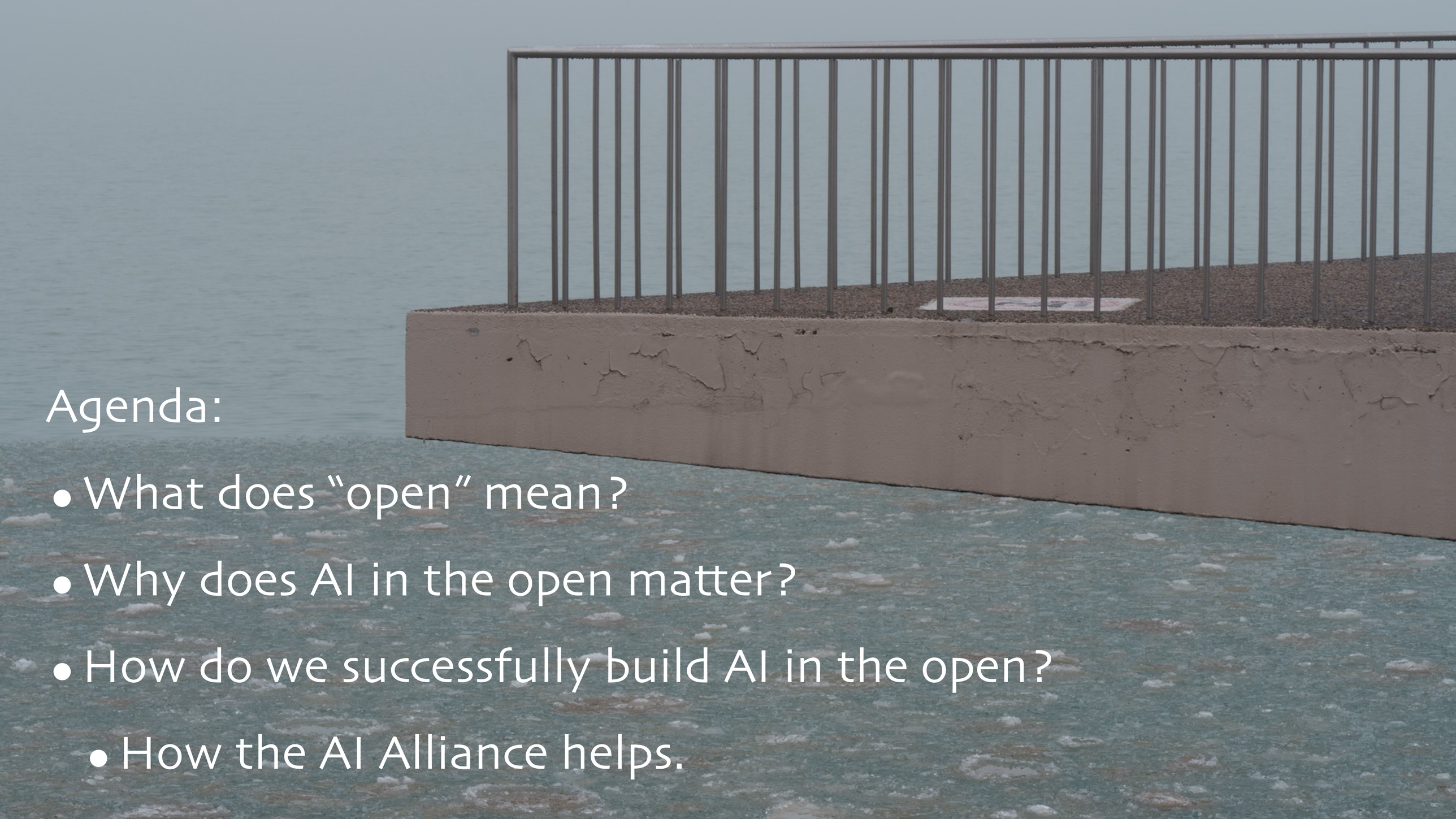
AI in the Open: Why It Matters. How to Achieve It.

