Common Criteria

EPOCHE & ESPRI

Common Criteria v 3.1 Tutorial part I

9ICCC Korea, 24/09/2008

Contents

a. IT Security Evaluations

b. The Common Criteria

c. Key Concepts

d. Security Specifications

IT Security Evaluations

The security search

It is possible to determine the security of a product? **NO.**
We can **only demonstrate the insecurity of the products.**

Then?
We can **offer confidence degrees** in the product security**.**

How to obtain this confidence?
If a method that generates secure products is followed and vulnerabilities have not been found, we will affirm that it is secure,
BUT

What conviction do we have?
In relation to the **effort** applied searching vulnerabilities.

IT Security Evaluations

The security search

What method does generate secure products?

Any "generic" development method should be able to obtain secure products, if the security is a desirable attribute.

IT Security Evaluations

The certification process

Independent inspection of the results of the evaluation leading to the production of the final certificate.

Security Evaluation

EPOCHE & ESPRI

EPOCHE & ESPRI | OUR SERVICES | SOLUTIONS | JOIN US | CONTACT US

Your best companion to CC certification!

WELCOME TO EPOCHE & ESPRI!
Evaluation of IT security

SEARCH GO

A new face is coming to the IT product security evaluation....
→ Click here to read more about us

- CC training
- Product evaluation
- Development best practices

Request a free consultation!

Our services ... from CC training to evaluation ...
→ Click here to learn more

Solutions ... to implement the best security practices ...
→ Click here to learn more

Join us ... we are expanding and need your skills ...
→ Click here to learn more

ENAC ENSAYOS Nº 622/LE1399

About Epoche & Espri | Our services | Solutions | Join us | Contact us

Epoche & Espri © 2007-2008. All Rights Reserved

The security evaluation is a perfect gear in the certification process

IT Security Evaluations

What does it mean a CC certificate?

a) The security specification is true.

b) The confidence level in this assertion.

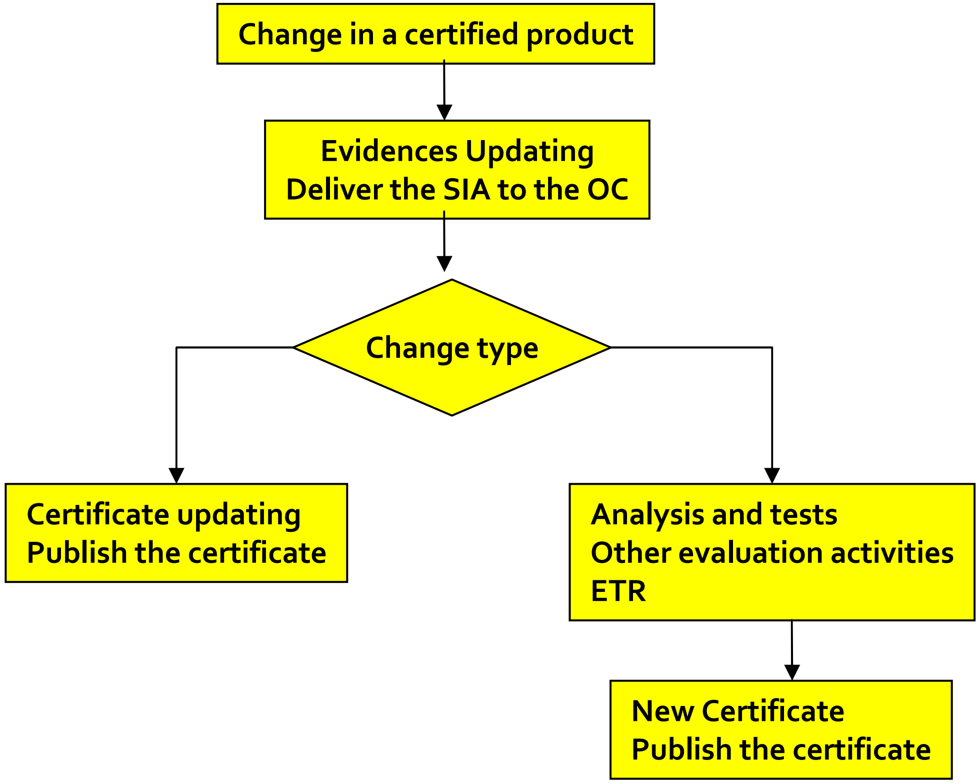
A technical report determines ↓

- if the evaluation of the security specifications and of the product have been satisfactory, and
- if the security assurance level have been obtained in the evaluation.

IT Security Evaluations

Certificates maintenance: “Assurance Continuity”

We have already certified a product. If we change the external colour does it lose the certification?



Out of the scope of CC

Contents

a. IT Security Evaluations

b. The Common Criteria

c. Key Concepts

d. Security Specifications

The Common Criteria

What is the ISO 15408 standard?

- Is an international agreement on the **secure development method and 7 discreet effort levels.**

- Is a **security architecture paradigm** to which a coherent **security functional requirements catalogue** is applied allowing the establishment of a common language for the expression of the IT products and systems security.

The Common Criteria

Application of the CC

Specially useful for:

- **Specifying security features** in a product
- Assisting in the **building of security features** into a product
- **Evaluating the security features** of products
- **Supporting the procurement of products** with security features.

The Common Criteria

CC structure: current version 3.1 R2 (Rome 2007)

- Part 1: Introduction and general model (R1)
- Part 2: Security functional components (R2)
- Part 3: Security assurance components (R2)
- CEM - Evaluation methodology (R2)
- Supporting documents

Target audience

- Consumers
- Developer
- Evaluators ......

