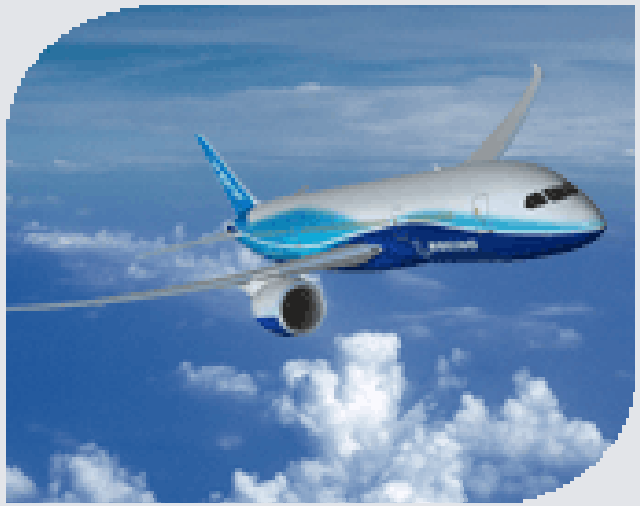
Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety

Richard Robinson[1], Mingyan Li[1], Scott Lintelman[1], Krishna Sampigethaya[2], Radha Poovendran[2], **David von Oheimb[3]**, Jens-Uwe Bußer[3], and Jorge Cuellar[3]

[1] Boeing Phantom Works, Seattle
[2] University of Washington, Seattle
[3] Siemens Corporate Technology, Munich

