

# Open Source Operating Systems for AADS<sup>1</sup>

*Notes on quality validation and security certification*

<sup>1</sup>Airplane Assets Distribution Systems



David von Oheimb and Wolfgang Schmid

Siemens Corporate Technology, Munich

OpenCert 2007 workshop  
Braga, Portugal, 31 March 2007

## Overview

- IT Security at Siemens Corporate Technology
- Airplane Assets Distribution System
- Validation Criteria for OSS Systems
- Survey Results on Current Operating Systems
- Certification According to the Common Criteria

# Siemens Corporate Technology: About 1,800 Researchers and Developers Worldwide ...

**SIEMENS**

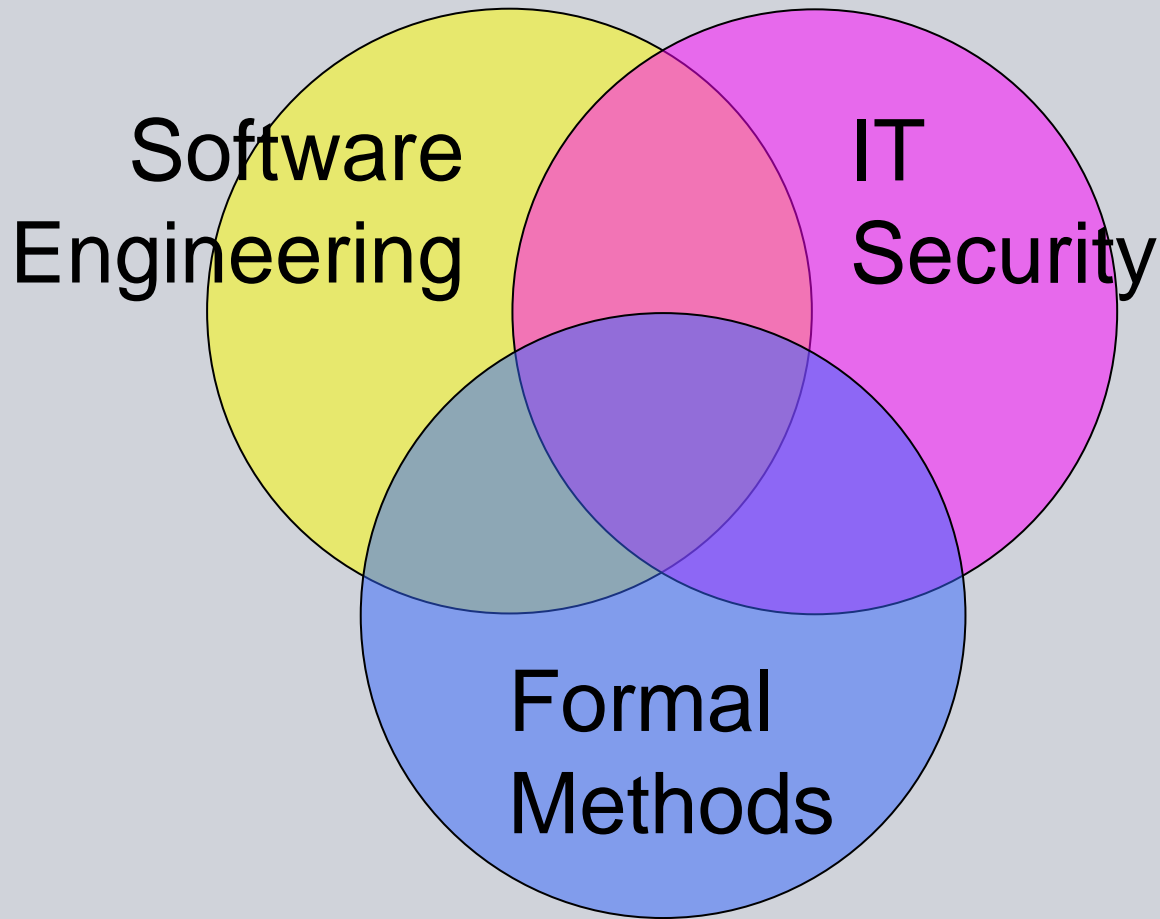


## Security Applications & Methods



- # **Secure Operating Systems, Trusted Platform Modules (TPM)**
- # **General Purpose Identity Management and Authorization**
  - # Role / Policy Based Access Control (RBAC)
  - # Public Key Infrastructure (PKI), Single Sign-On (SSO)
  - # Web Services and Business Process Security
  - # Security of Service Oriented Architecture (SOA)
- # **Application-level security: e-health, e-government, e-Commerce**
- # **Digital Rights Management (DRM) Privacy**
- # **Formal Methods and Certification**

