

# A Practical Approach for Using the Common Criteria in System Evaluations

---

Ken Elliott

[elliott@aero.org](mailto:elliott@aero.org)

The Aerospace Corporation

18th ACSAC Conference Presentation

# Overview

---

- ◆ Background
- ◆ The Problem
- ◆ Proposed Approach
- ◆ Defining “System”
- ◆ Constructing STs
- ◆ Assessment Activities
- ◆ Pros and Cons

# Background

---

## ◆ Common Criteria (CC)

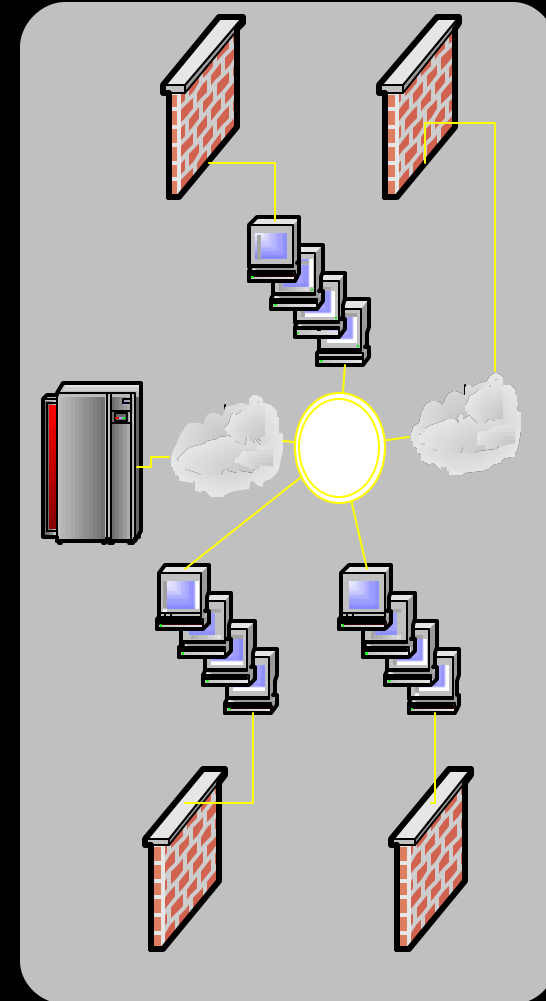
- Encyclopedia of Security Requirements
  - » Protection Profiles (PPs) (“I want”)
  - » Security Targets (STs) (“I will provide”)
- Primarily Product Evaluations

## ◆ Certification and Accreditation (C&A)

- Approval to Operate
- Generally Systems (Many Products)

# The Problem

- ◆ Specifying Requirements at “System” Level
  - Functional OK
  - Assurance “Bounds”
- ◆ *Systematic Evaluation*
  - DITSCAP
    - » Lots of Documentation
    - » Lacking in Procedural Rigor
  - Using Evaluated Products
    - » Existence
    - » Versioning
    - » Composition



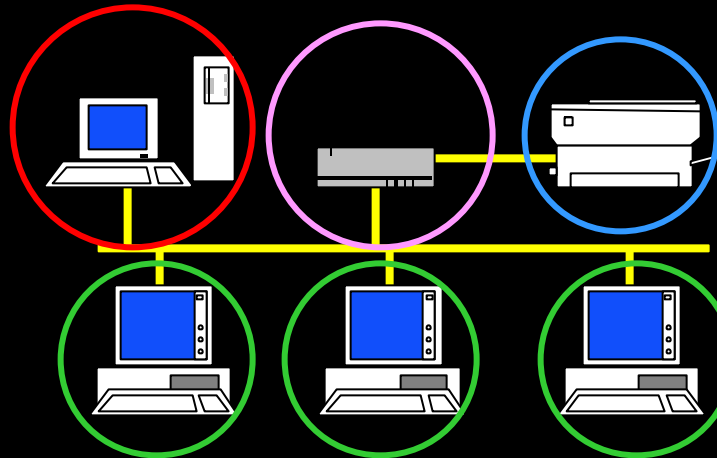
# The Solution (Theory)

