HPS

jonathan.decker@uni-goettingen.de

Dr. Jonathan Decker

AI-Chances and Risks for Research Software Engineers and Scientific Users

Use AI Now Or Be Left Behind

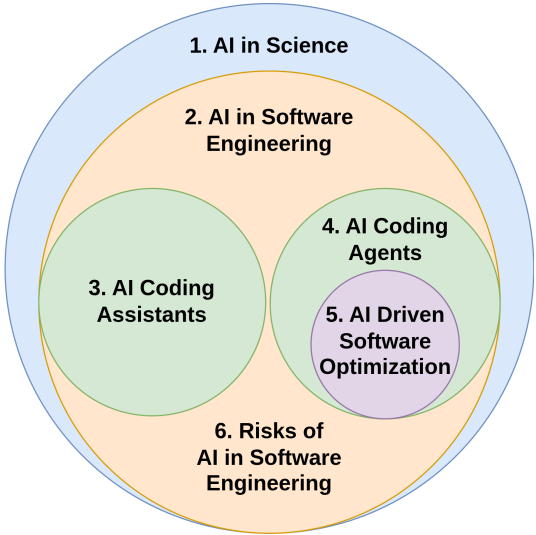
Avoid AI as much as you can, it is unreliable and possibly evil

According to 2025 report by academic publisher Wiley:

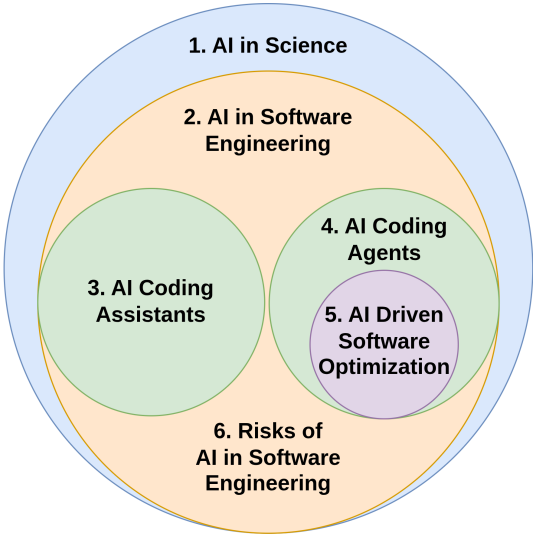
- 84% of scientists use AI in some aspect of their work
- 62% use AI for research or publication
  - Almost half were only "a little" successful in using AI
- 80% have used general-purpose AI tools, e.g., ChatGPT
- 25% have used specialized AI tools for research
  - Most use free AI tools
- 64% are concerned about inaccuracies and hallucinations
- 58% are concerned about information security and privacy
  - Initial peak hype about AI is dying down
- 85% report AI helped in their work efficiency

Wilkins *The More Scientists Work With AI, the Less They Trust It*, 2025
ExplanAItions, 2025

Overview



Overview



What has AI Recently Done for Us?

- Biology
  - AI helps explore biological interactions
  - Not feasible without AI
  - Prediction of molecules to boost drug discovery
  - Powered by Alphafold 3 by Google's Deepmind
- Space
  - AI helps detect anomalies in Hubble telescope data
  - Hundreds of million images
  - Anomalies include galaxies merging or exhibiting unusual shapes
  - ESA self-developed AI "AnomalyMatch"

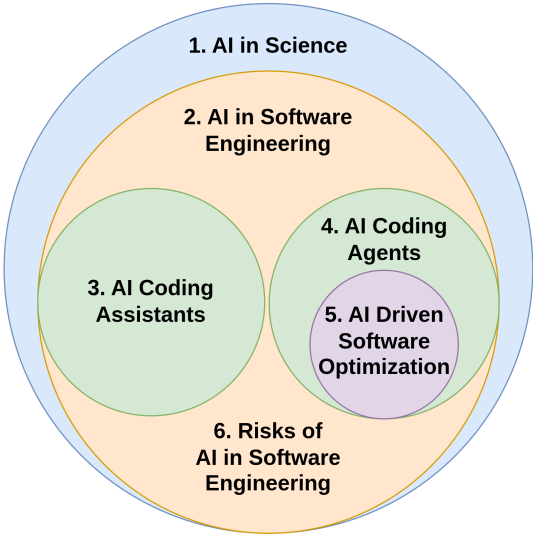
Colter *Artificial Intelligence and Biology*, 2026
AI Unlocks Hundreds of Cosmic Anomalies in Hubble Archive - NASA Science, 2026

