SafSec: Integration of Safety and Security
Why SafSec?

S.P1199.50.6
Issue: 1.3
Status: Definitive
2nd November 2006

Originator

Samantha Lautieri (Project Manager)

Approver

David Jackson (Safety Consultant)

Mark Suitters (FBG-3d)

Copies to:

Client
Mark Suitters (FBG-3d)

Praxis Critical Systems
Project File

Other
SafSec Website
Any who request

Why SafSec?

Are Your Problems:

SafSec addresses major risks in system acceptance

- How to ensure completeness in addressing safety and security?
- How to reduce overlap and duplication within safety and security?
- How to reduce costs involved with assuring safety and security?
- Realising Integrated Modular Avionics (IMA)?
- How to achieve certification of your product/system?

Or

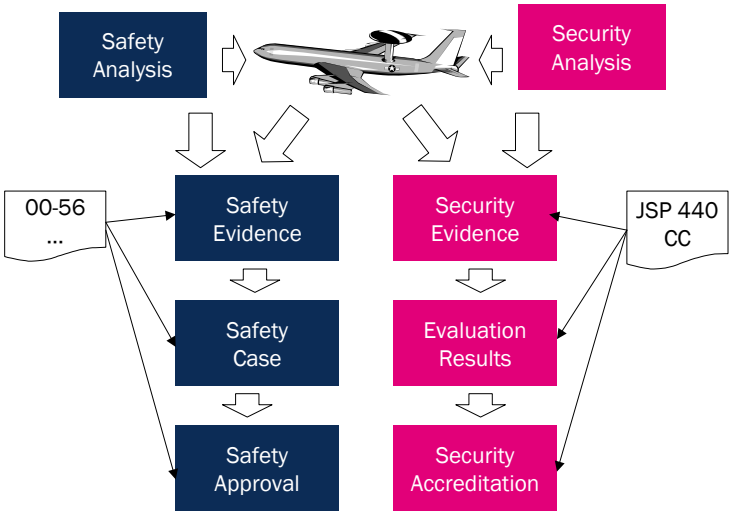
- Would you like to simplify the certification and re-certification of legacy systems?

If you've asked yourself any of these questions then it is very probable SafSec has a place within your organisation and on your development program.

Original Requirements for SafSec

Applicable, but not limited, to IMA

The MoD wished to address these issues, particularly with respect to new technologies such as Advanced Avionic Architecture (AAvA) and Integrated Modular Avionics (IMA). The MoD saw a problem in the duplication of different assurance activities:



This current practice has been applied successfully to many systems, but there are three aspects that needed to be addressed:

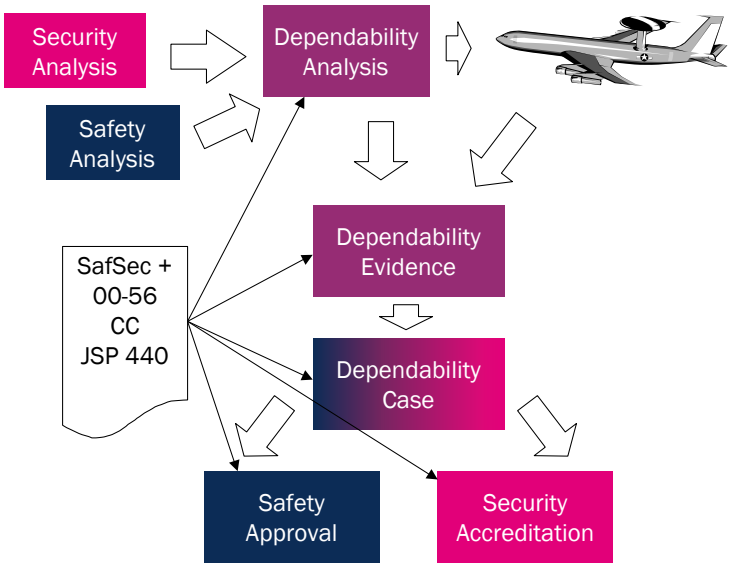
- reduction in overlaps and duplication
- explicitly addressing the conflicts and gaps in the safety and security
- tailoring current practice to facilitate effective application to modular systems

The first two points are applicable for any program. All the points can potentially produce cost savings and resulted in the original requirement for SafSec.

Specification of the SafSec Approach

Reducing effort and cost

To meet these requirements, the approach must minimise the overlaps and duplicated effort, combine best practice from both the safety and security domains and manage assurance in a way applicable to IMA.



Integrated approach to safety and security certification

These criteria suggest an integrated approach to *dependability*, whereby both safety and security should, where practicable, be handled in parallel. This approach can be adopted from the earliest phases of the programme, and aims to encourage collaboration between the safety, security and programme domains. Such an integrated approach enables conflicts, gaps and mitigations to be handled in the most appropriate way, and simplifies the maintenance of traceability and assurance evidence.

