Characterizing and Detecting Mismatch in ML-Enabled Systems

Interview Protocol

# Introductory Comments

* As noted in the slides that were provided with the interview invitation, the SEI is conducting a study on building, deploying and operating machine learning (ML) enabled systems. We are working on identifying key information that needs to be shared between different stages of the system lifecycle. In support of this study, the SEI is conducting a series of targeted interviews to gather data from practitioners involved in building, deploying, and operating ML-enabled systems. If you have not seen the slides, we can walk you through them at the beginning of the interview.
* This interview is entirely voluntary. All information provided in the interview will be treated as confidential information and will not be shared internally or externally beyond the research team without your express consent. We assume that you have permission from your organization to discuss your work [If being done during work hours: , in particular during work hours,], and will ask for this acknowledgement before we start.
* The information gathered from the interviews will be aggregated in the form of mismatches and consequences, and will have no connection to any organization.
* Please do not reveal any private or personally-identifiable information about yourselves or others in your answers.
* Before we begin, we would like to notify you that we intend to record the interview for transcription purposes. Only the PIs and Co-PIs will have access to the recordings and transcripts. This audio recording is being done in a private space so no passerby is inadvertently recorded. [If being done over the phone: You should also ensure that you are in a private space so no one is inadvertently recorded.]
* Before we begin, please provide your verbal consent by stating “My name is X, I acknowledge this interview is being recorded, and I have permission from my organization to discuss my work.”
* After the interview is transcribed and identifying information is removed from the transcript, the audio recording will be destroyed.

# Background and Context

1. Are there any questions about the project introduction slides?
2. As stated in the project introduction slides, in many organizations, there is an ML or data science team that builds and trains the ML model (ML Team), another team of software engineers that integrates the model into a larger system (SE Team), and a third IT Team (possibly external) that will operate the system once it is deployed. Have the ML projects that you have worked on at [organization name(s)] had this team structure?
   * If this description is inaccurate for your projects, can you describe the teams that work on the development life cycle of your ML projects?
   * What team(s) are you a part of (ML, SE, or IT)?

# Mismatch in ML-Enabled Systems

The diagram on Slide 5 (Motivation) shows a notional diagram of the elements of an ML-enabled system. A connector between elements is an indication that these elements should be in alignment. Note that this is not a complete list of connectors, as one could argue that there should be connectors between every pair of elements.



1. For any two elements in the diagram:
   * Can you think of a (story/event/incident) where there was an issue because “things didn’t fit together” the way they needed to, or there were assumptions made about elements of the system that were incorrect? For example, if an ML model is trained on data that is different from data in the operational environment, field performance of the ML component will be dramatically reduced.
   * What was the type and size of the system?
   * What were the consequences of the problem?
   * How was it solved?
   * What information could have been shared that would have avoided this problem?
     + How should it have been communicated or shared? Or is this information that could have been extracted from any of the elements?
   * If you knew then what you know now, would there have been a better way to solve the problem?
2. Alternate question: Or perhaps you can think of a time where there could have been a problem, but because certain critical information was shared, the problem was avoided.

# Software Engineering and Software Architecture for ML-Enabled Systems

1. What do you think are the biggest issues in software engineering of ML-enabled systems today?
2. What role does software architecture play in your organization for ML-enabled systems?

# Catch-All

1. Can you think of any other issues that you have seen with development, deployment, and operations of ML-enabled systems that we have not talked about yet?