Contents

a. IT Security Evaluations

b. The Common Criteria

c. **Key Concepts**

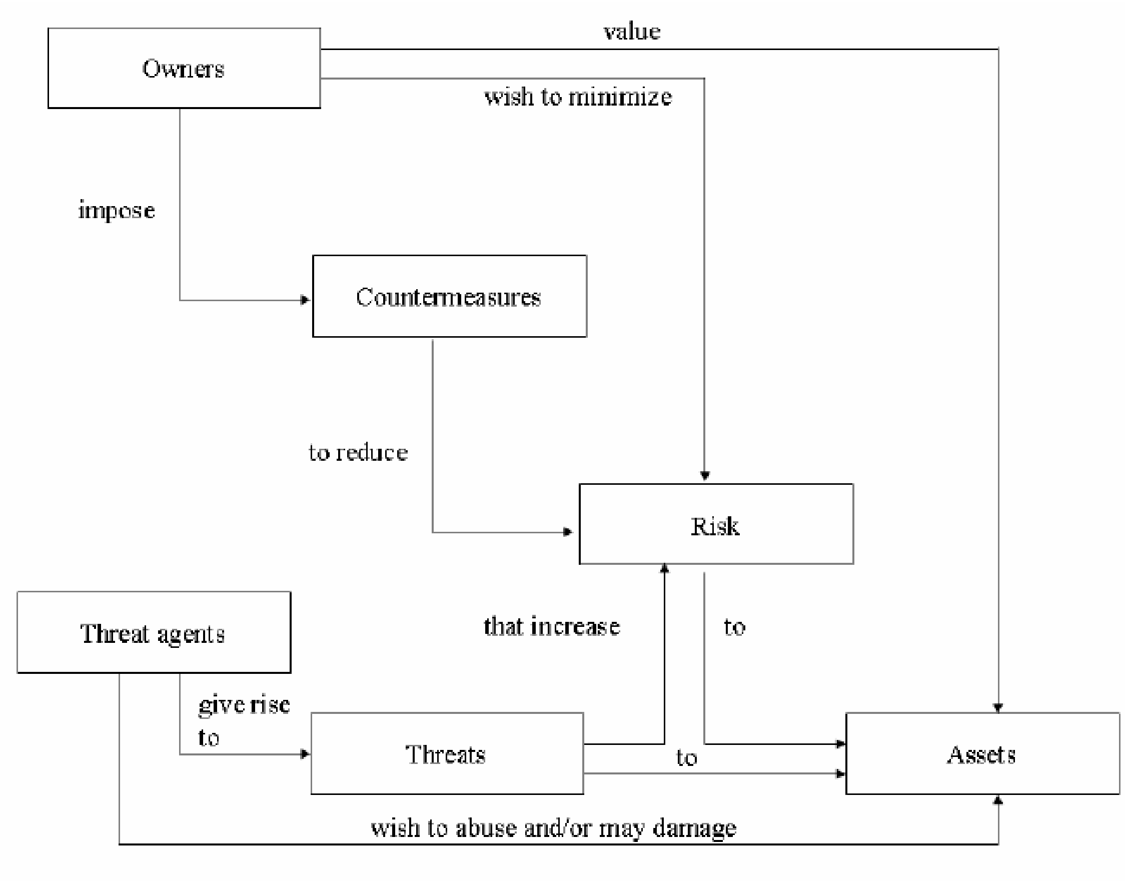
d. Security Specifications

Key Concepts

The security concept

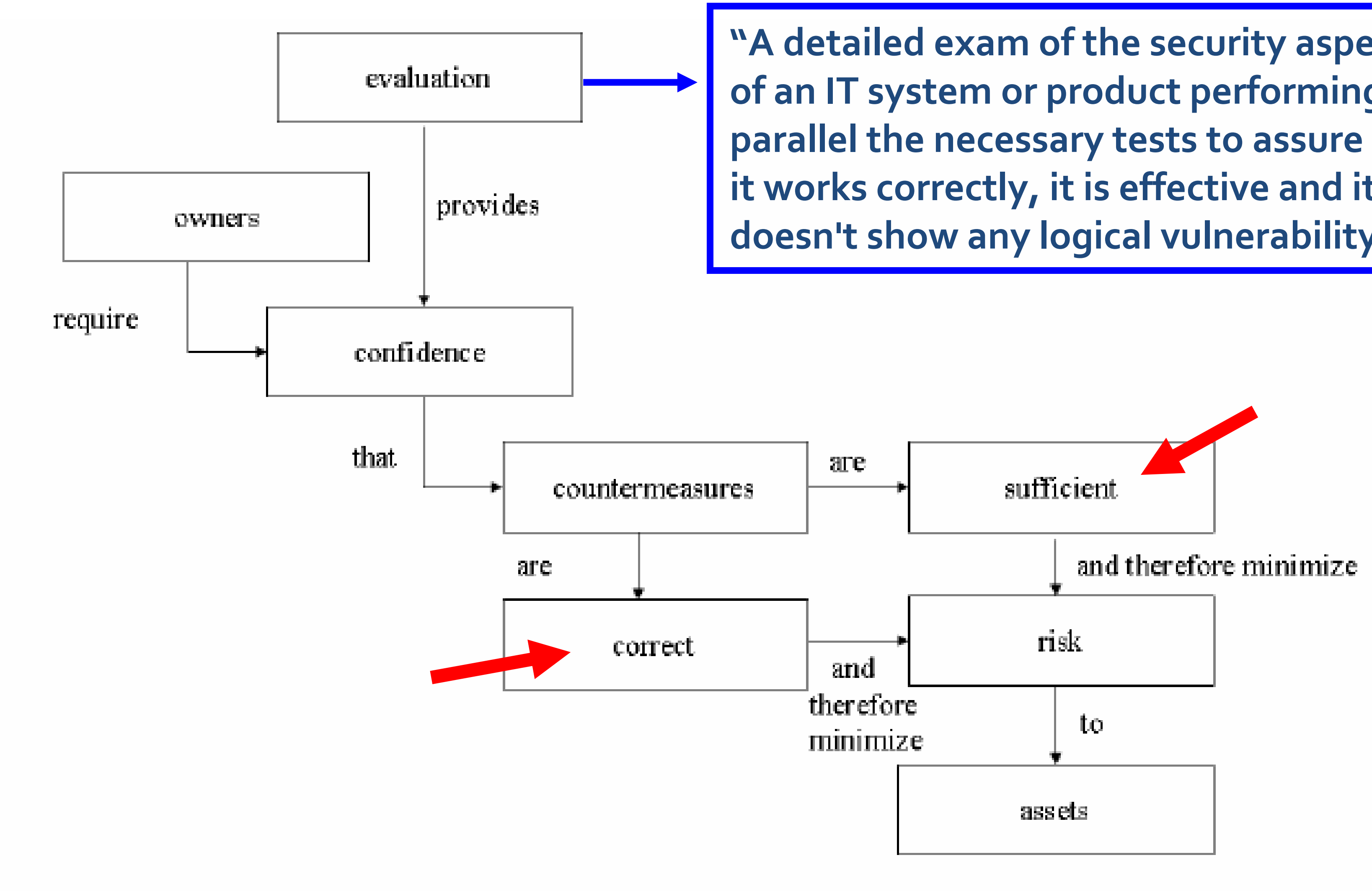
Security is concerned with the **protection of assets**.

