS 的结构，本研究在工业控制安全与智能电网背景下，实现能源管理系统（EMS）与网络物理系统（CPS）的深度集成。这种集成设计充分利用了 EMS 和 CPS 在各自领域的专长，通过构建一个模块化的接口层（API），实现了数据的共享和命令的传递。具体而言，该模块支持监控数据的实时获取、数据更新的自动化处理，以及 CPS 指令的即时发送（如图 4-9 所示）。

图 4-9 其预留集成接口的调试页面

集成模块的设计理念旨在降低维护成本并提升电网的长期可持续性。通过实时监控和 CPS 指令的发送，系统能够有效减少故障发生率，进而降低维护成本。此外，集成系统还显著提高了能源管理的效率，通过实时数据分析和预测模型，实现了能源使用的优化和分配的合理化。

更重要的是，集成系统展现出卓越的扩展性和适应性，能够适应不同定制化 EMS 的需求。通过开放的接口（API），系统能够轻松地与其他系统或组件集成，从而不断扩展其功能和应用范围。这种模块化的设计理念不仅为当前的智能电网提供了强大的支持，也为未来的技术创新和系统升级奠定了坚实的基础。

4.3.7 远程控制与自动化实现

在现代工业环境中，远程控制与自动化实现已成为提高生产效率和确保系统安全的关键组成部分。在本研究中，采用 Modbus 协议作为工业设备远程控制与自动化实现的通信标准。Modbus 协议以其广泛的应用和简单性而著称，被广泛用于各种工业应用中。

当系统中面临 FDI（恶意文件输入）攻击等安全威胁时，本模块的设计能够迅速响应，并立即采取措施对工业设备进行远程控制。这确保了在紧急情况下，系统能够快速采取行动，如重置、停止与启动（图 4-10），从而有效防止潜在的安全风险，保护设备和人员的安全。

图 4-10 远程控制功能点

通过实现远程控制与自动化，本模块（图 4-11）显著提高了工业设备的操作效率。它允许操作员在远离现场的情况下监控和控制设备，从而节省了时间和资源，并提高了整体生产效率。此外，自动化系统可以自动执行重复性任务，减少了人工操作的需求，进一步提高了生产效率。

图 4-11 远程控制与自动化实现

本模块的远程控制与自动化实现不仅提高了工业设备的操作效率，还确保了在面临安全威胁时能够迅速响应，从而保障了系统的安全性和稳定性。这为工业自动化和远程控制领域提供了有效的解决方案，并为未来的研究和应用提供了坚实的基础。

第 5 章　基于 EMS 的 FDIA 电力 CPS 检测系统测试与分析

5.1 基于 EMS 的 FDIA 电力 CPS 检测系统测试

本文将详细讨论系统验证的过程和方法，系统验证是确保系统满足需求和预期目标的关键步骤。通过系统验证，可以检测和纠正系统中的潜在问题和错误，确保系统的质量和稳定性。

为了保证本系统的稳定运行和良好性能，对其进行了严格的系统测试。首先，搭建一个符合实际运行环境的测试环境。测试环境的搭建包括硬件设备和软件环境的配置。硬件设备包括服务器、客户端计算机、网络设备等，选择了与实际运行环境相同或更高配置的设备进行测试。软件环境包括操作系统、数据库、中间件等，按照实际运行环境进行了相应的配置和优化。在图 5-1 中的生产环境当中部署本系统

图 5-1 真实环境部署位置

5.1.1 功能点测试

对本系统的各个功能模块进行了详细的功能测试，在本论文的前文中所提及的模块中。测试过程中，严格按照需求中的功能需求进行操作，验证系统是否能够按照预期执行。同时，还需要检查系统在各种正常和异常情况下是否能稳定运行，以及系统的用户界面是否友好，操作是否简便等。

在本章中，将深入探讨系统功能测试的过程。功能测试的主要目标是验证系

统是否实现了预期的功能，并确保其按预期工作。通过编写详细的测试用例，并执行这些测试来验证系统的关键功能。

（1）登录功能：可以通过对应的账号密码登入系统，确认用户身份得到有效验证，表明登录功能正常。

（2）调节报警敏感度的功能：通过给定的不同的卡方值实现了不同的告警敏感度，证明了报警敏感度调节功能的有效性。

（3）告警功能与消除告警：调节卡方值使采集到的消耗功率超出预期时，此时系统实现了能够正确标记数据，，并在界面上显示 FDIA 警告，说明告警功能符合设计要求。用户能够通过点击消除告警按钮，成功清除误报的警告信息，表明消除告警功能运行正常。

