CPS FORMAL METHODS

PROJECT PROPOSAL

TEAM MEMBERS:

Archana Narayanan (an2adv@virginia.edu), Hemanth Kumar (hg6va@virginia.edu)

TOPIC:

Dependability Analysis of Automated Lighting Control System by Probabilistic Model Checking using the PRISM Model Checker.

Automated Lighting has become an integral part of daily lives, not being constrained to home use but also in healthcare, education and corporate infrastructure. Automated Lighting is convenient, cost-efficient and enhances security. The aged and disabled also benefit greatly from an automated lighting system.

In such scenarios, it is crucial to evaluate the dependability of the system in order to make it safer and more reliable. We aim to utilize probabilistic model checking, one of the formal verification methods to study the dependability properties of this system and evaluate its reliability. Being able to predict the timeline and probabilities of failure of the components in automated lighting control, i.e., the sensors, actuators, I/O processors and main processors through the dependability analysis provides the framework to select the best possible iterations of the components and also to be well informed about maintenance intervals. This helps deploy a safe and secure system in place with increased efficiency. The analysis could also be extended to other automated systems whose behavior is highly reliant on a controller.

So far, formal methods have been used to evaluate systems such as autonomous driving vehicles, pacemakers, power management systems, etc. We propose to perform an experimental investigation on using probabilistic model checking using Markov modelling on the Automated Lighting System and evaluate the results.

An automated lighting system usually consists of sensors, processing units, actuators and connecting interfaces between them. The sensors detect human presence in the area and this information is passed onto the processor which is the controlling unit. The processors produce the desired output based on which the actuators are activated (lights in this case). The first step is to build states for each of these components using the Markov decision Processes (MDP's). We plan to identify the instances due to which the system can fail or produce undesirable results and calculate the probability of each of them. We will perform graph-based analysis and also calculate the average number of restarts that will occur due to the failure of these systems. In PRISM, the model will be built for each component, and translate the MDP states in PRISM. The delay and timer control values will be calculated from literature readings to evaluate the vulnerability of each component. From this, the probability of failure will be computed and the reliability results can be obtained. Using this, further solutions can be explored to improve the performance of the system and mitigate failures to a large extent.

In [1], a case study of an embedded control system is proposed where the applicability of probabilistic model checking and dependability analysis is illustrated. We intend to build our model in a similar fashion, addressing some issues which we face during practical implementation. In [1], the sensor and actuator failures are calculated using a fixed probability, once and twice per month respectively, but the models do not differentiate between peripherals which are working, but faulty and the ones which are not faulty. This lapse might push the input processor to detect a false positive. The input processor in our implementation will be an ADC, which converts the analog input from the sensor into a digital value. We plan to add the voltage check and corresponding constraints to the input processor module. The actuator in our case will be a relay, actuated by the processor. We plan to implement the voltage and current rating constraints at the actuator module, ensuring safety. Also, we plan to implement a new module, which deals with connecting the whole system to a cloud server and try to factor in the failure scenarios associated with it, like an insecure connection, unauthorized access, etc. We use temporal logic to specify the check properties. This formal verification approach can be easily combined with more traditional non-probabilistic verification processes for safety criticality.

REFERENCES:

[1] Controller dependability analysis by probabilistic model checking; Marta Kwiatkowska, Gethin Norman and David Parker

[2] Verification of Markov Decision Processes using Learning Algorithms; Toma´s Brazdil, Krishnendu Chatterjee et. al

[3] PRISM: Probabilistic Symbolic Model Checker; Marta Kwiatkowska, Gethin Norman, and David Parker.