Maintenance and safeguard of three basic aspects:
- **Confidentiality**
- **Integrity**
- **Availability**



Key Concepts

The evaluation concept



"A detailed exam of the security aspects of an IT system or product performing in parallel the necessary tests to assure that it works correctly, it is effective and it doesn't show any logical vulnerability".

Key Concepts

The Target of Evaluation

A **TOE** is a set of software, firmware and/or hardware accompanied by guidance documentation.

The evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product.

Multiple configurations are collective called "the TOE" and each configuration must meet the TOE requirements.

Key Concepts

Functionality

Defines the TOE security characteristics (SFRs)

Assurance

Confidence degree in the enforcement of the security objectives of a TOE (SARs) ⇔ **Correctness** & **Effectiveness**

Greater assurance results from the application of greater evaluation effort: Scope, Depth and Rigour

Key Concepts

Descriptive material: Security requirements expression

Component organization

Classes, Families, Components, Elements

Operations

Iteration, Assignment, Selection, Refinement

Dependencies

Extended Components

Key Concepts

Security Specifications

CC Security Specifications:

- Protection Profile (PP)
- Security Target (ST)

The end result of an evaluation is never

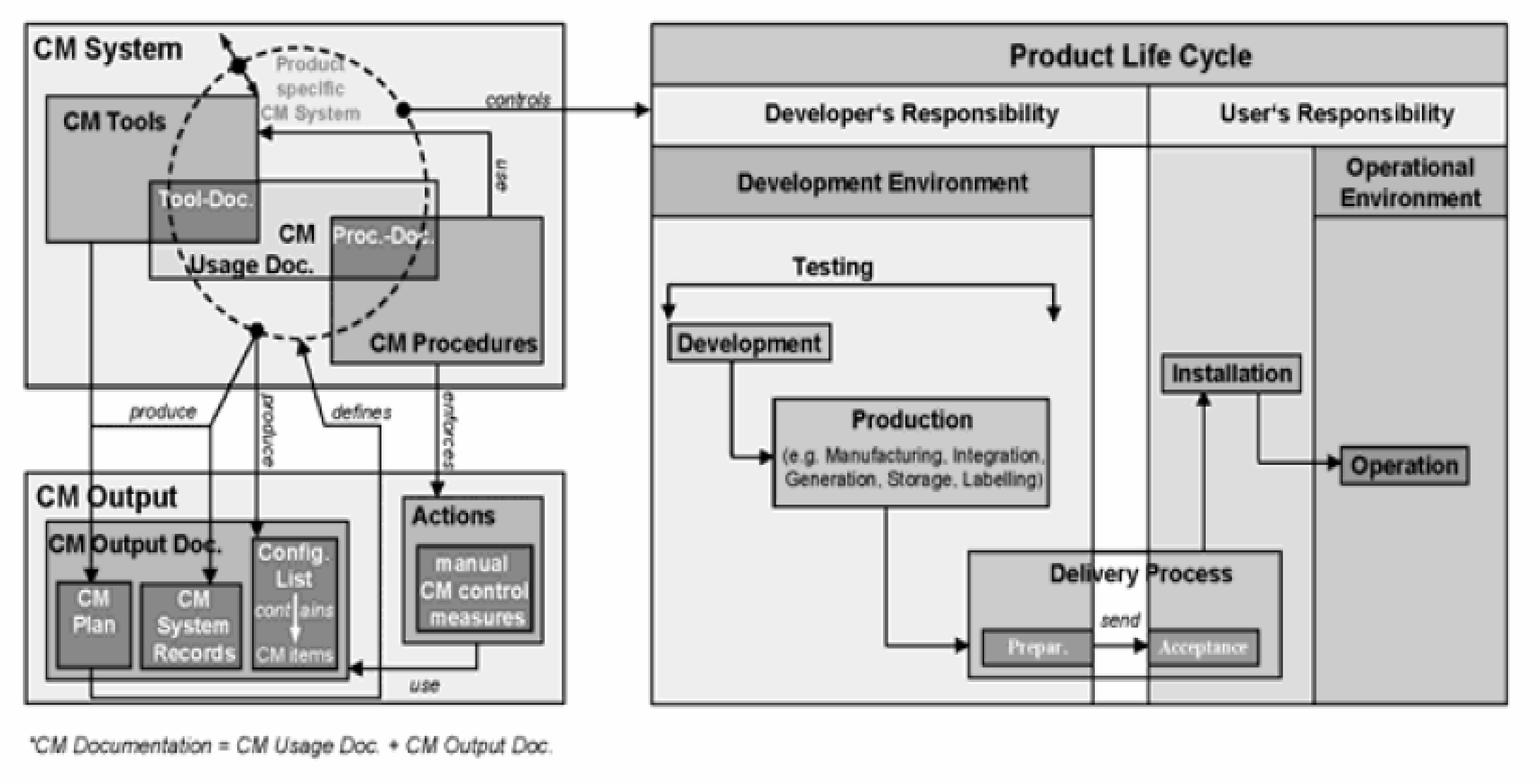
“this IT product is secure”,

but is always

“this IT product meets, or not, this security specification”

