AI / ML Software Development Lifecycle Overview

Supporting **Activities** Work items **Identify Opportunity**

Information gathering Prepare review materials, find and meet with representative customers,

summarize results.

Use customer research

methods to identify

stated / unstated needs



Reviews, meetings Begin to consider IF an Al / ML model is really needed. Iterate on business case until signed-off...

Build a business

case to fulfill the

opportunity



Reviews, meetings

Create detailed

requirements

Meetings with Engineering, Data Science and team to imagine the product. Consider if an Al / ML model is really needed. Reviews with Legal, Security, Privacy and other teams.



Reviews, meetings

Perform active

development

Design reviews with Engineering, Data Science and team members. Status, progress to build the product, model experiment results..

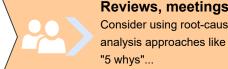


Reviews, meetings

Success! Release

product to production

Meetings with Engineering and Data Science to review "health" of the entire product in production. Review AI / ML model performance and results from "humans in the loop"



Consider using root-cause analysis approaches like "5 whys"..

Identify opportunity to be fulfilled

- Top down: Company or organization goals, executive management requests, etc.
- Bottoms-up: PM and engineering team identify an opportunity to address company or customer need

Needs Identification

- Interviewing
- Focus Groups
- External industry research
- Surveys
- AI/ML 'customer listening'
- Customer Service data
- Cognitive walkthrough(s), prototypes
- Usability testing
- Instrumented code in current production release

[Additional needs identification approaches as necessary]

Business Case

- Define customer/internal user. Define their location(s) (country, region, etc.)
- Opportunity clearly defined with "actionable metrics"
- Estimate human resources needed to design, develop, and maintain the product (ex: UX/CX, Developers, Data Scientists, DBA's, Humans in the loop, etc.)
- Budget \$ estimate
- Estimated project delivery timeframe
- Risks and change management initially defined
- Review and iterate on business case until signed off

Software Requirements

- Leverage prior Needs Identification results customer/internal user needs, country, etc.)
 - Consider globalization, localization, accessibility, etc.
 - Security, privacy, legal reviews
 - Create UI mocks if there is a
 - Consider product nstrumentation for user tracking
 - Requirements to capture "actionable metrics"
 - Production operational requirements ('health' monitoring, dashboards, etc.)
 - Determine production roll-out strategy (gradual roll-out, A/B testing, etc.), marketing surrounding the roll-out, change management defined, etc.

Implementation free requirements]

AI / ML Requirements

- [AI / ML requirements also derived from Software Requirements1
- translation approach
- Determine AI / ML model
- Consider monetary cost of
- Include ML Ops requirements
- Are "humans in the loop" needed?

- Consider data source(s) and
- Ethics and bias in data
- Consider AI / ML models (explainable models needed?)
- Determine data processing speed, cadence, etc.
- evaluation metrics to meet the opportunity (precision, recall...
- Determine threshold to re-train the AI / ML model based on business impact
- ncorrect predictions/results
- for model monitoring (Ops dashboards, etc.)

[Implementation free

requirements]

AI / ML impact included in change management

Software Development

- Create design doc(s)
- Tests and test automation framework
- Front-end/UI. back-end development (data store, data
 - pipe-lines, etc.) to implement prior Software Requirements

Product instrumentation and

Ops monitoring developed

Explore outliers. Is data

Garbage in, garbage out

Consider licenses if using

AI / ML Model Development

experiment doc(s). Re-use

model evaluation metrics.

A) Acquire and explore data

Design/model and

 How accurate is the labeled data? Class imbalance? etc.

B) Model experiments

external data

- Feature selection, feature extraction
- Select model(s)
- Setup and run experiment
- Write-up experiment results. Compare to model evaluation
- Make adjustments and repeat experiment if necessary

Software Operations

- Execute production roll-out strategy, marketing and change management
- Measure "actionable metrics" determine how closely the product meets the original opportunity
- Perform Dev Ops
- Review product instrumentation and Ops monitorina
- Track machine/resource consumption. PM compares actual \$ spend to \$ budget and adjusts budget.
- PM manages feature requests
- PM considers if customer or business needs have changed and if the current product, including the model, no longer meets those needs. If so, return to "Customer Research". Consider decomissioning the product.

AI / ML Operations (Ops)

- Deploy model(s) using production roll-out strategy
- Perform ML Ops
- Compare actual model results (ex: "human in the loop" feedback) to model retraining metrics. If results are beyond re-training threshold consider returning to "Model Development" to re-train the
- If the ML model is exposed via an API then measure API traffic, latency, failures, etc. and make updates as needed

Generative AI Ops:

- Prompt Engineers continue to guery the LLM to look for
- "Red teams" intentionally find failures in the Gen AI model(s)
- Update filters to exclude problematic responses and provide generic responses instead, etc.

prevent fulfilling the opportunity

Repeated model

experiment failures

- AI / ML Root-Cause(s) Work with Data Scientist to
- determine what specifically is failing (ex: model not generalizing to new, unseen
- Re-verify requirement goals. Are the evaluation metric(s) or monetary cost of incorrect predictions/results too high?
- Is the data quality, consistency or data subset(s) an issue?
- Could more data be used to train the model?

Important Notes

- This lifecycle does not suggest any project management approach like Waterfall, or any Agile approach like Scrum.
- This is a suggested overview to think through an AI/ML project. Use any preferred project management approach.
- · Work Items and Supporting Activities above can overlap and repeat if necessary.
- Not intended to be a complete list of all work that takes place on an AI/ML project.



AI / ML Software Development Lifecycle Overview (c) 2024 by Craig Guarraci and is licensed under CC BY 4.0. To view a copy of this license, visit: http://creativecommons.org/licenses/by/4.0/. File available at: https://TechPMCareerPath.com/downloads. Connect at: linkedin.com/in/Craig-Guarraci