A Safety Case Development Framework

Helen Auld
Helen.auld@awe.co.uk
0118 98 50080

© British Crown Owned Copyright 2013/AWE&Dstl

Published with permission of the Controller of Her Britannic Majesty’s Stationery Office.

“This document is of United Kingdom origin and contains proprietary information which is the property of the Secretary of State for Defence. It is furnished in confidence and may not be copied, used or disclosed in whole or in part without prior written consent of Defence Intellectual Property Rights DGDCDIPR-PL - Ministry of Defence, Abbey Wood, Bristol, BS34 8JH, England.”

Contents

- What is a safety case?
- Why develop a safety case development framework?
- The safety case development framework explained
- Conclusion

What is a Safety Case?

- “The Safety Case shall contain a structured argument demonstrating that the evidence contained therein is sufficient to show that the system is safe.” (Def Stan 00-56)

- UK approach is non-prescriptive

Difficulties with Current Safety Cases

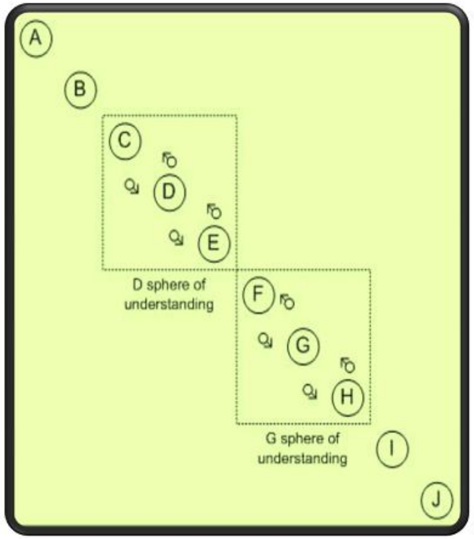
- Do not cope well with system of system issues
- Lack mechanisms to interface with each other
- Lack of standardisation allowing incompatible and difference in approaches
- Can be difficult for project teams and regulators to understand
- Often monolithic
- Can be difficult to update/change
- Can be hard to identify areas where the evidence does not support the claim

The Goals of the Safety Case Development Framework (1)

- To apply safety case best practice
  - underpinned by engineering models and existing practice
  - underpinned by detailed analysis such as formal methods

- To retain existing legacy evidence and arguments (by using 'black box' approach)

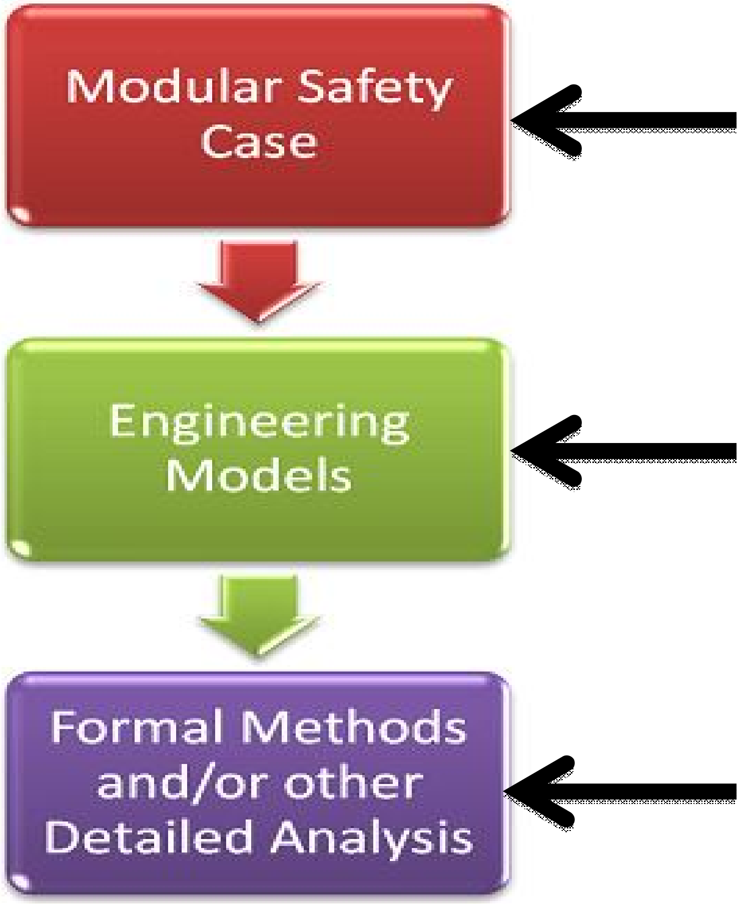
- To manage 'need to know'



The Goals of the Safety Case Development Framework (2)

- To handle complexity to make the safety case comprehensible while still being comprehensive
- To focus on dependencies between parts of the safety case
- To ensure context is considered and consistent

The Structure of the Safety Case Development Framework



Arguments
Comprehensible argument providing understanding of the safety, security and dependability requirements

Evidence
Models to provide evidence, and to exercise the arguments and the interfaces