SAFECOMP 2007, Nuremberg, Germany, 19 September 2007

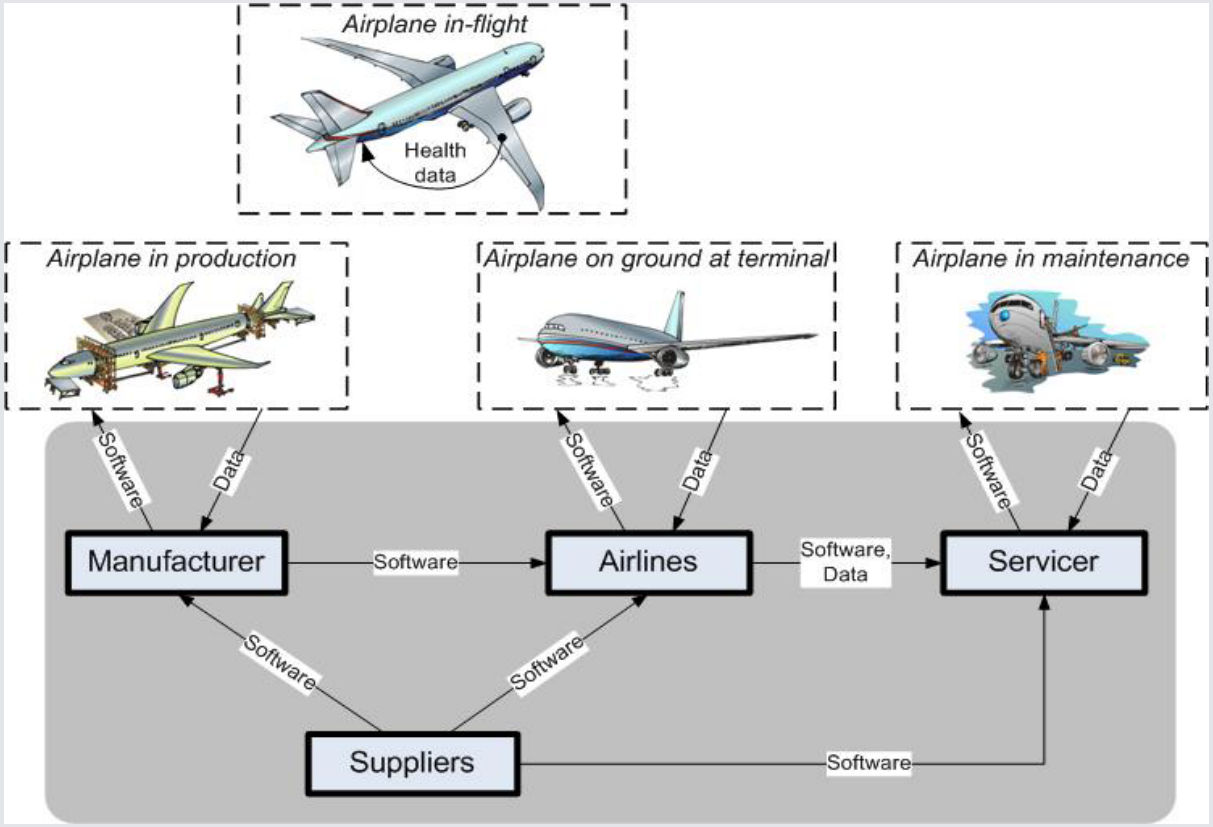


Overview

- **A**irplane **A**ssets **D**istribution **S**ystem
- Assessment according to the Common Criteria
- Conclusion

Airplane Assets Distribution System (AADS)

AADS: system for storage and distribution of airplane assets, in particular of *Loadable Software Airplane Parts (LSAPs)* and airplane health data



