R. Alexander, T. Kelly, G. Despotou

To appear in proceedings of the 29th International System Safety Conference (ISSC), 8-13 August 2011, Las Vegas, NV, USA.

Abstract

When you create a System of Systems (SoS), you are doing wilful design. It follows that you need a safety case: a justification of why that system will be safe. All safety cases must have certain common properties: they must focus on risk, they must provide appropriate confidence in their claims, and they must have a clear relationship to a causal model of the system's safety behaviour. None of those are particularly easy for SoS, and there are several areas where SoS are particularly problematic, such as what exactly "the system" comprises, and what on Earth its lifecycle actually is. On the other hand, not everything about SoS safety is necessarily hard, and not every problem faced in SoS safety is an "SoS problem".