Key Concepts

The process vs. The product



Key Concepts

Vulnerability Analysis

Determines the existence of exploitable vulnerabilities in the TOE in its operational environment:

- the identification of potential vulnerabilities;
- penetration testing

Determines whether the TOE is resistant to penetration attacks performed by an attacker possessing an attack potential **Basic, Enhanced basic, Moderate, High.**

Key Concepts

The Evaluation Assurance Levels (EALs)

7 predefined assurance packages increasing assurance

The assurance is increased by replacing components of the same family by another of higher hierarchy

The notion of **augmentation** allows adding components of higher hierarchy

EALs are the base for the mutual recognition

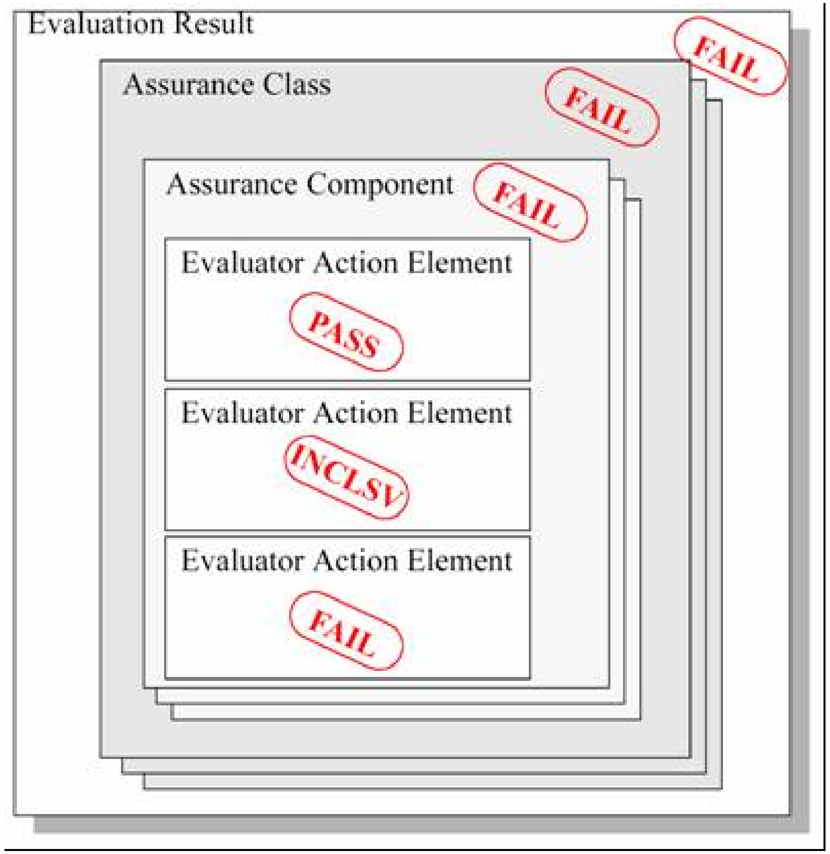
Key Concepts

EPOCHE & ESPRI

Evaluator Outputs

- ETR: Evaluation Technical Report
- OR: Observation Reports

The evaluator will report the conclusions of the evaluation, providing an overall verdict determined by all the constituent activities verdicts.



Contents

a. IT Security Evaluations

b. The Common Criteria

c. Key Concepts

d. Security Specifications

Security Specifications

Definition

Protection Profile (PP): an implementation-independent statement of security needs for a TOE type.

Security Target (ST): an implementation-dependent statement of security needs for an identified TOE.

Security Specifications

The role of the Security Specifications.

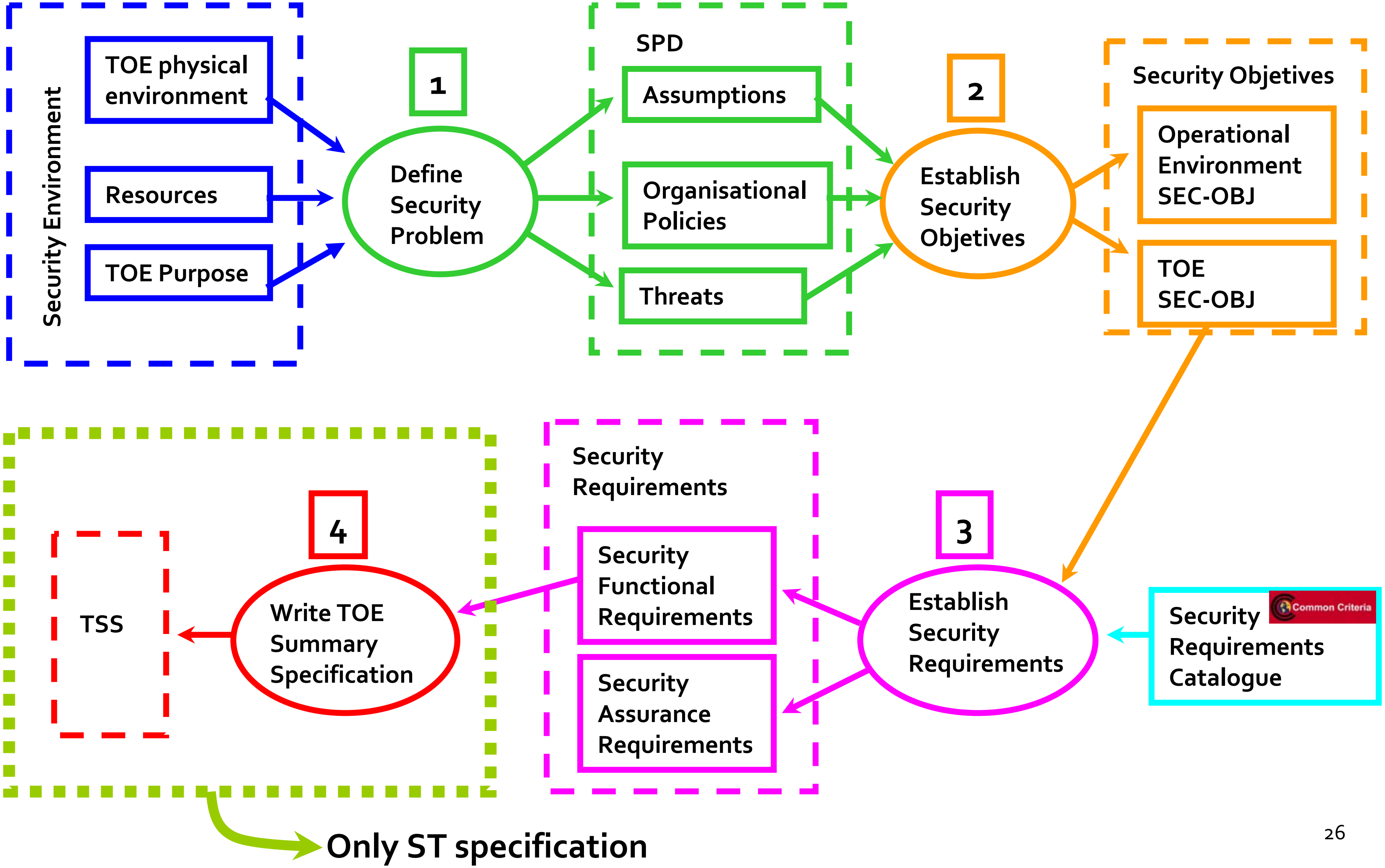
Two possibilities to buy a product:
- specification-based purchasing process.
- selection-based purchasing process.

