Lab 7 Question 3

Part A

The complexity of current embedded systems due to different economic, social and ecological constraints, encourages developers to revise the development process of these systems by using modeling and validation tools. This approach employs Model-Based Systems Engineering (MBSE), whose purpose is providing the ability to make early decisions based on simulation results, including safety critical decisions

To carry out safety analysis for connected and embedded systems, paper suggests methodology which composes of three phases. The first phase allows the semi-formal modeling of embedded systems by using the SysML language, an Unified Modeling Language (UML) extension for systems engineering. UML is a general-purpose modeling language in the field of software engineering that provides a standard way to visualize the design of a system, a profile is a collection of extensions that collectively customize UML for a particular domain. Papyrus and Eclipse plug-in have been chosen for SysML implementation

The methodology concerns the process of Model Driven Engineering that allows the representation of system and validation of its properties after needs and requirements capture. This automatic process is based on three phases: semi-formal representation, passage to the formal representation, and system validation. These three phases will be described in the following:

A. Semi-formal Representation in SysML and Connectivity Profile:
   The first phase includes the representation of all system properties in SysML using mainly State Machine Diagram and Sequence Diagram to cover the dynamic aspects, the block Definition Diagram (BDD) and Internal Block Diagram (IBD) for static aspects.
B. Mapping between SySML and NuSMV:
   The principle of this mapping is to generate a NuSMV code from the different SysML diagrams.
C. Validation:
   The formal model generated from the semi-formal one in the previous step makes it possible to perform system validation using model checking techniques. The principle consists of representing in temporal logic the safety constraint concerning attacks via connected components and checking it on the model.

Part B

A braking system model is provided along with the specifications. The analysis is done below using NUSMV

Specs: SPEC AG!((encrust_frame & !generate_frame) →AX (state=brake_on))

Which says: the brake is on when there is an encrusted frame, although no effective frame has been generated.

The specification is not validated, and a counterexample has been returned as shown in screenshot below. So, the design of this braking system should be corrected by adding secured components such as an authentication method.

Lab 7 Question 3