Armstrong Foundjem

AI-Based Cybersecurity | Risk Management | Sustainable Software Ecosystems | Trustworthy Safety-Critical AI Systems

Summary

I am an interdisciplinary researcher working at the crossroads of AI trustworthiness of safety-critical systems, AI-based cybersecurity, software ecosystems, and affective computing. My research examines how complex AI systems behave in real-world conditions and how their safety and reliability can be strengthened in practice. I study threat modeling, vulnerability prediction, and socio-technical mitigation strategies to make AI ecosystems more secure and accountable. Drawing on code-intelligence techniques such as AIWare and graph neural networks, I examine the evolving attack surfaces that appear throughout the machine-learning lifecycle and explore methods to build adaptive, resilient defenses. Much of my current work contributes to AI assurance, benchmark reliability, and the design of cyber-resilient infrastructures, aiming to create frameworks that make intelligent systems more interpretable, governable, and sustainable. As a core contributor to MLCommons, I continue to promote inclusive, transparent, and globally aligned AI innovation. I completed my Ph.D. in Computing at Queens University (2022) under the supervision of Prof. Bram Adams.

Education

2018–2022 **Ph.D. in Computing**, *Queen's University*
Thesis: *"Software Ecosystem Sustainability: A Socio-Technical Perspective"*

2015–2017 **M.A.Sc. in Computer Engineering – Data Science**, *Polytechnique Montreal*
Thesis: Improving reliability of live migration operations in clouds.

2012–2015 **B.Sc. in Computer Science**, *Bishop's University*

2004–2006 **Advanced Diploma in Micro-Electronics**, *City & Guilds of London Institute, U.K*
Completed comprehensive studies in micro-electronics design, system integration, and testing.

2001–2003 **Licentiate in Electrical Engineering**, *City & Guilds of London Institute, UK*
Micro-electronics and control engineering.

Awards and Scholarships

Awards

2025 **Designated Top Reviewer – NeurIPS 2025**

Scholarships

2018–2022 **Doctoral Studies (Polytechnique Montréal $\Longrightarrow \mathcal{P}$, Queen's University $\Longrightarrow \mathcal{Q}$)**
Graduate Fellowship/Scholarship, $\mathcal{Q}$: $21.5K, **Fondation Universitaire**, $\mathcal{P}$: $57K, **Pierre Arbour Foundation**, $\mathcal{P}$: $32K

2015–2017 **Master's Studies**
Fondation Universitaire, $\mathcal{P}$: $34K, **Pierre Arbour Foundation**, $\mathcal{P}$: $18K

Publications

2025

- ✍ **"Risk Management for Mitigating Benchmark Failure Modes: BenchRisk"** Sean McGregor, Vassil Tashev, *Armstrong Foundjem*, Aishwarya Ramasethu, Chris Knotz, Heather Frase, Kongtao Chen. *NeurIPS Conference paper*, 2025, Accepted.
- ✍ **DEpendable and ExpLainable Learning: from Research to Industry** Grégory Flandin,*Armstrong Foundjem*, Franck Mamalet, Yann Batiste Pequignot *IEEE – Transaction of AI*, 2025, submitted.
- ✍ **Multi-Agent Threat Assessment for AI-Based systems** *Armstrong Foundjem*, Lionel Tidjon, Leuson Da Silva, Foutse Khomh *TOSEM Journal*, minor revision.
- ✍ **Improving the Robustness of Large Language Models for Code Tasks via Fine-tuning with Perturbed Data** Yang Liu, *Armstrong Foundjem*, Xingfang Wu, Heng Li, Foutse Khomh *TOSEM Journal*, 2025, in progress.

—

- ✍ **Operationalizing Trustworthiness in AI Safety-Critical Systems: A Grounded Theory Approach** *Armstrong Foundjem*, Patrick Foalem, Foutse Khomh, Ahmed E. Hassan *TOSEM Journal*, 2025, in progress.

