Jiayang Song

Ph.D. Candidate · University of Alberta

9211 116 ST NW, Edmonton, AB, T6G 1H9, Canada

+1 226 374 9761 | jiayang.song@ieee.org | jiayangsong.me

Research Interests

- Software Engineering
- Cyber-Physical System
- Safety and Quality Assurance
- Trustworthy AI System
- Foundation Model
- Embodied Agent

Work Experience

Graduate Research Assistant Fellowship — *University of Alberta*

Advisors: Prof. Lei Ma — *01.2022 - Current*

- Quality and Safety Assurance for AI System Engineering
- Software Engineering Methodology for Trustworthy Foundation Model
- University research projects/grants: FES, MIF-RCES, Amii-Rap
- Industrial collaboration projects: Nvidia, TIER IV

NSERC Research Program — *Western University*

Advisor: Prof. Mehrdad R. Kermani — *04.2018 - 09.2018*

- Kinematic model design and construction for robotic arms
- Testing and evaluation for Magnetorheological clutches
- Magnetic field sensor network design and construction

Education

University of Alberta — *Edmonton, Canada*

Ph.D., Electrical and Computer Engineering — *01.2022 - 05.2025*

- Area of Interest: Software Engineering and Intelligent System
- Thesis: Quality Assurance for Trustworthy AI-enabled Cyber-Physical System
- Advisor: Prof. Lei Ma

University of Toronto — *Toronto, Canada*

M.Eng, Electrical and Computer Engineering — *09.2019 - 06.2021*

- Graduate with distinction
- Specialization: Deep Reinforcement Learning, Data Science

Western University — *London, Canada*

B.Eng, Electrical and Computer Engineering — *09.2015 - 04.2019*

- Graduate with distinction
- Specialization: Control System, Wireless Communication
- Dean's Honor List 2017, 2018, 2019

Research Projects and Collaborations

Foundational Models for Autonomous Driving System — *University of Alberta*

Advisor: Prof. Lei Ma — *2024 - Current*

- Collaboration with TIER IV, Tokyo, Japan
- Exploring the potential of Multimodal Foundation Model-driven autonomous driving systems
- Developing novel frameworks for ADS scenario understanding, annotation and prediction

Quality and Safety Assurance for Autonomous Driving Systems *University of Alberta*

Advisor: Prof. Lei Ma *2024 - Current*

- Collaboration with Autoware Foundation, Japan
- Developing an automated testing method for Autoware Software and simulator
- Designing system level testing criteria and reliability assessment through fault injection

AI-enabled Resilient Grid for Clean Energy Integration *University of Alberta*

Advisors: Assoc. Prof. Lei Ma, Prof. Yunwei Ryan Li, Prof. Robert Benkoczi *2024 - Current*

- Major Innovation Fund - Resilient and Clean Energy Systems Initiative (MIF-RCES)
- Investigating software-defined modelling for resilient grid via digital twin techniques
- Developing testing and validation frameworks for AI-enabled energy systems

Application of Foundation Models in Robotics with Safety Assurance *University of Alberta*

Advisors: Prof. Lei Ma *2023 - Current*

- Investigating the best practice of LLM-empowered embodied agent
- Adapting LLMs for both robotics development and operation

Trustworthiness Assurance and Engineering for AI-enabled Cyber-physical Systems *University of Alberta*

Advisors: Prof. Lei Ma *2023 - 2024*

- Alberta machine intelligence institute (Amii) Research Allocation Panel
- Developed runtime safety measurement and prediction methods for AI-CPS across domains
- Conducted empirical studies to identify the simulation-to-reality gap in the deployment phase of AI-CPS

Model-based Analysis and Testing Guidance for Autonomous Driving System *University of Alberta*

Advisors: Prof. Lei Ma *2023 - 2024*

- Industry collaboration
- Developed a model-based ADS test case selection framework
- The designed framework has been applied and validated on real ADS development

Safety and Reliability Assurance of Next Generation AI-enabled Cyber-Physical Systems for Energy Systems *University of Alberta*

Advisors: Prof. Lei Ma, Prof. Petr Musilek *2022 - 2024*

- University research project: Future Energy Systems (FES)
- Developed safety enhancement and monitoring frameworks for AI-CPSs across various application domains
- Designed two automated repair techniques for AI controllers