**Fields**

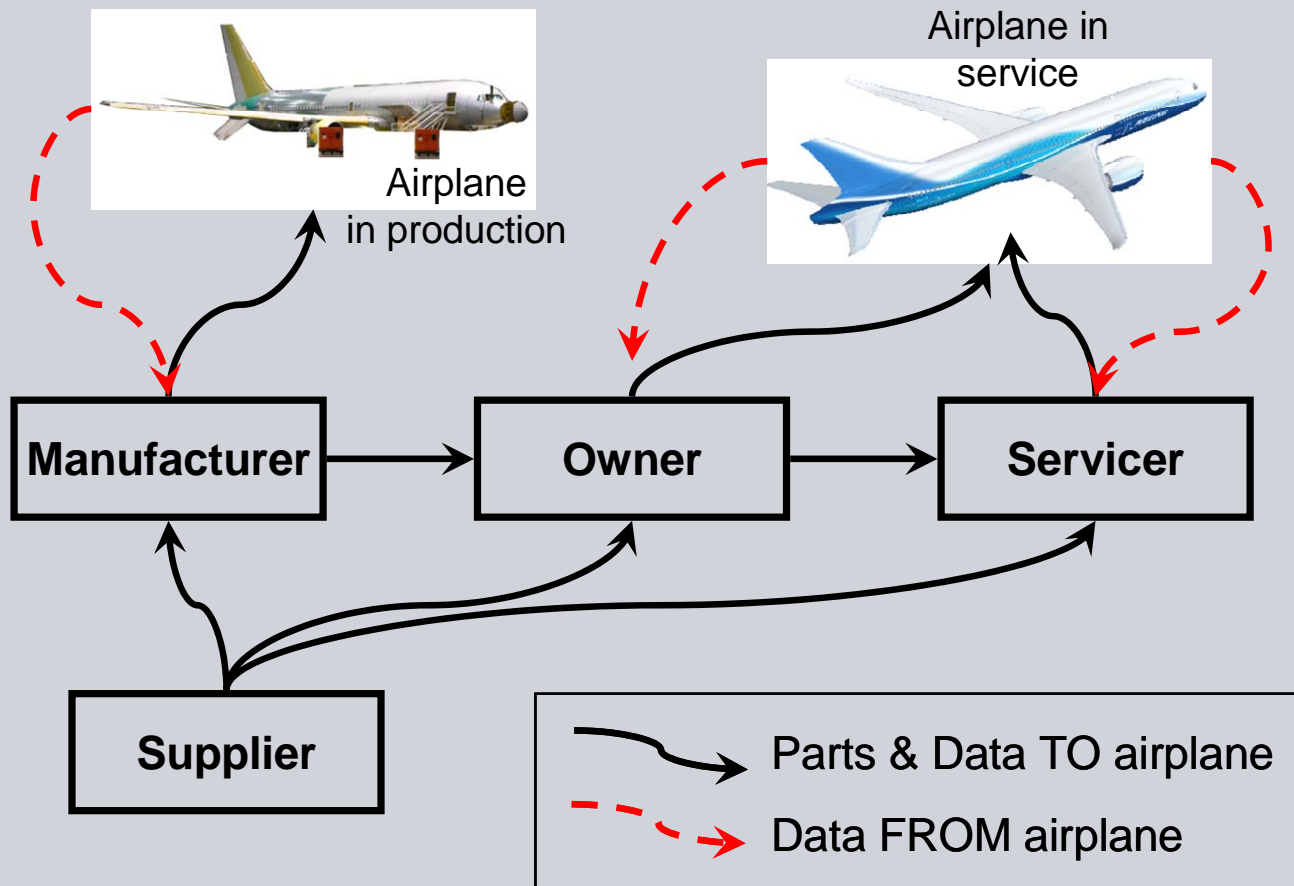


## Overview

- IT Security at Siemens Corporate Technology
- **Airplane Assets Distribution System**
- Validation Criteria for OSS Systems
- Survey Results on Current Operating Systems
- Certification According to the Common Criteria

## Airplane Assets Distribution System

AADS is a system for storage and distribution of airplane assets, including *Loadable Software Airplane Parts* and airplane health data



