GVSC Robotics Planning Discussion

Carnegie Mellon University
Software Engineering Institute
Emerging Technologies Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM19-1195

Carnegie Mellon University

- 1,442 total Faculty
- 13,285 Students
- 130 Research Centers
- Locations in Pittsburgh, PA, Silicon Valley, CA, and Doha, Qatar
- Rankings:
  - #17 University overall in US
  - #1 for Computer Science
  - #4 for College of Engineering

Carnegie Mellon University

Software Engineering Institute

- Founded in 1984 as a Federally Funded Research and Development Center
- ~700 total employees
- Headquarters in Pittsburgh, PA, but with offices in Washington, DC and California
- Divisions
  - CERT
  - Software Solutions Division
  - Emerging Technology Center

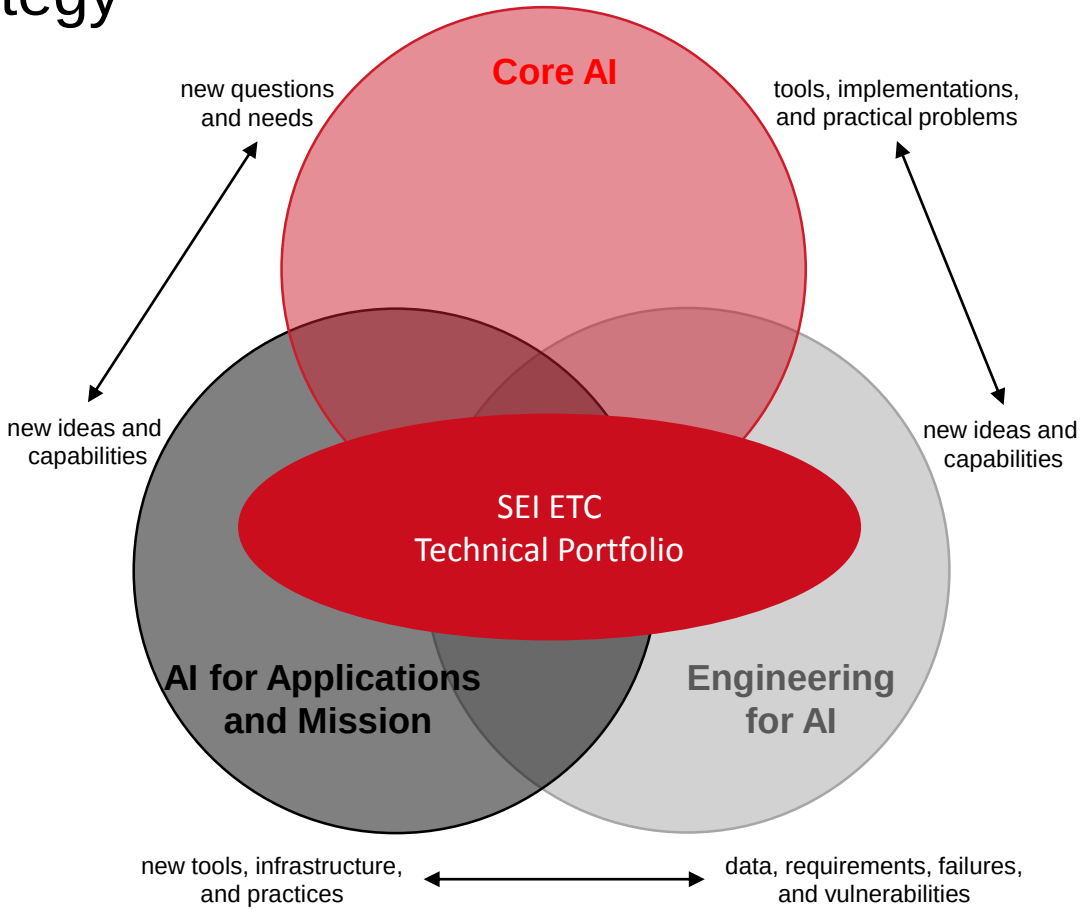
SEI Emerging Technology Center: Making the Recently Possible Mission-Practical

