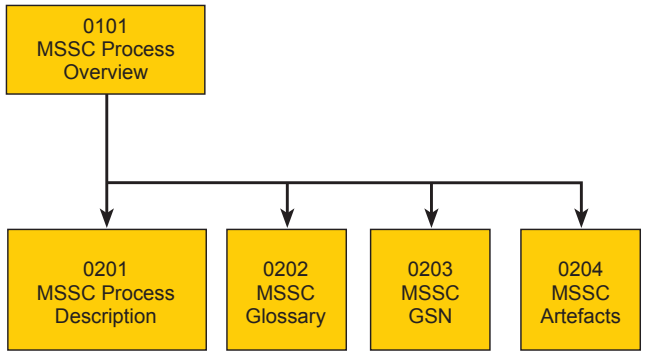
What are the Benefits of Modular Software Safety Cases?

- Modules can be replaced providing they satisfy the same safety properties
- Impact of change can be localised, based on safety argument module dependencies
  - ✓ Only update directly affected module arguments and/or evidence
  - ✓ Other modules are not affected
  - ✓ Reduces effort (cost) and timescales to assure changed system
- Supports distributed team-working
- Supports workshare between partners subcontractors
- Can be used to protect IPR or manage export restrictions

MSSC Process Documents and Guidance



Would MSSC be 'Right' for Me?

Criteria have been identified which help to determine whether your project is 'receptive' to modular Safety Cases. These criteria are based on what benefit you can expect from MSSC and how easy it is to implement a modular Safety Case

Maximising Benefits:

- ***System Size and Complexity*** – MSSC is most beneficial in managing change in large and/or complex systems
- ***Anticipated Change*** – MSSC delivers greatest benefit where there are expected to be a number of small to medium size changes implemented throughout the life of the system

Factors Determining Effectiveness:

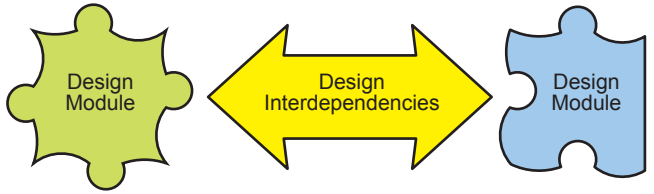
- ***Design Modularity*** – MSSC is simpler to introduce for systems that use modular design approaches
- ***Reusability*** – MSSC supports the re-use of existing design modules that have an existing safety argument
- ***Use of COTS/Legacy/3rd Party Software*** – MSSC can facilitate the use of COTS, Legacy or 3rd party software, provided there is suitable access to design information and evidence

A series of questions and a spread-sheet based tool have been developed to help you assess the 'receptivity' of your system to MSSC.

Contacts

www.capability-agility.co.uk
david.short@baesystems.com
charlie.hewitt@baesystems.com

Modular Software Safety Cases



Incremental Upgrade to Military Capability

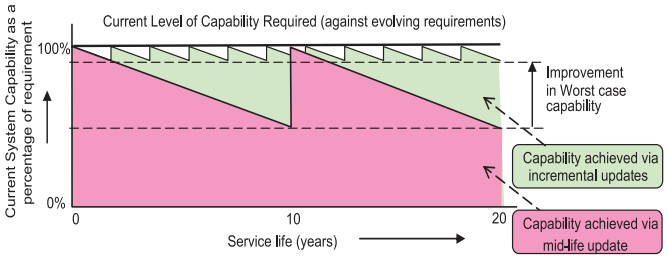
Managing the complexity of safety assurance

www.capability-agility.co.uk

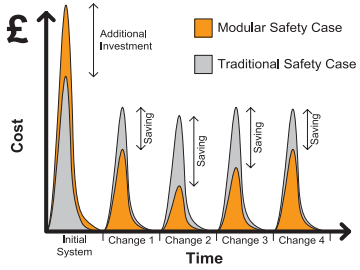
Introduction

The frequency and scope of changes to defence systems are typically constrained by the significant costs involved, yet the military capability provided by a system is perceived to decay over time when it is compared to the evolving 'state of the art' systems which may be available to cooperating or opposing forces.

Rather than addressing the short-falls against that perceived and constantly evolving military capability requirement, changes are typically 'parked' until they can be collated into a major upgrade programme, such as an aircraft mid-life update. If costs could be reduced, more frequent, smaller changes could be deployed, more closely 'tracking' the peak operational capability.

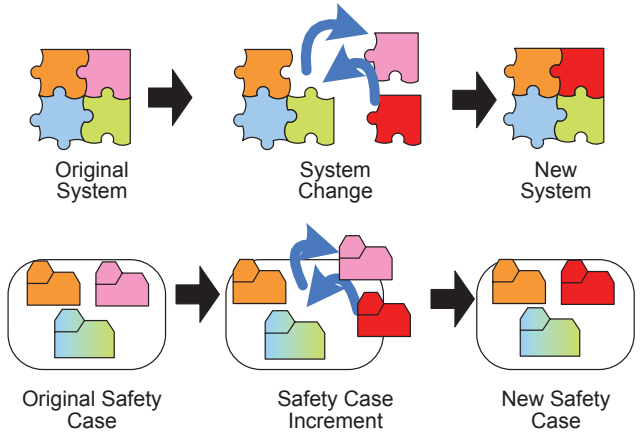


The safety certification for modified systems is a major contributor to the cost of change, often approaching the original certification costs for the system. A modular approach reduces the cost of re-certification of changed systems, leading to an overall through-life cost saving when compared to traditional Safety Cases



Modularity to Handle Complexity

A powerful way of dealing with the size and complexity of designs is to break them down into smaller 'modules'. This is true of many types of design, including software. However, existing safety assurance processes have always stressed the importance of considering the whole 'entity' and so the design modularity provides no assistance to assuring the safe operation of a system. Consequently, the Safety Case generated to demonstrate the safety assurance of a system is often complex and very inefficient to maintain when the system is changed. Demonstrating the safety of a changed system is therefore often costly and takes a long time, which can become a barrier to enhancing system capability.



www.capability-agility.co.uk

Modular Safety Cases – *Current Status*

As of the end of 2012, a modular Safety Case process has been trialled on real defence software systems. The software aspects have been matured and validated to a level suitable for immediate deployment.

Modular principles are being adopted for system safety assurance and performance qualification on several real aircraft programmes.

This approach has been demonstrated on military avionics, but the principles could equally be applied on other defence systems

What are Modular Software Safety Cases?

The Modular Software Safety Case (MSSC) process takes advantage of the modularity in software designs when providing assurance of a safe system composed from these modules.

The same principles that are used in modularising software designs are applied to safety arguments. Modules in the safety assurance argument are defined that map onto design module(s) with well defined safety properties.

When systems are composed from these modules, there is a clearer understanding of the dependencies between the design modules and between the Safety Case Modules related to them.