Difficulty – hard to determine for a customer:
- what kind of IT security he needs
- the security of a product is sufficient to meet his needs
- the security properties declared in a product are true

an evaluation of the product using CC may be useful, and in this case, PPs and STs play an important role.

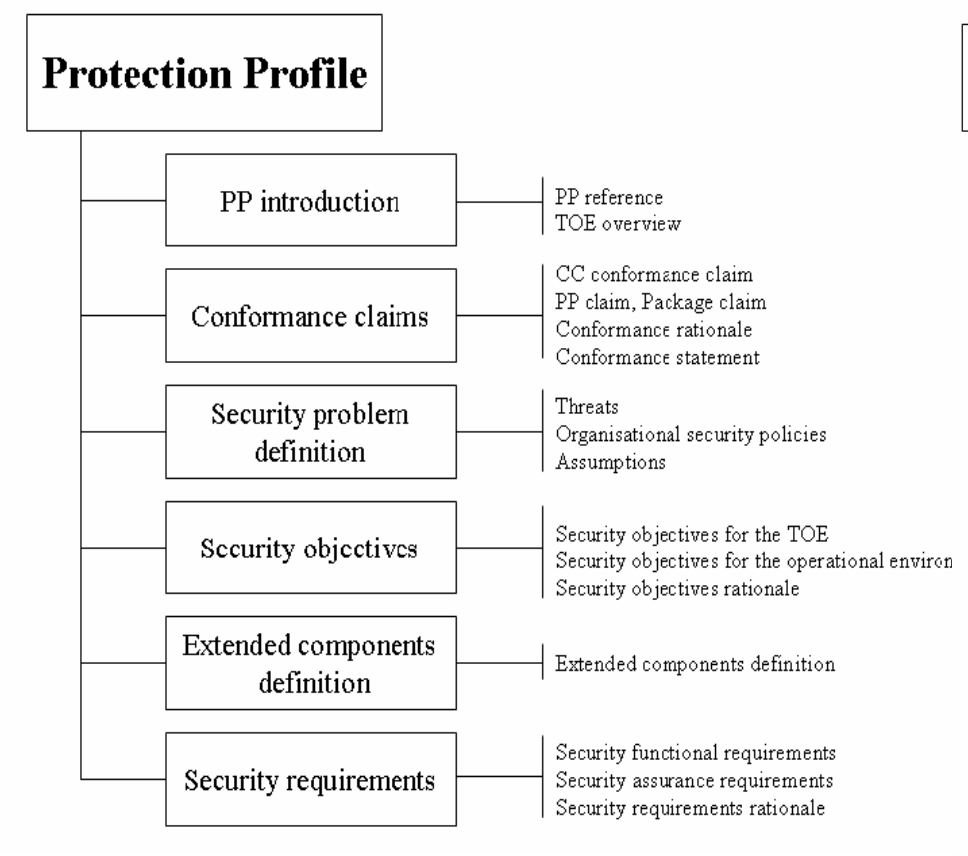
Security Specifications

The Process



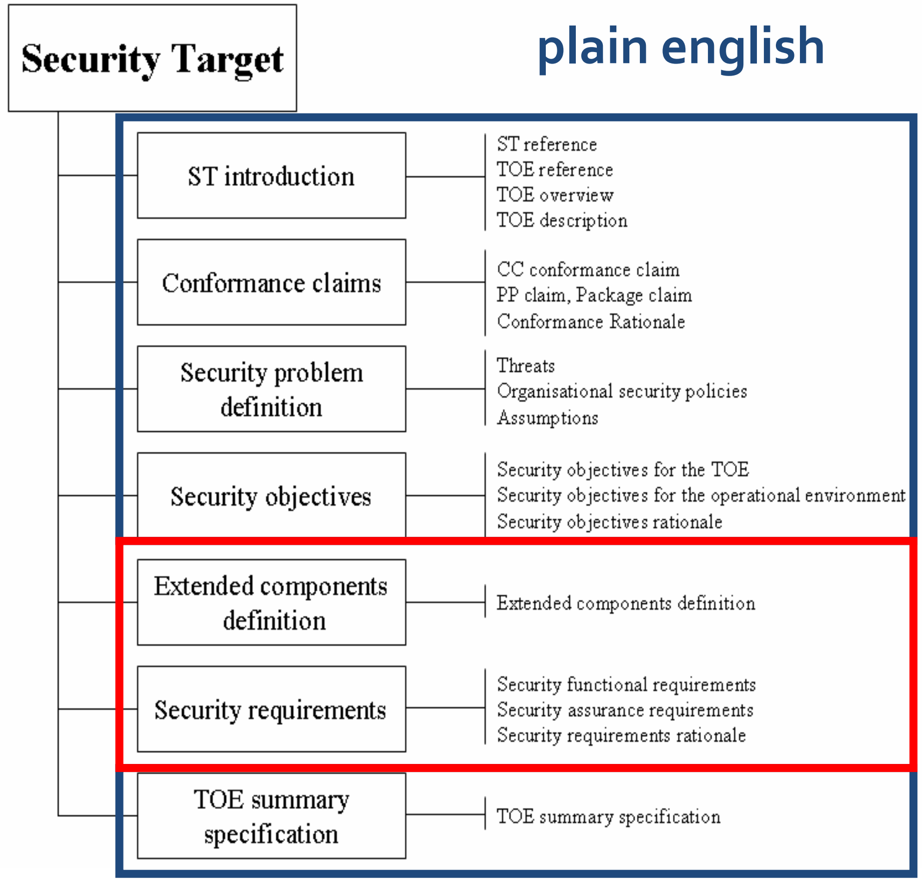
Security Specifications

PP&ST. Content.



Protection Profile

- PP introduction: PP reference, TOE overview
- Conformance claims: CC conformance claim, PP claim, Package claim, Conformance rationale, Conformance statement
- Security problem definition: Threats, Organisational security policies, Assumptions
- Sccurity objcctivcs: Security objectives for the TOE, Security objectives for the operational environ, Security objectives rationale
- Extended components definition: Extended components definition
- Security requirements: Security functional requirements, Security assurance requirements, Security requirements rationale



Security Target

