同行专家业内评价意见书编号：20240858148

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名： 谢郅炘

学号： 22160003

申报工程师职称专业类别（领域）： 能源动力

浙江工程师学院（浙江大学工程师学院）制

2024年04月01日

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1. 本专业基础理论知识和专业技术知识掌握情况

我在自动化控制与系统安全专业中扎实掌握了相关的基础理论知识和专业技术知识包括控制理论、传感器与执行器技术、系统建模与仿真、嵌入式系统、通信协议、故障诊断与容错控制等方面的内容。控制理论涵盖了从经典PID控制到现代的模型预测控制等各种方法，用于实现对系统行为的精确调节。传感器与执行器技术则涉及了各种传感器的原理及其应用，以及执行器（例如电机、阀门）的控制方法。系统建模与仿真是对实际系统进行抽象化描述和计算机模拟，以便分析系统行为和设计控制策略。嵌入式系统则负责将控制算法实现在实际硬件设备上，要求具备对实时性和稳定性的要求。通信协议保证了系统中各组件之间的信息交换和协同工作。故障诊断与容错控制则是为了保证在系统遭遇故障时能够快速诊断问题并采取措施，确保系统的安全性和稳定性。这些基础知识构成了自动化控制与系统安全这一领域坚实的理论基础。

2. 工程实践的经历

这个项目的目标是设计一个智能水塔水位控制系统，以确保水塔内的水位始终保持在一定范围内，避免“空塔”或“溢塔”的现象。我们选择了超声波传感器作为水位检测装置，具有非接触测量性和准确性。根据水位的变化情况，我们确定了合适的控制策略，例如，当水位过低时，自动开启水泵；当水位过高时，自动关闭水泵，以保持水位在设定范围内波动。在设计过程中，我们遇到了一些挑战，例如超声波传感器设计、温度误差和能量衰减。为了解决这些问题，我们采取了不同精度的传感器、放大器和A/D转换器，利用超声波的非接触测量性和准确性，以及将声学探头安装在自流道进口和出口处，实现自动测量。这个项目的设计和实现过程充满了挑战。

3. 在实际工作中综合运用所学知识解决复杂工程问题的案例

最近，我有幸参与了一个智能物流系统的优化项目。这个项目是由我们的团队负责的，我们的任务是对整个物流系统进行自动化控制与优化。这个系统在运行一段时间后，出现了持续性的故障，导致物料运输效率大幅下降。这个问题引起了我们的高度关注，因为它直接影响到了物流系统的运行效率和企业的生产效益。在分析系统时，我发现这个问题与控制算法和传感器数据异常有关。控制算法是物流系统自动化控制的核心，它决定了物流系统的运行效率和稳定性。而传感器数据则是控制算法的输入，它直接影响到控制算法的运行效果。如果传感器数据异常，那么控制算法的运行效果就会受到影响，从而导致物流系统的运行效率下降。

通过对系统进行全面的分析，我发现了其中的隐含问题。首先，我发现控制算法存在一些不足，这些不足导致了控制算法在处理某些特殊情况时的效果不佳。其次，我发现传感器数据存在一些异常，这些异常导致了控制算法无法准确地判断物流系统的运行状态，从而影响了控制算法的运行效果。为了解决这个问题，我提出了一个解决方案。首先，我对控制算法进行了修改，优化了控制算法在处理特殊情况时的效果。其次，我对传感器进行了校准，优化了传感器数据的准确性。通过这两个步骤，我成功地解决了这个问题，使得物流系统的运行效率得到了显著的提高。

在这个过程中，我深刻体会到了综合运用所学知识解决复杂工程问题的重要性。这不仅包括技术方面的知识，也需要在工程实践中培养对问题的洞察力和分析能力。只有这样，我们才

能在面对复杂的工程问题时，找到问题的根源，提出有效的解决方案，从而提高工程的运行效率和稳定性。这个项目的经验让我深刻理解到，无论是在学习还是在工作中，我们都需要不断地学习新的知识，提高自己的技能，以便能够更好地应对各种复杂的问题。同时，我也认识到，只有通过实践，我们才能真正地理解和掌握所学的知识，才能真正地提高自己的能力。我不仅学到了很多新的知识，也锻炼了自己的能力。