## AADS Architecture

A complex distributed store-and-forward middleware with OSS components

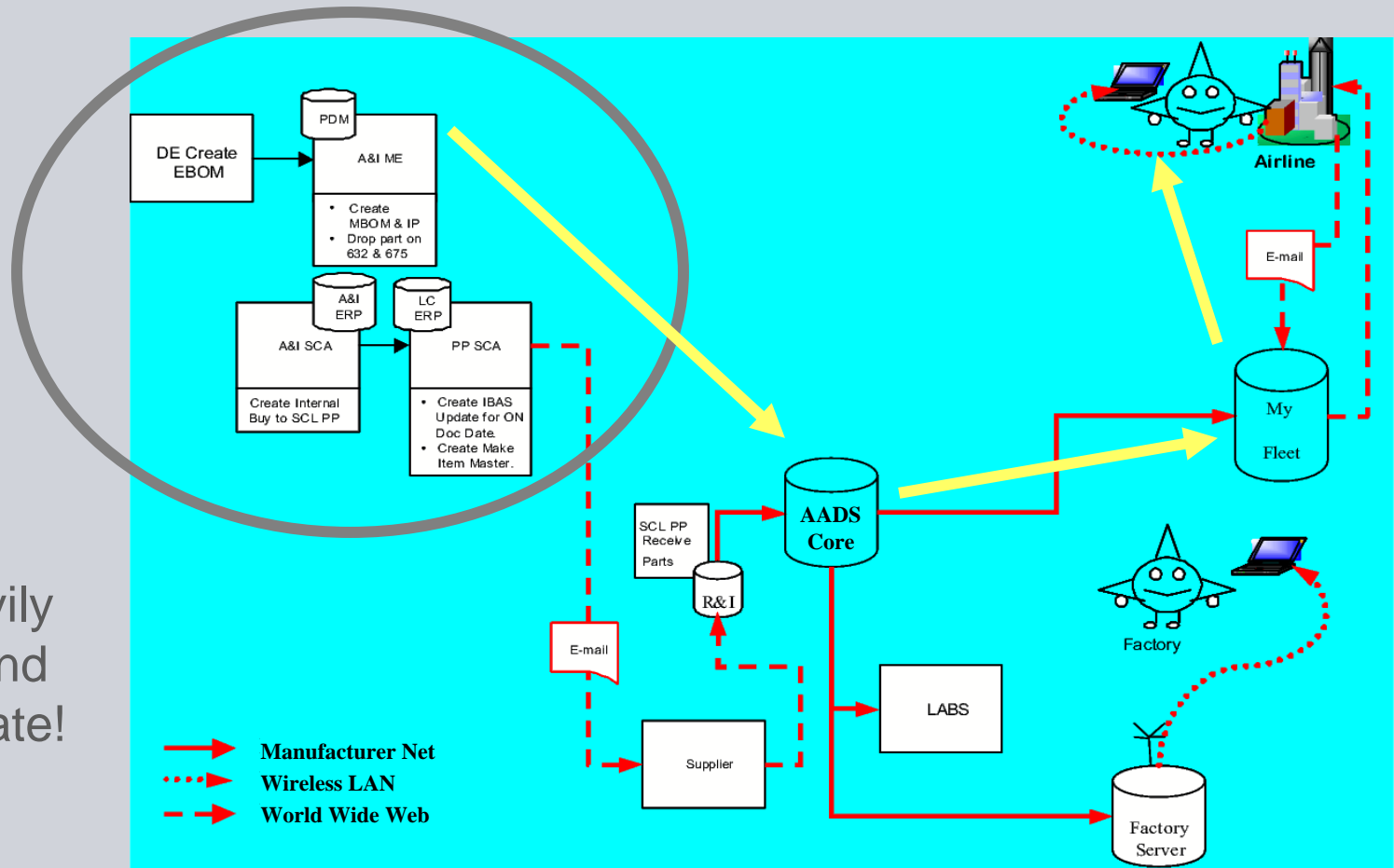
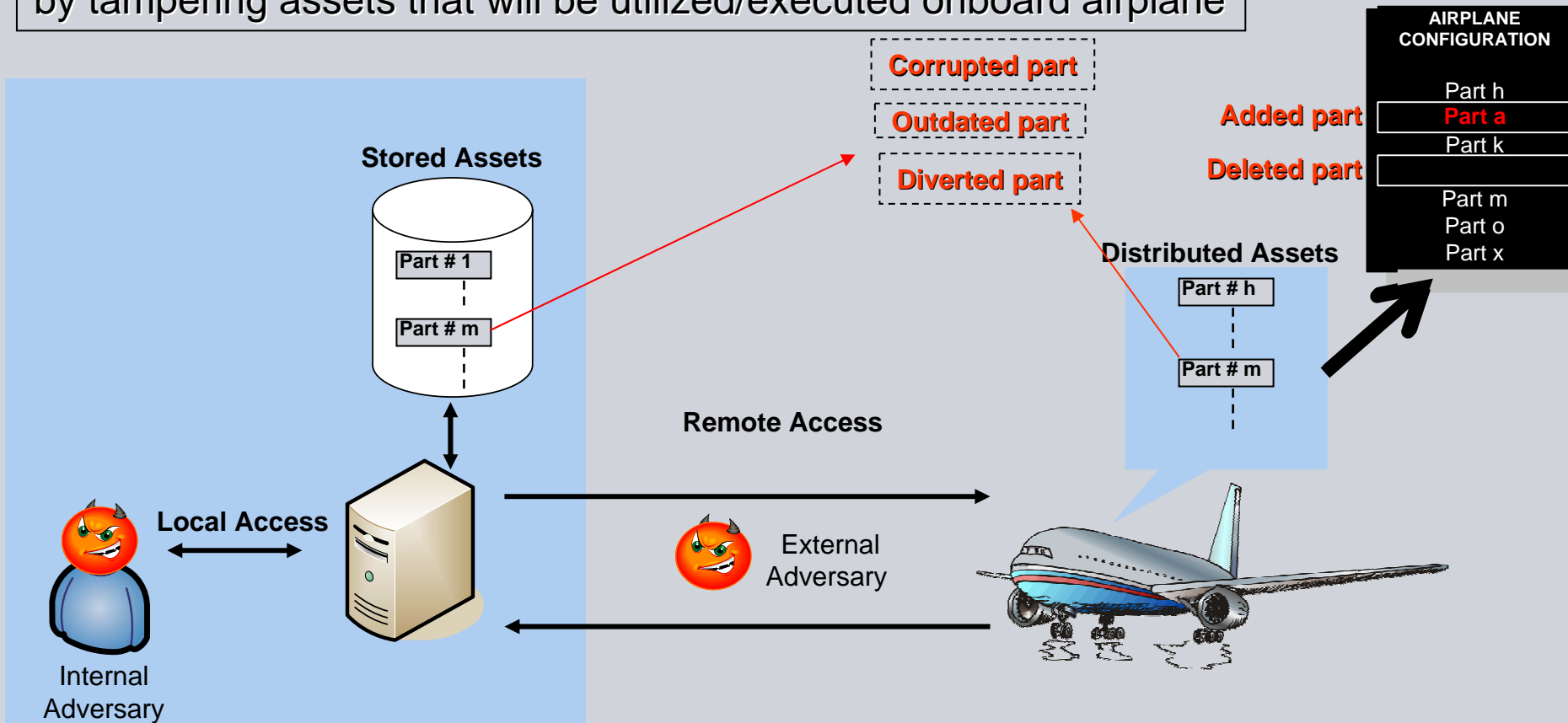