- ST introduction: ST reference, TOE reference, TOE overview, TOE description
- Conformance claims: CC conformance claim, PP claim, Package claim, Conformance Rationale
- Security problem definition: Threats, Organisational security policies, Assumptions
- Security objectives: Security objectives for the TOE, Security objectives for the operational environment, Security objectives rationale
- Extended components definition: Extended components definition
- Security requirements: Security functional requirements, Security assurance requirements, Security requirements rationale
- TOE summary specification: TOE summary specification

plain english

CC language

Security Specifications

Readable Parts.

Introduction

- **PP/ST reference. TOE reference (only ST).**
- **TOE overview:** usage, TOE type, non-TOE HW/SW/firmware
- **TOE Description (only ST)**: physical and logical scope

Conformance claim

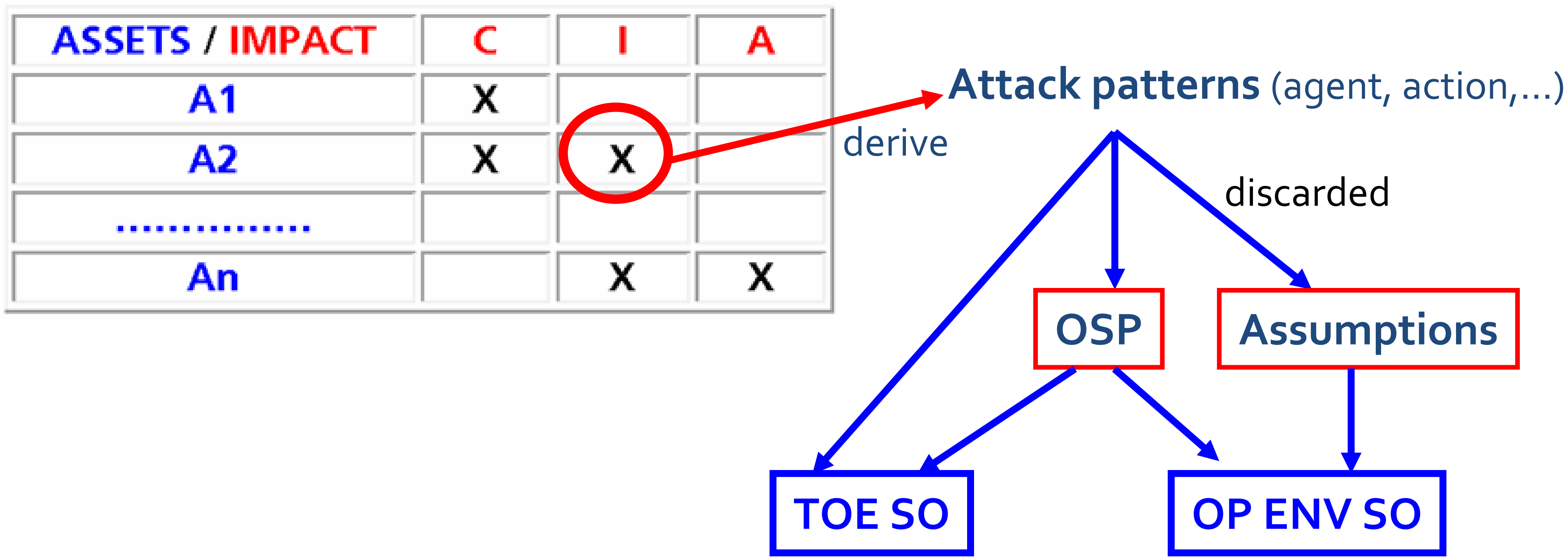
Conformance with the CC itself, PPs, Packages.

The PP **conformance statement** states how STs or other PPs must conform to that PP ("strict" or "demonstrable").