More AI Applications in Science

- Medicine
  - AI helps diagnose brain MRI scans
  - Detection accuracy of 97.5% in a few seconds
  - Detects brain hemorrhages, strokes, urgency of treatment
  - Uni Michigan self-developed AI "Prima"
- Physics
  - AI helps calculate thermodynamic properties of atoms
  - Calculations for predicting thermodynamics take up to weeks on HPC systems
  - Determine thermodynamic properties, e.g., high pressure metals and gases
  - Uni New Mexico self-developed AI "THOR"

An AI Model That Can Read and Diagnose a Brain MRI in Seconds | Michigan Medicine, 2026
THOR AI Solves a 100-Year-Old Physics Problem in Seconds, 2026

Overview



Developing with AI

- Software Engineering involves a wide range of tasks
  - Including code generation, defect prediction/detection, planing refactoring
- Code generation commonly via tools such as GitHub Copilot
  - Deepmind's Alphacode excelled in coding challenges
- Defect prediction determines code most likely to contain bugs
  - Said code may then be tested more extensively
- AI tools can identify where best to apply design patterns
  - Recommend refactoring opportunities, e.g., employ Singleton pattern

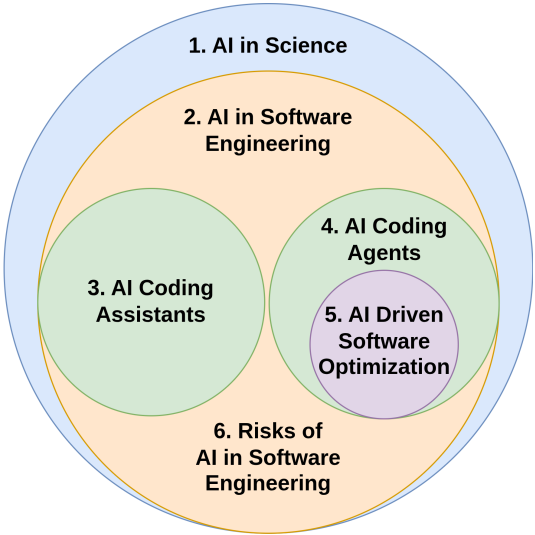
Alenezi and Akour "AI-Driven Innovations in Software Engineering", 2025

Reflect on AI in SE vs Other Fields

A few personal observations:

- SE is a large industry
  - Having better AI tools is an advantage
  - Being better at using AI is an advantage
  - New AI companies promising the best SE tools arise
  - Existing companies have to have an AI strategy
- AI for SE mostly consists of LLMs (or GenAI)
  - Many use cases seen earlier employ analytical AI
  - Reliance on LLMs made by few companies
  - Self-developed AI very rare
- Code generation is by far the biggest concern

Overview



Letting LLMs Help Write the Code

- Two workflows
  - Chat with LLM to generate code snippets, copy paste into code base
  - LLM integrated in IDE auto completes code segments
- Humans are closely involved in both
  - Coder (consciously) touches every code file
- Chat can be with any LLM through chat interface
- Coding assistant requires IDE integration
  - Most popular GitHub Copilot
  - We recommend open source Continue `continue.dev`

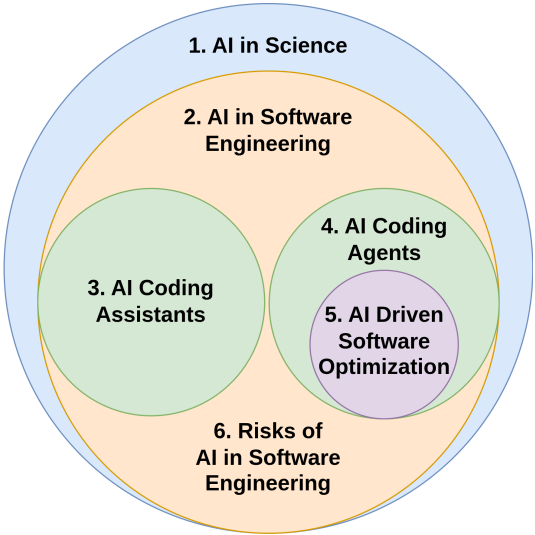
Which AI Coding Tools Do Developers Actually Use at Work?, 2026

Benefits and Harm of Coding Assistants

- Benefits
  - Significantly speeds up development
  - Even enables completing of tasks with unfamiliar languages
- Harm
  - Learning is hindered or even stunted
  - Junior developers fail to learn important coding skills
- Bring care in deploying coding tools, when to allow them

How AI Assistance Impacts the Formation of Coding Skills, 2026

Overview



What People Call Vibe Coding

- Give AI agents access to code base and documentation
  - Tell it what you want and let it run
- Effectively calls LLM in a loop until goal is accomplished
  - AI reads files, plans actions, edits files, executes code and tests
  - Depending on setup, doing so with same permission as user
- Achieving desired goals might take a while
  - Depends on LLM model speed, code base size, task complexity
  - Adding a feature to a medium sized code base might take 30 to 60 min
- Enabled through tools such as Claude Code or OpenCode