- ✍ **Automated Software Requirements mining from AI Regulations** Laila Abodinar, *Armstrong Foundjem*, Lina Marsso, Foutse Khomh *TOSEM Journal*, 2025, in progress.

- ✍ **Topology-Aware Cyber Defense: A Federated, LLM-Augmented Multi-Agent System for Adaptive and Explainable Malware Detection** *Armstrong Foundjem*, Foutse Khomh, in progress. *IEEE Transactions on Information Forensics and Security*, in progress.

- ✍ **RAGuardian: Hybrid Quality Assurance for Calibrated Evaluation and Actionable Optimization of RAG Systems** Junyu Huo, *Armstrong Foundjem*, Amine Merzouk, Foutse Khomh. *SANER 2026 Conference*, in progress.

- ✍ **Trustworthy Energy Metrics: Secure, Trace-Backed Benchmarking for HPC and AI Systems** . Laszewski, G.v., Kirkpatrick, C., Luszczek, P., *Foundjem, A.*, Barrett, G., Farrell, G. et al. Nat Mach Intel., in progress

2024

- ✍ **Adversarial Attack Classification and Robustness Testing for Code Generation Models** Yang Liu, **Armstrong Foundjem**, Foutse Khomh, Heng Li *Empirical Software Engineering Journal*, Accepted.

- ✍ **An Empirical Study of Testing Machine Learning in the Wild** Moses Openja, Foutse Khomh, *Armstrong Foundjem*, Zhen Ming (Jack) Jiang, Mouna Abidi, Ahmed E. Hassan *TOSEM Journal*.

2023

- ✍ **Deep Learning Model Reuse in the HuggingFace Community: Challenges, Benefits and Trends** Mina Taraghi, Gianolli Dorcelus, *Armstrong Foundjem*, Florian Tambon, Foutse Khomh *SANER 2023 Conference*, Rank A.

- ✍ **A Grounded Theory of Cross-community SECOs: Feedback Diversity vs. Synchronization** *Armstrong Foundjem*, Ellis E. Eghan, Bram Adams *TSE Journal*, Impact factor: 9.9.

2022

- ✍ **Software Ecosystem Sustainability, a Socio-Technical Perspective** *Armstrong Foundjem* *Ph.D. Thesis* , Queens Graduate Theses and Dissertations.

- ✍ **A Mixed-methods Analysis of Micro-collaborative Coding Practices in OpenStack** *Armstrong Foundjem*, Eleni Constantinou, Tom Mens, Bram Adams *Empirical Software Engineering Journal*, Impact factor: 8.41.

2021

- ✍ **Release Synchronization in Software Ecosystems** *Armstrong Foundjem*, Bram Adams *Empirical Software Engineering Journal*.

- ✍ **Onboarding vs. Diversity, Productivity, and Quality: Empirical Study of the OpenStack Ecosystem** *Armstrong Foundjem*, Ellis E. Eghan, Bram Adams *ICSE 2021 Conference*, Rank A*.

- ✍ **An Open Dataset for Onboarding New Contributors: Empirical Study of OpenStack Ecosystem** *Armstrong Foundjem*, Ellis Eghan, Bram Adams *ICSE-Companion 2021 Conference*.

2019

- ✍ **Release Synchronization in Software Ecosystems** *Armstrong Foundjem* *ICSE-Companion 2019 Conference*.

2017

- ✍ **Broadcast vs. Unicast Review Technology: Does It Matter?** Armstrong Foundjem, Foutse Khomh, Bram Adams *ICST 2017 Conference*, Rank A.

- ✍ **Towards Improving the Reliability of Live Migration Operations in OpenStack Clouds** *Armstrong Foundjem* *Masters Thesis*, Polytechnique Montreal.