Applied Artificial Intelligence and Machine Learning

Advanced Computing

Human-Machine Interaction

SEI AI Strategy

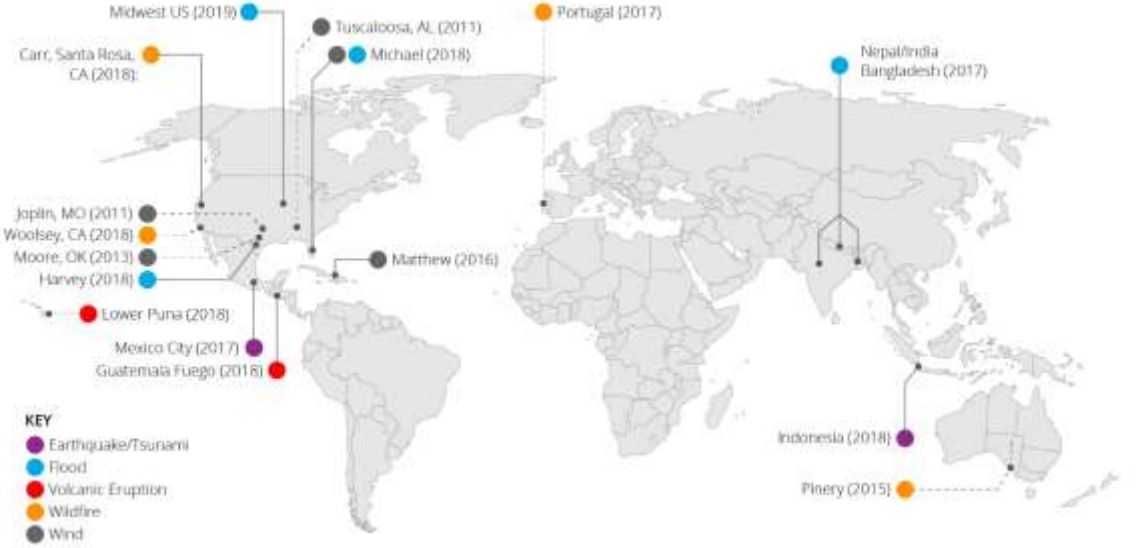


CMU-ETC Collaborations

DEFENSE INNOVATION UNIT

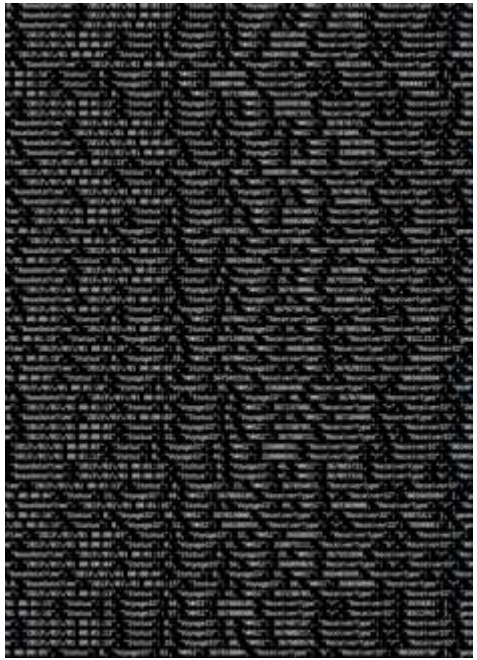
xView2 Challenge: Automating the Process of Assessing Building Damage After a Natural Disaster

- Dataset includes:
  - 6 disaster types across 15 countries
  - 850,736 buildings/structures
  - 45,361 square kilometers
- Joint Damage Scale to assess building damage