Benchmarking and Evaluating AI-enabled Cyber-Physical Systems for Robotic Manipulation *University of Alberta*

Advisors: Prof. Lei Ma *2022 - 2023*

- Collaboration with NVIDIA AI Tech Centre, Singapore
- Developed a benchmark and a testing framework for AI-CPSs in robotic manipulation using NVIDIA Isaac Sim
- Conducted performance and safety analysis for AI-CPSs in diverse robotic manipulation tasks

Mentoring

2022	**Jiaxuan Peng**, Master's thesis	*University of St Andrews*
2023	**Atsuhiro Matuyama**, Bachelor's thesis	*The University of Tokyo*
2023	**Ryosuke Miyake**, Bachelor's thesis	*The University of Tokyo*
2023	**Soma Sugihara**, Bachelor's thesis	*The University of Tokyo*
2024	**Yahan Gu**, Research Internship	*The University of British Columbia*

Teaching Experience

Winter 2025 Winter 2024 Winter 2023	**Exploring Software Development Domains**, Teaching Assistant *- Undergraduate course (approx. 60 participants per semester)* *- Advanced software engineering concepts using Rust* *- Support lectures and provide supervision to students*	*University of Alberta*
Fall 2023	**Analog Electronics**, Teaching Assistant *- Bachelor's course (approx. 300 participants per semester)* *- Circuit design with feedback topologies and amplifiers* *- Support lectures and provide supervision to students*	*University of Alberta*
Fall 2024	**Introduction to Digital Logic Design**, Teaching Assistant *- Bachelor's course (approx. 250 participants per semester)* *- Introduction to computer-aided design and simulation tools for digital design and implementation* *- Provide supervision to students*	*University of Alberta*
Fall 2024 Winter 2024 Winter 2023	**Fundamentals of Electrical Engineering**, Teaching Assistant *- Bachelor's course (approx. 300 participants per semester)* *- Physical concepts of passive circuit elements, Kirchhoff's laws and DC circuit equations*	*University of Alberta*
Fall 2020	**Sensory Cybernetics**, Teaching Assistant *- Graduate course (approx. 30 participants per semester)* *- Theoretical foundations of the senses from both a systems and a neurophysiological point of view*	*University of Toronto*

Professional Activities

Talks

- **Invited Talk** at *University of Alberta @ Guest Lecture, Edmonton, Canada (2023-2024)*
  - Topic: Quality Assurance for AI-enabled Cyber-Physical Systems
- **Invited Talk** at *East China Normal University, Shanghai, China (2023)*
  - Topic: AI-enabled Cyber-Physical Systems and Software Foundation
- **Invited Talk** at *44th International Conference on Software Engineering (ICSE 2022), May 2022*
  - Topic: When cyber-physical systems meet AI: A benchmark, an evaluation, and a way forward

Reviewer

- IEEE Transactions on Software Engineering (TSE)
- Empirical Software Engineering (EMSE)
- International Journal of Human-Computer Interaction (IJHCI)
- IEEE Transaction on Reliability (ToR)
- IEEE International Conference on Robotics and Automation (ICRA)
- Conference on Neural Information Processing Systems (NeurIPS), 2024
- International Conference on Artificial Intelligence and Statistics (AISTATS)
- International Conference on Learning Representations (ICLR)
- International Conference on Machine Learning (ICML)
- Annual AAAI Conference on Artificial Intelligence (AAAI)

Peer-reviewed Publications

Journal

Jiayang Song, Xuan Xie, and Lei Ma. SIEGE: A Semantics-Guided Safety Enhancement Framework for AI-enabled Cyber-Physical Systems. (TSE 2023, CORE Rank A*)

Yuheng Huang, **Jiayang Song**, Zhijie Wang, Huaming Chen and Lei Ma. Look Before You Leap: An Exploratory Study of Uncertainty Measurement for Large Language Models. (TSE 2024, CORE Rank A*))

Da, Song, Xuan Xie, **Jiayang Song**, Derui Zhu, Yuheng Huang, Felix Juefei-Xu, and Lei Ma. LUNA: A Model-Based Universal Analysis Framework for Large Language Models. (TSE 2023, CORE Rank A*)

