Overview of Part II

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

What does Part II do?

n Specifies the Security Functional Components from which SFRs are constructed

Ø*Functional Classes*

n Defines a Functional Paradigm

Ø*Model of Security Functionality*

n Provides guidance on use of Security Functional Components

Ø*Application Notes*

Structure of Part II

- Introductory Material
- Functional Requirements Paradigm
- Component Definitions
  - *Structure and 11 classes*
- Application Note Appendices
  - *Structure and 11 classes*

Introductory Material

- Introduction
- Scope
- Normative References
- Terms and Definitions, Symbols and Abbreviated Terms
- Overview of Document Structure

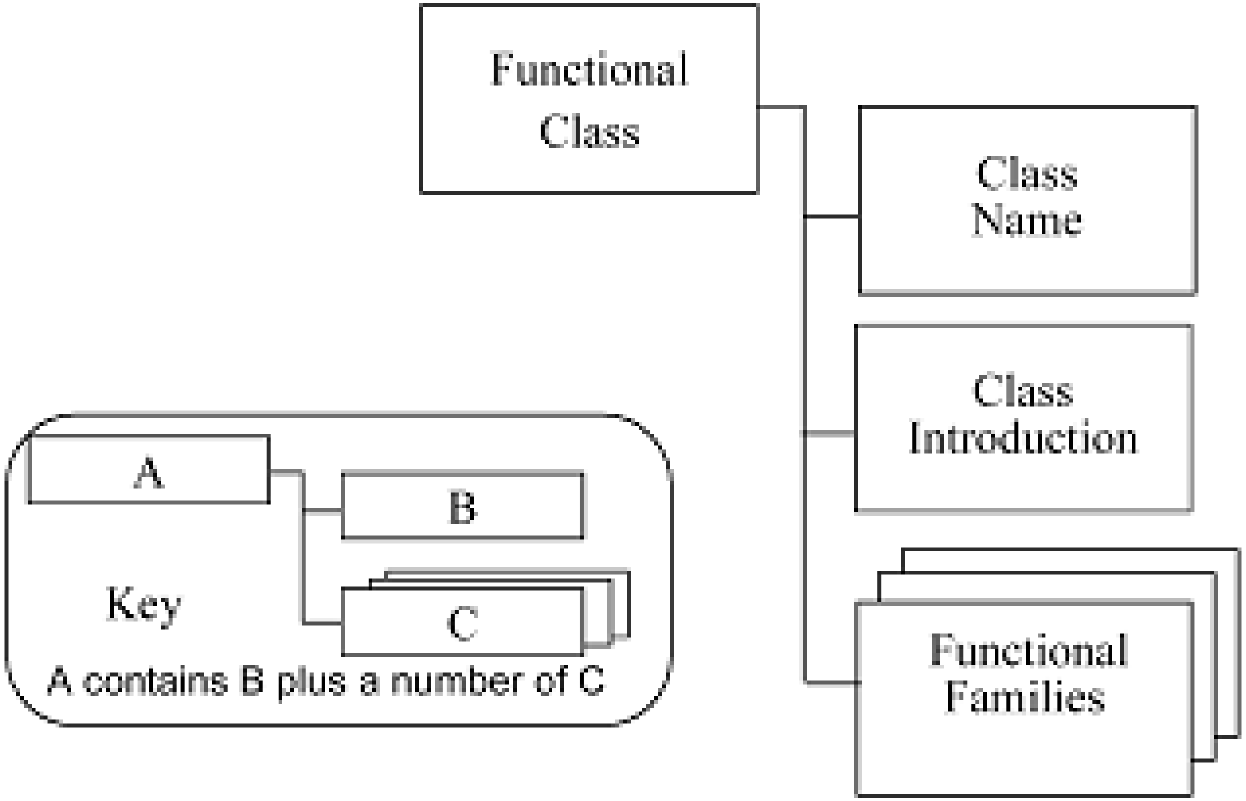
Requirements Paradigm

- Describes a model for security functionality
  - *Most concepts pretty standard*
    - *Users – information – security attributes etc.*
- Some unique concepts
  - *Security Function Policies (SFPs)*
    - *The rules a TOE must enforce*
  - *TOE security functionality (TSF)*
    - *Those portions of a TOE that must be relied on for the correct enforcement of the SFRs*
  - *TSF Interface (TSFI)*
    - *The set of interfaces through which resources are accessed or information obtained from the TSF*