我相信，这次的经历将对我未来的工作和学习产生深远的影响。我将继续努力，提高自己的专业技能和问题解决能力，以便在未来的工程实践中，能够更好地服务于社会，为社会的发展做出更大的贡献。总的来说，这个项目让我深刻体会到了工程实践的重要性和挑战性。通过这个项目，我不仅提高了自己的技术能力，也提高了自己的问题解决能力。我相信，这次的经历将对我未来的工作和学习产生深远的影响。我将继续努力，提高自己的专业技能和问题解决能力，以便在未来的工程实践中，能够更好地服务于社会，为社会的发展做出更大的贡献。

总结而言，通过本专业的学习和工程实践，我不仅深刻理解了自动化控制与系统安全的专业理论知识，同时也在实践中学会了如何综合运用所学知识解决复杂工程问题。这种综合实践锻炼不仅使我对专业有了更深刻的理解，也为未来工作打下了坚实的基础。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】					
1. 公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】					
成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
BitDance: Manipulating UART Serial Communication with IEMI	会议论文	2023年06月15日	The 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2023)	1/4	
一种基于电磁干扰的串口通信操纵方法	发明专利申请	2023年12月04日	申请号：202311642510 4	3/3	已经授权
一种基于功耗检测和电磁干扰的认证业务信任链漏洞注入方法	发明专利申请	2023年12月04日	申请号：202311642509 1	3/3	已经授权

2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 80 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1.2 年（要求1年及以上） 考核成绩： 88 分（要求80分及以上）
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ 申报人签名：谢士郑炘	

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22160003	姓名：谢郅炘	性别：男	学院：工程师学院	专业：电气工程	学制：2.5年
毕业时最低应获：24.0学分	已获得：31.0学分			入学年月：2021-09	毕业年月：2024-03
学位证书号：1033532024602119			毕业证书号：103351202402600345		授予学位：能源动力硕士

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2020-2021学年夏季学期	自然辩证法概论		1.0	76	跨专业课	2021-2022学年秋冬季学期	工程师实践能力训练		4.0	良	专业选修课
2020-2021学年夏季学期	中国特色社会主义理论与实践研究		2.0	87	跨专业课	2021-2022学年冬季学期	研究生英语		2.0	免修	公共学位课
2021-2022学年秋季学期	研究生英语基础技能		1.0	免修	公共学位课	2021-2022学年春季学期	数学建模		2.0	81	专业选修课
2021-2022学年秋季学期	工业互联网系统安全前沿技术		2.0	95	专业学位课	2021-2022学年春夏季学期	中国特色社会主义理论与实践研究		2.0	92	公共学位课
2021-2022学年秋季学期	工业互联网安全系统工程		2.0	92	专业学位课	2021-2022学年夏季学期	近代电磁场		2.0	61	专业选修课
2021-2022学年秋季学期	机器学习		3.0	64	跨专业课	2021-2022学年夏季学期	工业物联网与大数据实践		2.0	89	专业学位课
2021-2022学年冬季学期	工程伦理		2.0	66	公共学位课	2021-2022学年夏季学期	自然辩证法概论		1.0	65	公共学位课
2021-2022学年秋冬季学期	研究生论文写作指导		1.0	85	专业学位课	2023-2024学年秋季学期	数值计算方法		2.0	83	专业选修课

说明：1. 研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2. 备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2024-04-02

221600

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☑优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）：[illegible] 2024年3月31日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办**公室**审核签字（公章）： 年 月 日

RESEARCH-ARTICLE

BitDance: Manipulating UART Serial Communication with IEMI

Authors: Zhixin Xie, Chen Yan, Xiaoyu Ji, Wenyuan Xu Authors Info & Claims

RAID '23: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses • October 2023 • Pages 63–76 • https://doi.org/10.1145/3607199.3607249

Published: 16 October 2023 Publication History

BitDance: Manipulating UART Serial Communication with IEMI

Zhixin Xie
Zhejiang University
Hangzhou, Zhejiang, China
zhixinxie1999@zju.edu.cn

Chen Yan*
Zhejiang University
Hangzhou, Zhejiang, China
yanchen@zju.edu.cn

Xiaoyu Ji
Zhejiang University
Hangzhou, Zhejiang, China
xji@zju.edu.cn

Wenyuan Xu
Zhejiang University
Hangzhou, Zhejiang, China
wyxu@zju.edu.cn

ABSTRACT

Wired serial communication protocols such as UART are widely used in today's IoT systems for their simple connection and good industry ecology. However, due to the simplicity of these protocols, they are vulnerable to attacks that falsify the communication. In this work, we propose the `BitDance` attack that can arbitrarily flip the bits of serial communication without any physical contact utilizing intentional electromagnetic interference (IEMI). We describe the physical process of how electromagnetic interference influences the voltage, build up a model to demonstrate the bit-level control principle of our work, and implement the attack on 6 different sensors with UART, a widely used serial communication protocol. The result shows we can inject bit-level information and disable legitimate communication from the system with a maximum success rate of 45.4% and 100%. Finally, we propose countermeasures to mitigate the impact of this attack.

