Safety Analysis of Autonomous Vehicles

Newsletter September 2020

Autonomous Helicopter on Mars

NASA's Mars 2020 **Perseverance** rover lifted off from Cape Canaveral in Florida on July 30. The rover will take seven months to reach Mars where it will search for signs of life, explore the planet's geology, and do much more. The image below is an artist's rendering of the Mars Helicopter which is part of NASA's mission. It is a small helicopter that will become the first aircraft to fly on another planet. Its name is **Ingenuity**.

ASCA's Association with Mars 2020 and Ingenuity?

As described below, two ASCA projects are directly related to the Perseverance and Ingenuity missions.

Perseverance is powered by a Multi-Mission Radioisotope Thermoelectric Generator (MMRTG) provided by the U.S. Department of Energy, which converts the heat from the natural decay of plutonium-238 to generate electricity. Because of this material on board, a risk assessment of the launch phases of the Mars 2020 mission had to be carried out, and the results approved before the mission launch could be authorized. ASCA has been carrying out for NASA the launch vehicle portion of the risk assessment, not only for Mars 2020, but over the years for many other missions, like Pluto New Horizons and Mars Science Laboratory, which carried similar power sources on board.

Ingenuity is the product of a NASA/JPL technology demonstration project. Its mission is to prove that an autonomous Mars helicopter can be used for future exploration and science missions. ASCA was awarded a NASA Phase II SBIR project in August 2019 to demonstrate its safety analysis software for autonomous vehicles. With JPL's assistance, ASCA used the Ingenuity design and Mars helicopter mission concepts in a safety case-study and software development. The safety goal defined in the case-study is to avoid damage to an Ingenuity-like helicopter due to possible sand storms on Mars. Since it takes between 4 to 24 minutes for electronic signals to travel round-trip between earth and Mars, remote control to avoid fast moving storms, or other fast developing contingencies, is not practical. Future and more complex successors of the Ingenuity autonomous helicopter will need to autonomously identify and react to storms or other possible mission threat scenarios. In the sand storm scenarios analyzed by ASCA, a Mars helicopter is able to decide on its own if it has time to go back to a sheltered main base, if it should seek temporary shelter in a deep (and safe) crevice or crater, or if it should land as soon as possible in a shallower (less sheltered) crater to minimize potential damage. The case study has demonstrated that a real-time autonomous decision can be carried out using AI and logic-probabilistic software hosted in the helicopter flight computer.

The total cost of a typical exploration and science mission to Mars is in the order of $Billions. If the Ingenuity technology demonstration is successful, future Mars missions are expected to rely on expanded autonomous helicopter technology of considerable sophistication and cost. The NASA mission Dragonfly, designed by the Johns Hopkins University Applied Physics Lab (JHUAPL) and scheduled for launch in 2026, plans to use another type of autonomous helicopter to explore the Saturn moon Titan.

ASCA is continuing to perform off-line demonstrations of its technology to facilitate its use by NASA and its major laboratories and centers in actual missions.

Who Is ASCA?

ASCA, Inc. is a US firm located in Los Angeles, California, that provides risk assessment and reliability management tools and services for very complex systems. ASCA has 30 years of experience in providing these services to aerospace, defense, electric power, and chemical industries. The company founder (Dr. Sergio Guarro) has 40 years of experience in risk analysis, he is an Aerospace Fellow, has produced 90 publications, and has led, or had major roles, in numerous NASA risk assessments.

ASCA provides seamless integration of classical logic-probabilistic risk assessment and assurance

techniques (Fault Tree, Event Tree, Event Sequence Diagram, Failure Mode and Effects Analysis) with advanced design assurance techniques (e.g., multi-state and dynamic methods such as the Dynamic Flowgraph Methodology (DFM)) and AI techniques for system diagnosis and decision support (Neural Networks, Bayesian Belief Networks (BBN), Influence Diagrams (ID)).

Dr Guarro is the principal inventor of the DFM technology and he has led numerous projects on its development and applications for safety analysis. For more information, please visit our website (ascainc.com) or call us at (310) 316-6249.

How Is ASCA Different?

ASCA is a leader in the aerospace industry in terms of top-down analysis of system requirements and V&V. We plan and carry out validation of the system functional requirements, to be followed by verification that the system is designed and built right. Analytical verification of requirements is not always carried out in structured and systematic fashion, even in established industrial sectors like the automotive and software industries. Postponing validation to after a product is developed or built can potentially have a substantial cost implication.

What Is the Main Message in this Newsletter?

ASCA is now halfway through its two-year SBIR project. The team is working with NASA on deploying our safety methodology in future autonomous space systems. That part of the project is progressing well. We are now looking for a partner so we can demonstrate how to use our software for safety analysis of autonomous cars.

ASCA can team up in a 50/50 sharing of cost and benefits with a company who has expert understanding of ISO-21448 & SOTIF and can provide good use case(s) for the design assurance of autonomous or partially autonomous automobiles. The aerospace industry has a substantial amount of expertise in safety and design assurance analysis that can benefit the auto industry. ASCA'S approach is top-down, model-based, probabilistic, risk informed, and integrated in an MBSE.

Let us work together and then lead the industry in making autonomous vehicles safer at an economic cost.

We plan to send ASCA newsletters once per quarter. We will provide updates on how we proceed with the work for NASA as well as our entry into the auto industry. If you do not want to receive future newsletters, send us a return email to unsubscribe.

Map Functional Requirements to Analytical Models