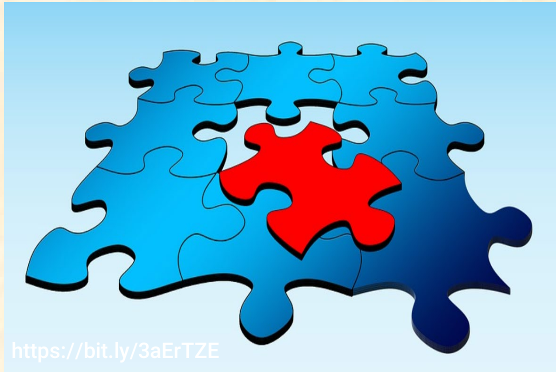
GETTING TO DEPLOYED + SAFE

Carnegie Mellon University

System Engineering

When the pieces are put together, will system work?



https://bit.ly/3aErTZE

- System-level design
  - Requirements management
  - Architecture (hardware, software, power, …)
- System integration
  - Component interfaces (sensors, software, hardware, …)
- Complexity & supplier management
  - Internal + external suppliers
  - Requirements to test plan linkage

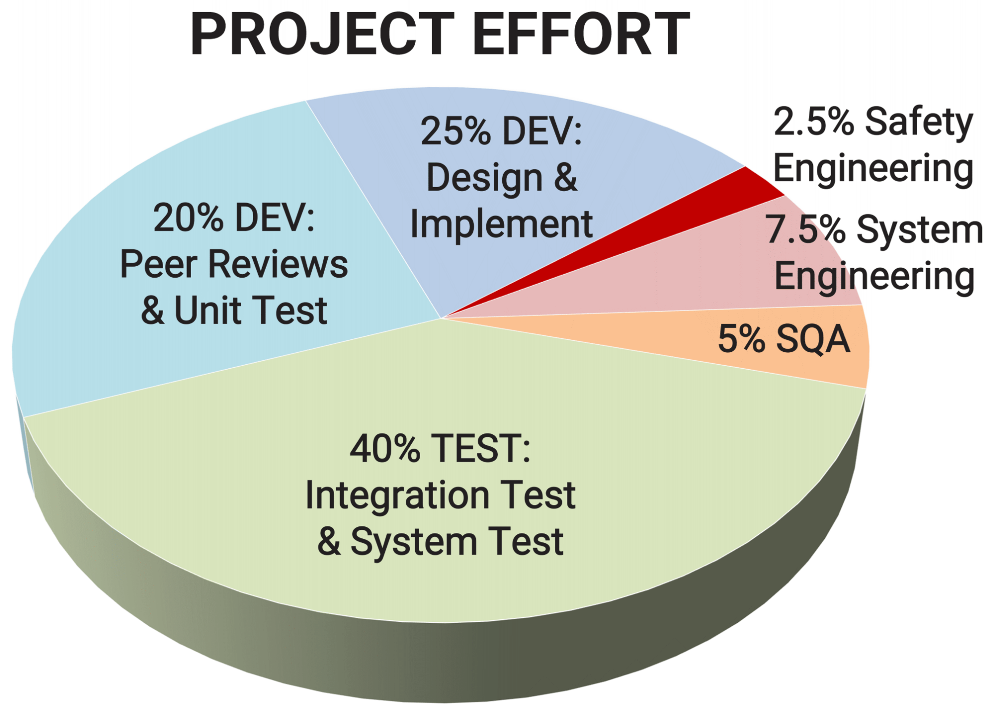
Computer-Based System Safety Engineering

Will the result be acceptably safe?

- Safety engineering:
  - Identifying hazards & mitigation strategies
    - Hazard analysis & safety concepts
    - Mitigations and safety validation
  - Ensuring acceptable safety
    - Safety requirements
    - Safety qualification (components, tools)
- Safety culture:
  - Safety Management System (SMS) & standards conformance
  - Safety practices across design, deployment, operations

Typical Staffing Profile

- Rough approximation of staffing proportions
  - Deep supply chain ➔ more system & safety engineers at interfaces



(security assumed to be part of system engineering)

Technical Safety Challenges

Carnegie Mellon University

- Perception & prediction
  - Safety of machine learning-based functions
  - Need more than object motion tracking
- Safety of Intended Function (SOTIF)
  - Drive/Fix/Drive iteration with lots of testing
    - Waymo: 6M test miles; 65K deployed miles
  - How will safety be argued for larger fleets?
    - Likely will involve UL 4600 concepts and safety cases
- Getting from "works OK" to "safe"
  - You can brute force the first few "nines" … but not all of them.
  - Field feedback into safety cases

Organizational Safety Challenges

Carnegie Mellon University

- Significant pressure to deploy
  - Flurry of empty driver seat demos in 2020
  - Can teams take the time needed for safety?
- Industry transparency needed
  - Safety collaboration rather than competition
  - Public trust in face of an adverse news event
- Ensuring robust safety cultures
  - Robotics meets automotive engineering
  - Silicon Valley culture + automotive culture + no human driver

https://youtu.be/nhqyrze30bk
Yandex demo video, Ann Arbor, Aug 2020

Getting To Deployed + Safe

- 10% System & Safety Engineering staff
- Resolve open technical safety challenges
- Robust safety culture is crucial