Academic Appointments & Professional Experience

Academic Positions

08/22 - 12/25 **Postdoctoral Fellow (Under Prof. Foute Khomh)**, *DEEL Project, Polytechnique Montréal*

- Led research on formal certifiability and robustness of safety-critical AI (Air transportation), producing guidelines mapped to the EU AI Act.
- Designed and ran experiments validating reliability bounds for deep-learning models under distribution shift and adversarial perturbations.
- Supervised and mentored M.A.Sc./Ph.D. students on projects in AI trustworthiness, bias mitigation, and ML cybersecurity.
- Organized and delivered six interdisciplinary workshops on emerging AI regulations and governance best practices.
- Authored quarterly internal reports and peer-reviewed journal articles, disseminating findings to academic, industry, and policy audiences.

2021 **Research Intern**, *Microsoft Research, Redmond, USA*

- Analyzed telemetry from 500K+ developers to identify workflow bottlenecks; implemented feature-usage dashboards with Power BI.
- Built backend data pipelines (Azure Databricks, Spark) to process Git and IDE usage logs for real-time analytics.
- Prototyped LLM-enhanced code-completion metrics to guide IDE UX enhancements.
- Presented findings and demo dashboards to engineering teams and senior leadership.

2015 - 2017 **Research Assistant**, *Polytechnique Montréal*

- Designed experiments to improve live-migration reliability in OpenStack, implementing fault-injection and performance monitoring.
- Developed Python-based orchestration scripts to automate test deployments across heterogeneous clouds.
- Analyzed log data and reported defect patterns, leading to a 25% reduction in migration failures.
- Co-authored two conference papers on cloud resilience and published in IEEE venues.

2014 **Undergraduate Intern**, *LASSENA Research Laboratory, Montréal*

- Optimized black-box vehicle simulator performance by 30% through algorithmic refactoring in C++.
- Led a 4-person agile team, conducting daily standups and sprint planning to adapt to evolving requirements.
- Validated simulator outputs against real-world accident data and documented findings for lab reports.

2013 **Intern**, *META (Facebook) Head Office, California, USA*

- Developed Scala/Python data-processing engines for geo-spatial analytics, handling 10M+ location events per day.
- Integrated services with Cassandra and Kafka for real-time data ingestion and fault tolerance.
- Collaborated with cross-functional teams to define API contracts and performance SLAs.

Industry / Consulting Experience

2025 **Freelance Computational Scientist**, *Independent Consultant*, Remote / Global

- Designed and implemented predictive analytics solutions (time-series forecasting of compute demand), boosting operational efficiency by 10% and cutting carbon emissions by 15%.
- Automated sustainability audits via NLP pipelines (LLMs for code and configuration analysis) and statistical anomaly detection, pinpointing high-impact remediation opportunities aligned with UN SDG 9/12.
- Developed real-time dashboards tracking KPIs (carbon-per-compute-unit, energy intensity), enabling data-driven policy iteration and stakeholder reporting.
- Conducted workshops with C-suite and engineers to translate sustainability metrics into actionable roadmaps.
- Authored client deliverables: technical reports, executive summaries, and RFP responses on carbon-aware AI deployment.
- Active collaboration with the SWAT Lab, under the supervision of Prof. Khomh.

2005 - 2009 **Electrical Engineer**, *Pastel Telecoms S.A., Douala, Cameroon*

- Designed and installed power-monitoring devices for remote base stations, reducing downtime by 20%.
- Engineered low-cost transmission units, cutting operational expenses by 15%.
- Conducted field audits and preventive maintenance planning across 50+ telecom sites.

2001 - 2005 **Consultant**, *Society of Engineers, UK*

- Led collaborative engineering projects with public and private sector clients, drafting technical specifications and standards.
- Facilitated professional development workshops on best practices and emerging engineering regulations.
- Provided strategic consultation on infrastructure planning and compliance with government agencies.

Teaching Experience

2023–2024 **Instructor (G)**, *Polytechnique Montreal*, Inf8102 – Sécurité dans les environnements infonuagiques

- Key concepts: operational safety in cloud computing, identity management, configuration security, incident response, and penetration testing.

  Conducted hands-on tutorials and final projects on cloud security automation and vulnerabilities.

