Driving the Development Process from the Safety Case

Christopher Hobbs[1], Simon Diemert[2] and Jeff Joyce[2]

1 Blackberry QNX, Ottawa, Canada
2 Critical Systems Labs Inc., Vancouver, Canada

Abstract. The production of a Safety Case is often seen as the "wrapping up" of the safety process – an activity that begins after earlier steps, such as hazard and risk analysis, have been completed. This misses the opportunity to benefit from the critical thinking that underlies a high-quality Safety Case. Especially when using Eliminative Argumentation, an incremental approach to the Safety Case can make the entire development process more efficient. In a range of industries including automotive, aerospace, energy, nuclear and rail, we have witnessed the benefits of starting Safety Case development early. We have used an incremental approach to the Safety Case to help shape the functional safety concept, derive safety requirements, influence system and software architectures, and focus validation and verification in a way that is commensurate with the system and is most likely to yield useful results.

Accepted for presentation at the International Workshop on Assurance Cases for Software-intensive Systems (ASSURE) at SafeComp 2023, https://www.nasa.gov/content/assure2023-program