Transition from media-based (CD-ROMs etc.) to networked transport

AADS Architecture

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

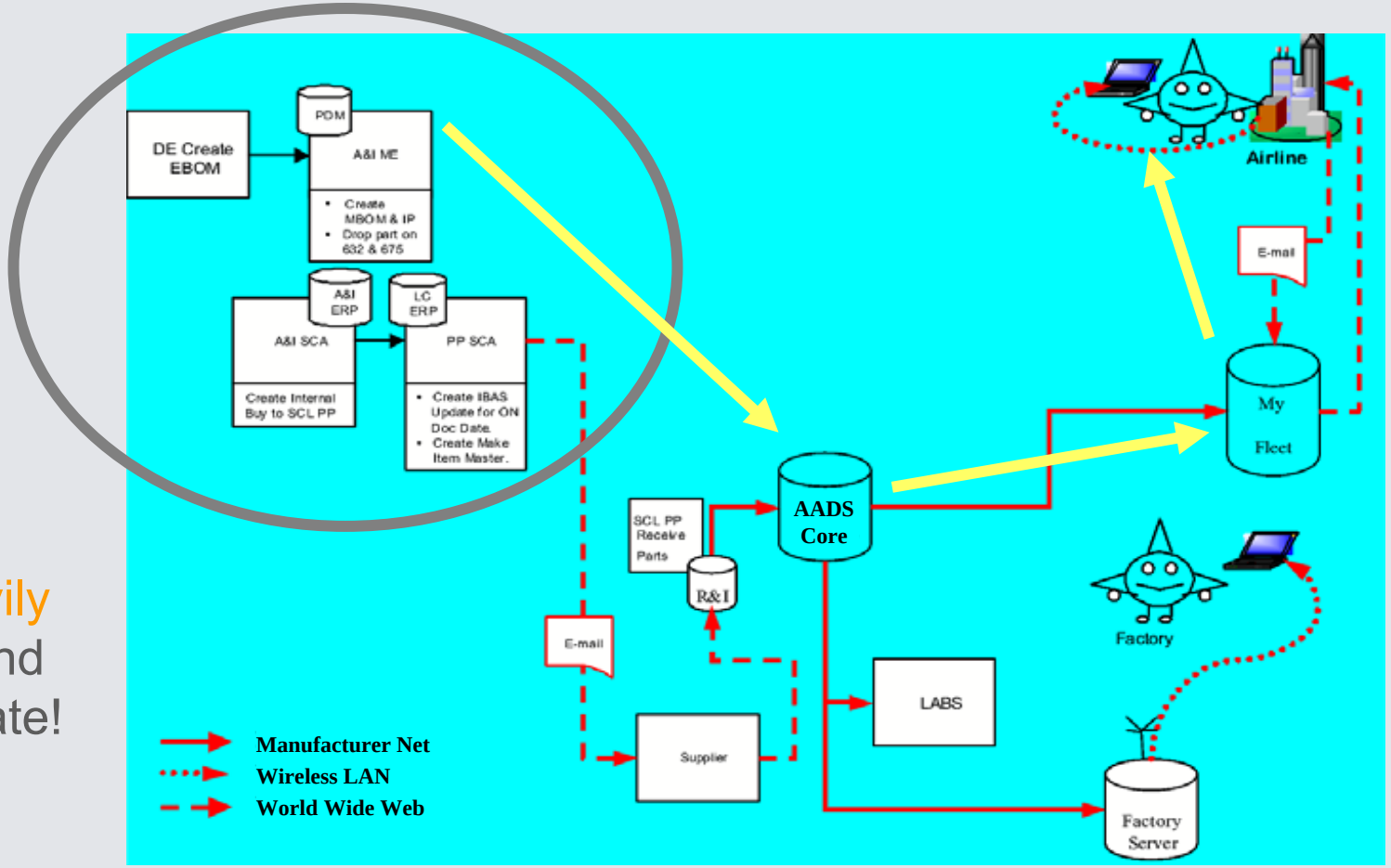
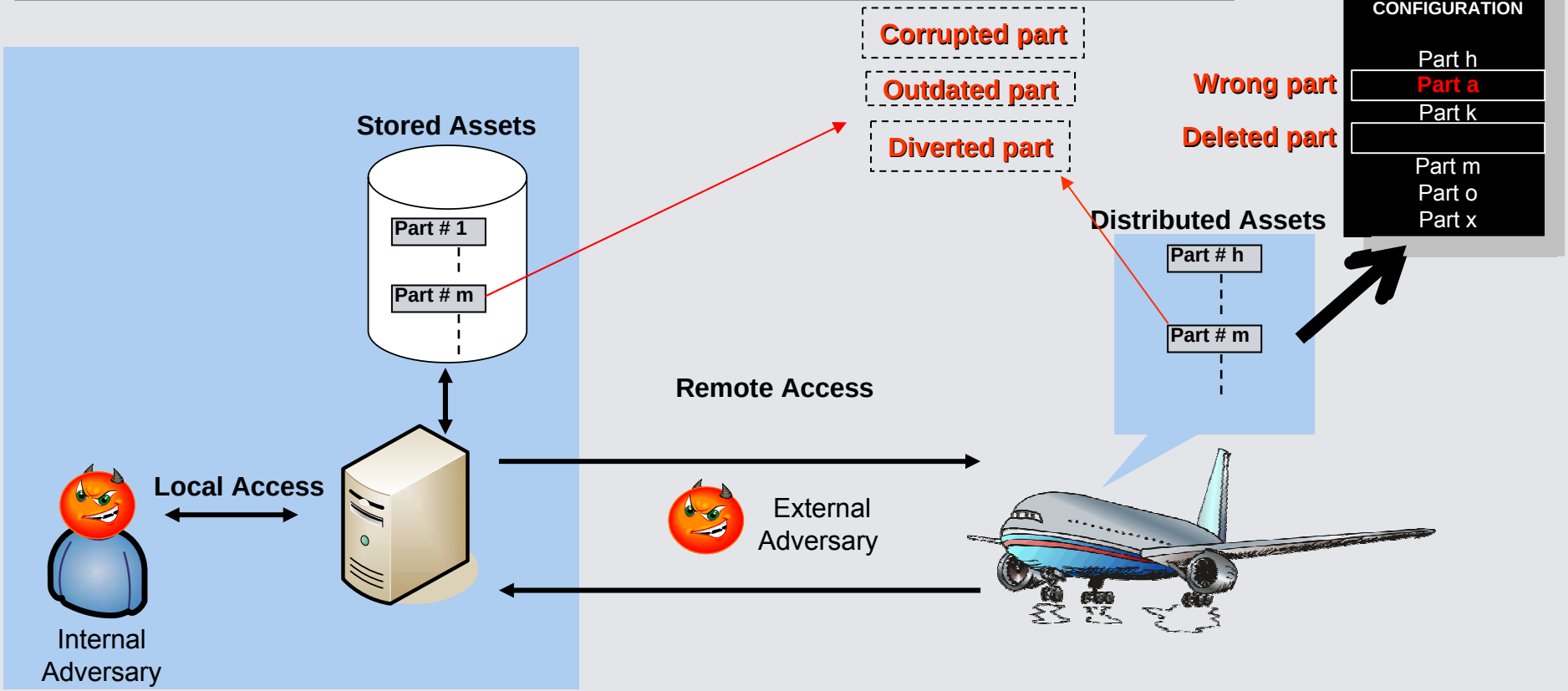


Figure heavily simplified and not up-to-date!