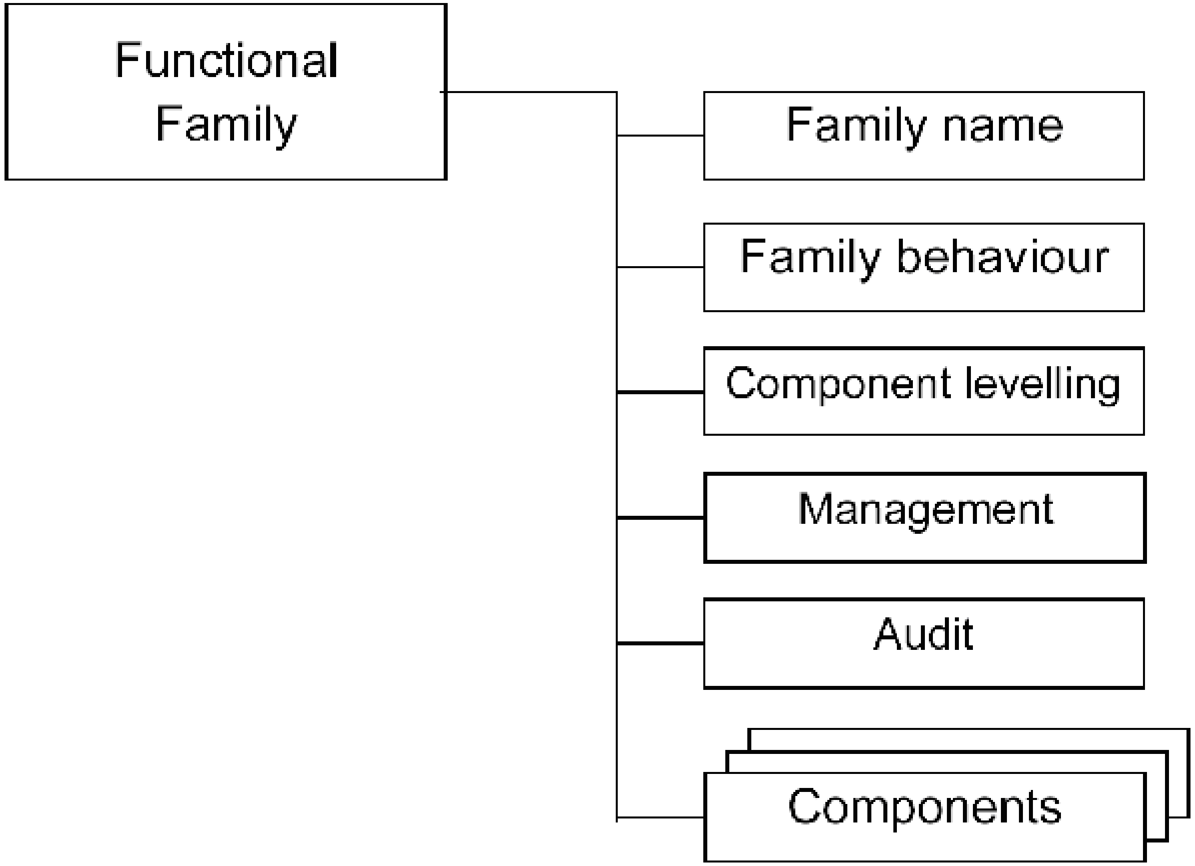
Component Definitions

- Define security functional components from which Security Functional Requirements can be generated for inclusion within the Security Requirements section of a PP or ST
- Related components grouped into families
- Related families grouped into classes
- One Part II chapter per class

