

Secrets of a successful safety case

An increasing number of Australian projects are required to provide safety cases. This is sometimes driven by regulators' requirements which, for example, require operators of hazardous plants to provide safety cases for their operations. However, even in industries where there may not be specific legal requirements to provide safety cases, regulators and operators may still require safety cases for specific projects. Even in the absence of customer pressure, some suppliers in Australia are supplying safety cases with their systems as part of their efforts to achieve good practice in their safety assurance, and thereby legal defence against negligence claims.

There are many standards available that set out requirements for safety cases, for example in the railway industry. However, developing a successful safety case requires more than just following requirements in standards. A successful safety case involves developing an appropriate safety acceptance strategy, planning the implementation of the strategy and then harnessing the efforts of managers and engineers on the project towards the achievement of the strategy. The project must deliver the evidence required to support the safety case. The safety professionals on the project must present the safety assurance in a manner that makes it possible for assessors and customers to endorse and accept the safety case.

This half-day tutorial will cover the secrets of a successful safety case, including how to develop a successful safety acceptance strategy, the fundamentals of a successful safety argument, techniques to achieve involvement and buy-in from managers and engineers on the project, the art of presenting the safety argument in the best possible manner, and common pitfalls in safety case development and how to avoid them. The tutorial will utilise a worked example from the railway industry.

The tutorial is aimed at system safety professionals as well as systems engineers, project engineers and project managers working on safety-related projects (for example projects delivering complex systems or software-intensive systems in the railway, oil and gas, automotive and defence industries). The tutorial focuses on safety cases, but the approach described will be useful for any project that wants to deliver convincing and valid safety assurance.

The presenters are Dr Neil Robinson of RGB Assurance and BJ Martin of Nova Systems. Together, Neil and BJ bring extensive experience from the railway, aerospace and defence industries.

Neil Robinson (*PhD, CEng, CITP, BSc(Hons)*) is a Director of RGB Assurance Pty Ltd providing services in high integrity systems engineering. Neil has more than 15 years experience in the field of high integrity systems engineering, including senior roles in system suppliers in the rail industry, consulting, training and education. Neil's experience includes development of safety cases, assessment of safety cases and liaison with customers, assessors and regulators of safety-critical systems. Neil is also an Adjunct Professor in the School of Information Technology and Electrical Engineering at The University of Queensland.

BJ Martin, (*GradDipTech Mgt, GradCertProjMgt, BEng(Aero)*) is the Nova Systems Competency Lead for System Safety and Technical Certification/Airworthiness providing professional services to defence and complex technology industries. He is an accomplished aerospace engineer with over 20 years broad work experience (including 11 years in the Air Force) for a variety of fixed and rotary wing aircraft types designed to both civilian and military certification standards. His specialisation has been in planning, negotiating and managing new aircraft type airworthiness certification, system safety programs and Safety Case evaluation. Over the past decade he has been involved in conducting number of Safety Case evaluations for safety-related software intensive military situational awareness and mission planning tools and collaborated in an effort to develop experience based guidance material for the Issue 2 of DEF(AUST) 5679. BJ has also been a developer and principal trainer for a 5-day System Safety Engineering introductory course to aerospace and maritime defence and industry audiences for over 6 years.