

Dynamic Assurance of Autonomous Systems through Ground Control Software

Irfan Sljivo, Ewen Denney

KBR/NASA Ames Research Center, USA
irfan.sljivo@nasa.gov, ewen.w.denney@nasa.gov

Abstract. Assurance cases are being increasingly acknowledged as a way to build trust in complex systems with autonomous capabilities [1]. An assurance case is a comprehensive, defensible, and valid justification that a system will function as intended for the specific mission and operating environment. Such justifications for systems with autonomous capabilities are often based on various probabilistic quantifications [2]. Due to the dynamic nature of the environmental conditions in which these systems operate, as well as the changing nature of the autonomous systems themselves, these probabilistic quantifications cannot be simply estimated once during design time. Rather, they need to be continually evaluated during systems operations to ensure that the assurance case justifications are valid. We refer to the assurance case that combines both the static and dynamic elements as a Dynamic Assurance Case (DAC). Such complex systems with autonomous capabilities are often deployed with a Ground Control Software (GCS) component to enable remote operation. Whether the system is composed of a single unit or a fleet of units, deployed distributed or in remote environments, GCS acts as a window into the behavior of the deployed system. It receives telemetry from the system, issues commands to the system and provides various functionalities to visualize the system performance.

We propose a dynamic assurance framework where the GCS acts as a relay between the autonomous system and its DAC. GCS can be used to measure both unit-specific as well as system-wide probabilistic quantifications using the incoming telemetry. We embed these quantifications throughout the DAC as variables that can be updated by external sources. We use the GCS to periodically update these variables, which allows us to continually evaluate the formally defined assurance case justifications.

We demonstrate our dynamic assurance framework in the NASA Ames project Troupe1 that aims at developing a fleet of rovers capable of autonomously mapping their environment. The rovers work cooperatively, each collecting data for different parts of the environment. Each rover runs an identical core Flight System (cFS) [4] application. Troupe1 uses OpenC3 Cosmos [5] as the ground system, and AdvoCATE [3] to capture the system DAC. We show how we can measure both rover-specific and system-wide quantifications in Cosmos using its Ruby scripting editor and pass them into the DAC modelled in AdvoCATE. Then, we show how these incoming variables can be embedded in different parts of the DAC and how effects of their updates can be observed.

References

- [1] E. Asaadi, E. Denney, J. Menzies, G. J. Pai, and D. Petroff. Dynamic assurance cases: A pathway to trusted autonomy. *Computer*, 53(12):35–46, 2020.
- [2] E. Asaadi, E. Denney, and G. Pai. Towards quantification of assurance for learning-enabled components. In *2019 15th European Dependable Computing Conference (EDCC)*, pages 55–62. IEEE, 2019.
- [3] E. Denney and G. Pai. Tool support for assurance case development. *Automated Software Engineering*, 25(3):435–499, 2018.
- [4] D. McComas. NASA/GSFC’s Flight Software Core Flight System. In *Flight Software Workshop*, volume 11, 2012.
- [5] OpenC3 Cosmos, <https://openc3.com/>.