Functional class structure



Functional family structure



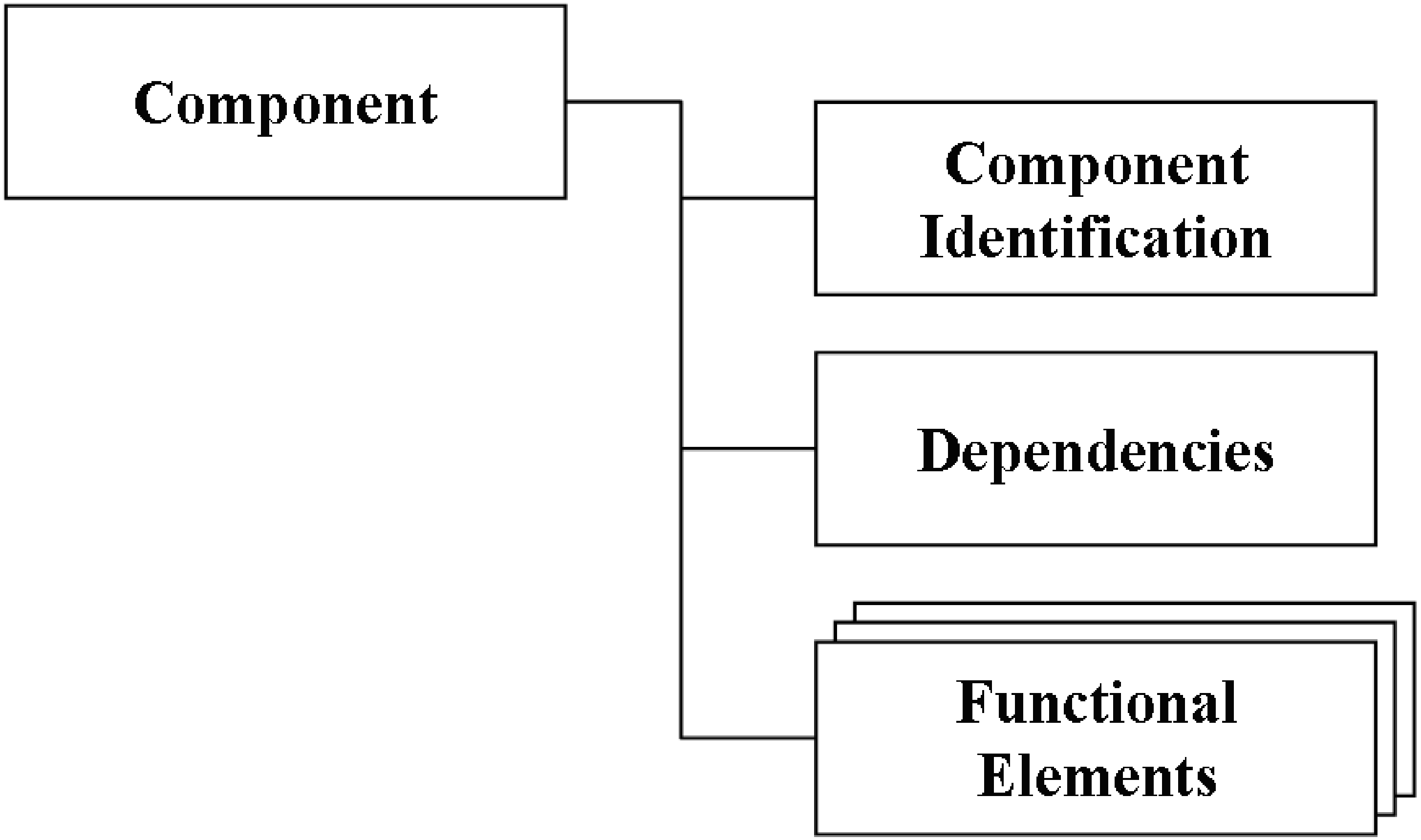
Family specification

- Everything in the family specification should be requirements, not guidance
  - *Guidance is found in the application notes*
- However, the family behaviour is descriptive
  - *How to use the family*
  - *Does not really belong here*

Configuration

- Levelling information tells you which components are interrelated
- Management information tells you which aspects of components could be configurable during operation
- Audit information tells you which aspects of components could be recorded during operation

Component structure



Components

n Identification is the name of the component Fxx_xxx.n <descriptive name>

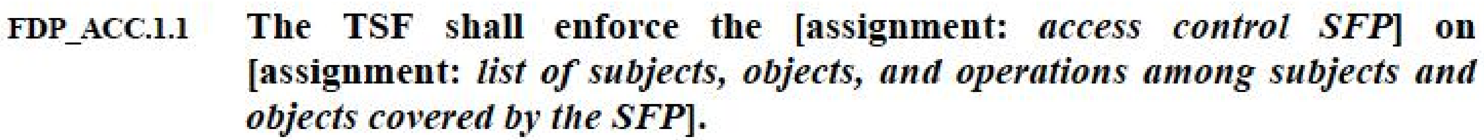
n Dependency information identifies other components that must be present in the TOE