CCS CONCEPTS

• **Security and privacy → Hardware attacks and countermeasures; Embedded systems security**;

KEYWORDS

Serial communication; IEMI attack; Embedded system

ACM Reference Format:
Zhixin Xie, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. 2023. BitDance: Manipulating UART Serial Communication with IEMI. In *The 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID '23), October 16–18, 2023, Hong Kong, Hong Kong*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3607199.3607249

*Chen Yan is the corresponding author.

RAID '23, October 16–18, 2023, Hong Kong, Hong Kong

ACM ISBN 979-8-4007-0765-0/23/10…$15.00
https://doi.org/10.1145/3607199.3607249

1 INTRODUCTION

Serial communication is the process of sending data sequentially, i.e., one bit at a time. Due to its simple structure, easy implementation, and low cost, it has been widely used to connect devices in the Internet of Things (IoT) and cyber-physical systems (CPS). For example, most sensors, e.g., laser range sensors, carbon dioxide gas sensors, infrared temperature sensors, and weight pressure sensors, adopt serial communication to transmit data to controllers. As one of the most fundamental communication methods, the trustworthiness of the transmitted data on serial communication is critical to the normal functioning of IoT and CPS. However, the security of serial communication has not received due attention. Many existing studies focused on the security of data before the communication, e.g., whether the data from sensors reflects the environment situation correctly or whether sensors transmit the correct data to other units [31][33][23][22][29][25][28].

Our motivation in this work is to investigate the research question of to what extent can an attacker falsify and manipulate the information transmitted in serial communication without any physical contact. In specific, we wonder whether it is feasible to accurately control every bit of the data transmission, i.e., flipping "1" to "0" and "0" to "1" arbitrarily at the attacker's will. Like any other communication methods, serial communication can also be influenced by external environment factors like electromagnetic interference (EMI in short) [3][17][16]. In addition to unintentional interference, we believe EMI can also become one of the attacker's means as it can affect the operation of the communication system without contact, which is beneficial to the concealment of the attack. However, at the first glance, the impact of EMI on serial communication seems to be largely unpredictable as the signal dissipates and changes rapidly with distance, hence it may be difficult to be exploited for the bit-level targeted attack against the wired protocol. Though the feasibility of EMI attack on serial communication has been verified before [3][6][20], to the best of our knowledge and as we elaborate in Section 2, there has been no published EMI attack that can manipulate arbitrary bits on the serial communication lines at a distance without any physical contact.

In this paper, we propose the BitDance, an EMI-based attack that can flip arbitrary bits and manipulate the content of the serial communication without any contact with the victim wires. The core idea is to use electromagnetic radiation to change the voltage of the signal line and then exert influence on every bit of the transmission. In specific, we design the attack against UART (Universal asynchronous receiver-transmitter), which is one of the most used serial