Zhehua Zhou, Xuan Xie, **Jiayang Song**,Zhan Shu and Lei Ma. GenSafe: A Generalizable Safety Enhancer for Safe Reinforcement Learning Algorithms Based on Reduced Order Markov Decision Process Model. (TNNLS, 2024)

Conference

Jiayang Song, Yuheng Huang, Zhehua Zhou and Lei Ma. Multilingual Blending: LLM Safety Alignment Evaluation with Language Mixture. (NAACL Findings 2025)

Jiayang Song, Deyun Lyu, Zhenya Zhang, Zhijie Wang, Tianyi Zhang, and Lei Ma. When cyber-physical systems meet AI: a benchmark, an evaluation, and a way forward. (ICSE 2022, CORE Rank A*)

Zhehua Zhou, **Jiayang Song(equal contribution)**, Xuan Xie, Zhan Shu and Lei Ma. Towards Building AI-CPS with NVIDIA Isaac Sim: An Industrial Benchmark and Case Study for Robotics Manipulation. (ICSE 2024, Core Rank A*)

Zhou, Zhehua, **Jiayang Song**, Kunpeng Yao, Zhan Shu, and Lei Ma. ISR-LLM: Iterative Self-Refined Large Language Model for Long-Horizon Sequential Task Planning. (ICRA 2024, Core Rank A*)

Zhijie Wang, Zhehua Zhou, **Jiayang Song**, Yuheng Huang, Zhan Shu, and Lei Ma. Towards Testing and Evaluating Vision-Language-Action Models for Robotic Manipulation: An Empirical Study. (FSE 2025, Core Rank A*)

Preprint Manuscript — Under Review

Jiayang Song, Zhehua Zhou, Jiawei Liu, Chunrong Fang, Zhan Shu, and Lei Ma. Self-refined large language model as automated reward function designer for deep reinforcement learning in robotics. (Under Review)

Xuan Xie, **Jiayang Song**, Zhehua Zhou, Fuyuan Zhang and Lei Ma. Mosaic: Model-based Safety Analysis Framework for AI-enabled Cyber-Physical Systems. (Under Review)

Yuheng Huang, **Jiayang Song**, Qiang Hu, Felix Juefei-Xu and Lei Ma. Active Testing of Large Language Model via Multi-Stage Sampling. (Under Review)

Xuan Xie, **Jiayang Song**, Zhehua Zhou, Yuheng Huang, aDa Songnd Lei Ma. Online Safety Analysis for LLMs: a Benchmark, an Assessment, and a Path Forward. (Under Review)

Xuan Xie, **Jiayang Song**, Yuheng Huang, Da Song, Fuyuan Zhang, Felix Juefei-Xu and Lei Ma. LeCov: Multi-level Testing Criteria for Large Language Models. (Under Review)

Renzhi Wang, Zhehua Zhou, **Jiayang Song**, Xuan Xie, Xiaofei Xie and Lei Ma. MORTAR: A Model-based Runtime Action Repair Framework for AI-enabled Cyber-Physical Systems. (Under Review)

Deyun Lyu, **Jiayang Song**, Zhenya Zhang, Zhijie Wang, Tianyi Zhang, Lei Ma, and Jianjun Zhao. AutoRepair: Automated Repair for AI-Enabled Cyber-Physical Systems under Safety-Critical Conditions. (Under Review)

Xiaoning Ren, **Jiayang Song**, Chongyang Liu, Jie Li, Yinxing Xue, Lei Ma. Antidote or Placebo? Unraveling the Efficacy of Neuron Coverage Criteria on Testing Transformer-based Language Models. (Under Review)

Zhijie Wang, Zhehua Zhou, **Jiayang Song**, Yuheng Huang, Zhan Shu, and Lei Ma. LADEV: A Language-Driven Testing and Evaluation Platform for Vision-Language-Action Models in Robotic Manipulation. (Under Review)

Shengming Zhao, Yuheng Huang, **Jiayang Song**, Zhijie Wang, Chengcheng Wan and Lei Ma. Towards Understanding Retrieval Accuracy and Prompt Quality in RAG Systems. (Under Review)