n Dependency information also includes any hierarchy position

Ø*Duplicates levelling information*

n But mainly a list of functional elements

Functional elements



FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

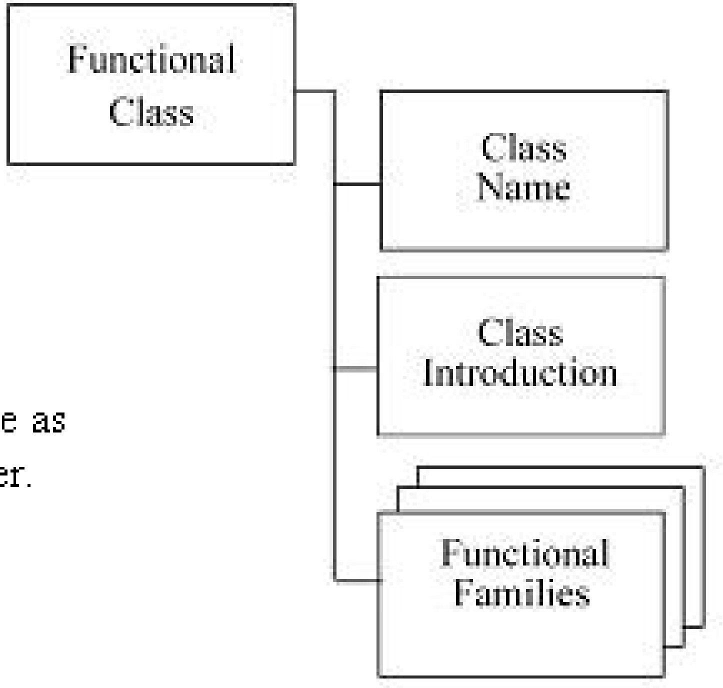
Creating SFRs

- Copy the selected component into the PP or ST
- Complete assignments, selections and refinements (ST, possibly PP)
- Repeat (iterate) if more than one requirement to be covered
- Editorial refinement to improve grammar or readability

Application notes

- Provide guidance on how to use component definitions
- Annex A contains introduction and dependency tables
  - *Annex B is empty*
- Then one Part II annex per class (Annex C to M)

Notes class structure



Functional Class

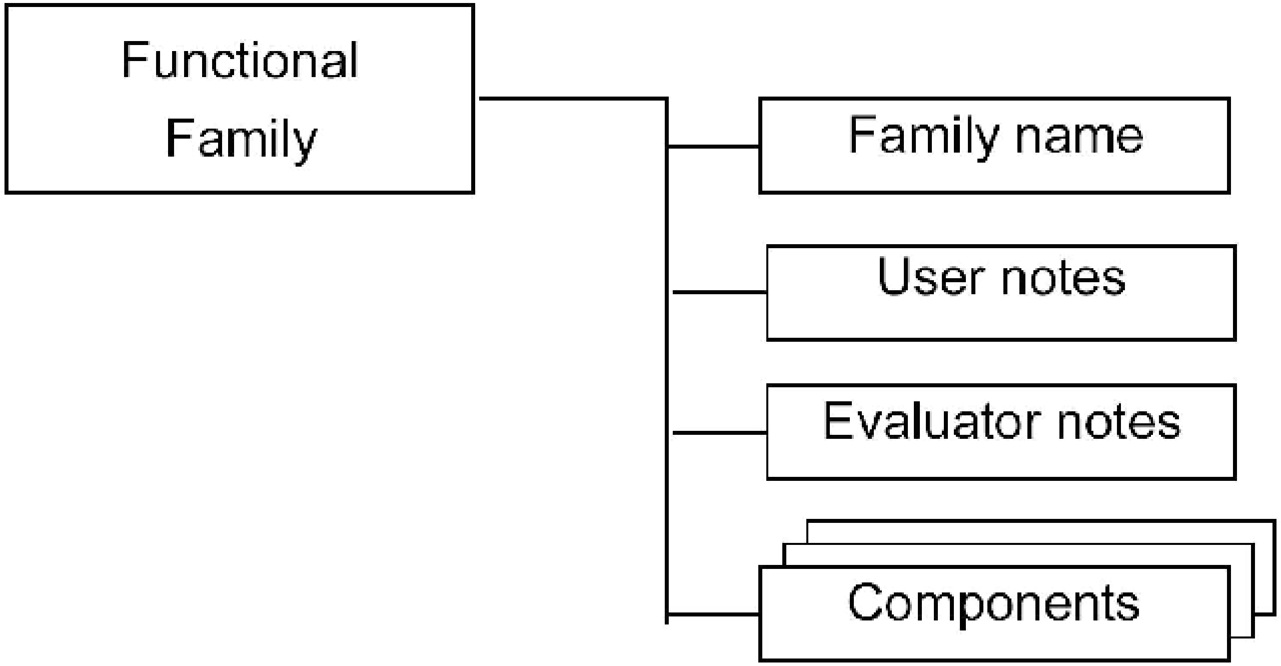
Class Name

Class Introduction

Functional Families

This is the same structure as the corresponding chapter.