（4）高度可视化功能测试：为了提高系统的可用性和用户体验，测试了高度可视化功能，确认系统能够美观且直观地展示数据库连接的其他字段，如地点、电压、频率、相角等，测试结果显示高度可视化功能提升了用户体验。

（5）还测试了知识库机器人功能，确认引用第三方 ChatGLM3 大模型 AI 机器人，通过询问遭受了 FDIA 攻击时的解决办法，可以结合本地知识库进行消息回复。测试表明知识库机器人功能能够有效辅助用户解决相关问题。

（6）关键基础设置参数配置功能：系统能够允许用户配置和管理关键基础设施的参数，测试结果显示参数配置功能灵活且稳定。

（7）多部门协作功能：通过选定部门，系统能够给所选部门负责任的相关信息，测试证实了多部门协作功能能够促进快速响应和协调工作。

（8）导航功能：通过存储导航连接，确认系统能够提供快速访问各个服务的能力，测试结果表示导航功确实可以提高系统的易用性。

（9）远程控制与自动化功能：通过测试命令，系统实现了对电力系统设备的远程控制和自动化操作，测试结果表明远程控制与自动化功能提高了系统的操作效率和响应速度。

（10）EMS 集成功能：通过输入与输出一些简单命令，确保了数据的实时同步和共享，测试结果显示 EMS 集成功能满足了系统集成的需求。

通过这些测试，验证了系统实现了所有预期的功能，并按预期工作。这将有助于验证系统的可用性和性能，并为系统的进一步开发和优化提供基础。

5.1.2 性能测试

其次进行了性能测试主要评估系统在各种负载情况下的性能表现，需要测试系统的稳定性，即在长时间运行过程中是否会出现性能下降或者其他异常情况。

拟定了在请求数为 10000 且并发数为 1000 的压力测试，其表现良好，如图 5-2 所示。

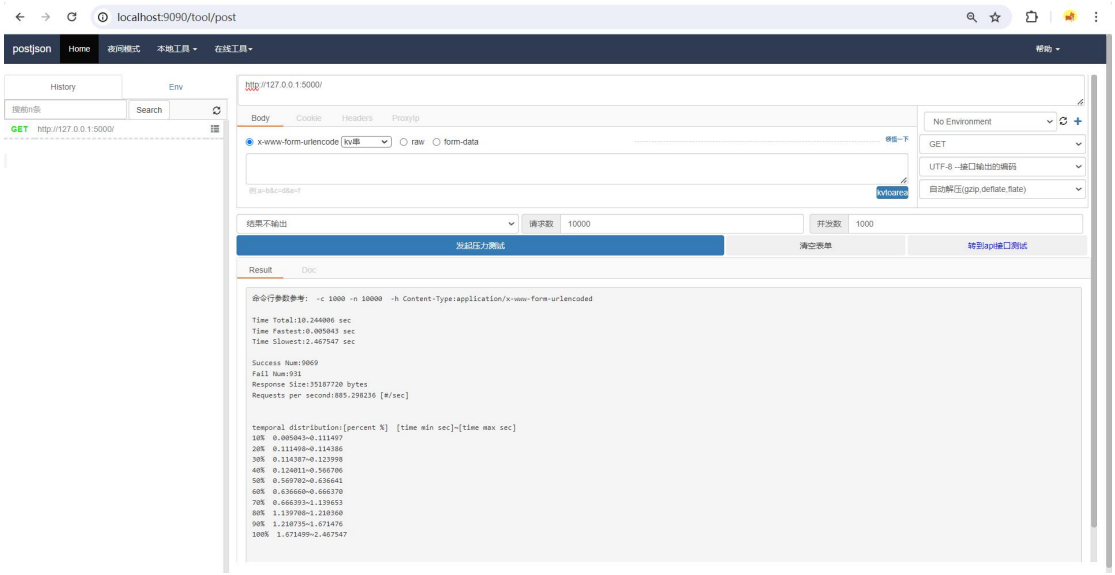

图 5-2 压力测试

5.1.3 安全测试

安全测试是检验系统是否能够保证并提升电网的安全基线。需要对系统进行安全风险评估，包括对系统的网络通信、数据存储、用户权限管理等方面进行安全测试。测试手段包括黑盒安全测试与白盒安全测试两大方面。通过安全测试，可以确保系统的数据安全和稳定运行。