2020–23,24 **Instructor (U4/G)**, *Polytechnique Montreal*, Log8371 – Ingénierie de la qualité en Logiciel

- Topics include software quality assurance, testing, CI/CD pipelines, maintainability, risk management, and performance testing.

  Designed and delivered lectures, quizzes, and final exams on industrial-scale software quality frameworks.

2016–2019 **Teaching Assistant (U3)**, *Polytechnique Montreal*, Log3000 – Software Engineering Processes

- Assisted in teaching software engineering life cycle phases, process evaluation, and empirical analysis of processes.

  Facilitated labs and graded assignments on software development processes and metamodels.

2015–2016 **Teaching Assistant (U4)**, *Polytechnique Montreal*, Log4420 – Conception of Dynamic Websites

- Delivered tutorials on web architecture, HTML5, Node.js, Angular2, and MongoDB databases.

  Supervised projects involving the design and implementation of complex, dynamic web applications.

2015–2016 **Teaching Assistant (U1)**, *Polytechnique Montreal*, Log1000 – Introduction to Software Engineering

- Topics: software development life cycle, configuration management, requirement analysis, and testing.

  Led active learning activities and provided office hours to support students.

Talks & Presentations

2025 **UN Open Source Week, June 16-20, 2025**, United Nations Headquarters, NYC, USA.

Quantifying Trust and Open Metrics for Sustainable & Safe AI: A session introducing an open certification framework to assess and improve the sustainability, fairness, and trustworthiness of open-source AI systems, focusing on supporting resource-constrained regions and promoting global digital equity.

GeoHackers: Despite its transformative potential, UNICEF's GeoSight API remains underutilized due to accessibility issues, opaque documentation for non-technical users, and the absence of turnkey functionality, which hinders actionability. Our solution enhances documentation, facilitates critical functional upgrades, improves offline reliability, and boosts energy efficiency.

2024 **AIware Leadership Bootcamp**, Queen's University, Downtown Toronto Campus, Canada.

Presenting works on (1) Trustworthiness of AI safety-critical systems and (2) Assessment of AI regulation Acts, a case study of the EU AI Act.

Participated in AIWare Leadership hands-on collaborative training sessions.

2023 **ICSE Student Mentoring Workshop (SMeW)**, Melbourne, Australia.

Engaged in mentoring activities, including research guidance and knowledge transfer in software engineering practices.

2017–2019 **Open Infrastructure Upstream Institute Training (Mentor)**, Sydney/Vancouver/Berlin/Shanghai.

Delivered mentorship on contributing to open-source projects, including CI/CD integration and best practices for upstream contributions.

2018–2020 **Software Engineering for Machine Learning Applications (SEMLA) Workshop**, Montreal, Canada.

Participated in discussions on integrating software engineering practices into ML systems, focusing on reliability and scalability.

2015 **Green Code Challenge**, Paris, France.

Achieved 5th place out of 82 teams by developing energy-efficient software solutions for sustainability.

Professional Service

Review Activities

PC Member

- **38/39th Annual Conference on Neural Information Processing Systems (NeurIPS 2024/25)**Datasets and Benchmarks Track, Vancouver, Canada.

- **39th Annual AAAI Conference on Artificial Intelligence (AAAI 2024)** Workshop on Datasets and Evaluators of AI Safety Track. Philadelphia, Pennsylvania, USA

- **47th IEEE/ACM International Conference on Software Engineering (ICSE 2025)** New Ideas and Emerging Results Track (ICSE 2025 NIER), Ottawa, Canada.

—

- **32nd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2025)** Reviewing research papers, Montreal, Canada.
- **Mining Software Repositories (MSR) 2021–2024** Junior PC member – Reviewing research papers.

Reviewer/ Journals

- **Empirical Software Engineering (EMSE)** – Since 2023.
- **ACM Transactions on Software Engineering and Methodology (TOSEM)** – 2025.
- **Journal of Software: Evolution and Process (JSEP)** – Since 2023.
- **Journal of Systems & Software: (JSS)** – 2025.
- **Chair –AI/HPC and Machine Learning, Open Infrastructure Summit (2019–2022)** Oversaw submissions in AI, HPC, and Machine Learning tracks.

Leadership Roles

2019 - 2022 **Track Chair, AI/HPC & ML**, *Open Infrastructure Summit*

- Oversaw call for papers, coordinated 150+ submissions, and managed a 40-member reviewer pool.
- Curated program of 12 sessions, selecting speaker slate and refining abstracts for strategic alignment.
- Liaised with sponsors and community leads to secure funding and technical resources.
- Delivered opening remarks and moderated panel discussions at each biannual summit.

2018 - Present **Mentor & Board Member**, *CHAOSS Project, Linux Foundation*

- Guided 20+ Google Summer of Code contributors on metrics projects, reviewing proposals and code deliverables.
- Served as Ethics Commissioner, drafting community code of conduct updates and leading conflict-resolution sessions.
- Defined key diversity and health metrics; authored white papers adopted by major open-source foundations.
- Organized quarterly community calls and workshops to onboard new contributors and present project roadmaps.

Membership & Certifications

IEEE Senior member

ACM Member

—

ML Vector Institute – University of Toronto

DL IVADO-Mila – University of Montreal

Technical Skills

Critical/Analytical Skills Reasoning about data using AI/ML techniques, Grounded theory, data visualization, and reporting to support decision-making and solve complex problems.

Programming Python, C/C++, Java, JavaScript, Julia, R, SQL, Shell scripting, Haskell, Lisp

DevOps & MLOps AgentWare (MCP), Containers (Docker), K8s, Monitoring and Feedback, automation, and release strategies (Shadow Launches, Blue-green, Rolling Updates), Deploying RAG Systems, Fine-tuning AI Models

Productivity Emacs + Org-mode, LaTeX, Activity/Task management, Scientific and technical writing, Collaborative coding

HPC Running scientific workloads and benchmarking on clusters

Volunteering & Outreach

08/23–08/24 **MLCommons AI Risk & Reliability, and Scientific Working Group**, *Remote*

- Lead of the *"Masakhane"* research project, incorporating African languages into MLCommons benchmarks based on linguistic coverage, evaluator availability, and demographic considerations.
- Defined benchmarks for specific AI use-cases and contributed to scientific analysis on AI safety and carbon footprint discussions.

2016–Ongoing **National/International Judge**, *Youth Science Canada/Canada Wide Science Fair, Canada*

- Evaluated selected scientific projects across diverse disciplines, including AI, machine learning, physics, mathematics, bioinformatics, and robotics.
- Applied critical thinking and analytical skills to assess originality and quality of projects under tight deadlines.
- Chaired teams, collaborating with leading Canadian scientists and professionals.

2020 **Student Volunteer**, *42nd International Conference on Software Engineering (ICSE 2020), Virtual Conference*

- Ensured smooth conference operations by allocating resources and facilitating participants' needs.
- Managed Q&A sessions during presentations to ensure maximum engagement and response rates.
- Coordinated effectively across global time zones.

2016–2018 **Final Projects Evaluation (U4) Engineering**, *McGill University, Montreal, CA*

- Evaluated multi-disciplinary final year undergraduate engineering projects across various fields.
- Assessed project originality, decision-making processes, and scientific rigor.

2017 **Student Volunteer**, *General Assembly and Scientific Symposium of the International Union of Radio Science (URSI-GASS), Montreal, CA*

- Assisted at the front desk registration, significantly reducing wait times for attendees.
- Supported speakers and participants by addressing their needs and facilitating session transitions.

2015 **Team Lead**, *Green Code Challenge, Paris, France*

- Mobilized a team of researchers and students to participate in the international Green Code Challenge.
- Led the development of energy-efficient software solutions, achieving 5th place out of 82 teams.

References

Available upon request