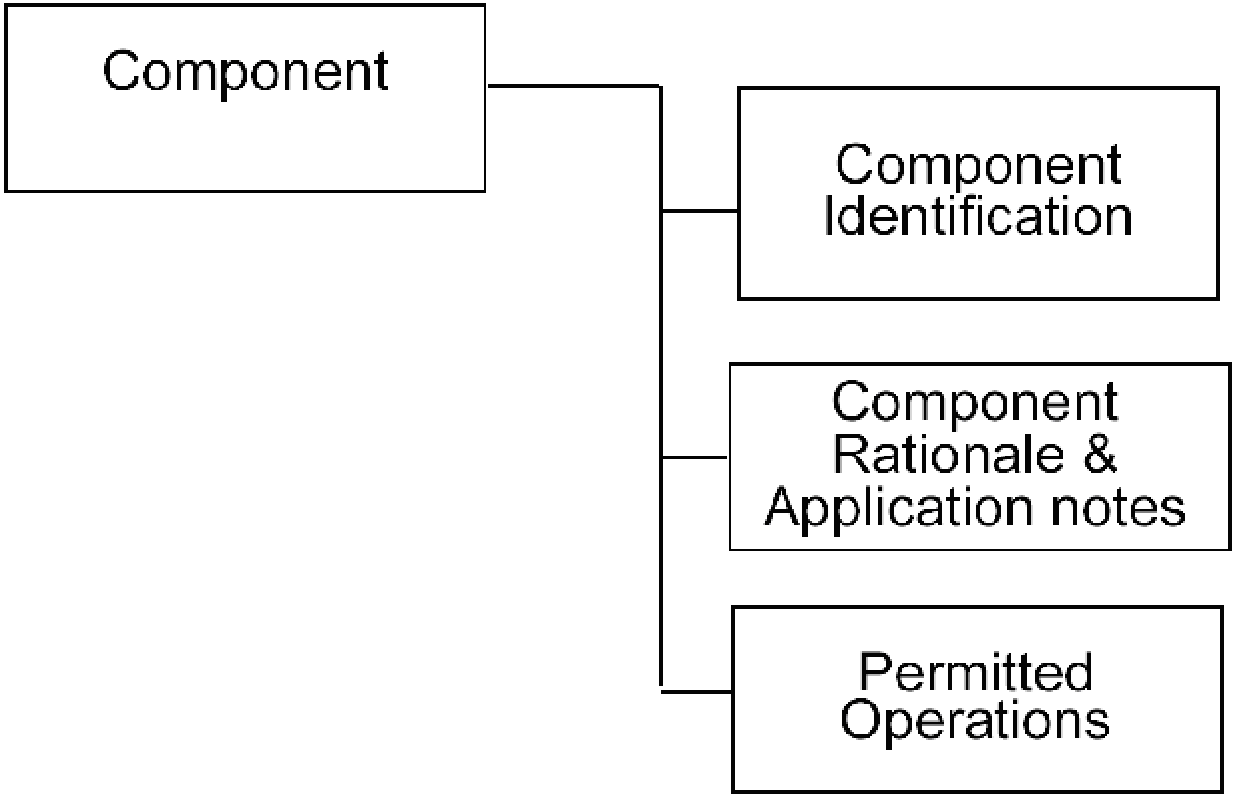
Notes family structure



Family notes

- User notes contain information relevant to users of components within the family
- Evaluator notes contain information relevant to developers and evaluators of products using components within the family

Notes component structure



Component notes

- Identification is the name of the component
- There are no component rationales
  - *Although paragraph 111 of Chapter 8 ought to be the component rationale for FAU_SAR.1*
- User application notes and/or evaluator notes apply only to this component
- Operations explain how to complete assignment and selection operations of the component

Complexity

- There are 147 pages of component specifications and 139 pages of application notes
- Many operation specifications (selection, assignment) are confusing
  - *Poor descriptive words*
- Flexibility, level of detail and explanation varies between classes
- Management and audit are inconsistent in detail

Why is Part II so confusing?

n Poor structure

- Ø*Defined in 1995 and unchanged since*
- Ø*Complex organisation*

n Overlapping components

- Ø*General components and specialist components*

n Designed to map directly from previous (and now obsolete) criteria

Improving Part II

n CC Version 3.0 tried to simplify Part II:

Ø*No appendices*
Ø*Stronger functional paradigm*
Ø*Simplified components*

n Failed to solve the reduction problem

Ø*All you actually need to express functionality is one component with three substitutions*
Ø*"A will do B to C"*

n Abandoned – no consensus support

Summary

- Part II specifies how to construct security functional requirements for PPs and STs
- Catalogue of Security Functional Components
  - *Rules for how to customise and complete them*
  - *Application notes on how to use them*
- Part II structure is complex but usable

Overview of Part II

Any questions?

Overview of Part II

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk