## 2.1 Software Verification and Model Checking Notes

The KeY verification uses JavaDL as its basis of logic and it evaluates formulas in a Kripke structure. A valid path through a Kripke structure could be an infinite sequence of transitions through states for which a formula can hold *(Kuhtz, L. & Finkbeiner, B. (2011))*. Safety, nothing bad happens, and liveness, something good happens, are two crucial aspects of a Kripke structure ensuring the model functions correctly, with deadlock-freedom also an ideal characteristic.

## 2.2 Logics

There are many types of logic available today however the main logics we focus on regarding deductive verification are first-order predicate logic, propositional logic and Hoare logic.

First-Order Predicate Logic is a basis for constructing formulas from using “symbolic structures comprised of predicates, functions, variables, constants, quantifiers and logical connectives” (*Yang, K.H., Olson, D. & Kim, J. (2004))*  and is the basis for many verification systems in use today, albeit expanded to include such theories as equality, linear arithmetic, purely applicative arrays and bit vectors (*Filliâtre, J. (2011))* .

Propositional Logic is a simplified version of predicate logic by assigning a true or false value to each variable in a formula and defining the connectives through truth tables (*Yang, K.H., Olson, D. & Kim, J. (2004))*. This logic is popular when constructing normal forms to be used in SAT solvers, discussed later in this chapter, to determine the validity of formulas, an example of which being the construction of Conjunctive Normal Forms to be used in the DPLL framework (*Nieuwenhuis, R., Oliveras, A. & Tinelli, C. (2006))*.

Hoare Logic was proposed by Tony Hoare in his paper “An Axiomatic Basis for Computer Programming” *(Hoare, C. (1983))*, and introduced applying deductive reasoning as a way to formally reason about and develop software programs, that could be mathematically proven to function as required. Inference rules and axioms were developed to reason with computer programs, such as the widely used {P}S{Q} notation stating “*If proposition P is true when control is at the beginning of statement S, then proposition Q will be true when control is at the end of statement S*” *(Hoare, C. (1983))*. These inference rules were applied using assertions to ensure all programs satisfied these inference rules.