Security Requirements

Security Requirements



C&A Team

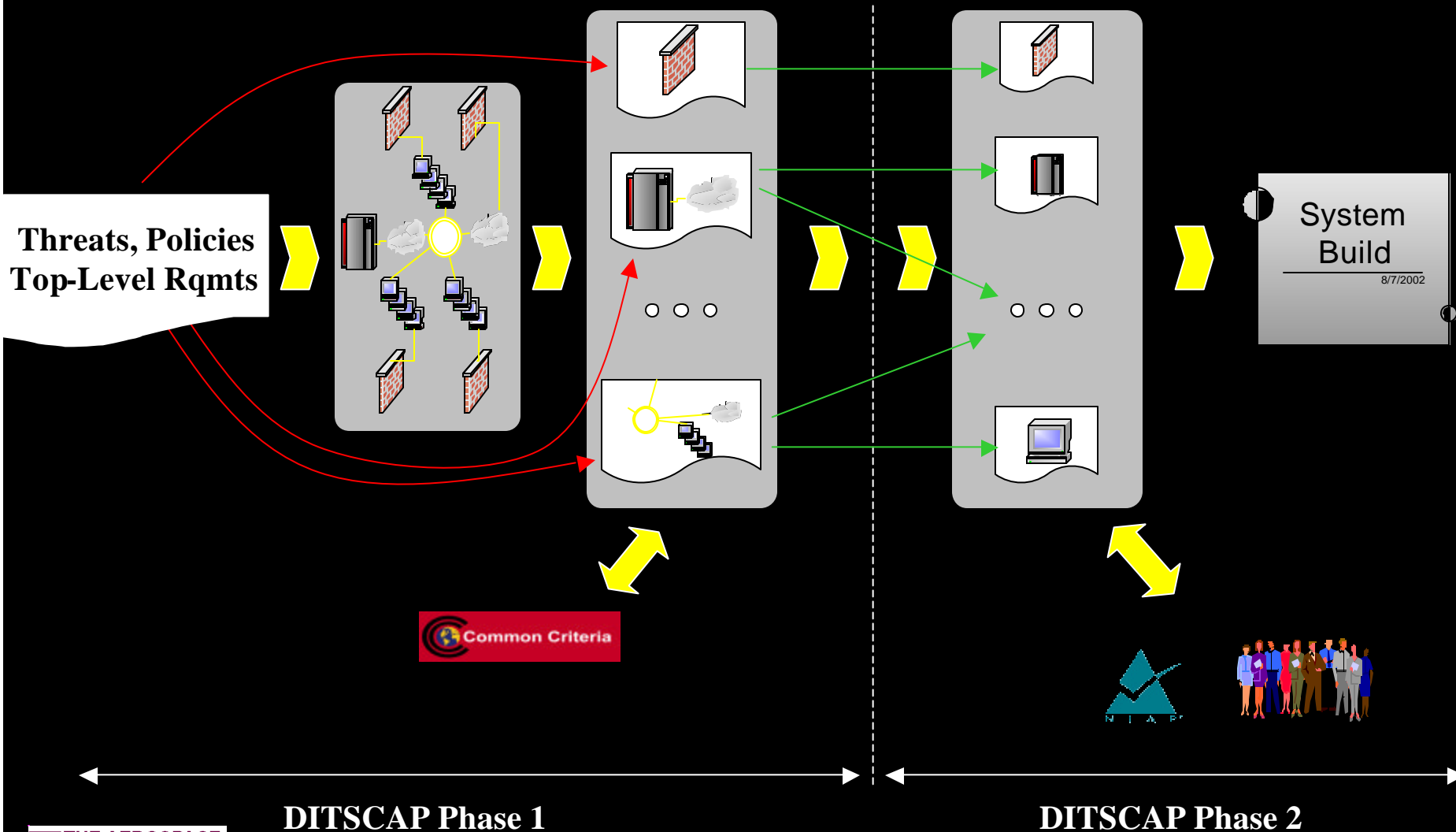


Security Requirements

Security Requirements



# The Solution (Practice)



# Design Analysis Approach

---

- ◆ Use CC Structure

- ST
- Requirements
- CEM-like activities

- ◆ Change definitions