首先利用 Goby 专业漏洞扫描系统进行黑盒测试，黑盒安全测试是一种安全测试方法，测试工具或安全专家不需要了解被系统的代码结构，以确保软件在真实环境中对各种安全威胁的抵抗力，图 5-3 所示，资产漏洞为零，表示本系统并无安全威胁。

图 5-3 系统黑盒安全测试

其次利用 Seay 专业源代码审计系统进行白盒测试，白盒安全测试是一种安全测试方法需要测试工具或安全专家检查代码以寻找潜在的安全漏洞。图 5-4 所示，该代码并无危险函数，本系统并无安全威胁。

图 5-4 系统白盒安全测试

5.1.4 兼容性测试

最后进行了兼容性测试，检验系统在不同硬件、操作系统、浏览器等环境下是否能够正常运行的测试。需要对系统进行多平台、多浏览器、多设备的兼容性测试，以确保系统在各种环境下都能够满足用户需求，通过用多种浏览器浏览打开并运行检测系统，可以通过市面上主要流行的浏览器打开，结果为兼容所有市面上主要流行的浏览器。

5.2 基于 EMS 的 FDIA 电力 CPS 检测系统优化分析

在完成了系统的测试阶段之后，对系统进行了全面的分析。从测试结果来看，系统的整体性能和功能都达到了预期的要求。然而，经过深入分析，发现系统仍存在一些需要改进和优化的问题。

首先，需要对系统的 FDIA 算法还是需要进行升级和完善。虽然当前的算法已经能够检测到大部分的攻击行为，但在实际应用中，仍然存在一定的博弈过程。因此，需要研究和开发更加先进的 FDIA 检测算法，以提高系统的 FDIA 检测能力和准确性。

其次，需要对 EMS 对执行器等的电网物理设备控制能力进行增强。在实际运行过程中，发现 EMS 不能实现所有物理硬件的控制。为了提高系统的执行效率，需要对 EMS 进行优化和改进，以增强对更多设备的控制能力。

其中，神经网络自动调节敏感度这也是一个最主要的问题，如果实现了神经网络自动训练大模型参数，降本增效，实现部署即运营的作用。

综上所述，虽然系统的整体性能和功能已经达到了预期要求，但仍存在一些需要改进和优化的问题。将根据这些问题，制定相应的改进计划，并投入相应的资源和时间进行优化和升级。相信，通过不断地改进和优化，系统将能够更好地满足用户的需求，为智能电网提供更高效、准确的系统服务。

结 论

1、成本核算

本检测系统设计在选择实物与对应的器件时参考第四章系统需求与系统实现所依靠 EMS 环境。在整个摸索过程中已经对整个系统设计有一个更高层次的认知。具体明细如表 1 所示，总成本控制在 36 万相比于市场中的其他竞品对象，在安全检测性高、价格低、可移植性强等优点，具有不错的潜力。

表 1 检测系统部分成本价格表

序号	产品名称	单价
1	Power BI 商业授权	10000
2	服务器	150000
3	客户机	6000
4	数据采集装置	10000
5	监控显示屏	15000
6	EMS 软件系统	80000
7	通信设备	14000
8	机柜	5000
9	UPS 电源	20000
10	数据库管理系统	50000

2、风险评估

本文设计的基于 EMS 的 FDIA 电力 CPS 检测系统在指导老师的指导下严格遵循了法律合规性，并确保了设计的创新性和合法性。该系统目的在于提高电力系统的供电稳定性、可靠性和安全性，并实现能源的高质量发展可持续使用，与建设环境友好型、资源节约型社会的目标相契合。系统设计过程中未对人类和环境造成任何损害，也未存在任何潜在的社会、健康、安全、法律、文化以及环境风险。