Validation
Detailed models to validate the key arguments and provide evidence

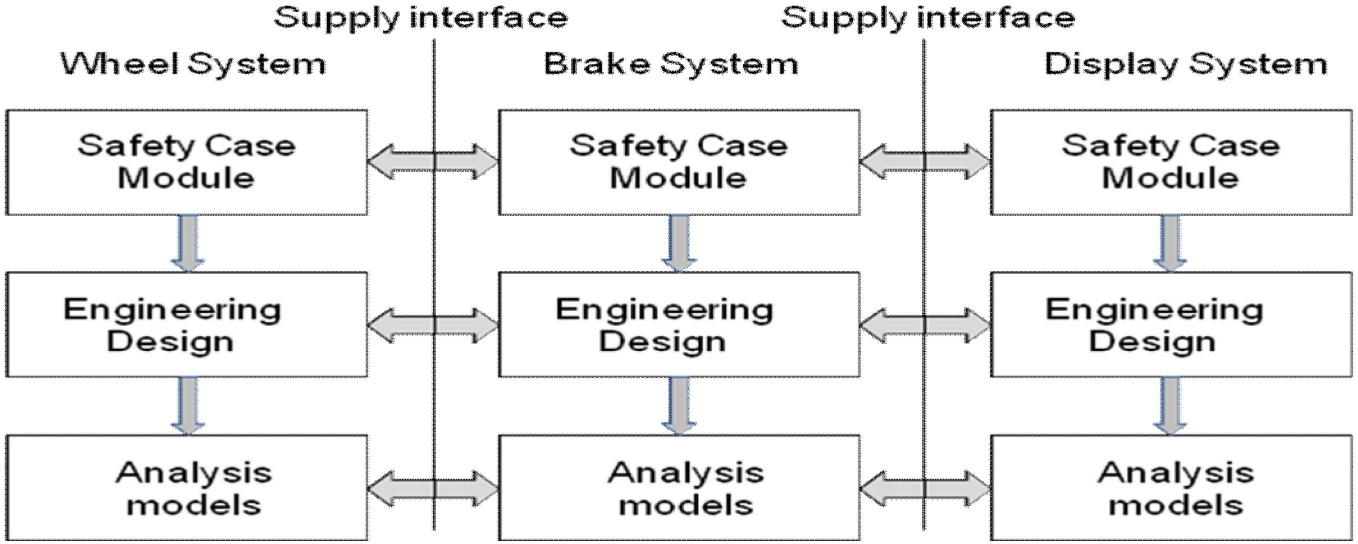
The Benefits of the Components of the Safety Case Development Framework

- **Modular Safety Cases** – isolation and security, ease of design and development, reduction in duplication of effort, division in effort
- **Engineering models**– early proofing of interfaces, simulation of design functionality, early human factors analysis
- **Formal Models** – quantitative evidence on high risk definable hazards, verification of supplier provided specifications

(All of the above can wrap existing evidence and arguments)

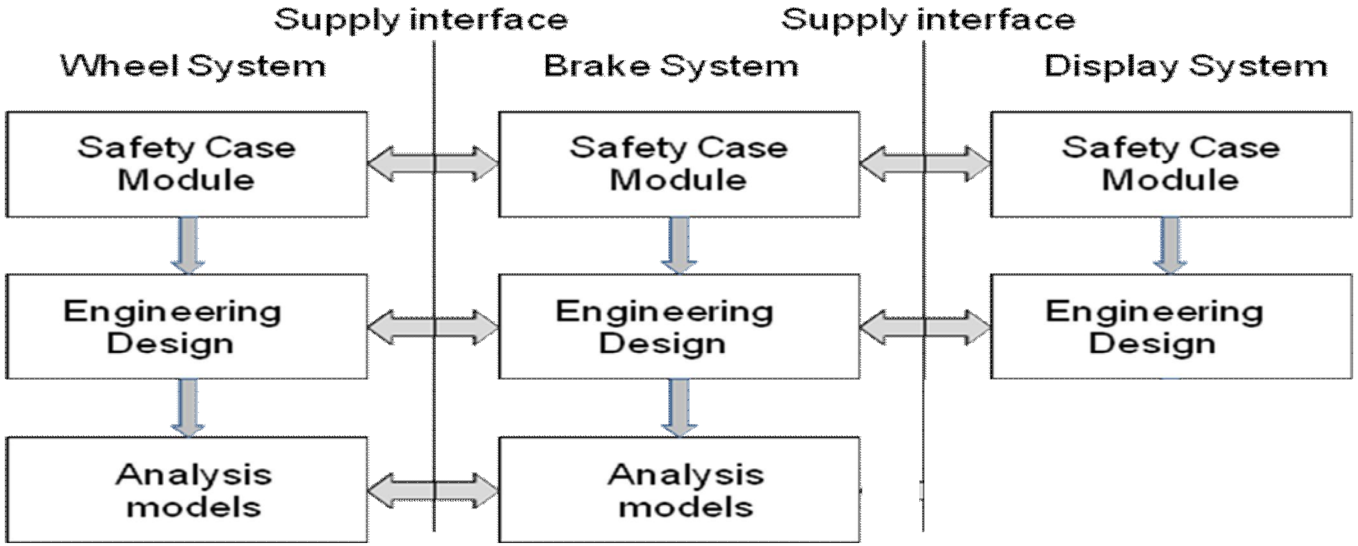
The Interfaces of the Safety Case Development Framework