Figure heavily simplified and not up-to-date!

## Safety-relevant Threats

**Safety-relevant Threats:** lower airplane safety margins by tampering assets that will be utilized/executed onboard airplane



**ST.Corruption**

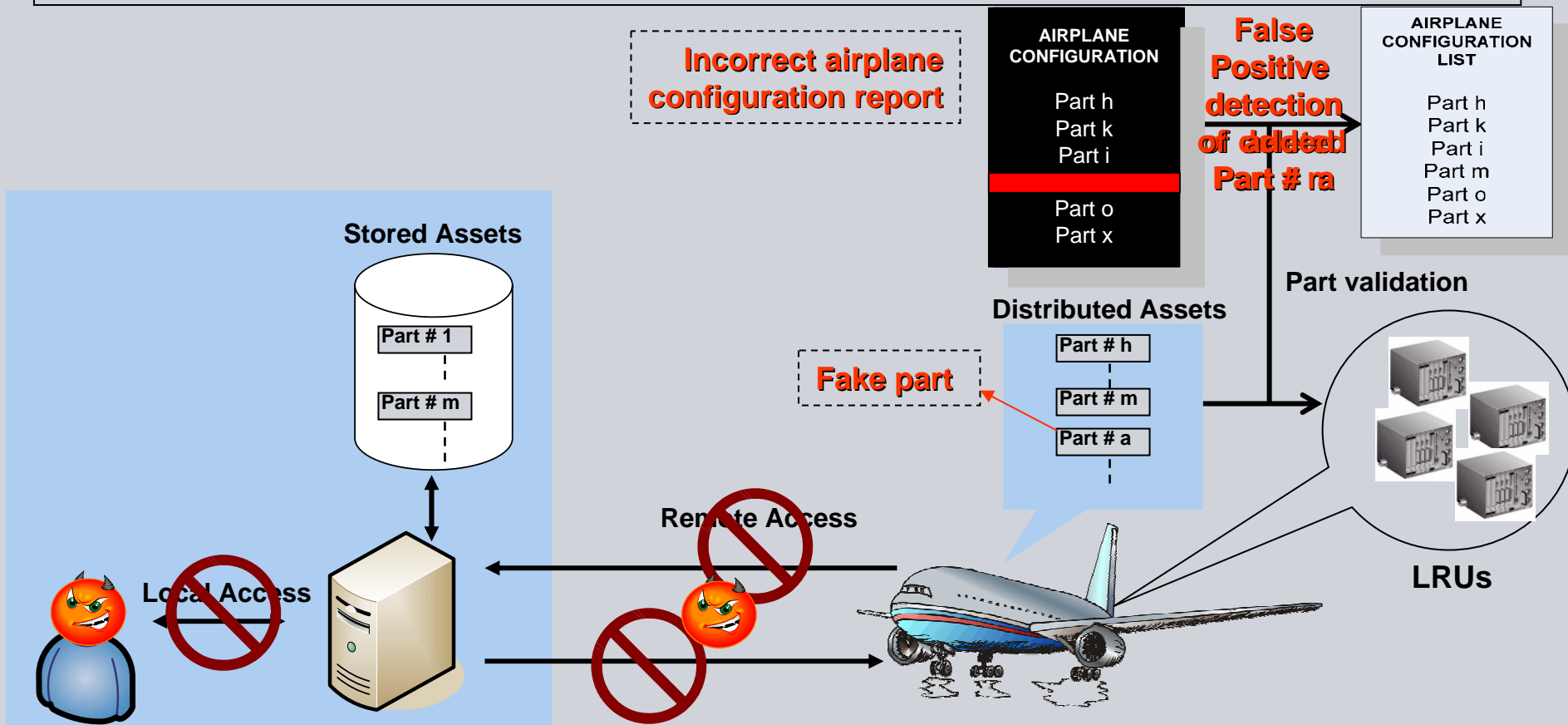
**ST.Staleness**

**ST.Diversion**

**ST.Misconfiguration**

## Business-relevant Threats

**Business-relevant Threats:** impede business of airplane production, operation, and maintenance organizations by disrupting airplane service



**BT.Late\_Detection**

**BT.False\_Alarms**

**BT.Denial\_of\_Service**

## Security as a SW Engineering Problem

- **IT / computer security** aims at preventing, or at least detecting, unauthorized actions by agents in a computer system.

complements

- **safety**: absence of damage due to mistakes or other *unintentional* failure

**Situation**: security loopholes in IT systems **actively exploited**

**Objective**: **thwart attacks** by absence of vulnerabilities

**Difficulty**: security is interwoven with the whole system.

IT systems are very complex, security **flaws hard to find**.

**Remedy**: follow the **Common Criteria** approach

- address **security in all development phases**
- do reviews and tests
- make use of **formal modeling / analysis**

## Development Phases and the Benefits of Certification

### Requirements analysis:

understanding the security issues

- **abstraction**: concentration on essentials, to keep overview
- **genericity**: standardized patterns simplify the analysis

### Design, documentation:

quality of specifications

- enforces **preciseness** and **completeness**

### Implementation:

effectiveness of security functionality

- demands systematic testing, in part even formal verification

## Overview

- IT Security at Siemens Corporate Technology
- Airplane Assets Distribution System
- Validation Criteria for OSS Systems
- Survey Results on Current Operating Systems
- Certification According to the Common Criteria

# Deploying Open Source Operating Systems

## Motivation

- Use **well accepted systems** like Linux, Apache, and OpenSSL
- **Save license costs** for the customers

## Criteria

- **Stability** (reduce patching and certification efforts)
- **Security** (counter safety and business threats)
- Support of Java (JDK)

## Questions

- Which are the **alternatives** (besides common Linux distributions)?
- What are their **pros and cons**?