3、论文主要工作及成果

本文针对工业控制安全领域的电力 CPS 中的网络安全问题，特别是虚假数据注入攻击的威胁，进行了深入的研究和分析。通过结合算法仿真模拟和 Web 开发技术，本文取得了一系列研究成果，现总结如下：

（1）本文通过 Matlab 对智能电网中的 FDIA 进行了详细的仿真分析，揭示了其对电力系统安全稳定运行的潜在影响和危害，为后续的检测系统设计提供了理论基础。

（2）设计并实现了一种结合卡方算法与卡尔曼滤波器，设计一种新的检测算法，用于实时监测和识别潜在的 FDIA。该算法能够有效提高电力系统对 FDIA 的检测能力，降低网络攻击的风险。

（3）开发了一套基于 Flask 框架的 Web 监控检测系统，该系统集成了 EMS，实现了电力系统参数的高度可视化和实时监控，增强了跨部门协作的能力，提升了电力系统的安全性和可靠性。

（4）通过将仿真结果应用于实际的电力系统环境中，验证了本文提出的检测系统的有效性和实用性，能够应对真实环境中的攻击，具有现实应用价值。

综上所述，本文的研究成果为电力 CPS 的网络安全问题提供了有效的解决方案，对于保障电力系统的安全稳定运行、促进智能电网的健康发展、提高电力系统的韧性和可恢复性具有重要的理论和实践意义。未来的研究可以进一步探索和优化本文提出的模型和算法，以应对不断演变的网络威胁，推动电力 CPS 的工业控制安全防护技术不断进步。

参考文献

[1] Nazeri A ,Biroon R ,Pisu P , et al.Design, Detection, and Countermeasure of Frequency Spectrum Attack and Its Impact on Long Short-Term Memory Load Forecasting and Microgrid Energy Management[J].Energies,2024,17(4):

[2] 吴壮.电力信息物理系统中的虚假数据注入攻击检测[D].兰州理工大学,2023.

[3] 李媛媛. 基于PMU/SCADA量测的智能电网虚假数据攻击检测及防御方法的研究[D].东北大学,2023.

[4] 余飞. 工业网络边界拟态防护关键技术研究及其实现[D].战略支援部队信息工程大学,2022.

[5] Kumar P J ,Subhojit G ,Ebha K , et al.Design of AC state estimation based cyber-physical attack for disrupting electricity market operation under limited sensor information[J].Electric Power Systems Research,2022,205

[6] 伊娜,徐建军,陈月等.电力 CPS 多阶段低代价虚假数据注入攻击方法[J].浙江电力,2023,42(11):39-47.

[7] Huang X ,Qin Z ,Xie M , et al.Defense of Massive False Data Injection Attack via Sparse Attack Points Considering Uncertain Topological Changes[J].Journal of Modern Power Systems and Clean Energy,2022,10(06):1588-1598.

[8] Cao J ,Wang D ,Qu Z , et al.A Novel False Data Injection Attack Detection Model of the Cyber-Physical Power System[J].IEEE Access,2020,895109-95125.

[9] 郭丽,孙华.基于K-means和支持向量机SVM的电力数据通信网络流量分类方法[J].网络安全技术与应用,2024,(04):64-66.

[10] Pinceti A ,Sankar L ,Kosut O .Generation of synthetic multi-resolution time series load data[J].IET Smart Grid,2023,6(5):492-502.

[11] 吴铭辉,高文根,华峰等.基于最大似然估计的智能电网 FDIA 检测[J].四川轻化工大学学报(自然科学版),2023,36(02):38-45.

[12] Y. R ,Kiran T .Detection and reconstruction of measurements against false data injection and DoS attacks in distribution system state estimation: A deep learning approach[J].Measurement,2023,210

[13] Khare G ,Mohapatra A ,Singh S .A Real-Time Approach for Detection and Correction of False Data in PMU Measurements[J].Electric Power Systems Research,2021,191106866-.

[14] Shen Y ,Qin Z .Detection, differentiation and localization of replay attack and false data injection attack based on random matrix.[J].Scientific report,2024,14(1) :2758-2758.

[15] 杨玉泽,刘文霞,李承泽等.面向电力 SCADA 系统的 FDIA 检测方法综述[J].中国电机工程学报,2023,43(22):8602-8622.