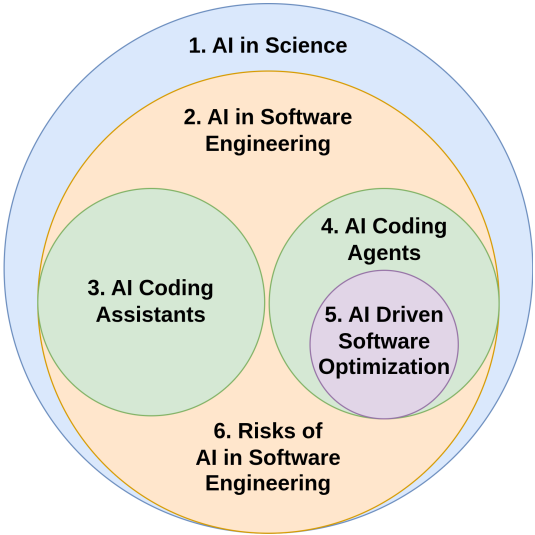
Ray “A Review on Vibe Coding”, 2025

Inside Vibe Coding

- Operate via one or more AI agents
  - Agents take different roles via system prompts and information
  - In background all agents may still use same LLM
- Agents need to manage their context window
  - LLMs have limited capacity (context windows) that can go into a call
  - May run full for larger code bases or when including external knowledge bases
- Different levels of delegation possible
  - Let agents build one feature, check it by hand and commit
  - Let agents build and deploy multiple features
  - Let agents build entire applications from scratch and deploy them

Ray “A Review on Vibe Coding”, 2025

Overview



Code Level Optimization via AI

- Employ AI agents on a code base with metric to optimize
  - Must be possible to test metric automatically
- Let agents analyze code base and hypothesize potential performance upgrades
  - Agents propose a number of potential changes
  - Create a version of code base for each proposed change
  - Build each proposed version and benchmark
- Let agents review benchmark results
  - Keep winners
  - Propose further changes
- Potential tool for this is Karpathy's "autoresearch"

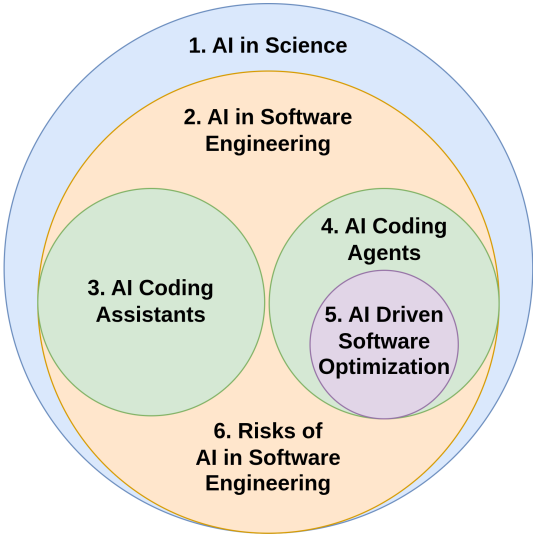
Kim *Research-Driven Agents*, 2026

Example Use Case: llama.cpp

- llama.cpp is a widespread LLM inference engine
- Researchers sought to improve its performance, token generation rate
  - Letting AI agents just run limits them to knowledge of LLM mode
- They included a research stage for the agents
  - Agents search and review project forks, research papers, similar projects
- From over 30 experiments, 5 successfully improved performance metrics
  - Running tests required a farm of cloud VMs to build and run tests
- Overall, 3 h of experiments across 4 VMs to achieve up to 15% performance improvement

Kim *Research-Driven Agents*, 2026

Overview



What could go wrong?

- Security
  - AI code generation may introduce vulnerabilities
  - Without human oversight, vulnerabilities end up in production code
  - Rise in CVEs due to AI code changes
- Rogue Agents
  - AI agents can write code, install dependencies and execute tests
  - Run on workstation, may push credentials, affect files outside of project
  - Install malicious dependencies that infect workstation
- Debugging Nightmares
  - AI agents can quickly generate a lot of code without human insight
  - Debugging a specific issue without knowledge of code base

Wang et al. “AI Code in the Wild”, 2025
Ray “A Review on Vibe Coding”, 2025

Risks to the Industry

- Lack of experience for junior developers
  - Junior developers learn less from using AI
  - Companies replace junior developers with AI
  - Eventually, senior developers retire or move on
  - Then no junior developers to replace them
- Data sovereignty
  - AI providers limited to a few large (mostly US) companies
  - E.g., OpenAI, Anthropic, DeepSeek
  - Companies buy AI services to not fall behind
  - Give up data by using foreign AI services
  - Requires national or at least EU-level effort