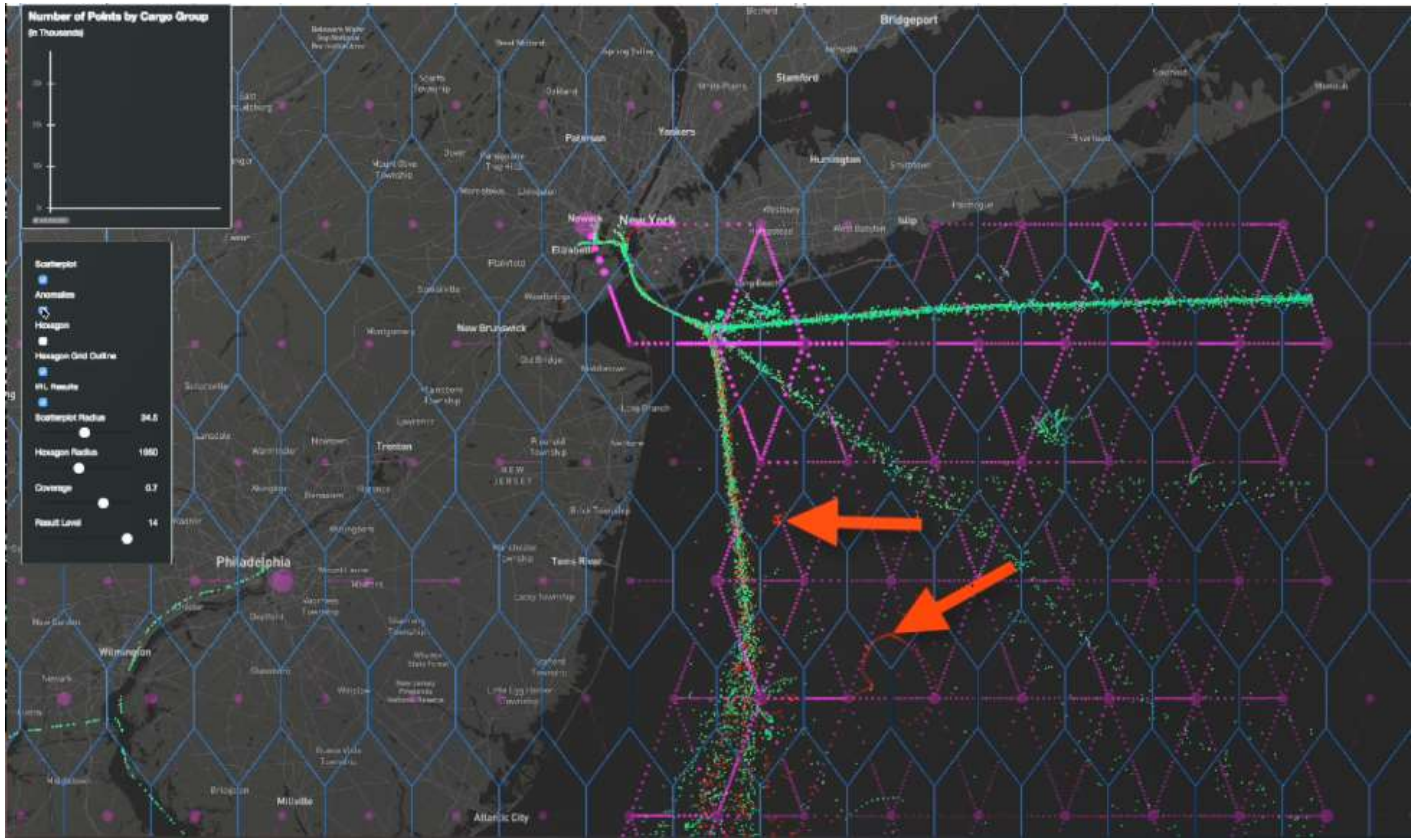


Disaster Level	Structure Description
0 (No Damage)	Undisturbed. No sign of water, structural or shingle damage, or burn marks.
1 (Minor Damage)	Building partially burnt, water surrounding structure, volcanic flow nearby, roof elements missing, or visible cracks.
2 (Major Damage)	Partial wall or roof collapse, encroaching volcanic flow, or surrounded by water/mud.
3 (Destroyed)	Scorched, completely collapsed, partially/ completely covered with water/mud, or otherwise no longer present.

Identifying Anomalous Behavior via Inverse Reinforcement Learning



U.S. Coast Guard data



Cyber Table Top (11/4 – 11/6 @ Detroit Arsenal)

- Study the behavior of RTK / MRZR in a real-world scenario
- OPFOR (Red) team theoretically attacks the OPS (Blue) team, which evaluates the results of the attack
- Develop threat model
- Prioritize attack vectors highlighted during the exercise
- Use results to inform IDS/IPS research moving forward
- Learn the most effective processes and techniques for a CTT exercise
- Follow up with additional CTT exercises using lessons from the previous

IPS/Anomaly Detection

- Software prototyping and simulation
  - AI/ML techniques to enhance autonomous operation
  - Includes documentation and test procedures
- Publish research in conjunction with CCDC GVSC
  - Joint effort with Carnegie Mellon faculty
- Areas of interest:
  - Extend anomaly detection to continuous state space (rather than just grid world)
  - On-the-fly anomaly detection (rather than discovering through complete log traces)
  - Anomalies in multi-agent (i.e. distributed) robotic systems
  - Prioritizing robotic system data for input into IDS/IPS

RTK

- Add AI/ML features to aid in autonomous operation
  - Object detection
  - Multimodal sensing (sensor fusion)
    - Less uncertainty in results
    - More robust failure modes
- Port RTK to ROS 2
  - ROS 2 more standards-based (e.g. Data Distribution Service, DDS)
    - More flexible, reliable
    - DDS widely-used in mission-critical systems
  - ROS 2 still in development, in flux
    - Develop best practices for developing / deploying ROS 2 nodes

Other Areas to Explore

- How can humans trust the results of an autonomous system?
  - How did it arrive at those results?
- How do we arrive at an “anomaly decision?”
  - Standard methods arrive at an opaque “YES” or “NO” decision
- Need to be able to interpret reasons for decisions
  - Understand why a decision was made (less of a black box)
- Human in the loop
  - Develop human trust of AI systems
- Especially important for fast-paced warfighting situations