Brian Rodriguez
u853593

Quiz 8

The Amazon article was a great read and exposed me to a field of software engineering that I did not know existed. I understood that systems are composed of models but I did not know that such a level of great detail go into these complicated and massive models that a company such as Amazon struggles with this problem. Descriptive models and model checking is an important part in massive systems and the article gives great insight on how Amazon approached the problems they were facing.

Engineers at Amazon have been combating these massive and descriptive models since its inception. They have had to create models with no downtime and maintain the user experience that their users expect out of Amazon. With these complex models comes an increase probability of human error in design, code, and operations. These errors in a complex system could cause catastrophic errors such as loss or corruption of data, or a violation of other interface contracts that Amazon customers depend on.

Amazon uses Precise Designs to find subtle bugs in their system designs. They use precise designs because the author of the design is forced to think about their model more clearly, which helps eliminate hand-wavy ideas, and model check tools can be applied to look for subtle bugs in the design. Amazon uses TLA+ as their descriptive formal specification language. TLA+ is based on discrete math, which all engineers are supposed to be familiar with. TLA+ specification describes the set of all possible legal behaviors of a system that is being designed and or tested. This language is used to show that a system is working as intended. The confidence level is based off of the desired correctness properties, either by conventional mathematical reasoning, or by a tool such as the TLC model checker.

TLA+ provides many benefits when designing a complex system. Once correctness properties have been defined, the author of the system can create abstract versions of the design along with an operating environment. This allows for an exhaustive test environment that can be operated and tuned as the design gets more complex and features are added.

Amazon battled many different descriptive model languages internally for quite sometime as described in the article through multiple sections. TLA+ was not always the go to language of choice for amazon. It wasn’t until huge milestones such as the release of DynamoDB that Amazon had to defer their old language and use TLA+ because of how descriptive of a modeling language it was.