



Software Look Ahead

Mission Drivers, Technology, Acquisition, T&E

William L. Scherlis

DSB

15 Sept 2022

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2022 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.

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

DM22-0798

Topics

Drivers:

Mission

Engineering and acquisition

Pathways:

Software systems

AI

Framework:

Secure, Adaptable, Resilient, and Capable (SARC) systems

Drivers

Mission

- BMC2, kinetic and cyber
- Integrated / federated
- IoT/OT at scale
- Proliferated distributed enclaves
- Pervasive trustworthy autonomy

Systems Engineering, Acquisition, T&E

- Linear → IID with continuous T&E
- Emergent architecture → Architecture leadership
- Process compliance → Direct evidence
- Data lakes → Federated granular enclaves
- Unsafe integration → Resiliency-enabled scale

Pathways

Software systems

- IID enabled through tools and evidence (5, 6)
- Direct evidence and metrics for rapid T&E (1, 7)
- Translucency in supply chains (1, 4 ,5)
- Managed architectures (3, 4)
- Design for security: software, cloud, enclaves (2, 4)
- Enabling cyber-physical and hardware security (2)

AI

- Trustworthiness and metrics
- Statistical / symbolic hybrids
- Learned symbolic
- Human / system symbiosis
- No labels and few labels
- Distributed analytic fusion

(1-7 identify SARC key technical ideas that support the pathways)