- Framework helps to form an opinion of the interface interactions
- Enables the definition of dependency relationships at appropriate supply interfaces at the different levels of the Framework



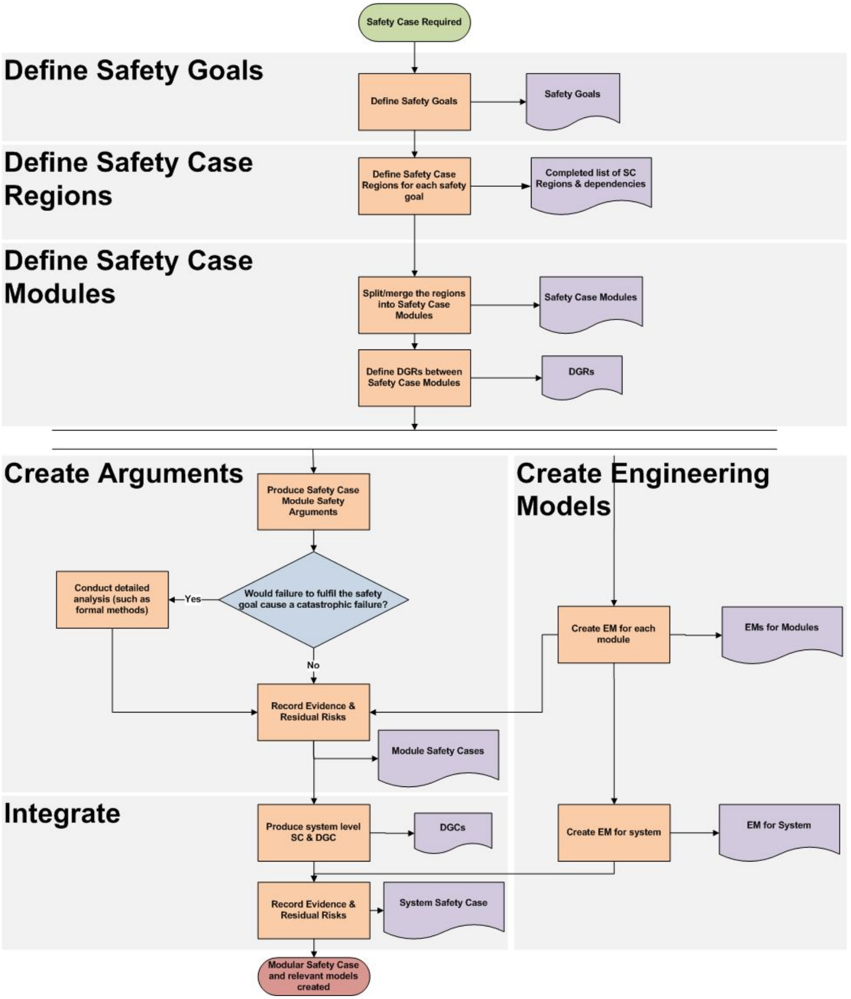
The Interfaces of the Safety Case Development Framework

- Framework helps to form an opinion of the interface interactions
- Enables the definition of dependency relationships at appropriate supply interfaces at the different levels of the Framework
- Only share sufficient information in each framework layer



The Safety Case Development Framework (1)

- 1. Define Safety Goals & Functions
- 2. Define Safety Case Regions
- 3. Define Safety Case Modules
- 4. Create Arguments
- 5. Create Engineering Models
- 6. Integrate



Safety Case Required

Define Safety Goals

Define Safety Goals

Safety Goals

Define Safety Case Regions

Define Safety Case Regions for each safety goal

Completed list of SC Regions & dependencies

Define Safety Case Modules

Split/merge the regions into Safety Case Modules

Safety Case Modules

Define DGRs between Safety Case Modules

DGRs

Create Arguments

Produce Safety Case Module Safety Arguments

Would failure to fulfil the safety goal cause a catastrophic failure?

Yes

Conduct detailed analysis (such as formal methods)

No

Record Evidence & Residual Risks

Module Safety Cases

Create Engineering Models

Create EM for each module

EMs for Modules

Integrate

Produce system level SC & DGC

DGCs

Create EM for system

EM for System

Record Evidence & Residual Risks

System Safety Case

Modular Safety Case and relevant models created

Conclusion (1)

- Arguments have traceability to the *evidence* and the *models of the evidence*

- Arguments are grouped together into modules allowing each to be understood in isolation and the whole safety case to be understood by an individual

- Models can be used to inform, aid and provide verification evidence of the system

- Models can be used to aid understanding of the system including interfaces and human relationships

Conclusion (2)

- Integration risk is reduced as interfaces are clearly defined

- Legacy, bespoke, and COTS systems can be integrated into the system safety case

- Issues surrounding IPR and sensitive information can be managed

Contributors

- Mike Standish Dstl
- Paul Caseley Dstl
- Mark Hadley Dstl