

---

***EWICS London, January 18, 2005***

***Safety-Related Security***

***Concepts***

# *Safety Requirements*

---

- ◆ **Top-level requirements for the PES:**
  - **functional behavior**
- ◆ **System Safety depends on other “attributes”, i.e.:**
  - **accuracy**
  - **reliability and availability**
  - **fail-safe behavior**
  - **time response**
  - **throughput (e.g. transactions/second)**
  - **response to overload**
  - **security (from attack)**
  - **long term maintainability**
  - **usability**
  - **integrity**

From:  
Justifying the use of software of  
uncertain pedigree (SOUP) in  
safety-related applications  
Prepared by Adelard  
for the Health and Safety Executive  
CONTRACT RESEARCH REPORT  
336/2001

## *Security Questions*

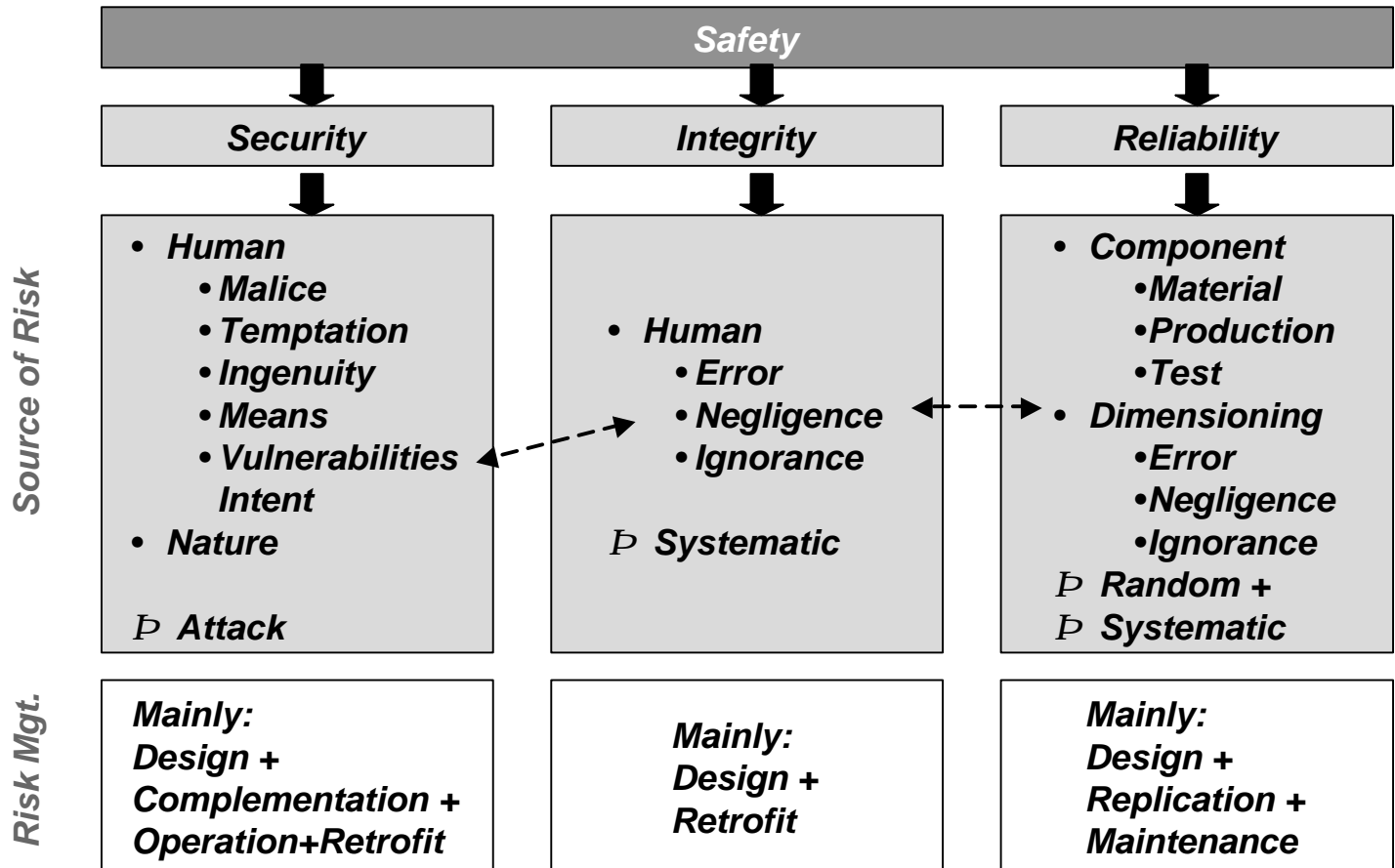
---

---

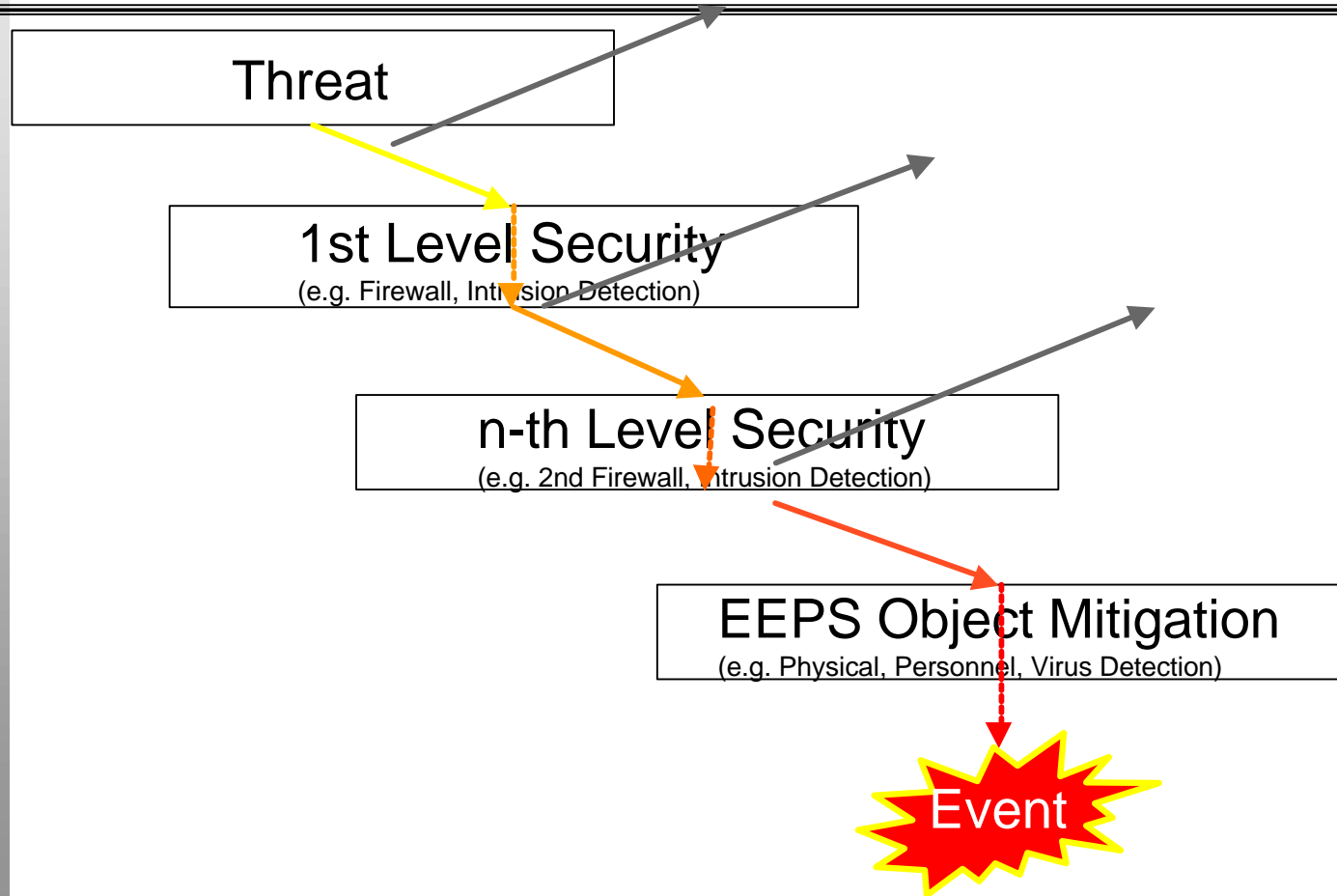
### ***Security Questions (e.g., NIST)***