Safety-relevant Threats

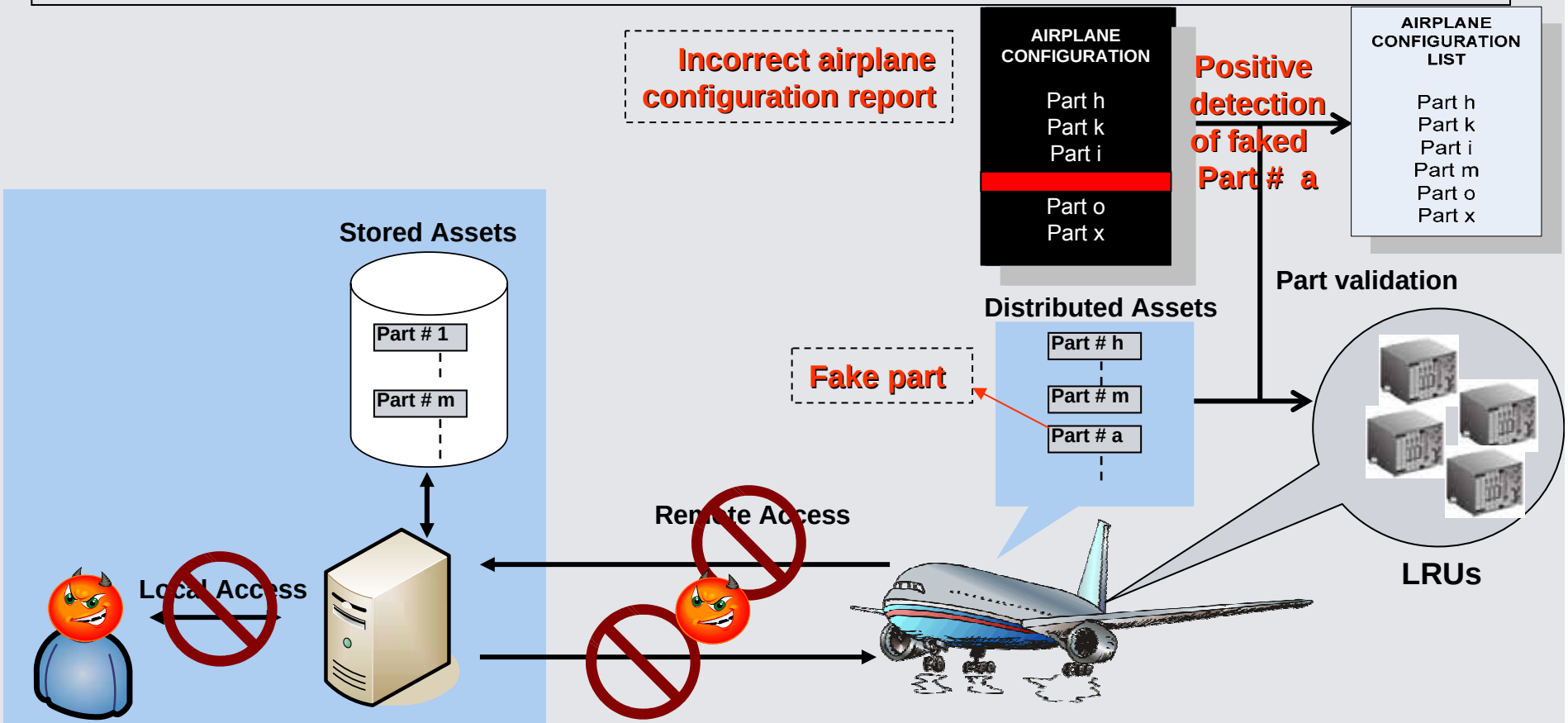
Safety-relevant Threats: lower airplane safety margins
by tampering assets that will be utilized/executed onboard airplane



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 BT.Repudiation

IT Security as a System Engineering Problem

- Security aims at preventing, or at least detecting, unauthorized actions by agents in an IT system.

