Jiayang Song

1104-10045 111 St, Edmonton, AB, Canada

(+1) 226 374 9761 | jiayang.song@ieee.org | December 11, 1995 | jiayangsong.me

Research Interests

Cyber-Physical System, Software Engineering, Large Language Model, AI System Engineering, Robotic Manipulation

Education

University of Alberta *Edmonton, Canada*

Ph.D. student in Electrical and Computer Engineering *Jan 2022 - Present*

- Research Assistant
- FES Highly Qualified Personnel
- **Area of Interest:** Software Engineering and Intelligent Systems

University of Toronto *Toronto, Canada*

M.Eng in Electrical and Computer Engineering *Sept 2019 - Nov 2021*

- Graduated with Distinction
- **Specialization:** Data Science, Cloud Computing, Deep Learning

Western University *London, Canada*

B.Eng in Electrical and Computer Engineering *Sept 2015 - Apr 2019*

- Graduated with Distinction
- Dean's Honor List 2017, 2018, 2019

Research Experience

Momentum Lab *Edmonton, Canada*

Research Assistant | University of Alberta *June 2021 - Present*

- Quality, Safety and Security Assurance for AI System Engineering.
- Automated Analysis, Testing, Repairing and Enhancement Techniques for AI-enabled systems.
- Cyber-Physical Systems and Robotic Control, e.g., Testing and Analysis of Autonomous Vehicles, power and energy systems, etc.
- Specifications-oriented measurements and AI controllers to estimate and improve the reliability of the AI module.

Robotics & Mechatronics Systems Lab *London, Canada*

Research Assistant | Western University *Sept 2018 - Apr 2019*

- Control system design for a 5-DOF Magnetorheological manipulator.
- Kinematic and dynamic model construction for the robotic arm. Simulation-based testing for safety and reliability purposes.
- Mechanical modelling with SolidWorks for 3D printing.
- Embedding system development for Magnetorheological clutches.

NSERC Research Program *London, Canada*

Research Intern | Western University *Apr 2018 - Sept 2018*

- Investigating magnetic field sensing performance for digital and analog sensors for a Magnetorheological clutch.
- Sensor communication and fusion network design with UART communication protocol.
- RS232 interface development in modules, including initialization, transmitting, receiving, decoding and execution module.
- PCB design and soldiering. Clutch assembly and repair.

Publications

- **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*)
- **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*)
- **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)
- **Jiayang Song**, Yuheng Huang, Zhehua Zhou and Lei Ma. Multilingual Blending: LLM Safety Alignment Evaluation with Language Mixture. (Under Review)
- Zhehua Zhou, **Jiayang Song**, 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*)
- 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*)
- 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**, 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*))
- Yuheng Huang, **Jiayang Song**, Qiang Hu, Felix Juefei-Xu and Lei Ma. Active Testing of Large Language Model via Multi-Stage Sampling. (Under Review)
- 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)
- 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)
- 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. (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)
- 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)

Work Experience

University of Alberta *Edmonton, Canada*

Teaching Assistant *Sept 2022 - Present*

- Presenting the designed technical tutorials in the classroom and assessing the project progress of participants.
- Exams & assignments grading.

University of Toronto *Toronto, Canada*

Teaching Assistant *Sept 2020 - Dec 2020*

- Exams & assignments grading.

Comba Company *Taiyuan, China*

Engineering Assistant *Apr 2017 - Sept 2017*

- Inspecting network stations on site, using an Integrated Plant Control System (IPCS), collected reports regarding excessive vibration of the units, interruptions during phone calls, and reported issues to the production supervisor.
- Close collaboration with the process engineering department to make recommendations based on the units' collected results and day-to-day operations.

Projects

Resilient Grid for Clean Energy Integration *Edmonton, Canada*

Major Innovation Fund | University of Alberta *Sept 2023 - Present*

- Constructing a system-level digital twin for various resilient grids and microgrids, which should identify and bridge the gaps of sim2real.
- A new type of hybrid control framework that traditional controllers and AI-enabled controllers cooperate to deliver beyond performance than any individual can achieve.

Trustworthiness Assurance and Engineering for AI-enabled Cyber-physical Systems *Edmonton, Canada*

Amii Research Allocation Panel | University of Alberta *Apr 2023 - March 2024*

- Test and analysis for quality assurance of AI-CPSs in the development phase.
- Differential test for the simulation-to-reality gap for AI-CPS deployment.

Safety and Reliability Assurance of Next Generation AI-CPS for Energy Systems *Edmonton, Canada*

Future Energy System | University of Alberta *Jan 2022 - April 2024*

- Focusing on the AI modules of CPS in the context of the energy domain and researching a novel falsification/testing framework for safety and reliability issue detection of AI modules.
- Investigating to better understand the advantages and limitations of the traditional software component and AI components in CPS.
- Developing novel methods to enhance and improve the AI modules to reduce safety risks and high energy efficiency by considering both designing new AI algorithms and traditional and AI software fusion methods towards achieving AI-enabled CPS that is safe and high performance.

Canadian CubeSat Project *London, Canada*

Canadian Space Agency | Western University *Sept 2018 - Apr 2019*

- Designing communication subsystem for monitoring and relaying housekeeping data of a Cube satellite.
- Conducting practical tests with a novel imaging system for engineering technology demonstration with the potential to provide virtual reality images.

Service

Journal Reviewer

- IEEE Transactions on Software Engineering (TSE)
- Empirical Software Engineering (EMSE)
- International Journal of Human-Computer Interaction (IJHCI)
- IEEE Transaction on Reliability (TR)

Conference Reviewer

- IEEE International Conference on Robotics and Automation (ICRA)
- Conference on Neural Information Processing Systems (NeurIPS)
- International Conference on Learning Representations (ICLR)
- International Conference on Artificial Intelligence and Statistics (AISTATS))
- International Conference on Machine Learning (ICML)

Skills

Programming	Python, MATLAB, C/C++, SQL
Technical Skills	PCB design, SOLIDWORKS, dSPACE(embedded system), AWS, Linux, Git, LaTeX
Training Programs	Coursera Deep Learning Specialization, Engineering Leadership and Innovation Certificate