- a. Are the access restrictions imposed on operators, managers, and other personnel fully defined?***
- b. Do requirements exist to prevent unauthorized personnel from interacting with the software system?***
- c. Do requirements exist to prevent unauthorized changes to the software system?***
- d. Are the security requirements individually identified?***
- e. Can each security requirement be verified, either through inspection, analysis or test of the completed software product?***
- f. Are the security requirements, taken as a whole, mutually consistent?***

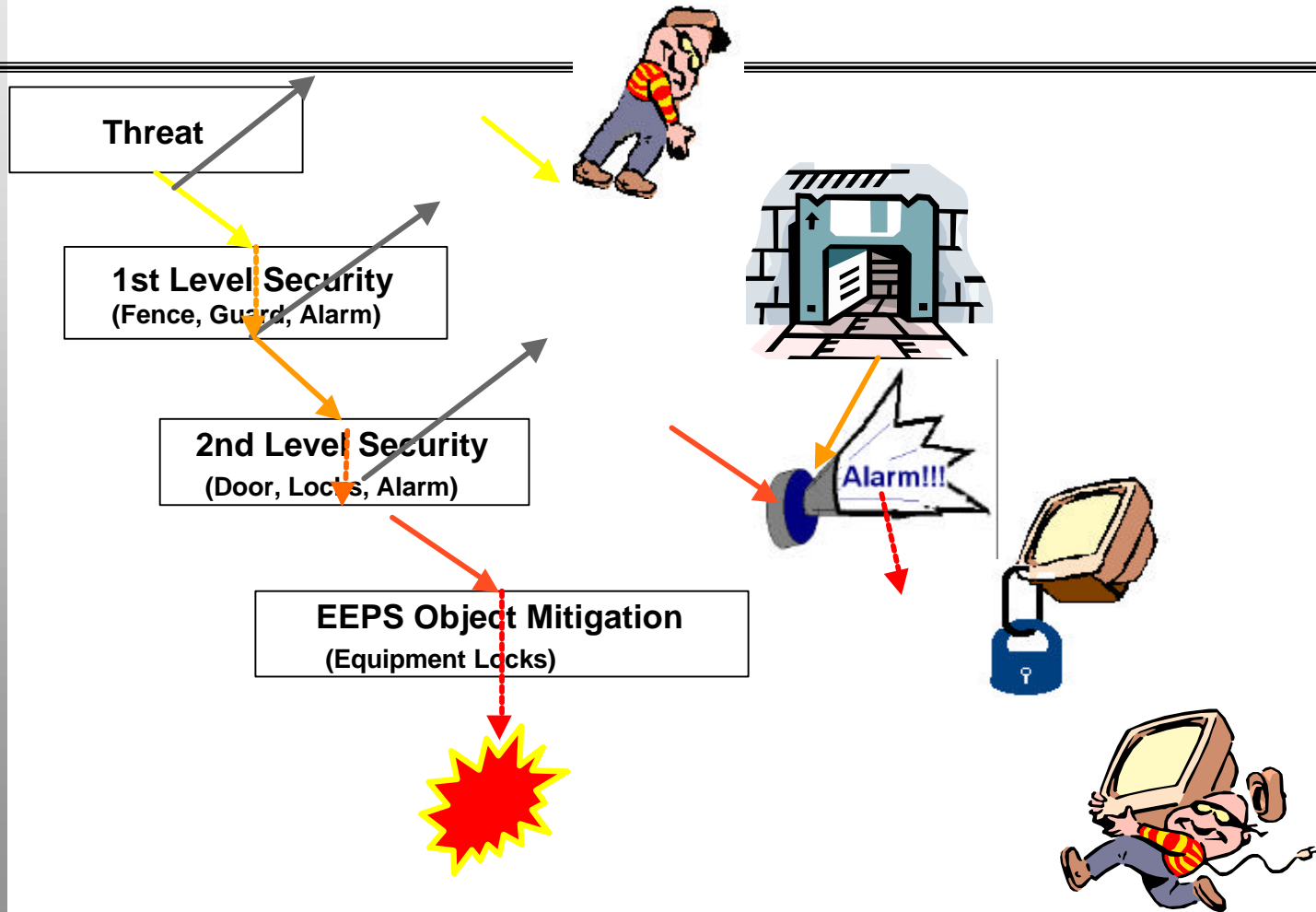
# Concepts



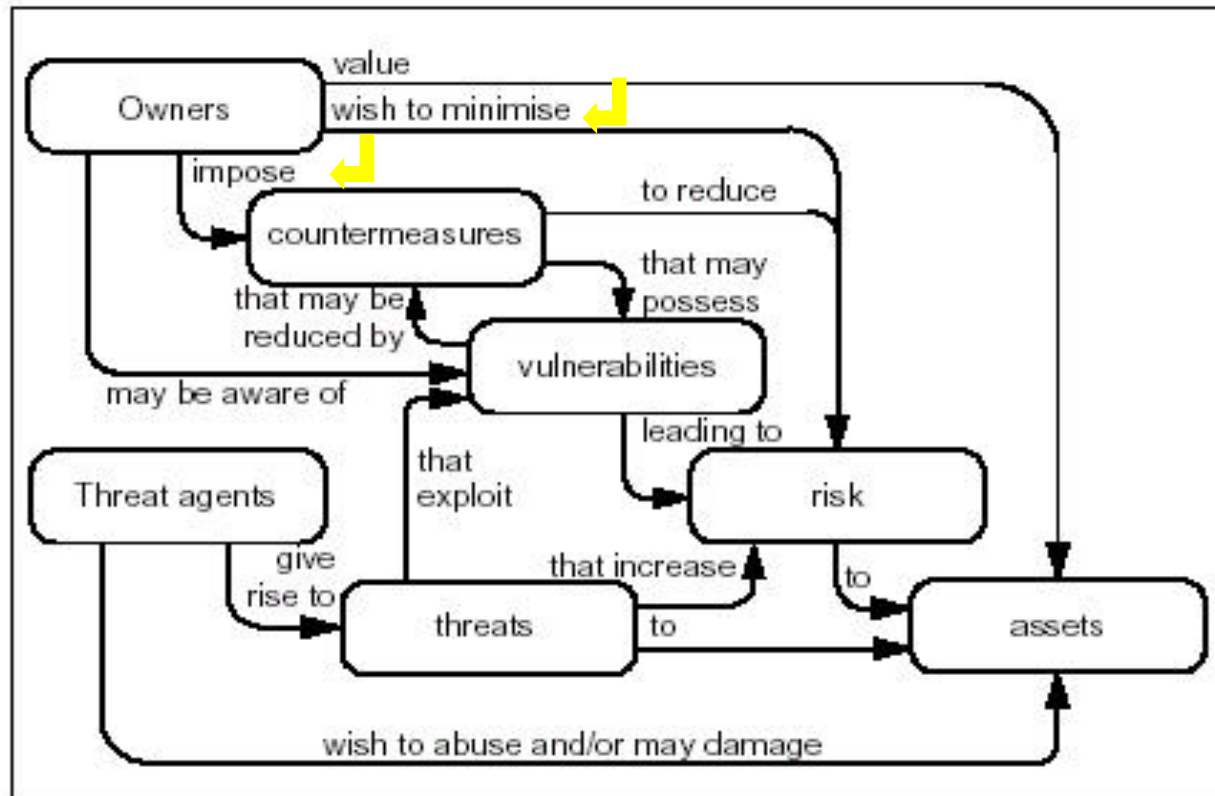
## Threat to Event chain



# Example: Threat to Event chain

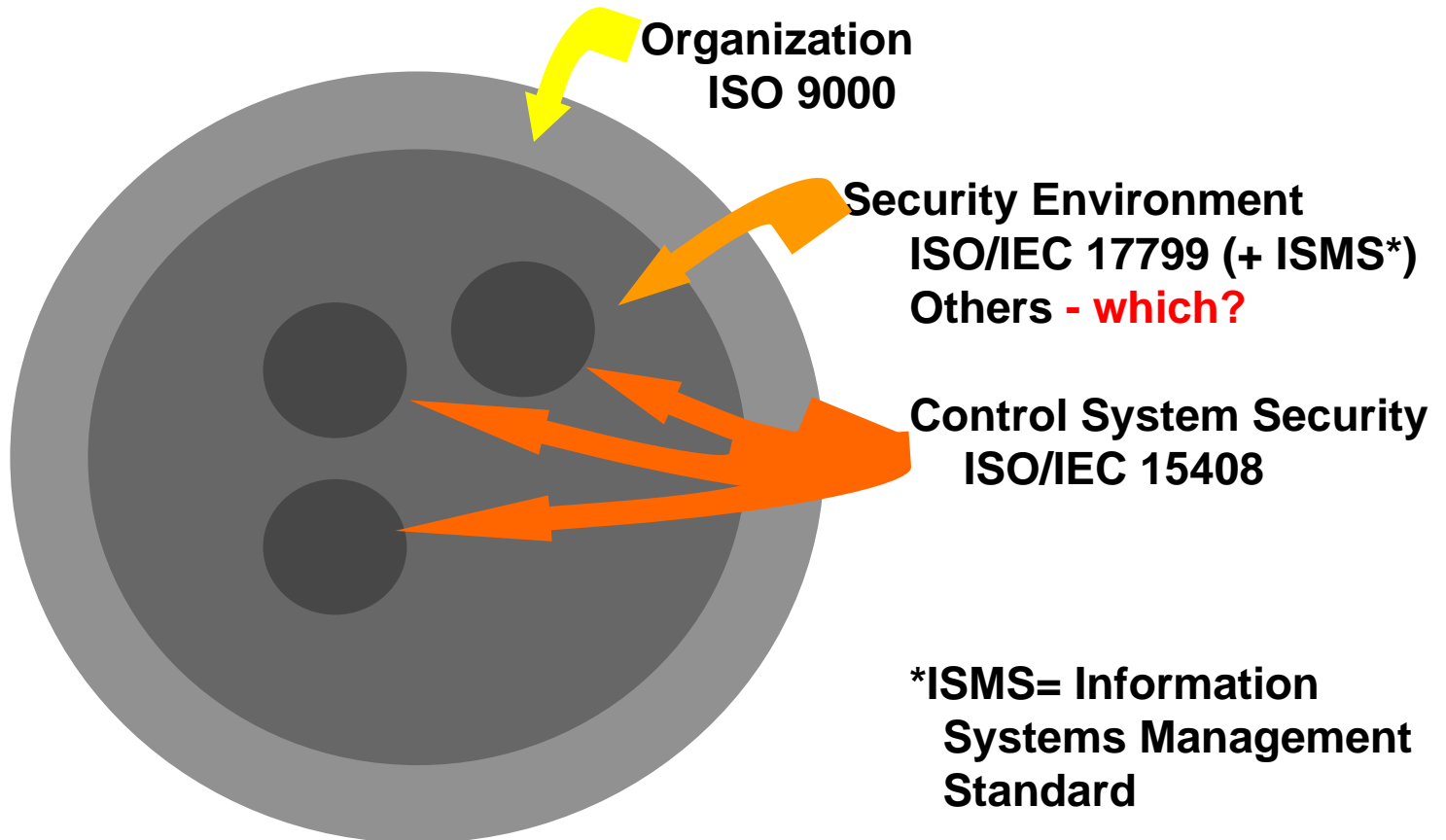


# Security Concepts

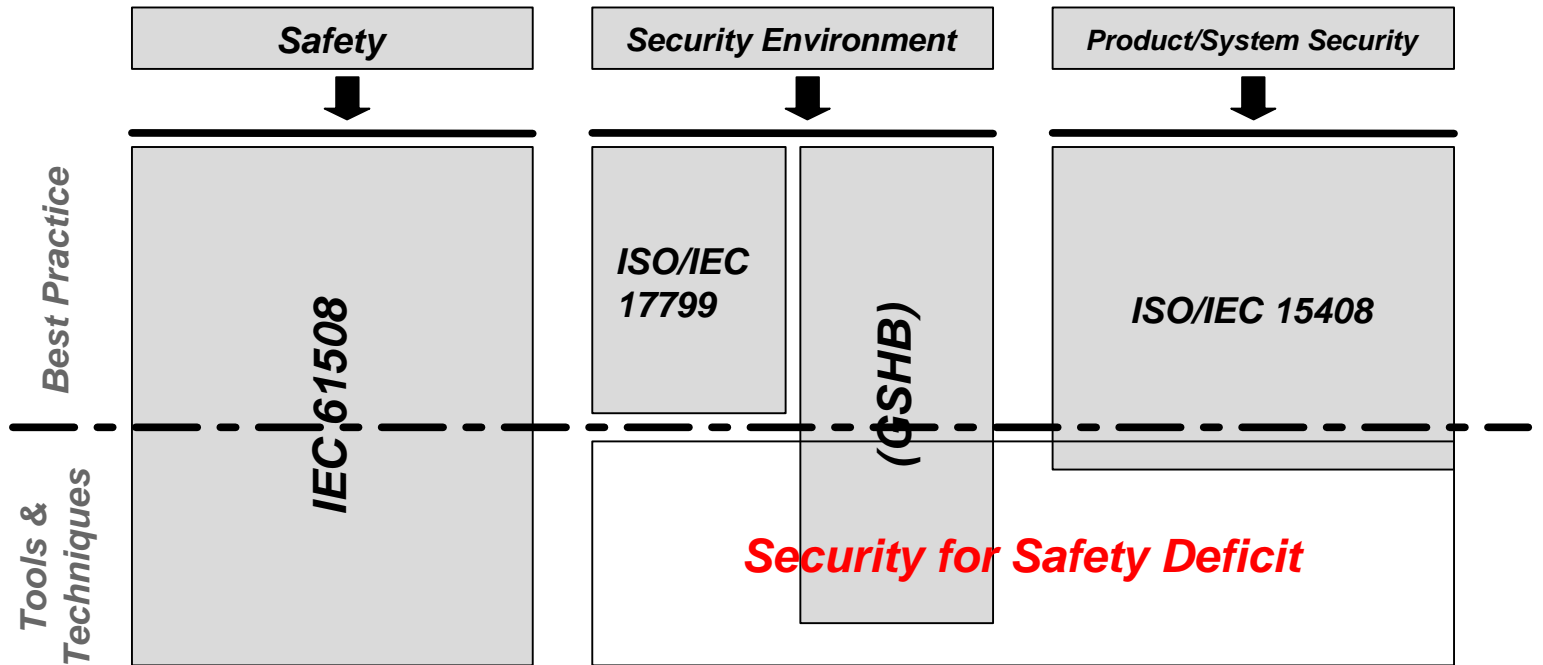


RE: ISO/IEC 15408

## Organizational Context



# Depth of Standards

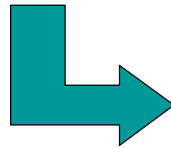