Dean Wampler
IBM Research and The AI Alliance
thealliance.ai

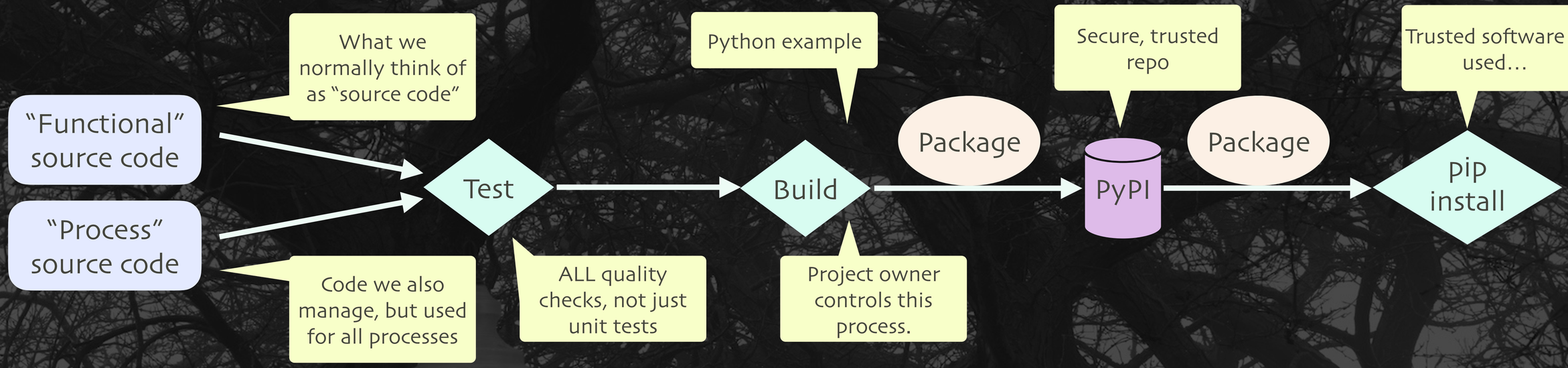


Agenda:

- What does “open” mean?
- Why does AI in the open matter?
- How do we successfully build AI in the open?
  - How the AI Alliance helps.

What does "open" mean?

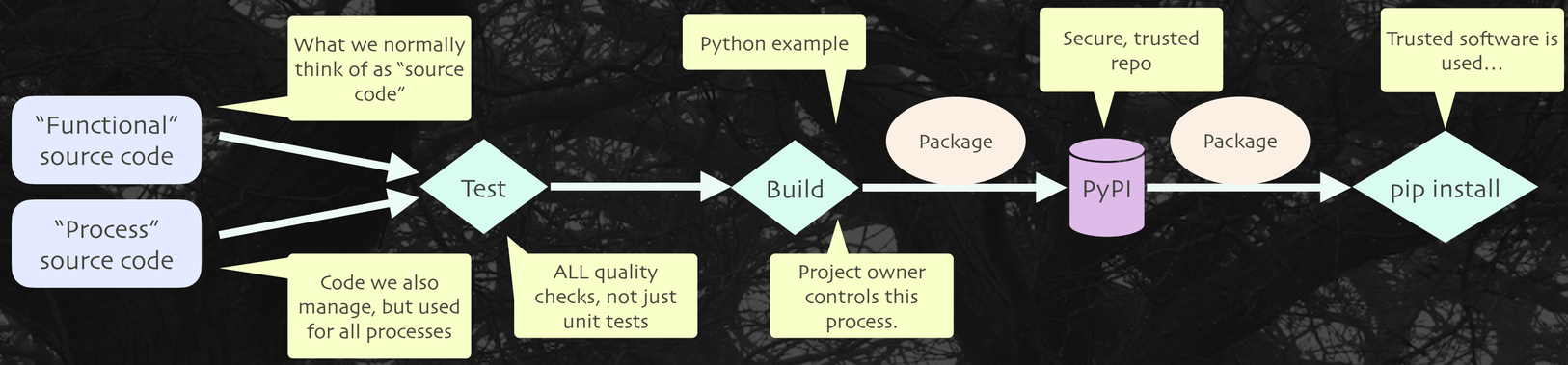
Is AI like other software?

