OT&E Takeaways on Credentialing Machine Learning

AI4SE & SE4AI Workshop 2023
September 27, 2023
George Washington University
Washington, DC

Tyler Cody, Ph.D.
Virginia Tech National Security Institute (VTNSI)
tcody@vt.edu

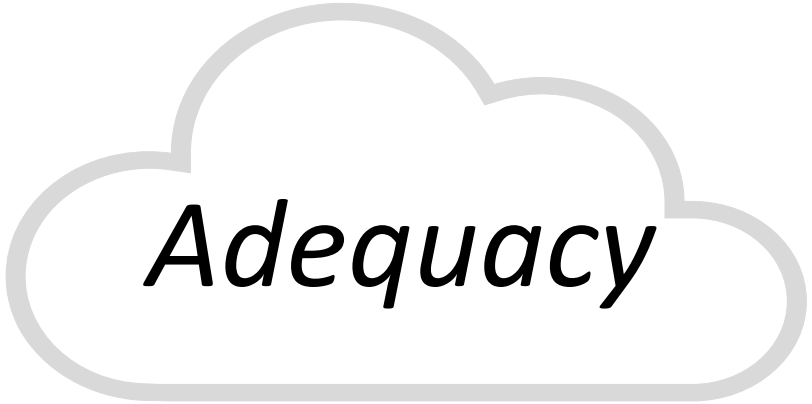
Executive Summary

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

Takeaways

1. Properties of AI/ML depend on system, and vice versa
2. AI/ML is more than software
3. Life cycle of AI/ML and programs bear heavily on risk

Adequacy in Title 10



"items or components actually tested are effective and suitable"

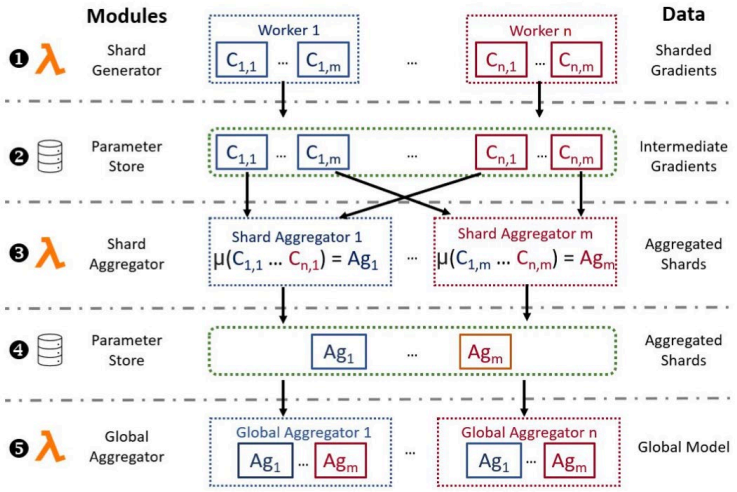
"T&E performed was adequate"

"the Director has approved in writing the adequacy of the plans"

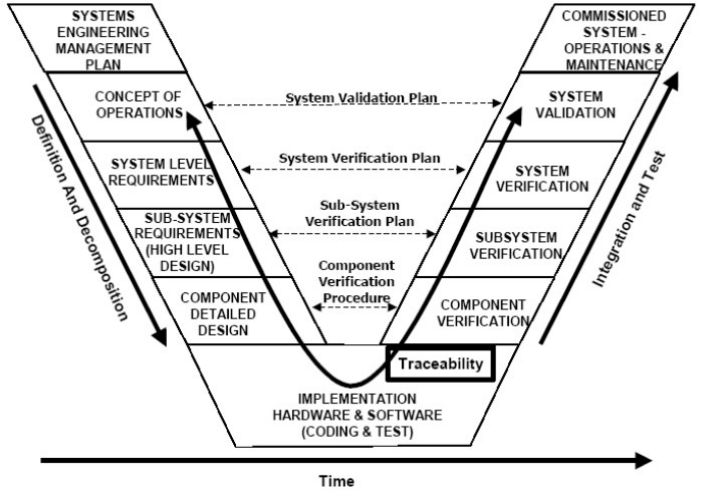
Scope

$$
\begin{aligned}
\textbf{minimize:} \quad & f(\mathbf{x}) \\
& \mathbf{x} \in \Re^n \\
\textbf{subject to:} \quad & \mathbf{g}_L \leq \mathbf{g}(\mathbf{x}) \leq \mathbf{g}_U \\
& \mathbf{h}(\mathbf{x}) = \mathbf{h}_t \\
& \mathbf{a}_L \leq \mathbf{A}_i\mathbf{x} \leq \mathbf{a}_U \\
& \mathbf{A}_e\mathbf{x} = \mathbf{a}_t \\
& \mathbf{x}_L \leq \mathbf{x} \leq \mathbf{x}_U
\end{aligned}
$$