- Mainly:
- Design +
- Operation

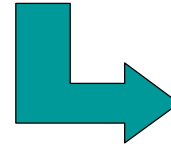
Mainly:  
 Design +  
 Complementation +  
 Operation+Retrofit

## *Safety and Security Similarities*

**ANALYSIS**



**REQUIREMENTS**



**VERIFICATION**

### **SECURITY**

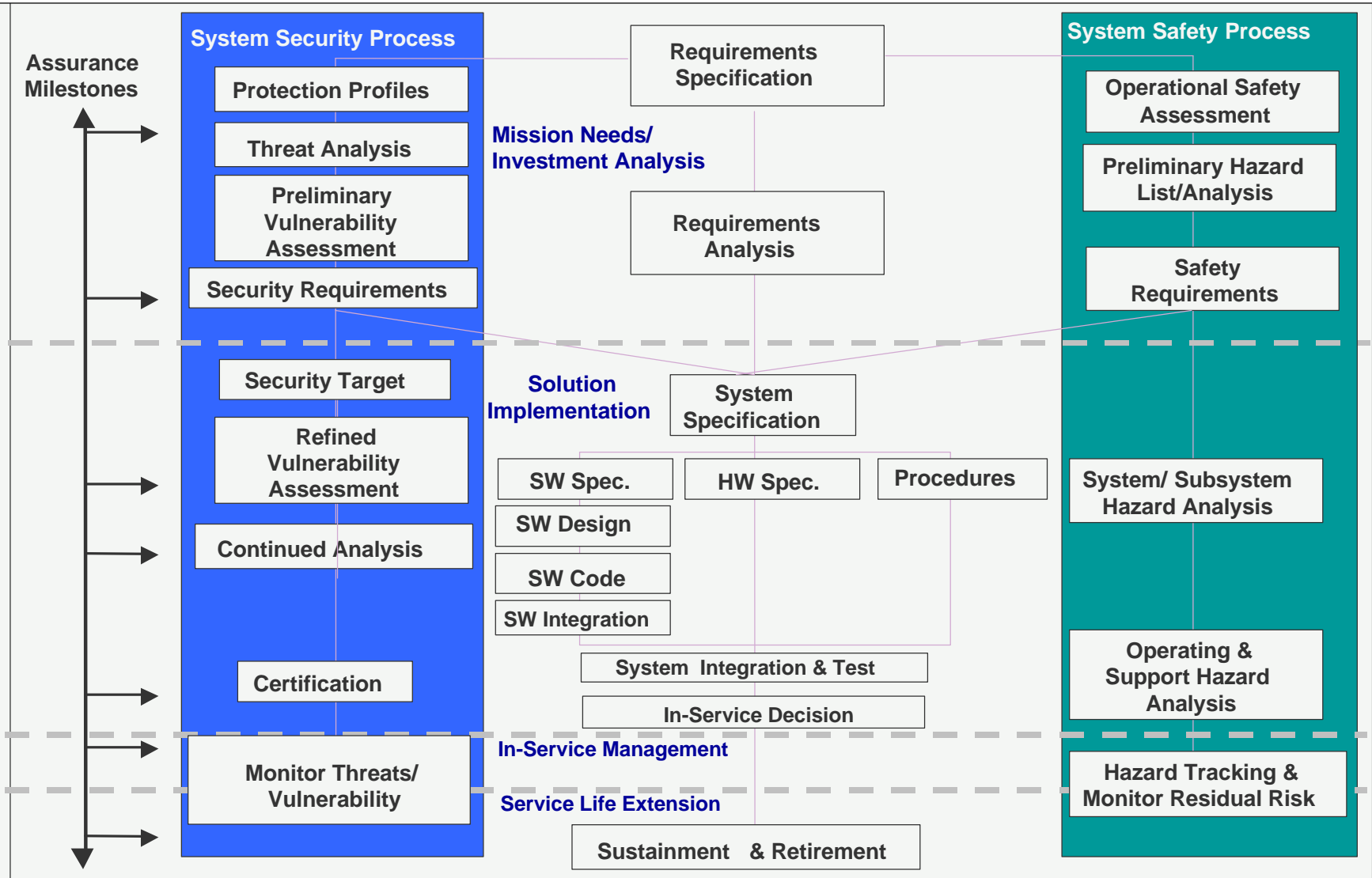
- ◆ *Vulnerability/Threat Assessment*
- ◆ *Risk Determination*
- ◆ *Security Requirements*
- ◆ *Design, Test, V&V*
- ◆ *Evaluation/Certification*
- ◆ *Penetration testing*



