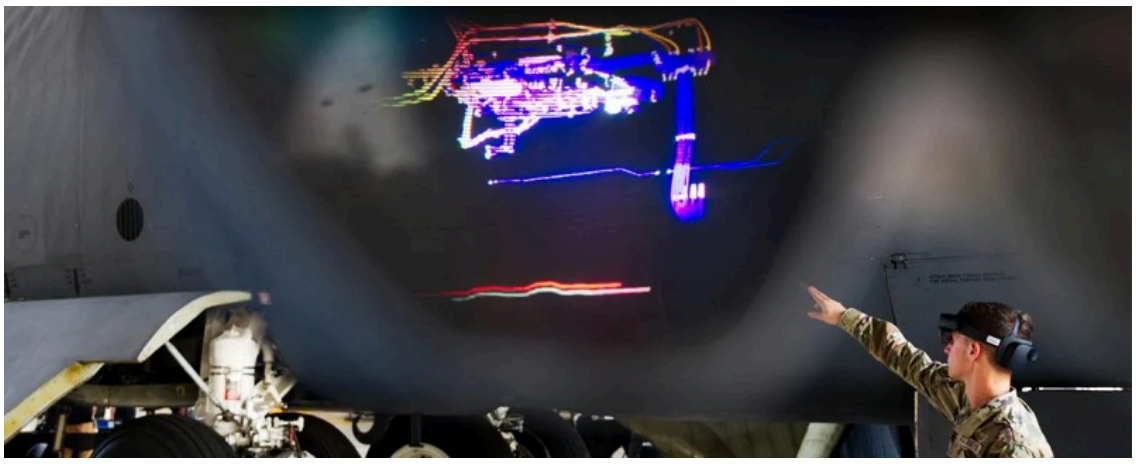
SEI Bulletin 40 years



SEI Tool Helps Determine Causes of AI Bias, Improves AI Trust

July 23, 2025 — Trust in artificial intelligence (AI) robustness is a critical issue as the use of AI classifiers increases in the Department of Defense and across the federal government. A recent Office of Management and Budget memo acknowledged the urgency of monitoring AI for potential adverse effects. The SEI's free AI Robustness (AIR) tool helps agencies meet this critical need by determining the causes of adverse impacts of AI classifiers.

"Powerful AI and machine learning tools are revolutionizing fields of prediction, automation, cybersecurity, intelligence gathering, training and simulation, and object detection, and more. Yet we know there are weaknesses associated with these tools that we must consider," said Anita Carleton, director, SEI Software Solutions Division. "The AIR tool offers insight into not only where AI might go astray, but also why it happens."

Read more »

SEI News

Secure Software by Design 2025 Event Announces Keynote Speakers
The August event will feature speakers with deep industry experience.

Data Exchange Standard Enables Better Insider Incident Research and Practice
Version 1.0 of the standard is the first comprehensive schema for connecting insider incident data.

Software Engineering Institute Marks 40 Years of Innovation and a Renewed Contract with Defense Department
The U.S. Department of Defense has renewed its contract with Carnegie Mellon University to operate the Software Engineering Institute, the only federally funded research and development center focused on advancing software for national security.

See more news »

Latest Blogs

Managing Security and Resilience Risks Across the Lifecycle
This post introduces the Security Engineering Framework, a detailed schema of software-focused engineering practices that acquisition programs can use to manage security and resilience risks across the lifecycle of software-reliant systems.

A Practitioner-Focused DevSecOps Assessment Approach
Aaron Reffett and Timothy A. Chick discuss why regular DevSecOps assessments are necessary to track progress, adapt to evolving needs, and ensure you are consistently delivering value to your end users with speed, security, and efficiency.

See more blogs »

Latest Podcasts

Mitigating Cyber Risk with Secure by Design
SEI CERT Division director Greg Touhill and Matt Butkovic highlight recommendations, built on prior joint efforts by the SEI and the Cybersecurity Infrastructure Security Agency, for making software secure by design.