AI Research



AI Engineering Research



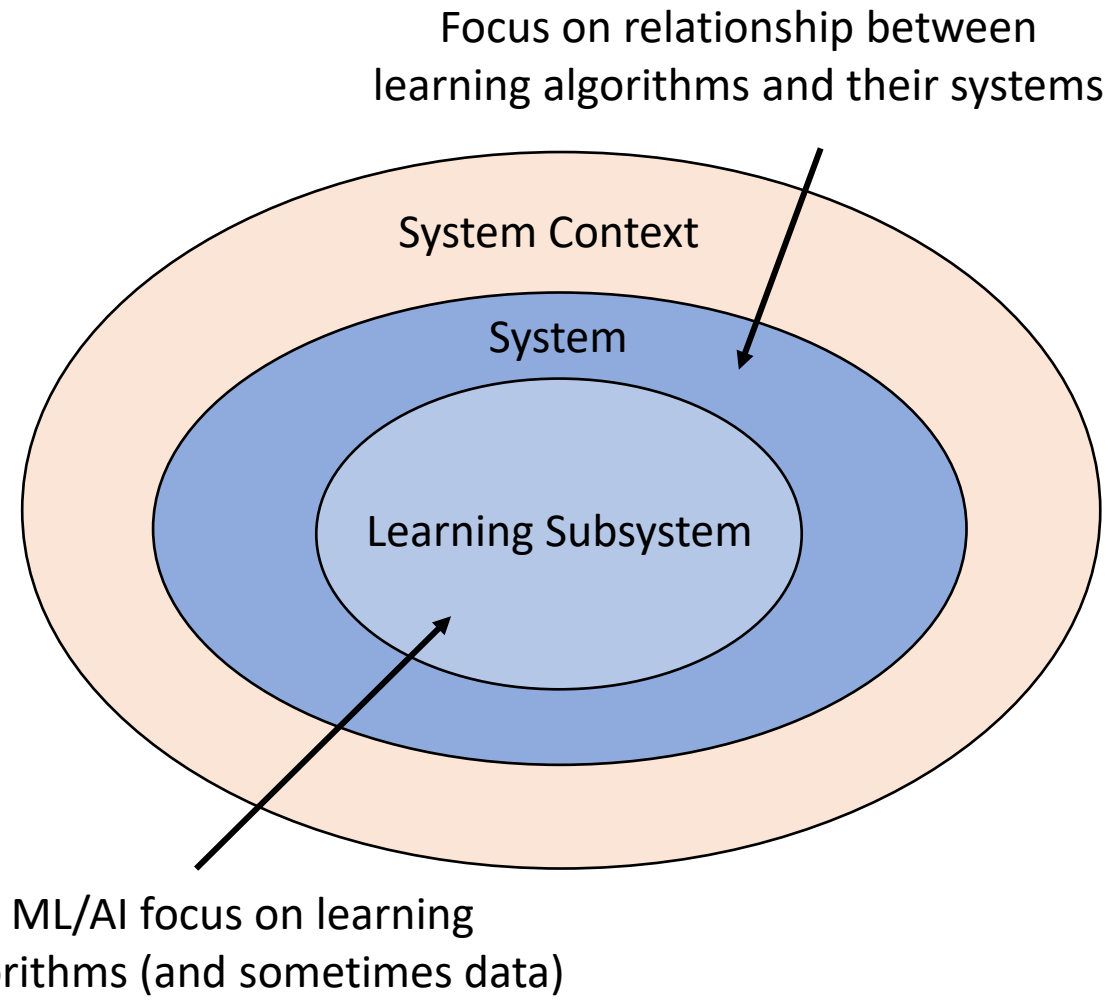
AI Systems Engineering Research

Test Engineering for AI

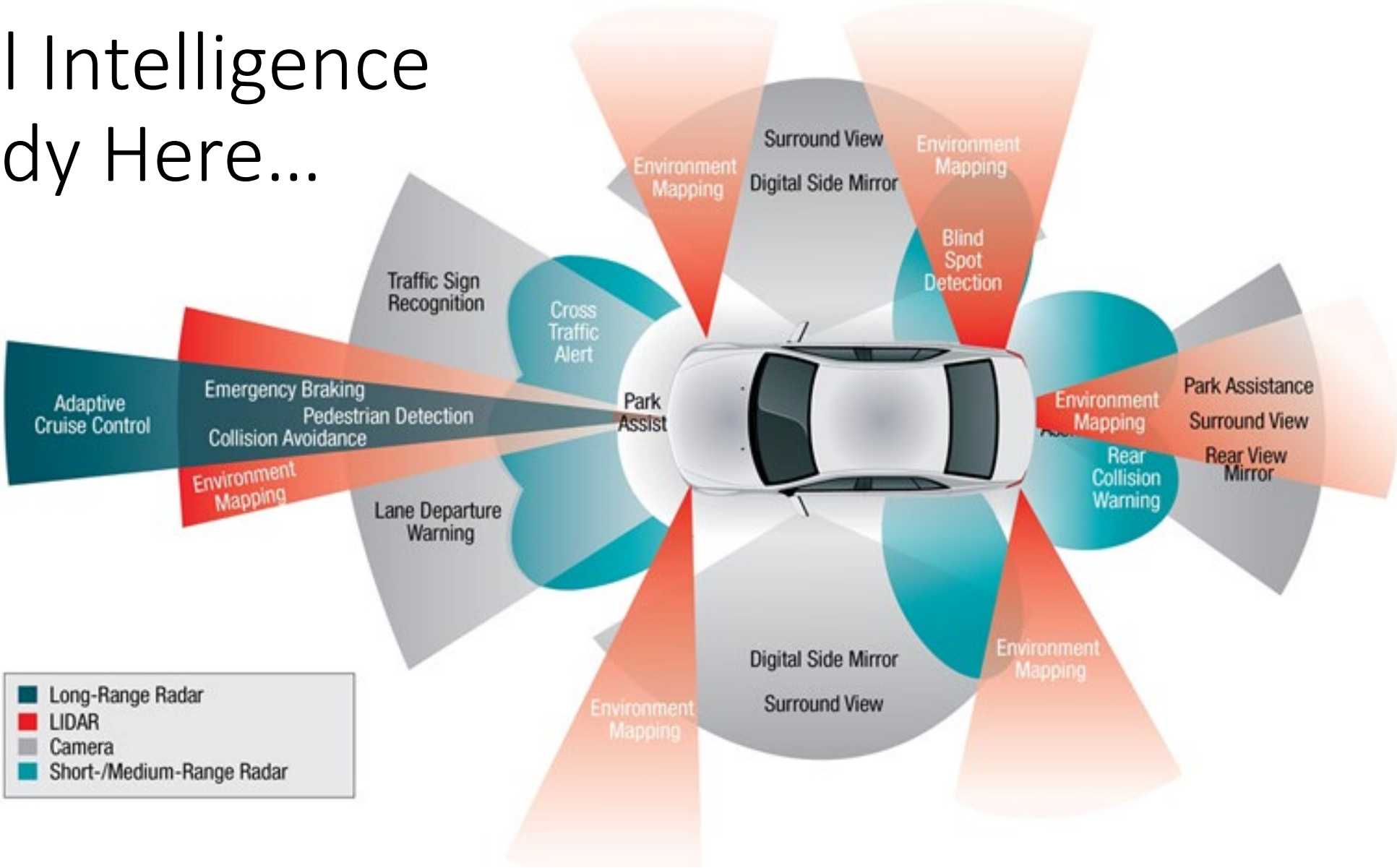
Takeaway #1

Properties of AI (trust, robustness, etc.) depend on the system the AI operates within—and the converse is true—system design and operation are affected by the AI.