[16]李中伟,佟为明,金显吉.智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J].电力系统自动化,2016,40(08):147-151.
[17]吴壮.电力信息物理系统中的虚假数据注入攻击检测[D].兰州理工大学,2023.
[18]曹戈.信息物理融合下微电网运行评估及控制研究[D].东南大学,2021.
[19]Mews S, Langrock R, Ötting M, et al. Maximum approximate likelihood estimation of general continuous-time state-space models[J]. Statistical Modelling, 2024, 24(1): 9-28.
[20]王立达,韩成浩,陈冠文.卡尔曼滤波在农电网系统中的研究分析[J].农业与技术,2022,42(12):46-49.
[21]吴小凤,王天淼,朱文秀.基于 Flask 框架的监控平台可视化设计研究[J].工业控制计算机,2024,37(03):90-91.
[22]刘密富.基于 PowerBI 构建数字化共享平台的应用[J].云南水力发电,2023,39(09):339-341.
[23]范蓝志. 网络化控制系统虚假数据注入攻击的设计与检测[D].北方工业大学,2022.
[24]Shengda W ,Mingming Z ,Danni L , et al.Attack and Protection Technology of Intelligent Terminals for New Energy Internet Transmission, Transformation, and Distribution[J].Journal of Control Science and Engineering,2022,2022
[25]应君裕,李凡,温兵兵,等.电力客服聊天机器人知识库快速更新方法研究[J].计算机产品与流通,2020(06):85.
[26]吕中梁,韦化,祝云,等.EMS 高级应用微服务 Web 架构[J].电力系统及其自动化学报,2019,31(05):33-41.
[27]Pinceti A ,Sankar L ,Kosut O .Detection and Localization of Load Redistribution Attacks on Large-scale Systems[J].Journal of Modern Power Systems and Clean Energy,2022,10(02):361-370.
[28]H. Li, J. H. Yeo, A. L. Bornsheuer and T. J. Overbye, “The Creation and Validation of Load Time Series for Synthetic Electric Power Systems,” in IEEE Transactions on Power Systems, vol. 36, no. 2, pp. 961-969, March 2021.
[29]孟梅,李凤刚,曹红艳,等.发动机传感器执行器检测仪设计[J].内燃机与配件,2023,(20):38-40.

致 谢

在我完成这篇论文的过程中，有许多人给予了我无私的帮助和支持。在此，我想向他们表达我最真挚的感谢。

首先，我要感谢我的导师高新成教授，他博学多才、亲切友善、严谨治学、思维敏捷、热爱知识、做事踏实、能力超群，给我留下了深刻的印象。在撰写论文的过程中，他耐心地指导我，帮助我梳理思路、优化结构，并给出了许多宝贵的学术建议。他的指导与教诲让我受益无穷，使我在学术上取得了显著的进步。

其次，我要感谢我的家人。他们是我生命中最重要的人，是我坚强的后盾。在我写作论文的过程中，他们给予了我无尽的关爱和支持，让我能够全身心地投入到研究中。感谢他们在我遇到困境时给予的鼓励，让我坚定信心，勇往直前。

感谢我所在东北石油大学以及高新成教授所带领的实验室团队的优良学术环境，为我提供了广阔的学习和研究平台。感谢江添艺，李林旭，王晨旭等实验室的同学们，他们为我提供了珍贵的想法和宝贵的建议，让我能够顺利地完成论文的撰写。

我还要感谢刘恩光，于佳旭，陈李等同学们朋友们，他们在我本科学习期间给予了我许多帮助。感谢他们在论文写作过程中给予的关心和鼓励，让我在艰难的时刻始终保持信心。此外，感谢他们在我生活中带来的快乐和陪伴，让我在忙碌的学业中得以放松和调整。

最后，我要感谢我自己。在论文写作的过程中，我克服了许多困难和挑战，始终保持热情和专注。感谢自己坚持不懈地追求真理，不断拓展自己的知识和视野。感谢自己在学业上取得的成果，为这个阶段画上了圆满的句号。

在此，再次向所有给予我帮助和支持的人表示衷心的感谢。感谢他们让我在这个充满挑战和机遇的求学路上，不断成长和进步。我将永远怀揣感激之情，继续前行，以东北石油大学为荣，为东北石油大学争光。