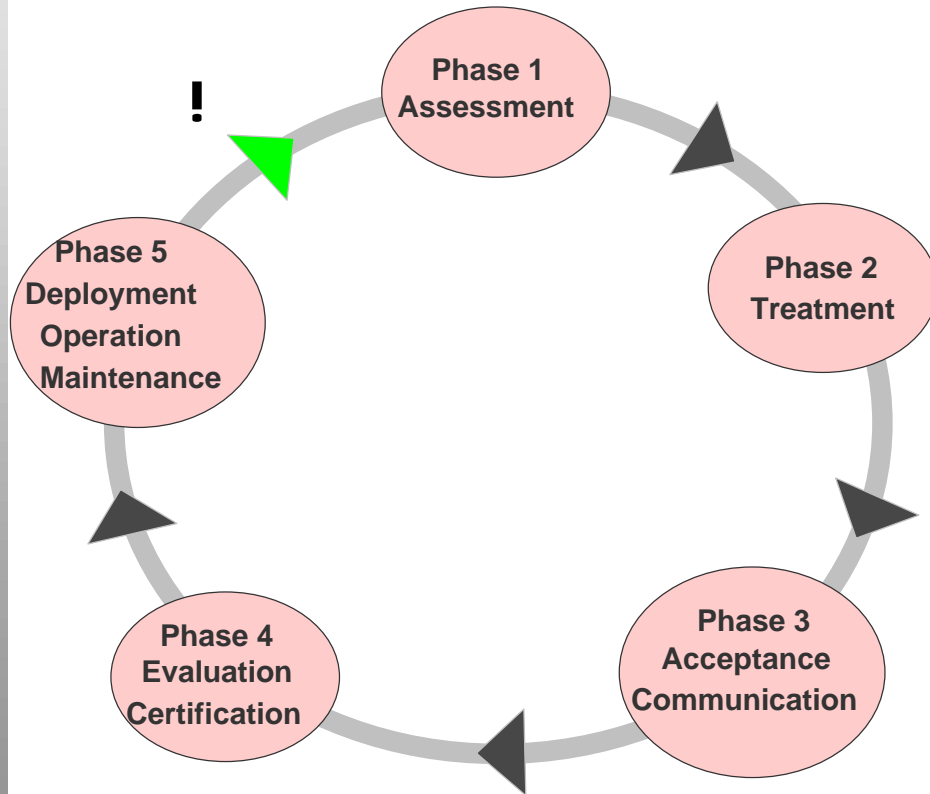
### **SAFETY**

- ◆ *Operational Safety Assessment*
- ◆ *Risk Determination*
- ◆ *Safety Requirements*
- ◆ *Design, Test, V&V*
- ◆ *Evaluation/Certification*
- ◆ *Requirements-based testing*

# System Development Process



## *Safety/Security Assurance Circle*



- ◆ **Mainly in Operation**
- ◆ **Monitor Threats/ Vulnerability**
- ◆ **Hazard Tracking and Monitor Residual Risk**

⌋ **Never ending**

⌋ **Especially important in Security**

## *Proposal: Security Assessment in Safety*

Black box		White box	
Test evidence	Field experience	Test evidence	Analytic evidence
“Hacker” tests	Security performance past systems		Analysis of security features  ITSEC compliance  Code assessment for security holes (e.g. weak passwords, lack of network access protection, deliberate “trap-doors”, etc.)  (Part 7 C5.15, C5.16)

**C.5.15 Fagan inspections**

**C.5.16 Walkthroughs/design reviews**

Source: Adelard

## *Proposal: Variation of evidence with SIL and size*

---

- ***Security Security in operation – evidence examined for all SILs.***
- ***At higher SILs will need augmenting with analysis implying some white box information (of code, design) or knowledge of process.***
- ***At high security levels, not related to SIL but to security environment, code assessment for security holes required (e.g. weak passwords, lack of network access protection, deliberate “trap-doors”, etc.)\****

\* *Important issue for SOUP (Software Of Unknown Pedigree) especially if pedigree shows security weaknesses.*

Source: Adelard

## *Proposal: Example evidence profile for a PLC*

---

---

Security	Physical key needed for local update, password needed for remote update over network.
----------	---

**From:**  
**Justifying the use of software of uncertain pedigree (SOUP) in safety-related applications**  
Prepared by **Adelard**  
for the Health and Safety Executive  
**CONTRACT RESEARCH REPORT**  
**336/2001**

## *Example: GSM-Railway Threat Scenario*

---

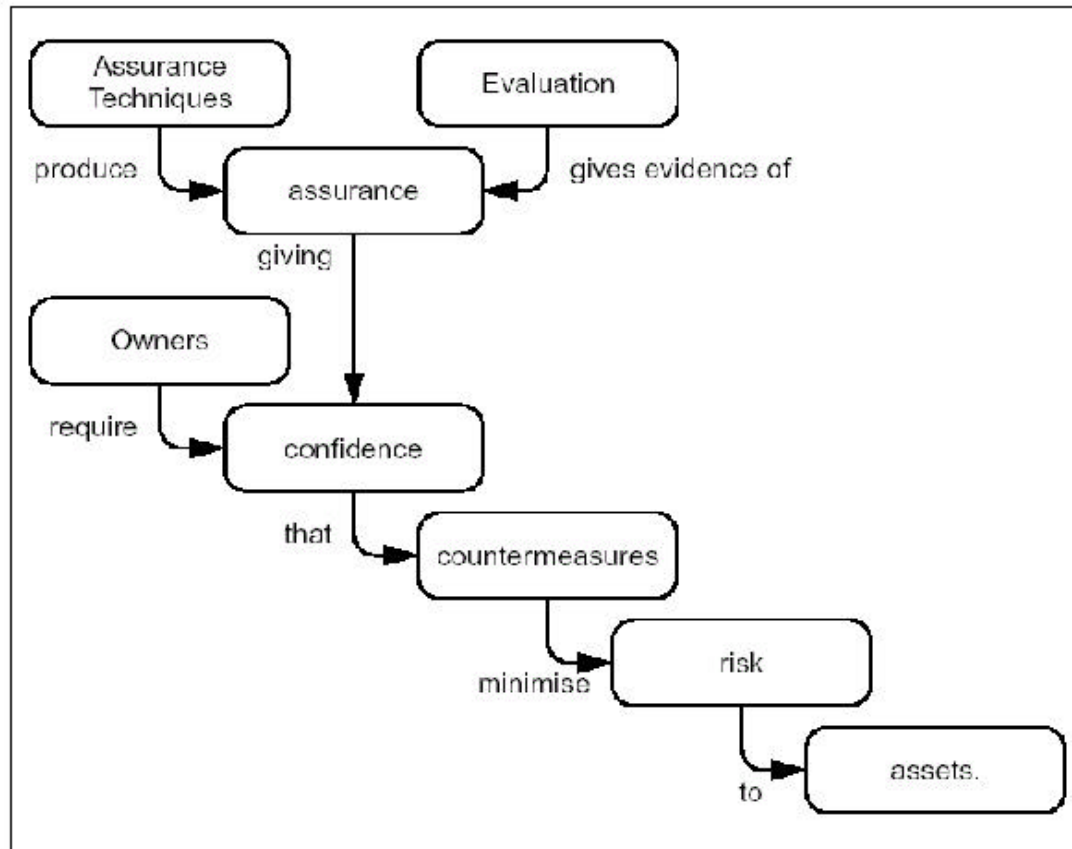
- ◆ **GSM-R = Messaging by public cell-phone-system**
- ◆ **GSM-R is in an open wireless network**
- ◆ **Security threat: information might be compromised**
- ◆ **Reasons include: malicious attack from outside, system error**
- ◆ **Scenarios:**
  - a. **Threat: The information is destroyed, either disappeared or unreadable.**  
**Consequence: no communication**  
**Mitigation: Bring equipment to safe state (e.g., stop the train, call central)**
  - b. **Threat: Receiving component gets overloaded and unable to reply or acknowledge**  
**Consequence: no communication (known as “denial of service”)**  
**Mitigation: Bring equipment to safe state (e.g., stop the train, call central)**
  - c. **Threat: information, even with error checking, is modified after being sent, still readable but false.**  
**Consequence: potential safety hazard (e.g., the train might accelerate instead of breaking)**  
**Mitigation: No solution in 61508**
  - c. **Threat: information is copied, multiplied after being sent, the information remains correct (i.e. “Replay”)**  
**Consequence: potential safety hazard (e.g., the train might accelerate instead of breaking)**  
**Mitigation: No solution in 61508**
- ◆ **Mitigation thru security engineering:**
  - **Encryption guarantees integrity**
  - **Digital signature guarantees authenticity**
  - **Time stamping guarantees time-sensitive information**