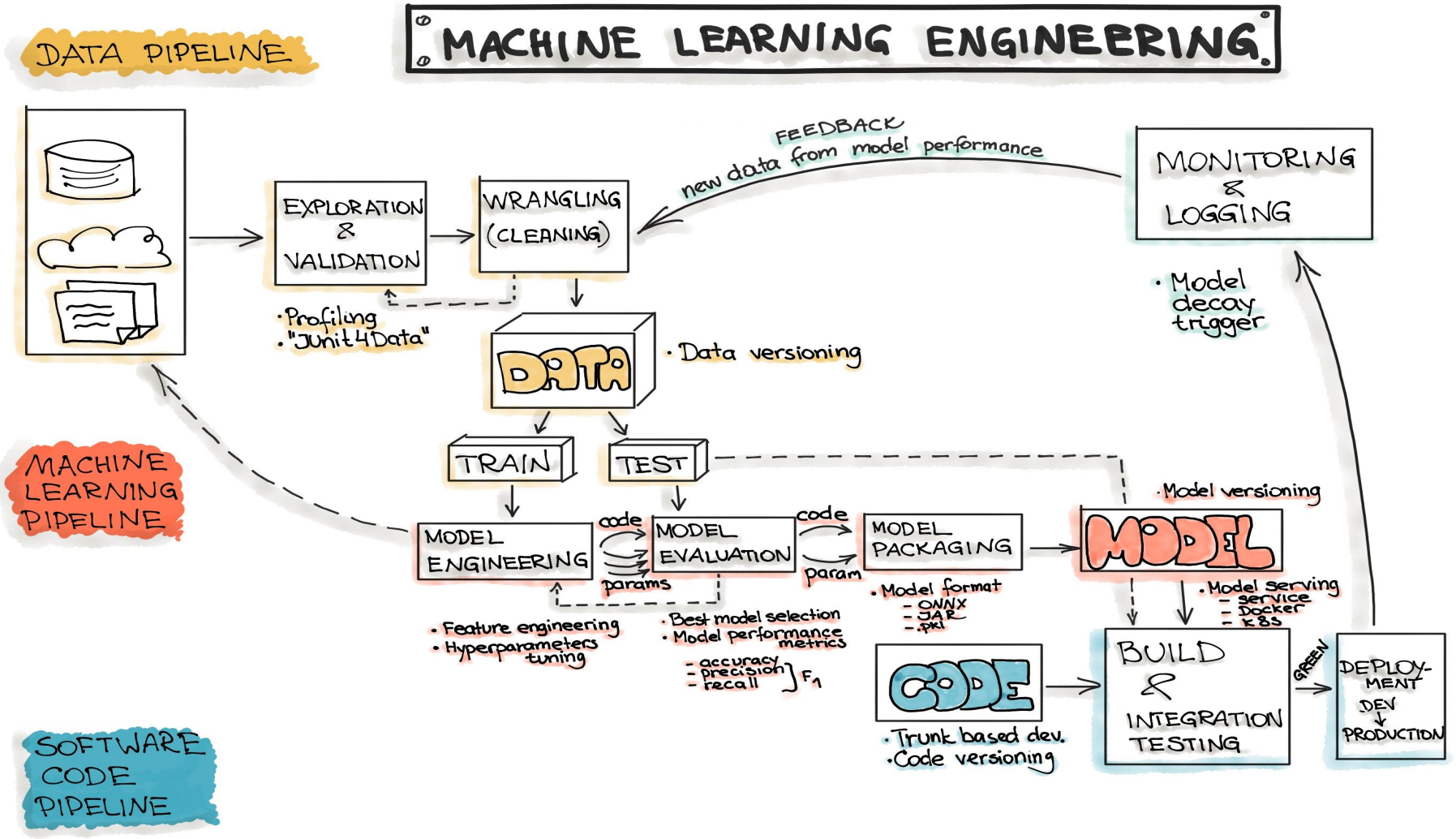
Understanding these relationships is key to test (and systems) engineering success.



General Intelligence is Already Here…



ML Pipelines (And What They Miss)