How AI Assistance Impacts the Formation of Coding Skills, 2026
Demand for Junior Developers Softens as AI Takes Over, 2025
AI Sovereignty's Definitional Dilemma | Stanford HAI, 2026

Closing Words

- More and more AI tools to explore
  - Empowers individuals to make significant contributions
  - Attempting to optimize a code base can be done in a few days instead of weeks
- Many risks to watch out for
  - Review and understand code changes made by AI
  - Properly jail AI agents, for example, via container
- Keep track of your data
  - Recommendation: Employ GWDG as your AI provider
    `https://kisski.gwdg.de/leistungen/2-02-llm-service`

References I

AI Sovereignty's Definitional Dilemma | Stanford HAI. Feb. 17, 2026. URL: https://hai.stanford.edu/news/ai-sovereigntys-definitional-dilemma (visited on 04/14/2026).

AI Unlocks Hundreds of Cosmic Anomalies in Hubble Archive - NASA Science. Jan. 27, 2026. URL: https://science.nasa.gov/missions/hubble/ai-unlocks-hundreds-of-cosmic-anomalies-in-hubble-archive/ (visited on 04/14/2026).

Alenezi, Mamdouh and Mohammed Akour. "AI-Driven Innovations in Software Engineering: A Review of Current Practices and Future Directions". In: *Applied Sciences* 15.3 (Jan. 28, 2025). ISSN: 2076-3417. DOI: 10.3390/app15031344. URL: https://www.mdpi.com/2076-3417/15/3/1344 (visited on 04/14/2026).

An AI Model That Can Read and Diagnose a Brain MRI in Seconds | Michigan Medicine. Feb. 6, 2026. URL: https://www.michiganmedicine.org/health-lab/ai-model-can-read-and-diagnose-brain-mri-seconds (visited on 04/14/2026).

Colter, James. *Artificial Intelligence and Biology: AI's Potential for Launching a Novel Era for Health and Medicine*. The Conversation. Apr. 8, 2026. DOI: 10.64628/AAM.n6wsmkvmr. URL: https://theconversation.com/artificial-intelligence-and-biology-ais-potential-for-launching-a-novel-era-for-health-and-medicine-275170 (visited on 04/14/2026).

Demand for Junior Developers Softens as AI Takes Over. CIO. Sept. 24, 2025. URL: https://www.cio.com/article/4062024/demand-for-junior-developers-softens-as-ai-takes-over.html (visited on 04/14/2026).

References II

ExplanAItions: Key Findings | Wiley. 2025. URL: https://www.wiley.com/en-us/about-us/ai-resources/ai-study/key-findings/ (visited on 04/14/2026).

How AI Assistance Impacts the Formation of Coding Skills. Jan. 29, 2026. URL: https://www.anthropic.com/research/AI-assistance-coding-skills (visited on 04/14/2026).

Kim, Alex. *Research-Driven Agents: What Happens When Your Agent Reads Before It Codes*. SkyPilot Blog. Apr. 8, 2026. URL: https://blog.skypilot.co/research-driven-agents/ (visited on 04/14/2026).

Ray, Partha Pratim. "A Review on Vibe Coding: Fundamentals, State-of-the-art, Challenges and Future Directions". In: *TechRxiv* 2025.0509 (May 9, 2025). DOI: 10.36227/techrxiv.174681482.27435614/v1. URL: https://www.techrxiv.org/doi/full/10.36227/techrxiv.174681482.27435614/v1 (visited on 04/14/2026).

THOR AI Solves a 100-Year-Old Physics Problem in Seconds. ScienceDaily. Mar. 2026. URL: https://www.sciencedaily.com/releases/2026/03/260315004344.htm (visited on 04/14/2026).

Wang, Bin et al. "AI Code in the Wild: Measuring Security Risks and Ecosystem Shifts of AI-Generated Code in Modern Software". In: (Dec. 21, 2025). DOI: 10.48550/arXiv.2512.18567. arXiv: 2512.18567 [cs]. URL: http://arxiv.org/abs/2512.18567 (visited on 04/14/2026). Pre-published.

References III

Which AI Coding Tools Do Developers Actually Use at Work? | The Research Blog. The JetBrains Blog. Apr. 2, 2026. URL: https://blog.jetbrains.com/research/2026/04/which-ai-coding-tools-do-developers-actually-use-at-work/ (visited on 04/14/2026).

Wilkins, Joe. *The More Scientists Work With AI, the Less They Trust It*. Futurism. Oct. 13, 2025. URL: https://futurism.com/artificial-intelligence/ai-research-scientists-hype (visited on 04/14/2026).