---

***EWICS London, January 18, 2005***

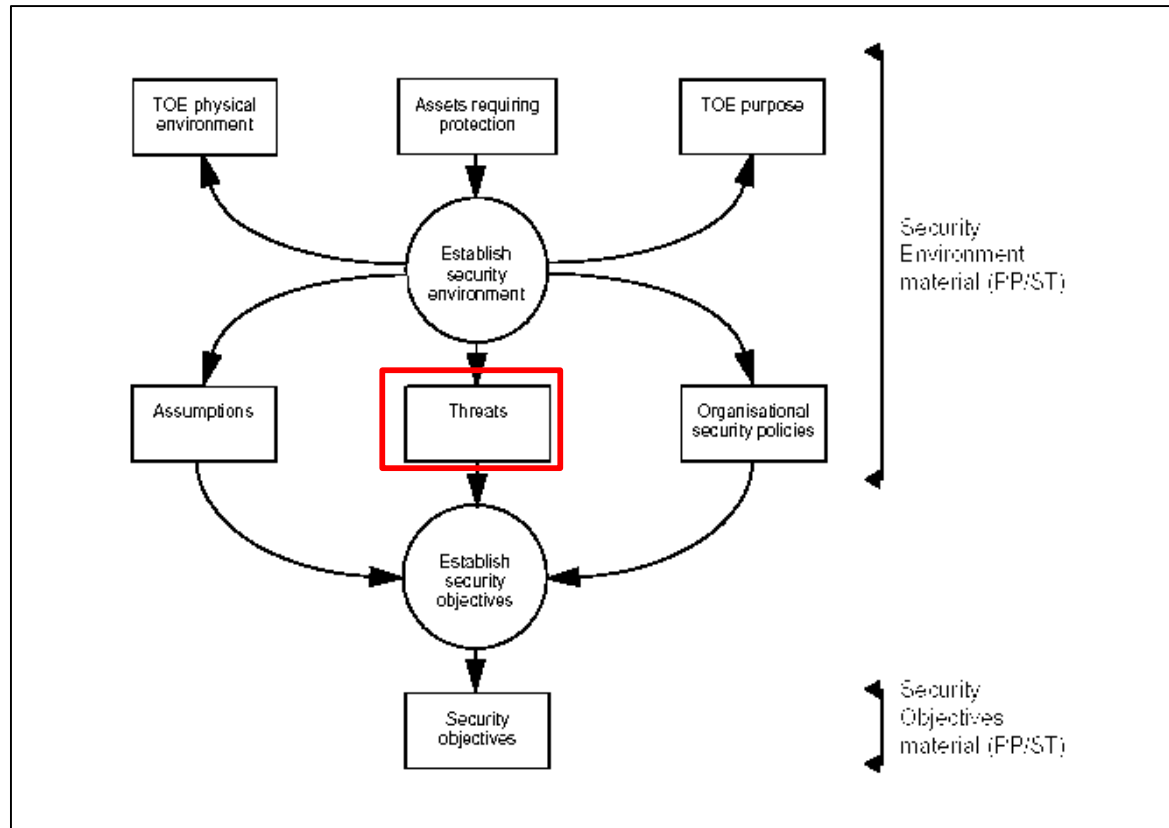
***Safety Related Security  
Assurance based on 15408***