Security Specifications

Security Problem Definition

Many approaches: risk/threat analysis, threat DB, …., a simple one:

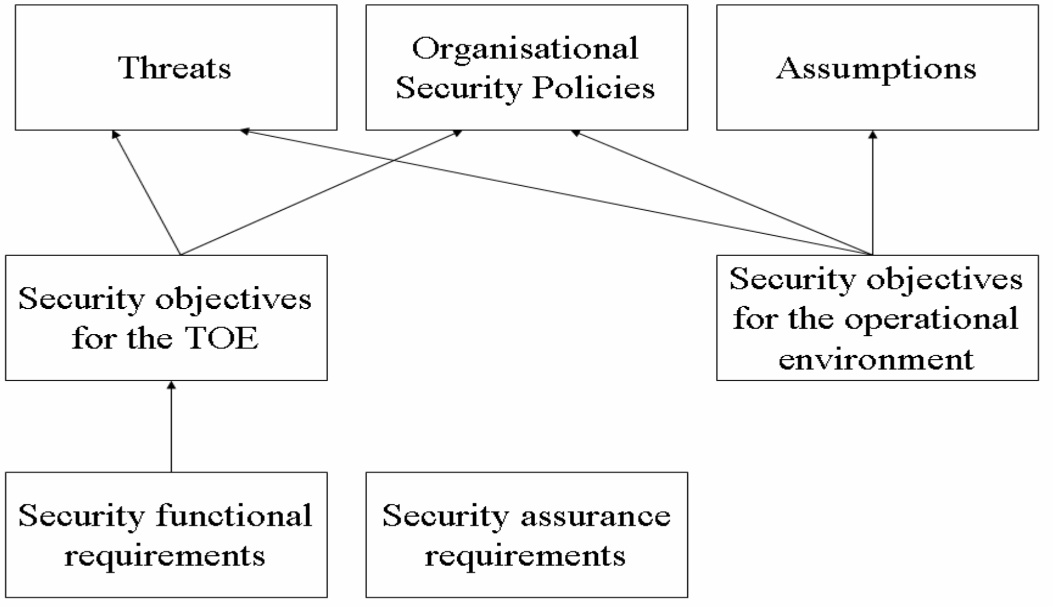


ASSETS / IMPACT	C	I	A
A1	X		
A2	X	X	
....			
An		X	X

Security Specifications

Final conclusion

E P O C H E & E S P R I

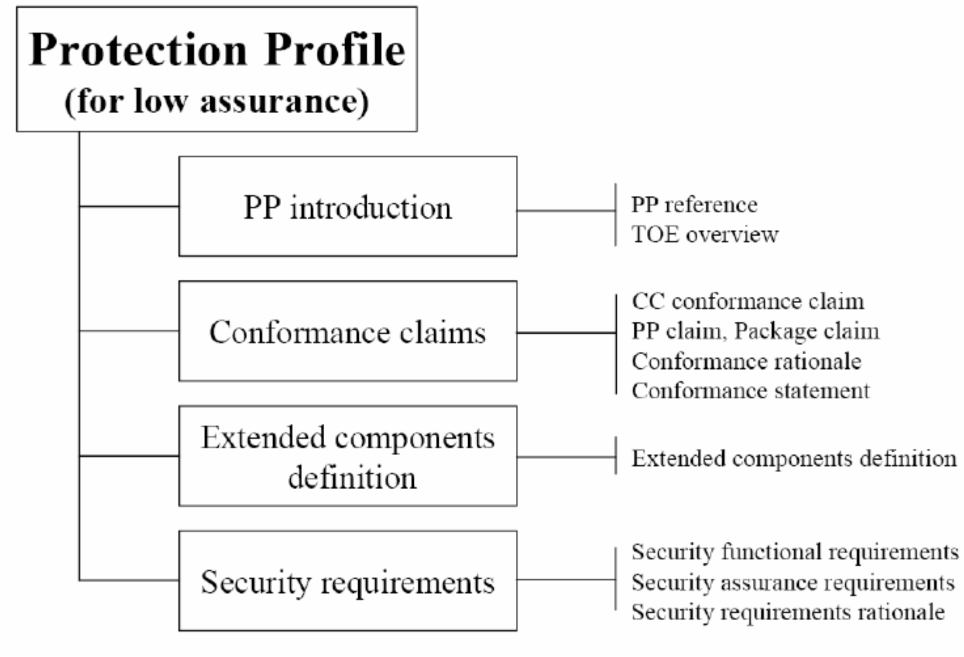

Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Conclusion

If all SFRs and SARs are satisfied and all SOs for the operational environment are achieved, then the security problem is solved.

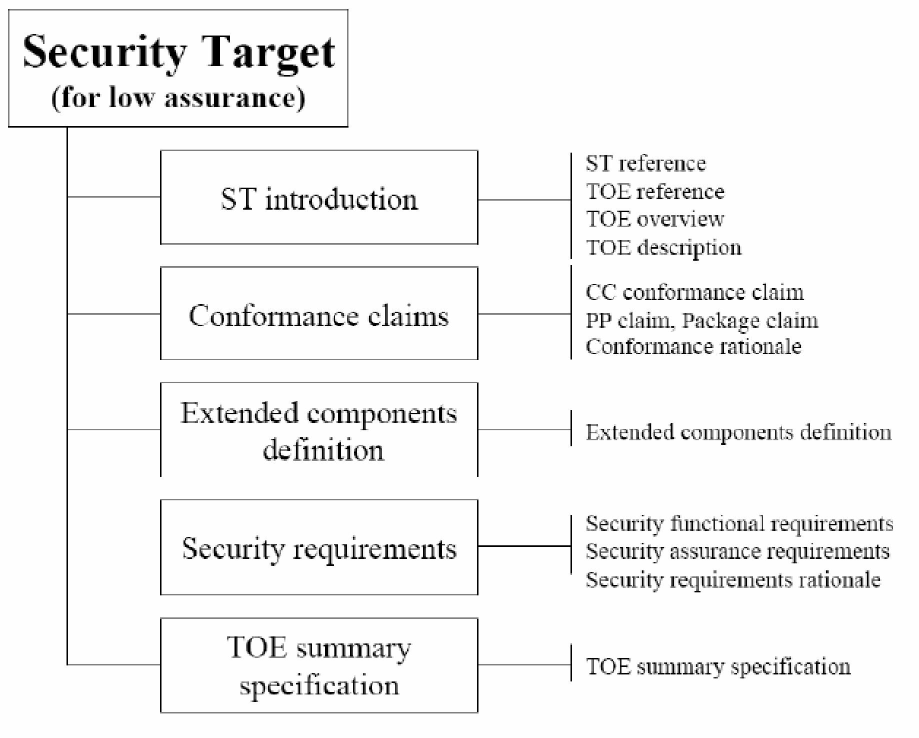
Security Specifications

PP&ST for low assurance. Content.



