



Presented by

C. VAN GULIJK / UNIVERSITY OF HUDDERSFIELD / TNO HEALTHY LIVING

G. BEARFIELD / UNIVERSITY OF HUDDERSFIELD / ROCK RAIL

R.J. THOMAS / UNIVERSITY OF BIRMINGHAM

SECURITY / SAFETY ASSESSMENT WITH THE STAIRCASE MODEL

BACKGROUND

Digitalization transforms the railway undertakings, from services, rolling stock, infrastructure and all components within. With such systems it becomes increasingly difficult to demonstrably assure safety critical functions with a traditional safety case approach.

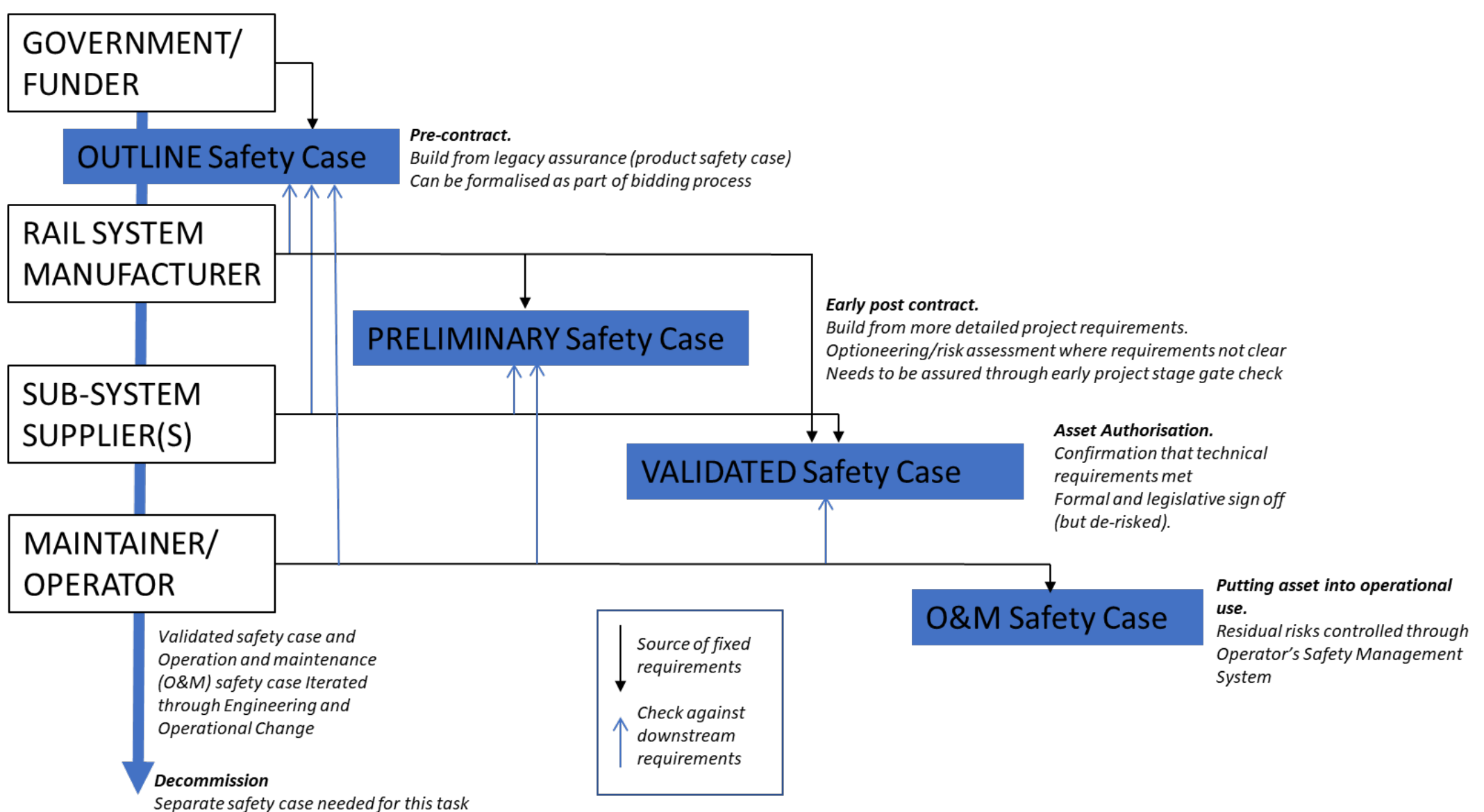
PROPOSAL

This work proposes a revised assurance lifecycle model, the safety 'STAIRCASE'. The method proposes better preparation of current safety case practices (the VALIDATED safety case) by developing a pre-contract OUTLINE safety case and an early post-contract PRELIMINARY safety case. It also proposes an O&M safety case for end-users. Benefits of the approach include, but are not limited to:

- The scope of the safety case is clear before contracts are signed,
- There is clarity about the (software) architecture of the train early on,
- It creates a commercial incentive to enhance safety and security by design,
- It also allows early engagement with the future user/operator on operational risks, and
- It sets really clear safety requirements for the tier 1 & tier 2 supply chain.

THE FUTURE IS PRESENT

The approach forces all stakeholders to think more carefully about safety and (cyber) security and is better equipped to deal with complex data systems and rapidly changing software. The maintains current assurance methods. Regulatory oversight could be beneficial but that is not strictly necessary.



c.vangulijk@hud.ac.uk / +31-629207659



IRSC 2022

INTERNATIONAL RAILWAY SAFETY COUNCIL

SEVILLA, OCTOBER 16-21, 2022