

# Workshop on Software and AI Engineering; Breakout 1; Important Research Focus Areas

**JUNE 16, 2023**

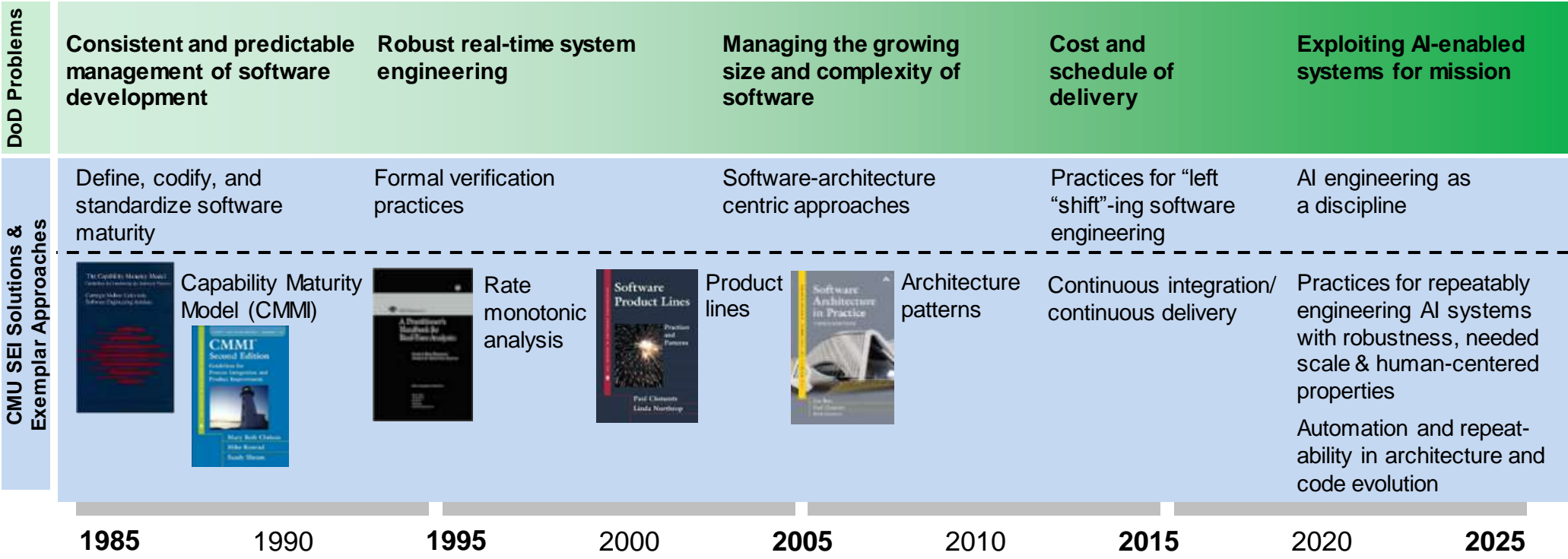
Dr. Tom Longstaff  
Chief Technology Officer, SEI