Protection Profile (for low assurance)

- PP introduction
  - PP reference
  - TOE overview
- Conformance claims
  - CC conformance claim
  - PP claim, Package claim
  - Conformance rationale
  - Conformance statement
- Extended components definition
  - Extended components definition
- Security requirements
  - Security functional requirements
  - Security assurance requirements
  - Security requirements rationale



Security Target (for low assurance)

- ST introduction
  - ST reference
  - TOE reference
  - TOE overview
  - TOE description
- Conformance claims
  - CC conformance claim
  - PP claim, Package claim
  - Conformance rationale
- Extended components definition
  - Extended components definition
- Security requirements
  - Security functional requirements
  - Security assurance requirements
  - Security requirements rationale
- TOE summary specification
  - TOE summary specification

Security Specifications

Protection Profile

How a PP should be used

- part of a specification for a specific consumer
- part of a regulation from a specific regulatory entity;
- as a baseline defined by a group of IT developers.

How a PP should NOT be used

- a detailed specification;
- a complete specification;
- a specification of a single product.

Security Specifications

Security Target

How an ST should be used

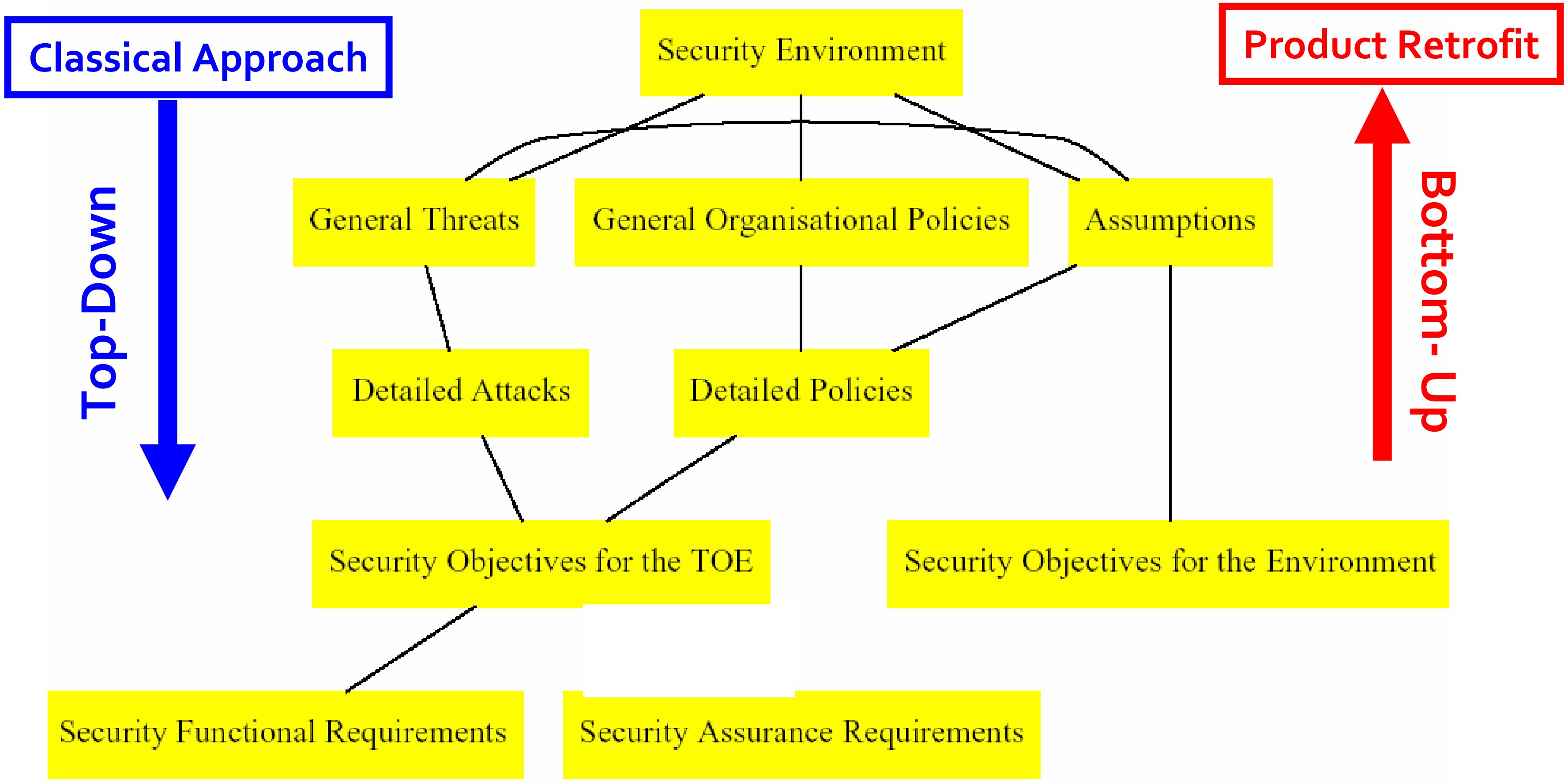
- Before and during the evaluation, the ST specifies "**what is to be evaluated**".
- After the evaluation, the ST specifies "**what was evaluated**".

How an ST should NOT be used

- a detailed specification;
- a complete specification.

Security Specifications

How-to.


Classical Approach
Top-Down
Security Environment
General Threats
General Organisational Policies
Assumptions
Detailed Attacks
Detailed Policies
Security Objectives for the TOE
Security Objectives for the Environment
Security Functional Requirements
Security Assurance Requirements
Product Retrofit
Bottom- Up

Questions welcomed & Thanks!

Jose Emilio Rico

Epoche & Espri, S.L.U.
Avda. de la Vega, 1
28108, Alcobendas,
Madrid, Spain.

tech@epoche.es