

SEI Bulletin

Trouble reading this email? [View in browser.](#)



New Tool Detects Mismatches in Machine Learning System Development

February 15, 2023—The SEI recently released a new tool to help software developers better integrate machine learning (ML) components into software systems. Developers can use the [TEC ML Mismatch Detection Tool](#) to identify disruptive disagreements among stakeholders' assumptions about ML components.

"As the Department of Defense adopts machine learning to solve mission-critical problems, the inability to detect and avoid machine learning mismatch creates delays, rework, and failure in the development, deployment, and evolution of these systems," said Grace Lewis, SEI principal researcher, Tactical and AI-Enabled Systems (TAS) Initiative lead, and lead of the SEI's ML mismatch research.

[Read more »](#)



[New Tool Detects Mismatches in Machine Learning System Development](#)

The TEC ML Mismatch Detection Tool aims to reduce delays and rework in software development projects by helping developers align their assumptions about machine learning components.

[ISHPI AIS Division to Receive IEEE CS/SEI Humphrey Software Quality Award](#)

The group's decades of dedication to software quality earned it the 2023 award.

[See more news »](#)



[Play it Again Sam! or How I Learned to Love Large Language Models](#)

Jay Palat explores what new advancements in AI and large language models mean for software development.

[2 Approaches to Risk and Resilience: Asset-Based and Service-Based](#)

Emily Shawgo discusses the benefits and challenges of two approaches to risk and resilience management: asset based and service based.

[Software Modeling: What to Model and Why](#)

John McGregor and Sholom Cohen describe modeling and analysis activities intended to achieve robust design, define the modeling chain, and effect evolution from specification to implementation.

[See more blogs »](#)



[Securing Open Source Software in the DoD](#)

Scott Hissam talks with Linda Parker Gates about free and open source

software (FOSS) in the DoD, building on insights from a workshop for producers and consumers of FOSS for DoD systems.

[A Model-Based Tool for Designing Safety-Critical Systems](#)

Sam Procter and Lutz Wrage discuss with Suzanne Miller the Guided Architecture Trade Space Explorer (GATSE), a new SEI-developed model-based tool to help with the design of safety-critical systems.

[Managing Developer Velocity and System Security with DevSecOps](#)

Alejandro Gomez talks with Suzanne Miller about how his team explored—and eventually resolved—the two competing forces of developer velocity and cybersecurity enforcement by implementing DevSecOps.

[**See more podcasts »**](#)



[**Latest Publications**](#)

[FloCon 2023 Assets](#)

These presentations and posters are from FloCon 2023, the SEI's annual conference on applying collected data to defend enterprise networks.

[Zero Trust Industry Day 2022: Areas of Future Research](#)

This paper describes the future research discussed at the 2022 Zero Trust Industry Day event.

[Getting Started with ACE/PoPs](#)

This fact sheet helps your organization prepare to participate in the ACE/PoPs pilot program and set your expectations.

[**See more publications »**](#)



[**Latest Videos**](#)

[Does Your DevSecOps Pipeline Only Function as Intended?](#)

In this webcast, Tim Chick discusses how a DevSecOps model can be built using model-based systems engineering.

[Finding Your Way with Software Engineering Buzzwords](#)

In this webcast, Hasan Yasar discusses the new technologies and buzzwords that are required to implement a complete software delivery pipeline.



[Upcoming Events](#)

[Addressing Supply Chain Risk and Resilience for Software-Reliant Systems](#),

February 21

In this webcast, Carol Woody and Charles Wallen discuss the Acquisition Security Framework (ASF) and how the ASF provides a roadmap to help organizations build security and resilience into a system.

[DevSecOps Days Pittsburgh 2023](#), May 11

DevSecOps Days Pittsburgh 2023 will be held virtually by the Software Engineering Institute on May 11.

[See more events »](#)



[Upcoming Appearances](#)

[AFCEA Rocky Mountain CyberSpace Symposium](#), February 20-23

See our exhibit at this national forum for industry and government to work together on the challenges of cybersecurity, community cyber readiness, and national defense.

[Navy League Sea Air Space \(SAS\) 2023](#), March 3-5

See our exhibit at the largest maritime exposition in the U.S.

[Women in Cybersecurity \(WiCyS\) 2023](#), March 16-18

Join us to support the recruitment and retention of women in cybersecurity.

[See more opportunities to engage with us »](#)



Upcoming Training

[Insider Threat Analyst](#)

May 2-4, 2023 (SEI, Pittsburgh, Pa.)

[Managing Computer Security Incident Response Teams](#)

May 9-11, 2023 (SEI, Live Online)

[**See more courses »**](#)



Employment Opportunities

[Security Researcher](#)

[Associate Security Researcher](#)

[Embedded Software Engineer](#)

[**All current opportunities »**](#)

Carnegie Mellon University

Software Engineering Institute



Copyright © 2023 Carnegie Mellon University Software Engineering Institute, All rights reserved.

Want to subscribe or change how you receive these emails?
You can [subscribe](#), [update your preferences](#) or [unsubscribe from this list](#).