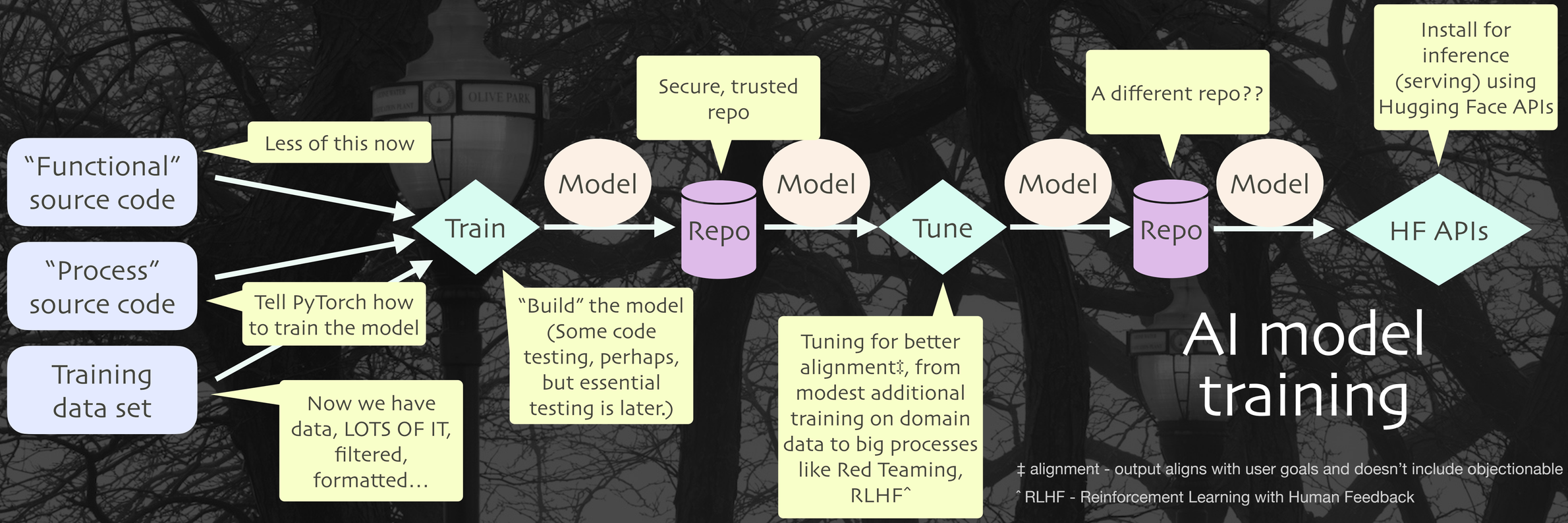


Part of the conventional software lifecycle.

AI applications include lots of conventional software, but what about models?

Is AI like other software?