Sound due to its solid foundation and stakeholder backing

The specification was developed through the formulation of sound academic principles for integrating safety and security. These principles have been described in a paper (S.P1199.50.1), and provide a solid foundation for an integrated approach. Combining the academic principles of an integrated approach with

- stakeholders' input;
- case studies;
- developments in IMA;
- consideration of best practice;
- analysis in the production of a dependability case;
- and related research conducted to date

resulted in a SafSec standard (S.P1199.50.2) and a guidance document (S.P1199.50.3), which provide a methodology for use on programmes with safety and security requirements and document its relationship with existing safety and security practices. The standard and guidance are written with IMA programmes in mind, but the methodology is more widely applicable.

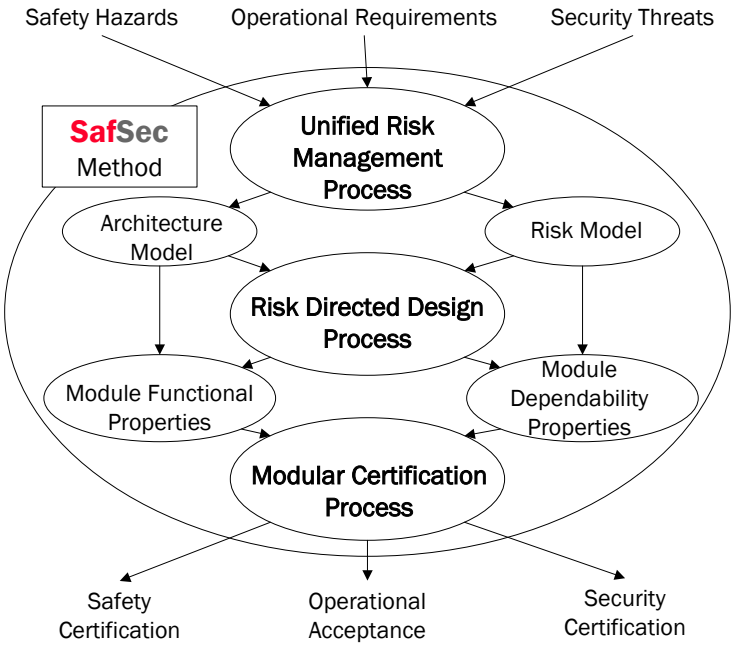
Practical Implementation of SafSec

Assurance of SafSec dependability through:
- **Unified Risk Management**
- **Risk Directed Design**
- **Modular Certification**

In terms of applying SafSec the standard defines the principal objectives that the systems' developments has to achieve. The principle objectives are encapsulated within a:

- Unified Risk Management: takes account of safety hazards and security threats, together with the operational requirements of the target system, to produce a risk model (capturing the relevant causal relationships) alongside the architectural model of the system;
- Risk Directed Design: uses the risk model, together with the architectural model of the system, to define the dependability properties of all the system modules in parallel with their functional properties, and produces the arguments supporting traceability of this process;
- Modular Certification: takes the module's functional and dependability properties in the form of clear specifications, and uses supporting arguments and evidence to justify certification of a module. As modules can be composed from collections of other modules, multiple application of this process can be provided for in system certification. The result of the process is a set of safety and security certificates, and information that can support operational acceptance.

The Guidance Document illustrates how the principal objectives, set out in the standard, can be achieved and includes a mapping of the relationship between SafSec and DefStan 00-56, Common Criteria.



The Benefits

If you are a developer, purchaser, owner, certifier, user, or accreditor SafSec has something to offer you

SafSec offers advantages for all stakeholders concerned with proving assurance of safety and security on a programme.

- To the Developers:
  - A single accreditation framework
  - Reduced effort and cost
- To Certifiers and Accreditors:
  - Evidence re-use and sharing
  - A structure for modular certification
- To Purchasers and Users:
  - Reduced certification and re-certification costs

— Practical implementation path for those with IMA

Way Forward

SafSec is currently being verified and validated through Case Studies that are anticipated to complete in Q1 of 2005. In the mean time if you would like to find out more or want to obtain the SafSec standard and guidance documents feel free to contact us:

www.praxis-his.com/SafSec

praxis-his-safsec@praxis-his.com

Praxis:

Samantha Lautieri, Project Manager,
Praxis High Integrity Systems,20
Manvers St, Bath, BA1 1PX

direct dial: 01225 823775
switchboard: 01225 466991
samantha.lautieri@praxis-his.com

MoD DPA:

Mark Suitters FBG 3d, Project Sponsor
MOD DPA FBG, Larch 2, Abbeywood,
Bristol, BS34 8JH

direct dial: 0117 9134180
fbg-3d@dpa.mod.uk