

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE  
ACTIVITIES (D5)

Quality and safety, a challenge for traditional and new space (1)

Author: Mr. Matthew Driedger  
University of Manitoba, CanadaDr. Allison Ferguson  
CanadaDr. Philip Ferguson  
University of Manitoba, CanadaA SAFETY MONITORING METHOD FOR NON-DETERMINISTIC FUNCTIONS IN MISSION  
CRITICAL TASKS FROM THE COMMERCIAL DRONE INDUSTRY**Abstract**

Non-deterministic algorithms (e.g., machine learning) have been proposed for various areas of spacecraft development and operations, such as for calculating orbital transfers and interpreting scientific data. However, the inherent unpredictability of these algorithms introduces risks that are difficult to quantify or test for; inaccurate training sets or unanticipated environmental conditions may cause intelligent algorithms to fail spectacularly. Due to these risks, the adoption of machine learning type algorithms for mission critical spacecraft tasks has been slow. This work proposes using the ASTM F3269-17 software encapsulation standard, developed for the commercial drone industry, to monitor and isolate instabilities or runaway conditions in modern, potentially non-deterministic mission critical algorithms. This paper presents a case study using this standard as a wrapper around a recurrent neural network (RNN) for range-only spacecraft state estimation. This case study consists of an observing spacecraft receiving range-only data from a series of low-power RF beacons in unknown orbits. Over time, the observing spacecraft learns the orbital parameters and states of itself and the beacons. Following the ASTM F3269-17 standard, the estimator includes a safety monitor which observes the output of the RNN. If the RNN output exceeds pre-set bounds, the safety monitor switches the output of the estimator to a recovery control function: a high-reliability (and deterministic) control function that can revert the spacecraft to a safe state. Results indicate that the performance of the RNN is not adversely affected by the presence of the safety monitor. Further, the computational overhead imposed by the monitor is negligible when compared to the RNN. We suggest that the space industry adopt ASTM F3269-17 as a means of enabling a more advanced and risk-tolerant approach to space systems guidance, navigation and control development.