- Will require little “internal” documentation
- Procedural Objectives

- ◆ C&A focus

- Level of assurance about EAL3
- Can waive requirements

# Design Analysis Approach

---

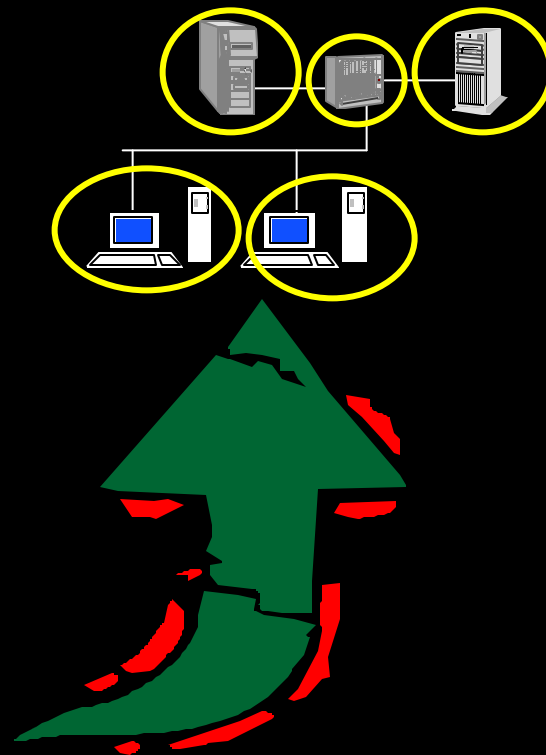
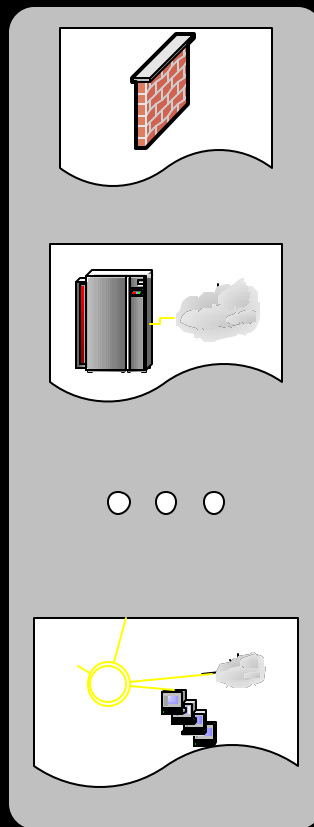
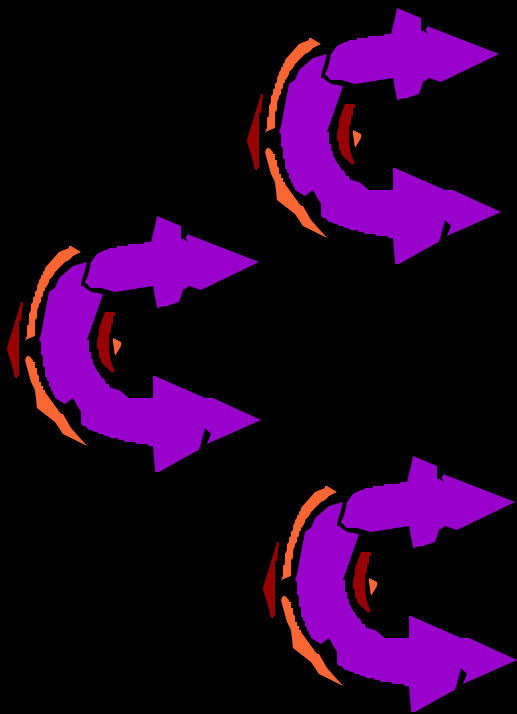
- ◆ Identify Interfaces