1. BitDance: Manipulating UART Serial Communication with IEMI

Accession number: 20234515025508
Authors: Xie, Zhixin (1); Yan, Chen (1); Ji, Xiaoyu (1); Xu, Wenyuan (1)
Author affiliation: (1) Zhejiang University, Zhejiang, Hangzhou, China
Corresponding author: Yan, Chen(yanchen@zju.edu.cn)
Source title: ACM International Conference Proceeding Series
Abbreviated source title: ACM Int. Conf. Proc. Ser.
Part number: 1 of 1
Issue title: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2023
Issue date: October 16, 2023
Publication year: 2023
Pages: 63-76
Language: English
ISBN-13: 9798400707650
Document type: Conference article (CA)
Conference name: 26th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2023
Conference date: October 16, 2023 - October 18, 2023
Conference location: Hong Kong, China
Conference code: 193555
Sponsor: Blocksec Inc.; KAUST; Resilient Computing and Cybersecurity Center (RC3)
Publisher: Association for Computing Machinery
Abstract: Wired serial communication protocols such as UART are widely used in today's IoT systems for their simple connection and good industry ecology. However, due to the simplicity of these protocols, they are vulnerable to attacks that falsify the communication. In this work, we propose the BitDance attack that can arbitrarily flip the bits of serial communication without any physical contact utilizing intentional electromagnetic interference (IEMI). We describe the physical process of how electromagnetic interference influences the voltage, build up a model to demonstrate the bit-level control principle of our work, and implement the attack on 6 different sensors with UART, a widely used serial communication protocol. The result shows we can inject bit-level information and disable legitimate communication from the system with a maximum success rate of 45.4% and 100%. Finally, we propose countermeasures to mitigate the impact of this attack. © 2023 Copyright held by the owner/author(s).
Number of references: 34
Main heading: Signal interference
Controlled terms: Electromagnetic pulse - Electromagnetic wave interference - Embedded systems - Network protocols
Uncontrolled terms: Bit level - Control principle - Embedded-system - Intentional electromagnetic interference attack - Intentional electromagnetic interferences - Physical contacts - Physical process - Serial communications - Serial communications protocols - Simple connections
Classification code: 701 Electricity and Magnetism - 711 Electromagnetic Waves - 716.1 Information Theory and Signal Processing
Numerical data indexing: Percentage 1.00E+02%, Percentage 4.54E+01%
DOI: 10.1145/3607199.3607249
Funding Details: Number: 61925109,62071428,62201503,62222114, Acronym: NSFC, Sponsor: National Natural Science Foundation of China;
Funding text: We appreciate the anonymous reviewers'valuable comments. This work is supported by China NSFC Grant 62222114, 62201503, 61925109, and 62071428.
Compendex references: YES
Database: Compendex
Data Provider: Engineering Village

国 家 知 识 产 权 局

310013

浙江省杭州市西湖区古墩路 701 号紫金广场 C 座 1506 室 杭州求是专利事务所有限公司

万尾甜(0571-87911726-819)韩介梅(0571-87911726)

发文日：

2023 年 12 月 04 日

申请号：202311642509.1　　**发文序号：**2023120400754440

专 利 申 请 受 理 通 知 书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日等信息通知如下：

申请号：2023116425091

申请日：2023 年 12 月 04 日

申请人：浙江大学

发明人：徐文渊,冀晓宇,谢郅炘

发明创造名称：一种基于功耗检测和电磁干扰的认证业务信任链漏洞注入方法

经核实，国家知识产权局确认收到文件如下：

权利要求书 1 份 2 页,权利要求项数 ： 7 项

说明书 1 份 4 页

说明书摘要 1 份 1 页

专利代理委托书 1 份 2 页

发明专利请求书 1 份 4 页

实质审查请求书 文件份数：1 份

申请方案卷号：万-231-271-李

提示：

1.申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。

2.申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。

审 查 员：自动受理

联系电话：010-62356655

审查部门：初审及流程管理部

国家知识产权局 专利审查业务章 1101081359734

200101 纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收

2022.10 电子申请，应当通过专利业务办理系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

国 家 知 识 产 权 局

310013

浙江省杭州市西湖区古墩路 701 号紫金广场 C 座 1506 室 杭州求是专利事务所有限公司

万尾甜(0571-87911726-819)韩介梅(0571-87911726)

发文日：

2023 年 12 月 04 日

申请号：202311642510.4　　**发文序号：**2023120400754580

专 利 申 请 受 理 通 知 书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日等信息通知如下：

申请号：2023116425104
申请日：2023 年 12 月 04 日
申请人：浙江大学
发明人：徐文渊,冀晓宇,谢郅炘
发明创造名称：一种基于电磁干扰的串口通信操纵方法
经核实，国家知识产权局确认收到文件如下：
权利要求书 1 份 1 页,权利要求项数 ： 2 项
说明书 1 份 3 页
说明书摘要 1 份 1 页
专利代理委托书 1 份 2 页
发明专利请求书 1 份 4 页
实质审查请求书 文件份数：1 份
申请方案卷号：万-231-270-李

提示：

1.申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。

2.申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。

审 查 员：自动受理
联系电话：010-62356655

审查部门：初审及流程管理部

国家知识产权局 专利审查业务章 1101081359734

200101 纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收
2022.10 电子申请，应当通过专利业务办理系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。