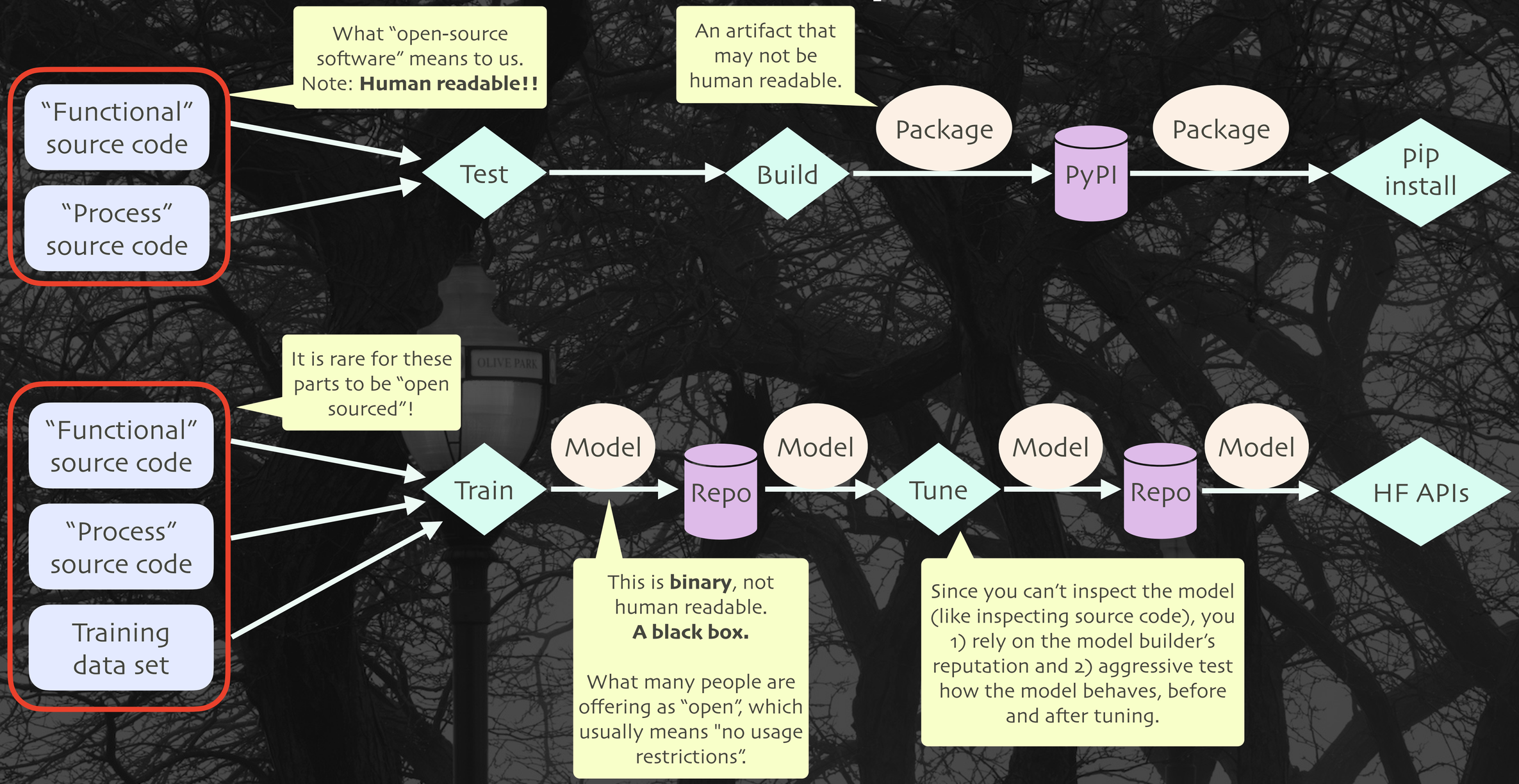


AI model training

‡ alignment - output aligns with user goals and doesn't include objectionable content.

ˆ RLHF - Reinforcement Learning with Human Feedback

So, what does open mean??



Summary

Unique aspects of AI compared to to conventional software:

1. Models are binary, "black box" artifacts:
   1. They are usually released without the code and data used to build them.
   2. You have to trust the builder's reputation.
   3. You have to test the model behavior yourself.
   4. You probably need to tune for "alignment" of behavior.

Another crucial difference:

5. Model outputs are probabilistic! Developers are used to deterministic outputs, which are easier to test and reason about!

Why does AI in the open matter?

- For all the reasons open-source software is a win…
  - … with some new considerations.

Why does AI in the open matter?

- Open models and data…
  - Stimulate research innovations:
    - Improved architectures, alignment methods, optimizations (especially for inference)
  - Stimulate commercial innovations by developers:
    - Novel applications
    - Accelerated productivity
    - Support for private hosting
  - Support tuning, which is cheaper than training from scratch

Why does AI in the open matter?

- One size does not fit all. In 2023 we learned useful model size tradeoffs:
  - Big models:
    - ✓ More generalizable
    - ✓ Highest benchmark scores
    - 𝒙 Much higher costs, carbon footprint
  - Small models:
    - 𝒙 Less generalizable
    - ✓ Easy to tune to be "good enough" for specific applications
    - ✓ Much lower costs, carbon footprint

Why does AI in the open matter?

- Inspection for safety and alignment is critically important:
  - AI adds new "attack vectors".
  - Human readable code and data are also computer scannable for vulnerabilities, bad content.
    - If they aren't provided you must:
      - Rely on the reputation of the model/dataset builder.
      - Do lots of black-box "red teaming" yourself.


How do we
Successfully build
AI in the open?

- Train more people in AI concepts, including safety
- Work together, pooling resources, to…
  - Broaden available models and applications tools
  - Create useful standards
  - Test and align models for particular goals
  - Fund innovation for basic research
  - Advocate for the benefits of AI in the open
    - But with appropriate safeguards

Meet the AI Alliance

thealliance.ai

Founding Members and Collaborators*

- Universities
- Startups & Enterprises
- Science Organizations & Non-profits

~80

Total annual R&D funding represented

>$80B

Students supported by these academic institutions

>400,000

Total staff members

>1,000,000

Meet the AI Alliance

thealliance.ai

Recap

- The AI Alliance was founded on the premise that the successful open-source software model still applies to AI.
- However, we need to work together to maximize access to AI technologies with appropriate safety constraints.

Questions?

- Visit thealliance.ai
  - (Join our mailing list: see the “learn more” page)
- Let me know what you think!
  - dean.wampler@ibm.com
  - Mastodon and Bluesky: @deanwampler
  - These slides: polyglotprogramming.com/talks