The Magic in the Middle: Evolving Scaled Software for National Defense
SEI chief technical officer Tom Longstaff discusses the SEI's long-standing work to help the DoD rapidly scale technology including artificial intelligence and autonomous systems.

Making Process Respectable Again: Advancing DevSecOps in the DoD Mission Space
The SEI's Eileen Wrubel and Bill Nichols, with George Lamb of the Department of Defense (DoD), talk about how DevSecOps has become crucial to overall mission success in high-stakes DoD environments where security, efficiency, and speed are critical.

See more podcasts »

Latest Publications

Software Bill of Materials (SBOM) Harmonization Plugfest 2024
This report describes how differences in SBOM generation can result in different SBOM outputs.

What Can Generative AI Red-Teaming Learn from Cyber Red-Teaming?
This paper investigates the applicability of established cyber red-teaming methodologies to the evaluation of generative AI systems, addressing the growing need for robust security assessments in AI-driven applications.

Machine Learning Operations (MLOps) Evaluation Rubric
The MLOps Tool Evaluation Rubric can help acquisition teams identify priorities, evaluate capabilities, and select tools to support ML developers and systems across the ML lifecycle.

See more publications »

Latest Videos

Identifying AI Talent for the DoD Workforce
Eric Keylor, Intae Nam, and Dominic Ross go beyond traditional knowledge and skill assessments as they introduce prototype tools that reveal key information about evaluating talent for AI and data positions.

Model Your Way to Better Cybersecurity
Natasha Shevchenko and Alex Vesey discuss the increasingly important role that Model-Based Systems Engineering can play in creating cybersecurity approaches that match this era of greater, more sophisticated cyber threats.

DevSecOps: See, Use, Succeed
Hasan Yasar, Vaughn Coates, and David Shepard discuss the value of observability in DevSecOps to help system developers understand and perform quality attribute tradeoffs and to gain confidence about system performance.

See more videos »

Upcoming Events

Webcast - Achieving Balance: Agility, MBSE, and Architecture, July 31
Assuring that Agile implementation outcomes meet senior stakeholders' expectations is not a given. In this webcast, Peter Capell addresses the role of a practical vision to meet those expectations, highlighting the value of model-based systems engineering and architecture.

Secure Software by Design 2025, August 19-20, Arlington, Va.
Join thought leaders in secure software by design for presentations and discussions on all aspects of secure software systems development.

Model-Based Systems Engineering (MBSE) in Practice 2025, August 21, Arlington, Va.
Join us to gain practical insights from seasoned MBSE adopters, discover

innovative solutions to common challenges, and shape the future of systems engineering in an increasingly complex world.

Webcast - Quantum Computing Meets High Performance Computing Skills in the Class, August 27
SEI AI researcher Dan Justice and NVDIA senior technical marketing engineer Monica VanDieren assess the university preparation of quantum machine learning students for work in high performance computing environments.

See more events »

Upcoming Appearances

Space and Missile Defense (SMD) Symposium 2025, August 5-7, Huntsville, Ala.
Visit the SEI at booth E106.

AFCEA TechNet Augusta 2025, August 18-21, Augusta, Ga.
Visit the SEI at booth T825.

AFA Air Space Cyber Conference 2025, September 22-24, National Harbor, Md.
Visit the SEI at booth 116.

See more opportunities to engage with us »

Upcoming Training

Software Architecture Design and Analysis
August 12-15 (Live Online)

Designing Modern Service-Based Systems
August 11 (Live Online)

E-learning - CERT Artificial Intelligence (AI) for Cybersecurity Professional Certificate

E-learning - Introduction to Artificial Intelligence (AI) Engineering

E-learning - Effective Communication of Technical Concepts

See more courses »

Employment Opportunities

Senior Embedded Software Engineer

Technical Lead

Embedded Software Engineer - Alabama

All current opportunities »

Carnegie Mellon University
Software Engineering Institute