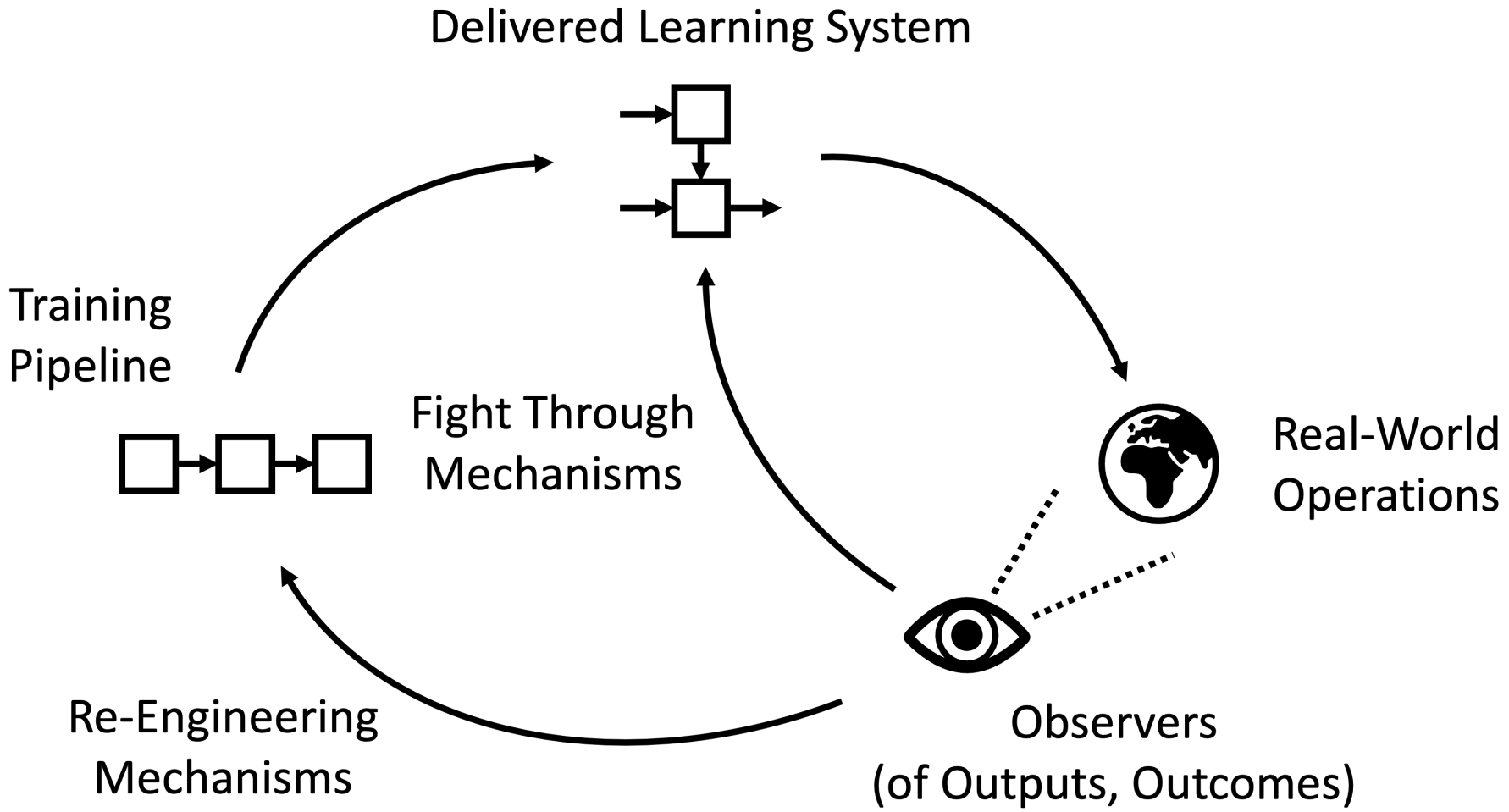


AI/ML is More Than Software

Takeaway #2

Software is just part of AI/ML. Focus on software and data as the only levers on AI/ML performance is misplaced. In addition to the cyber-physical platforms, choices about how, when, where, and who to use AI/ML are key to evaluating effectiveness and suitability.

On The Shoulder of a Learning System



Life Cycle of AI/ML and Programs

Takeaway #3

Risk mitigation strategies for test inadequacy vary over life cycles.

Tests for support systems that make sure learning can continue, degradation can be detected, and alternatives can be engaged are often more available than direct tests of the AI/ML itself earlier on in the life cycle of a program.

Summary

Takeaways

1. Properties of AI/ML depend on system, and vice versa
2. AI/ML is more than software
3. Life cycle of AI/ML and programs bear heavily on risk

Working Conclusion

Operational credentialing is system-, user-, and life-cycle-dependent.

Contact

Tyler Cody, Ph.D.

Research Assistant Professor

Intelligent Systems Division, Virginia Tech National Security Institute

tcody@vt.edu

LinkedIn as “Tyler Cody”

Figure References

https://towardsdatascience.com/how-to-make-a-vehicle-autonomous-16edf164c30f

https://www.nestorsag.com/blog/lessons-from-building-a-small-ml-ops-pipeline/

https://ml-ops.org