# Security Assurance Model

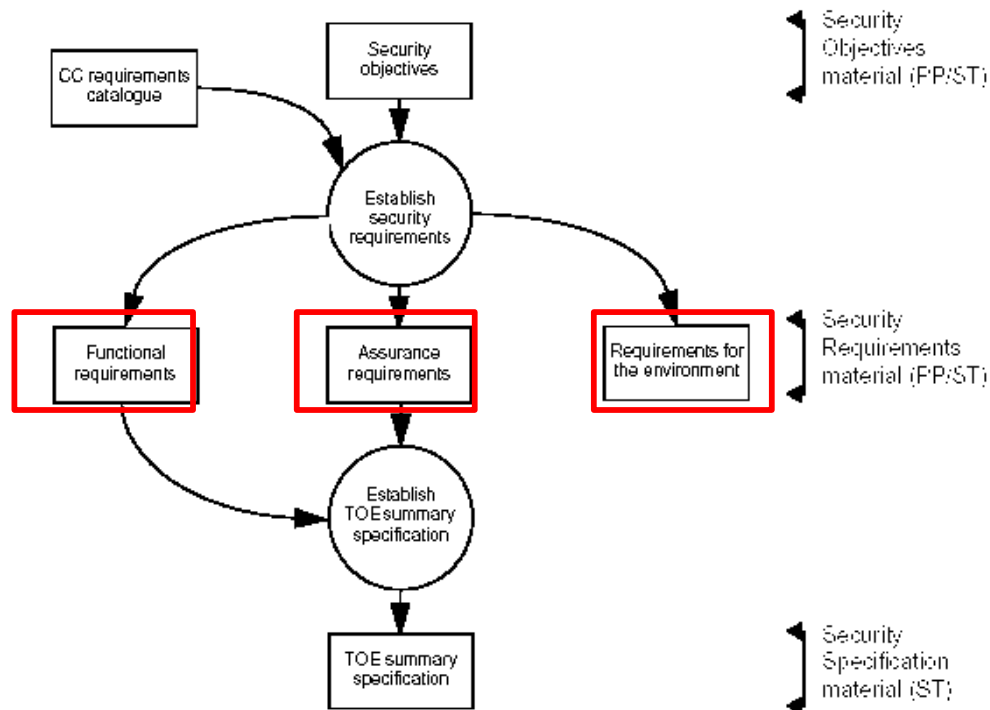


RE: ISO/IEC 15408

# Security Objectives



# Target of Evaluation - Summary Specification



# Target of Evaluation Development Model

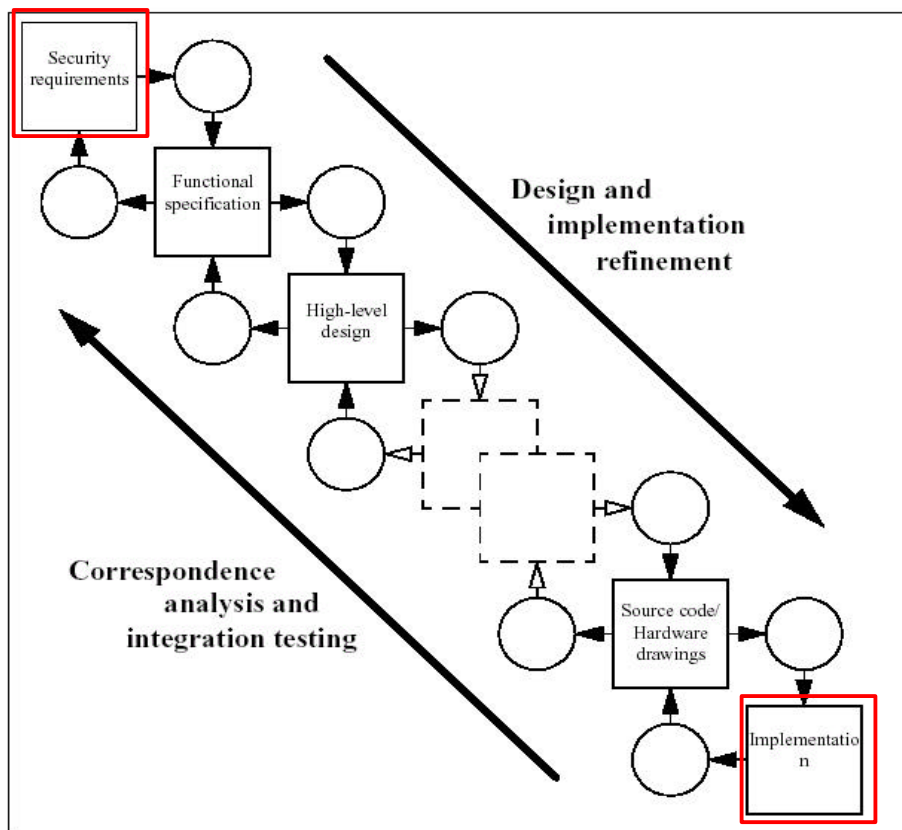
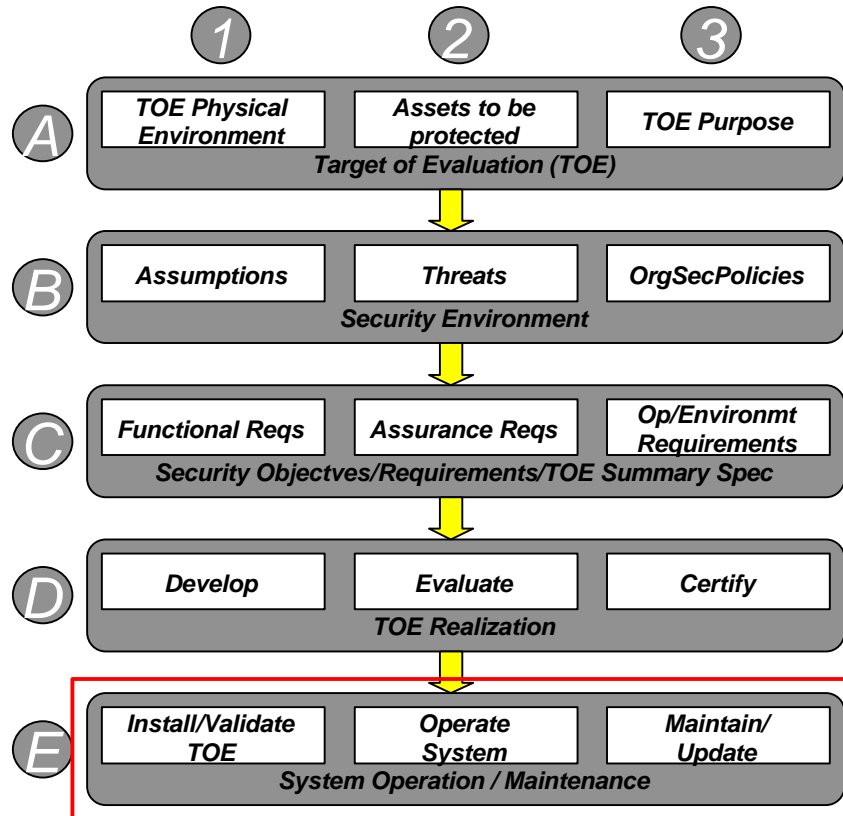


