MORE PROFOUND COLLABORATION
ADSA-24

OCTOBER 2021

LEE SPANIER
TRANSPORTATION SECURITY LABORATORY

Remarks Are Inspirational or Aspirational, Not Policy nor Policy Recommendations

MORE PROFOUND COLLABORATION (1)

PROBLEM: OEMs Relying on ML-Crafted Components

- For Security & Safety Critical Missions – such as **Threat Detection**
- Many Benefits, but many **New Significant Risks** *to Trustworthiness*
  - Easy, Quick to Make – "*Anyone Can Code ML*" – No Craft Guild
  - Opacity Hides Complex Fragility, Overfitting, Technical Debt …
  - Challenge to Find all Critical, Dynamic, Pernicious Defects or Holes
  - Need New Approach

MORE PROFOUND COLLABORATION (2)

POTENTIAL PATHS TO CONSIDER

- **Develop** New Standards (Data Readiness, Test Harness...) Jointly
  - Build-on DoD's *Joint Federated Assurance Center* Guidance
  - Define ML-Components as *New Subsystem* in MIL-STD-881E (WBS)
  - Define Fidelity of Augmented Data // Embedded Interpretability
- **Create** Central, Secure, Custom Render Farm – Shared Asset
- **Explore** Structured, Ops Feedback for NON REAL-TIME Adaptive Systems Learning
- **License** ATRs *Like Pilots* with Duration Cert & Enduring Service