- Use available documentation
- Forms basis of analysis

- ◆ Identify Systems with Higher-Assurance needs

- Boundary Devices
- Devices “Visible” Through Boundary Devices

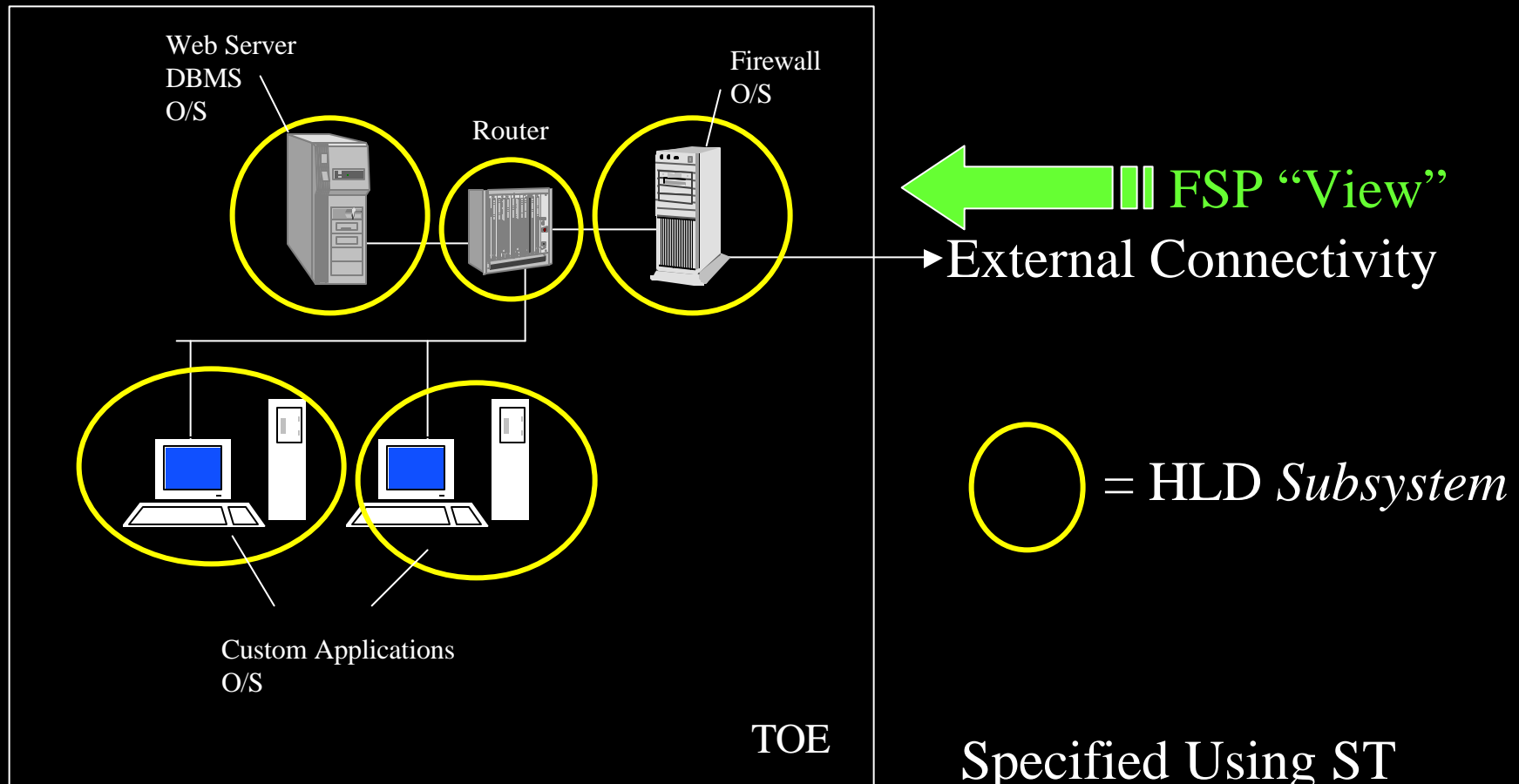
# Types of Analysis



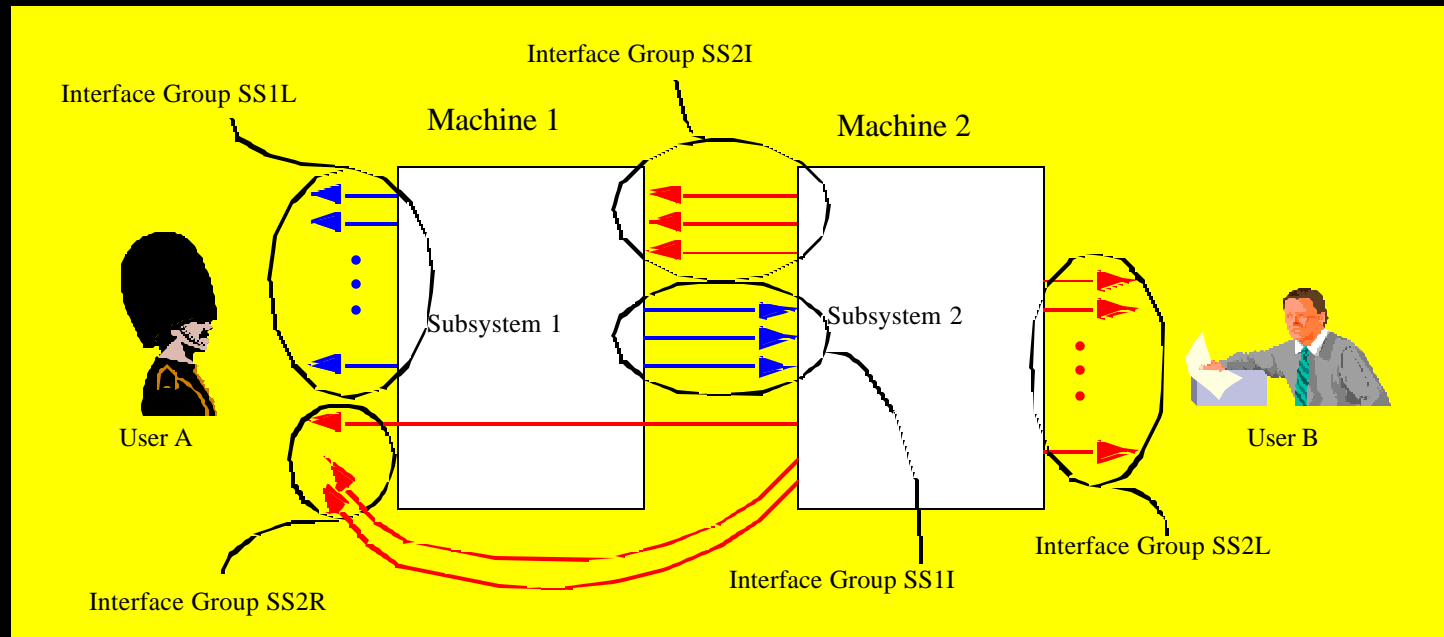
←  
**Recomposition  
Analysis**

**System/Subsystem  
Analysis**

# “System” Definition



# “System” Definition (continued)



External Interfaces: SS1L, SS2L, SS2R

Internal Interfaces: SS2I, SS1I

# Constructing a System ST

---

## ◆ TOE Description

- Include Connectivity Architecture
- Users
  - » Untrusted
  - » Semi-trusted
  - » Trusted

## ◆ TOE Environment

- Items that “generate” procedural objectives

## ◆ Objectives

- Procedural objectives
- Rationale identifies basis for evaluation

# Performing System Analysis

---

## ◆ Assessment using the CEM

- Probably needs to be tailored
- TOE, ST, and developer evidence considered
- Unmet requirements
  - » Discard
  - » Addressed by developer
  - » Risk analysis written

## ◆ Role of developer

- “Developer” likely to be SI
- Affects ALC, ACM, ADO

# Pros

---

- ◆ Does Not Require In-depth Design Documentation
- ◆ Scopes and Focuses Analysis
  - Common language using CC
  - Analysis methodology using CEM
- ◆ Addresses composition problem

# Pros (continued)

---

- ◆ Using evaluated products
  - Use when higher assurance needed
  - Documentation Exists (Need to Require)
  - Increased Assurance
    - » Documented Interfaces
    - » Security Functionality
- ◆ Uses risk analysis approach
- ◆ Procedures, actual configuration part of assessment

# Cons

---

- ◆ Requires Production of Documentation
  - System-level PPs, STs
  - “Developer” Documentation
- ◆ Application of Requirements at Subsystem Level
- ◆ Recomposition Analysis Required
- ◆ Less Internal Documentation => Reduced Assurance
- ◆ SI Performs Developer Actions
- ◆ CC Skills Needed