Figure 4.3 - TOE development model

# Common Criteria Basic Process Structure



**Not the strength of 15408 but  
e.g. 17799**

## Target of Evaluation - Evaluation Process

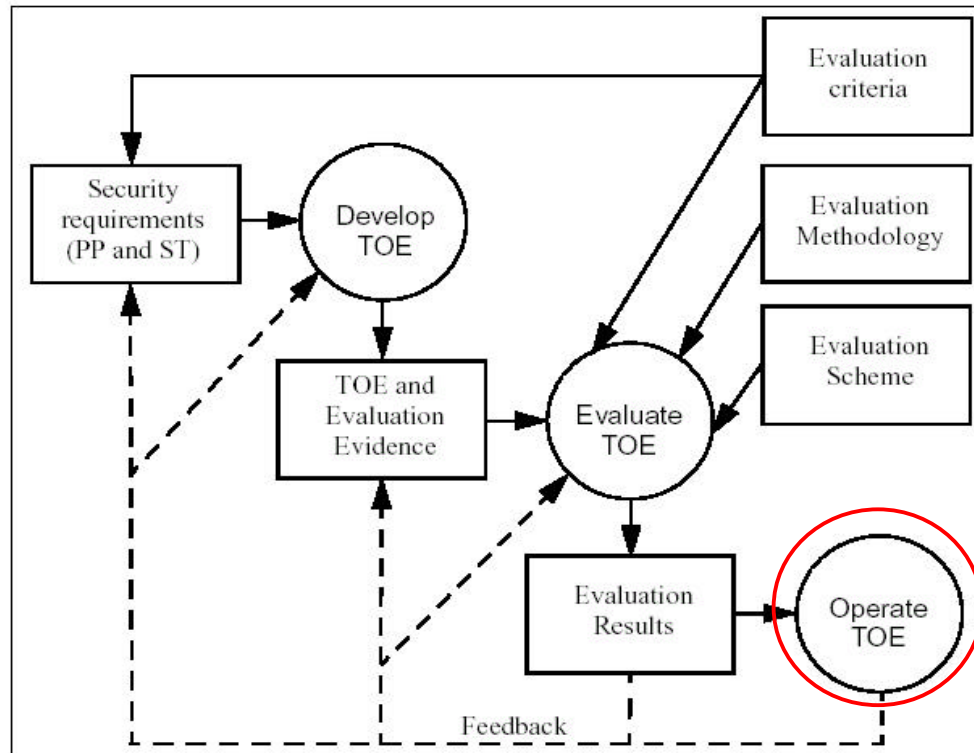


Figure 4.4 - TOE evaluation process

**Evaluation and Certification according to**

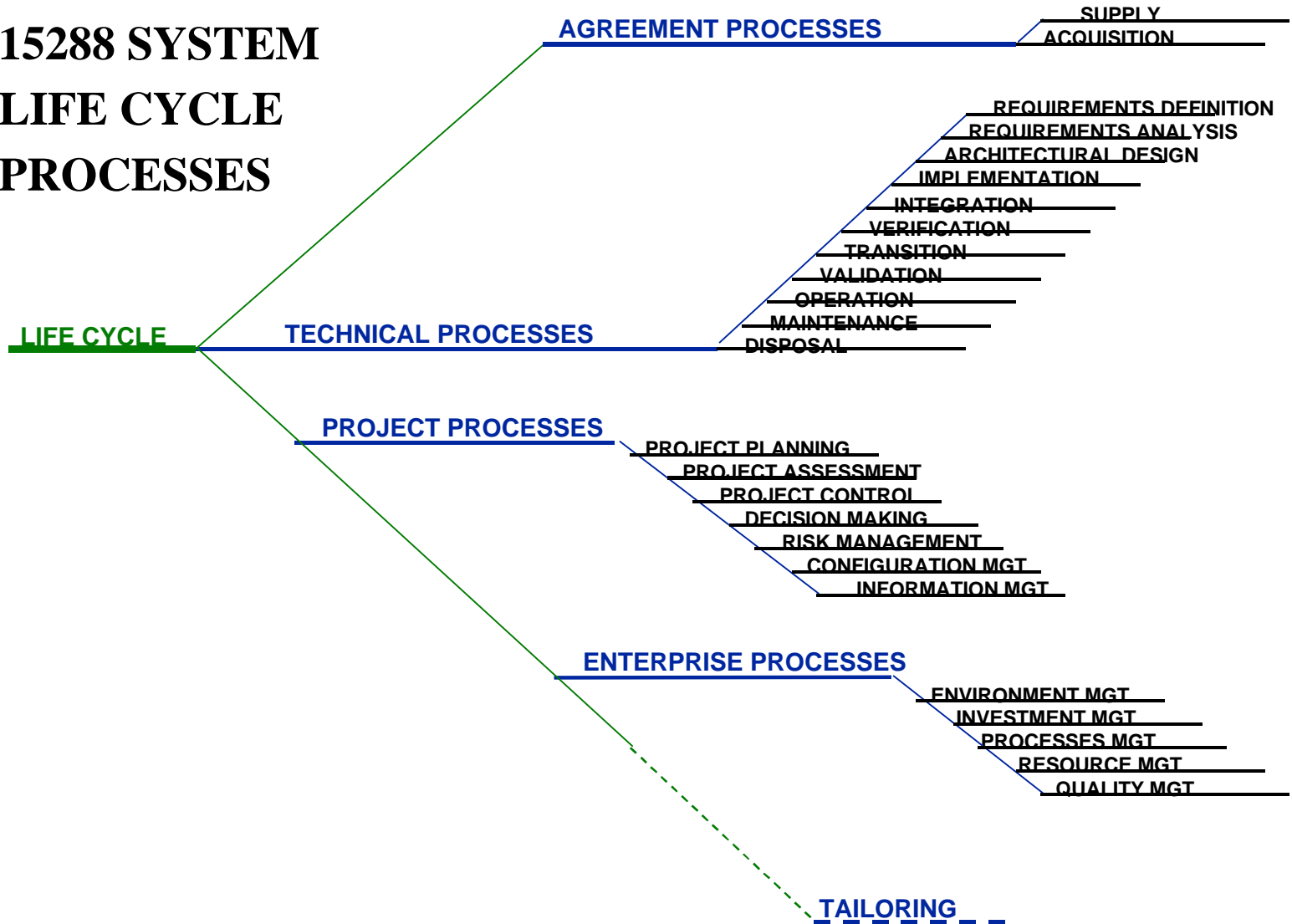
- **15408,**
- **BS7799-2**

---

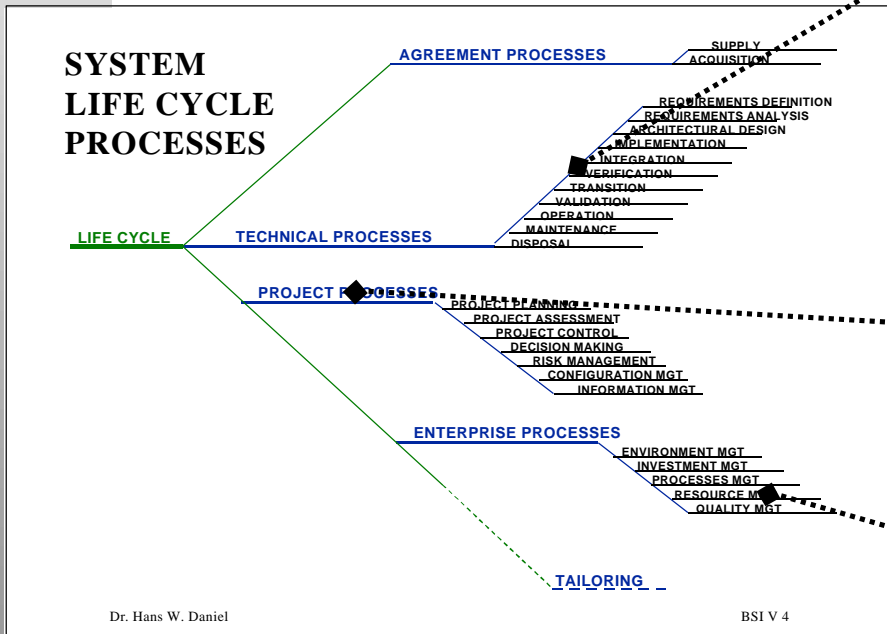
***EWICS London, January 18, 2005***

***Integrity Assurance Processes  
within the ISO/IEC 15288 Life Cycle Processes***

# 15288 SYSTEM LIFE CYCLE PROCESSES



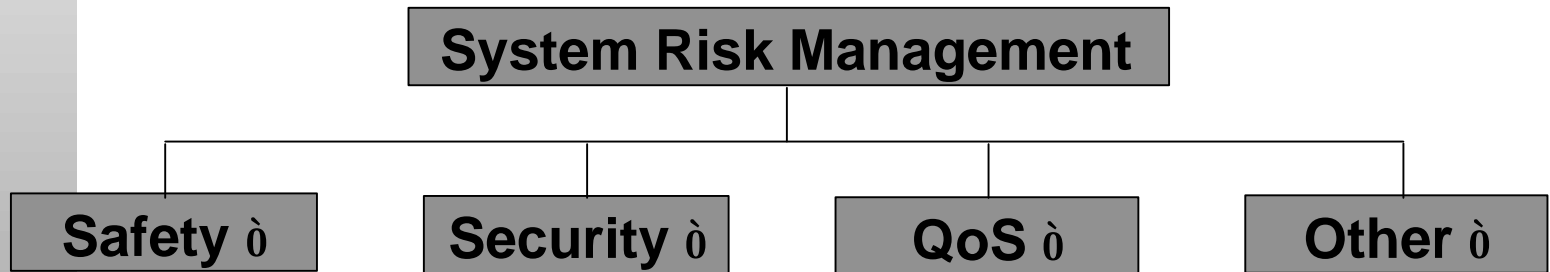
# System Dependability Engineering = System Engineering +



Add technical processes and activities if required by safety integrity

Add „Safety Integrity Management Process“

Add „Safety Integrity Management Process“ Process Management



## System integrity

The property that a system performs its intended [system] function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system. [TR 13335-1: 1996 Information technology - Guidelines for the management of IT Security]