ABSTRACT

This study examines the adoption of the Structured Assurance Case Metamodel (SACM) as a formal framework to support the safety assurance of machine learning (ML)-based object recognition systems in autonomous vehicle (AV) applications within smart factory environments. As AI and ML technologies are increasingly integrated into safety-critical domains such as autonomous transportation, ensuring their safe and reliable operation has become essential. While existing research commonly employs structured frameworks for safety assurance, these often lack the capability to explicitly model the dialectical aspects of safety arguments. Addressing this gap, this research integrates SACM with the AMLAS (Assurance of Machine Learning in Autonomous Systems) lifecycle to develop a structured safety assurance case for an ML-based object recognition system. The study demonstrates how SACM enables explicit modelling of claims, assumptions, counterclaims, and evidence, supporting rigorous, traceable, and dialectical safety arguments throughout the entire AMLAS process. The proposed approach is implemented using a YOLOv8 object detection model deployed on the Donkey Car S1 platform within a simulated smart factory scenario. The results show that adopting SACM improves the transparency, maintainability, and scalability of safety arguments while explicitly supporting the representation of dialectical elements such as counterclaims and assumptions. This offers a replicable methodology for ensuring the safe deployment of AI/ML components in safety-critical domains, filling a critical gap in existing assurance practices.

Keywords: SACM, Machine Learning (ML), Safety Assurance, Object Recognition (OR), Autonomous Vehicles (AVs), AMLAS, YOLOv8.