## Open Source SW Licenses

Ranking from lower to higher restrictions:

License	Full Name
1. ISC License	Internet Systems Consortium (ISC) license
2. New BSD License	New Berkley Software Distribution License
3. BSD License	Berkley Software Distribution License
4. CDDL	Common Development and Distribution License
5. LGPL	GNU Library or "Lesser" General Public License
6. GPL	GNU General Public License

## Indicators for OSS Quality

- How many lines of code does the system encompass?

The more lines the higher the **likeliness of errors**.

- How long does the system exist?

The longer the better (**maturity**).

- How active are the development mailing lists?

Shows if the project is **alive** and **vulnerabilities** are **fixed quickly**.

- How large is the user base?
- How frequently is it used per user?
- Is it used within diverse scenarios?

The more use the more likely **problems** are **detected and reported**.

## Further Criteria

- Development process (anarchic, supervised)?
- Development history
- Use history
- Maintainability
- Is the list of bugs/fixes available?
- Severity of bugs so far?
- How long does it take for a bug to be fixed?

## Overview

- IT Security at Siemens Corporate Technology
- Airplane Assets Distribution System
- Validation Criteria for OSS Systems
- Survey Results on Current Operating Systems
- Certification According to the Common Criteria

## Linux (various distributions)

### Advantages:

- Well known
- Well maintained
- Available for almost all platforms
- Very large group of users
- Very low “Defect Reports/kLOC”
- Certifications according to the Common Criteria

### Disadvantages:

- Changes occur frequently and may have substantial impact
- Older (stable) versions do not necessarily gain full attention
- Licensed under the GPL

## SELinux: Security Enhanced Linux

### Advantages:

- Fine-grained continuous **mandatory access control** to resources
- Part of the standard Linux kernel
- Extends update intervals

### Disadvantages:

- **Complex setup**

## OpenBSD Unix

### Advantages:

- Long history of the “Berkley Software Distribution”
- Second most popular system within BSD community
- Publicly open development, but continuous code auditing for security problems -> **almost no security loopholes over years**
- Binary API for Linux and others
- **Built-in memory protection, cryptography, and privilege separation**
- Licensed under the ISC license

### Disadvantages:

- **Small user community** (after split due to legal problems with AT&T)
- **No certifications** according to Common Criteria

## Open Solaris by Sun Microsystems

### Advantages:

- High code quality expected (inherited from Solaris)
- Certifications according to Common Criteria

### Disadvantages:

- Special license type (CDDL) which is considered to be incompatible with the GPL, which is used for many other Open Source packages
- As an open source project, still premature
- Mailing lists relatively quiet
- Knowledge of source code are scarce within the OSS community

## Overview

- IT Security at Siemens Corporate Technology
- Airplane Assets Distribution System
- Validation Criteria for OSS Systems
- Survey Results on Current Operating Systems
- Certification According to the Common Criteria

## Common Criteria (CC)



product-oriented

IT security assessment

**ISO/IEC standard 15408**

Version 3.1 of 2006

**Generic** approach (“construction kit” for specifying evaluations):

- Building blocks for defining *Security Functional Requirements (SFRs)*
- Scalable in depth and rigor: *Evaluation Assurance Levels (EALs)*

