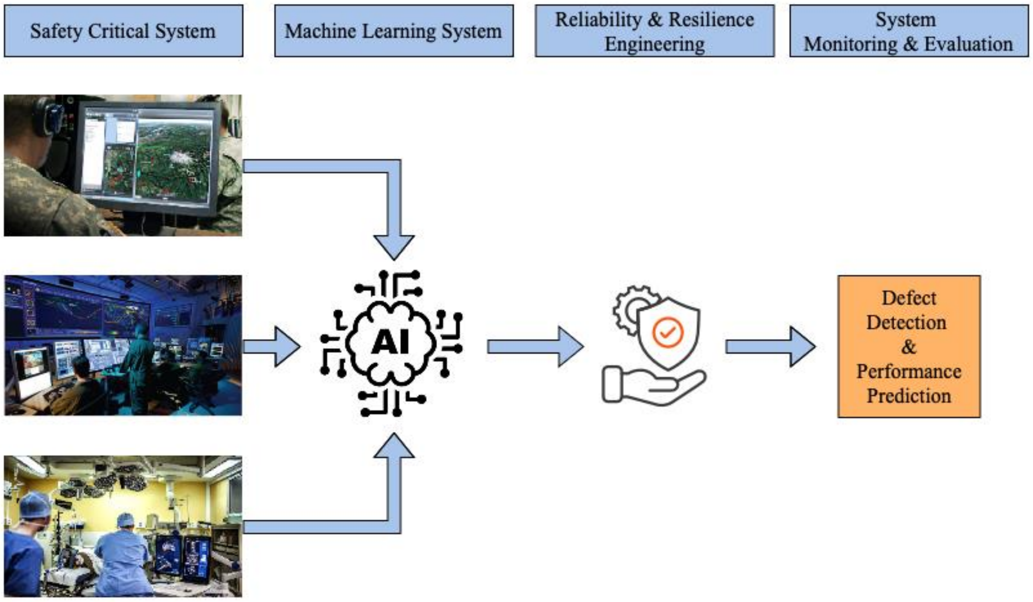
Indo/US Collaborative Research Grants

National Science Foundation of US and Technology Innovation Hubs of India

सत्यमेव जयते

Title: Application of Reliability and Resilience Models to Machine Learning
Indian PI: Prof. Susmita Ghosh, Professor and PI of the project "Software Reliability and Security Risk Assessment: Modelling and Algorithms" in the Department of Computer Science & Engineering, Jadavpur University, Kolkata India.
US PI: Prof. Lance Fiondella, University of Massachusetts Dartmouth, Dartmouth, MA, US.

Machine Learning (ML) has become integral to numerous domains due to its potential to automate decision-making processes and handle complex tasks. The deployment of ML models in real-world scenarios requires that these models can adapt to changing conditions and handle uncertainties effectively. This ability to be reliable and resilient is critical, especially when dealing with complex tasks. ML models must be able to perform well even when faced with incomplete or ambiguous information and make decisions that are robust to uncertainty. Without solutions to address these challenges, the reliability of ML models will remain uncertain, leaving many industries vulnerable to potential failures. **This research (i) demonstrates how to collect ML-based systems data that are suitable for software reliability and resilience models, (ii) applies these models, respectively, to track and predict failures and performance of the system impacted by known adversarial attacks, (iii) and draws conclusions from statistical inference to obtain valuable insight into the maturity of critical ML systems.** Results suggest that renewed efforts to collect high-quality data related to the defect tracking lifecycle can help developers to identify training and testing methods that are more effective at exposing and resolving defects, improving reliability and resilience of ML systems. Moreover, reliability and resilience models can evaluate the uncertainty associated with ML predictions, enabling users to understand system limitations, make informed decisions and effectively guide the allocation of restorative efforts.


Safety Critical System
Machine Learning System
Reliability & Resilience Engineering
System Monitoring & Evaluation
AI
Defect Detection & Performance Prediction