# 30 Years in Software Engineering

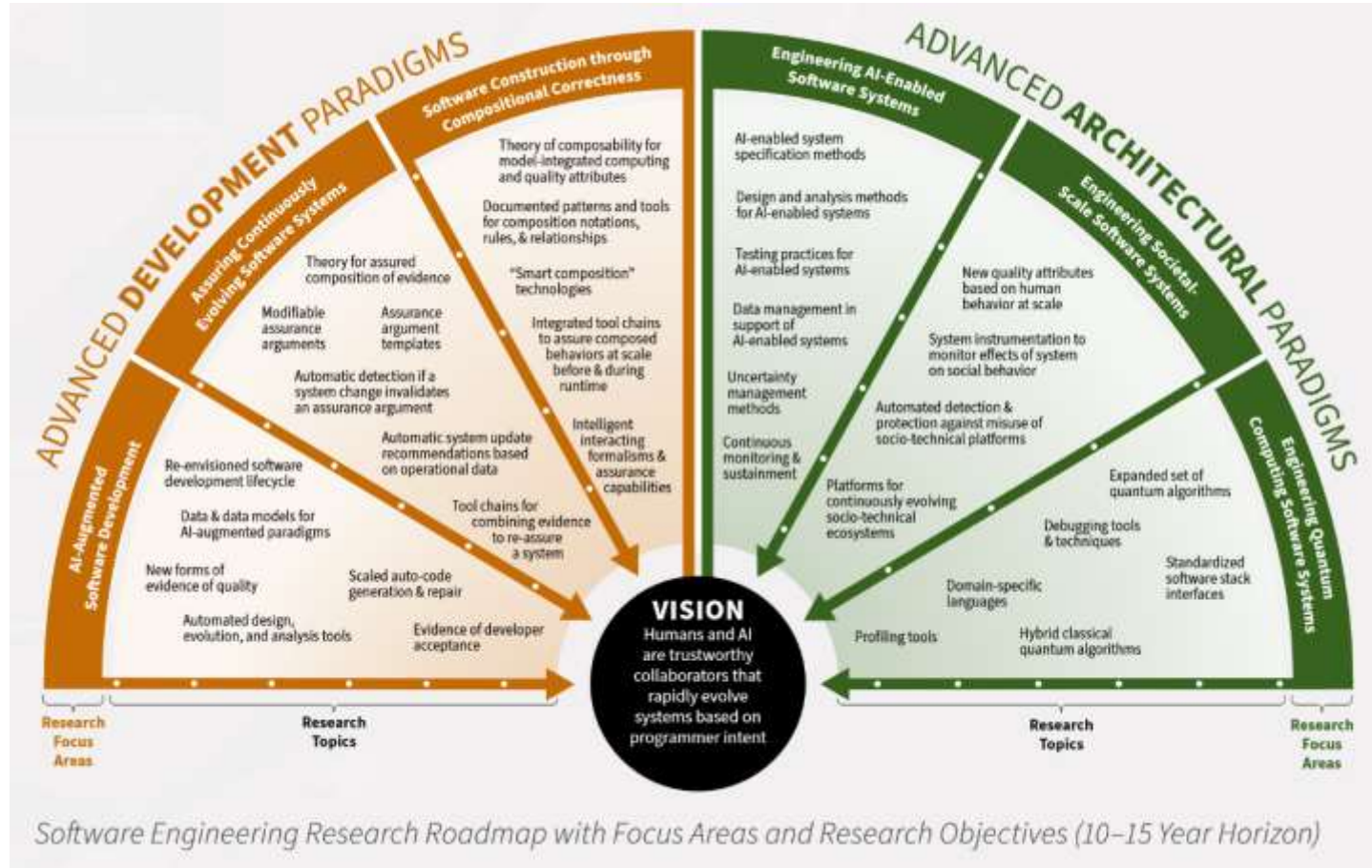


# Research to Meet the Evolving Needs in Software



Software is never done -- the evolving mission(s) and operational environment change the requirements and assumption

# Software Engineering Research Roadmap



Software Engineering Research Roadmap with Focus Areas and Research Objectives (10–15 Year Horizon)

# Cyber Research Roadmap




**A NATIONAL INITIATIVE FOR CYBERSECURITY ADVANCEMENT**

Shaping the Future of Cybersecurity Engineering

Carnegie Mellon University  
Software Engineering Institute



# AI Engineering

	<p><b>Scalable AI</b> <i>Accommodate the size, speed, and complexity of mission needs</i></p>	<ul style="list-style-type: none"> <li>• Scalable management of data and models</li> <li>• Enterprise scalability of AI development and deployment</li> <li>• Scalable algorithms and infrastructure</li> </ul>
	<p><b>Robust and Secure AI</b> <i>Operate reliably when faced with uncertainty or threat</i></p>	<ul style="list-style-type: none"> <li>• Robustness of AI components and systems</li> <li>• Designing for security challenges in modern AI systems</li> <li>• Testing, evaluating, and analyzing AI systems</li> </ul>
	<p><b>Human-Centered AI</b> <i>Designed with the goal of working with, and for, people</i></p>	<ul style="list-style-type: none"> <li>• Understand context of use, sense changes over time</li> <li>• Scope and facilitate human-machine teaming</li> <li>• Methods, mechanisms, and mindsets for critical oversight</li> </ul>

# Fundamental Research Efforts and Breakthroughs

## Advanced development

- AI augmented SW development
- Assuring continuously evolving SW systems
- SW construction through compositional correctness

## Advanced architectures

- Engineering AI-enabled SW systems
- Engineering societal-scale SW systems
- Engineering quantum computing SW systems

## AI engineering

- Scalable AI (for all definitions of scale)
- Robust and secure AI
- Human-centered AI

# Document Markings

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0617