## CC Certification Aim and General Approach

**Aim:** gain **confidence** in the security of a system

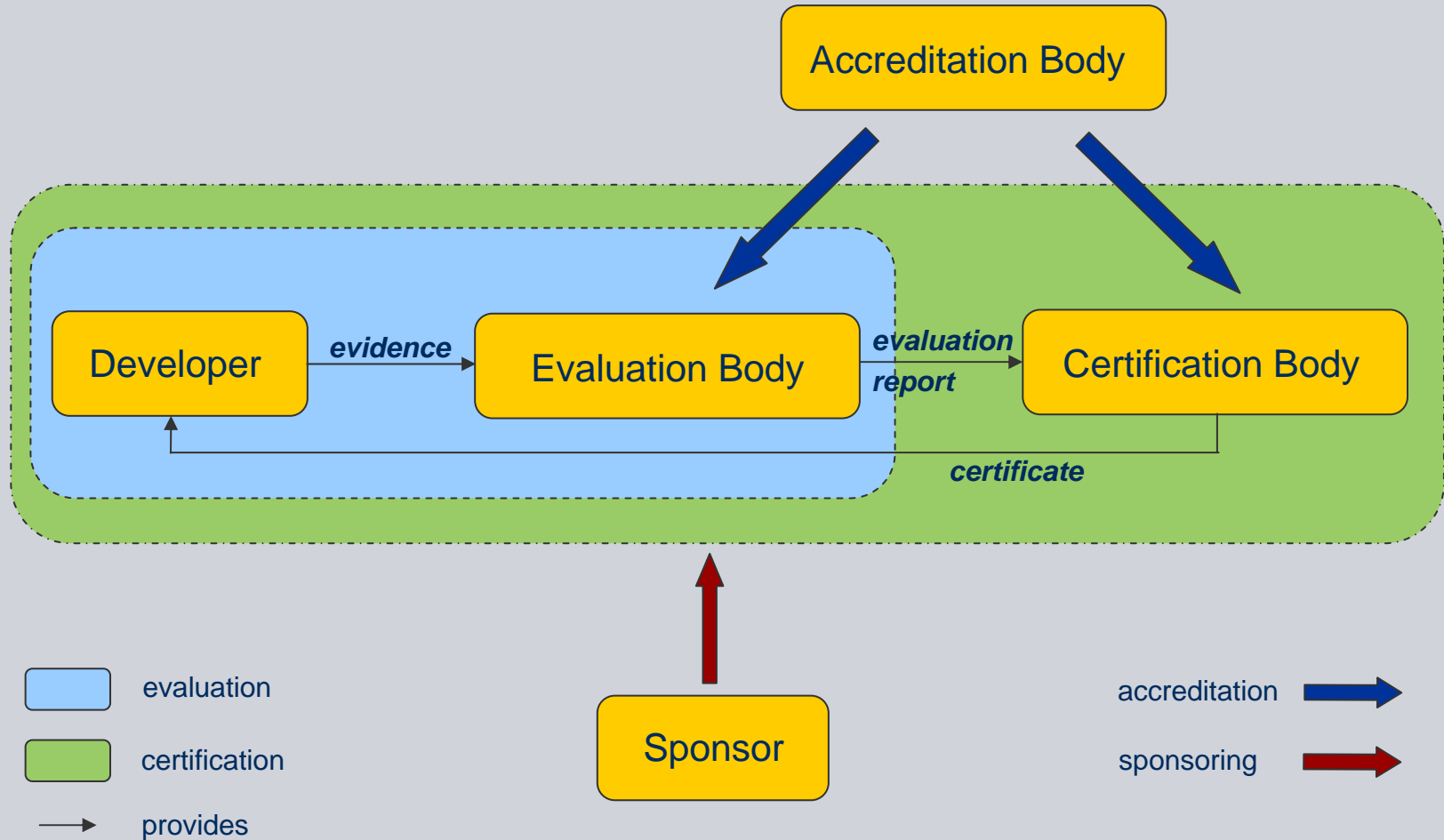
- What are the **objectives** the system should achieve?
- Are the **measures** employed **appropriate** to achieve them?
- Are the measures **implemented and deployed correctly**?

**Approach:** **assessment** of the system **by neutral experts**

- **Understanding** the security functionality of the system
- Gaining **evidence** that the functionality is correctly implemented
- Gaining **evidence** that the integrity/configuration of the system is kept

**Result:** a successful evaluation is awarded a **certificate**

## CC Process Scheme



## CC *Security Target* (product-specific) or *Protection Profile* (generic)

1. Introduction (product advertisement)
2. *System Description: defines Target of Evaluation (TOE)*
3. Security Environment
  - Assets and related Actions
  - Threats
  - Required Evaluation Assurance Level
  - Assumptions
4. *Security Objectives*
  - ...
  - Rationale wrt. threats
5. *Security Functional Requirements*
  - ...
  - Rationale wrt. objectives

## OS Operating Systems certified according to the CC

Security certification according to the Common Criteria is a rather **complex**, **time consuming** and **expensive** task.

System	Assurance Level
SuSE Linux Enterprise Server	up to EAL 4+
Red Hat Enterprise Linux	up to EAL 4+
Sun Solaris	up to EAL 4+

All based on the **Controlled Access Protection Profile (CAPP)**

Limited in scope (target of evaluation, objectives, etc. in the Security Target).

**Certifications appreciated** as effort to **assure quality and security**.