In the AADS context, security is a prerequisite of safety.

- Safety aims at the absence of accidents (→ airworthiness)

Situation: security loopholes in IT systems actively exploited

Objective: thwart attacks by eliminating vulnerabilities

Difficulty: IT systems are very complex. Security is interwoven with the whole system, so very hard to assess.

Remedy: evaluate system following the Common Criteria approach

- address security systematically in all development phases
- perform document & code reviews and tests
- for maximal assurance, use formal modeling and analysis

Overview

- Airplane Assets Distribution System
- Assessment according to the Common Criteria
- Conclusion

Common Criteria (CC) for IT security evaluation

product-oriented methodology

for IT security assessment

ISO/IEC **standard** 15408

Current version: 3.1 of 2006

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?

CC General Approach

Approach: assessment of system + documents by neutral experts

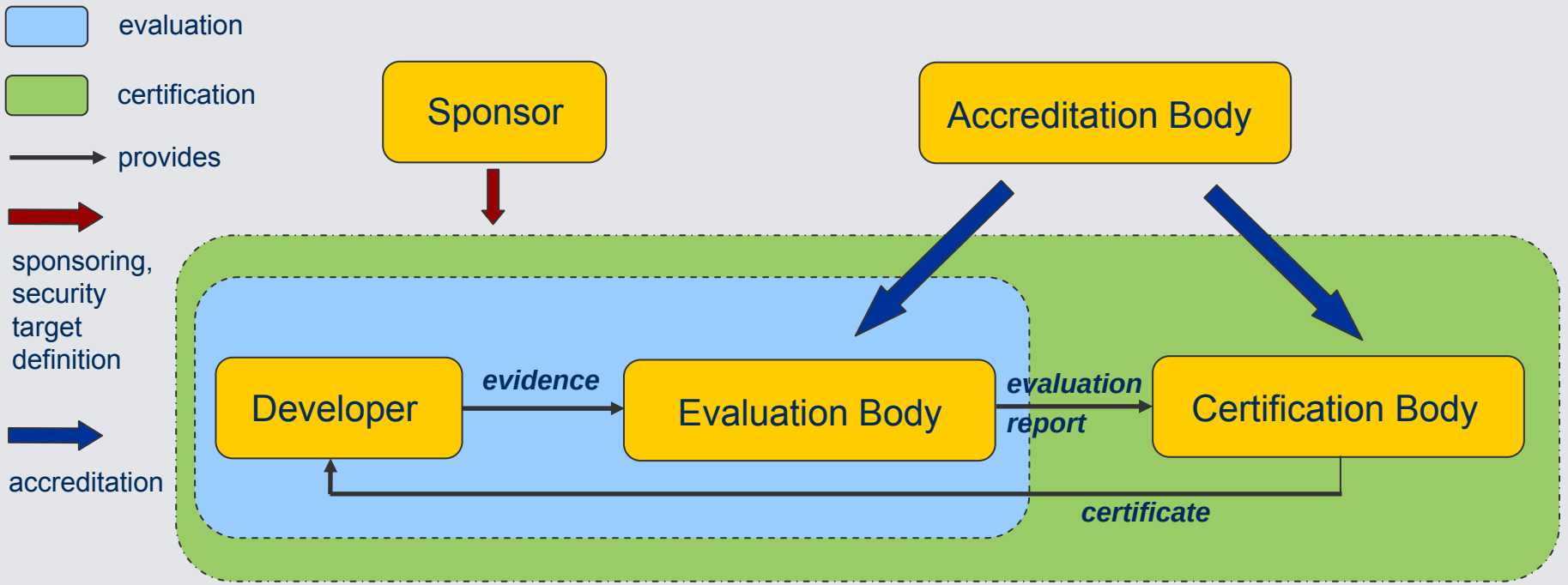
- Gaining understanding of the system's security functionality
- Checking evidence that the functionality is correctly implemented
- Checking evidence that the system integrity is maintained

Generic "construction kit" for specifying evaluations:

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

layered as *Evaluation Assurance Levels (EALs)*

CC Process Scheme



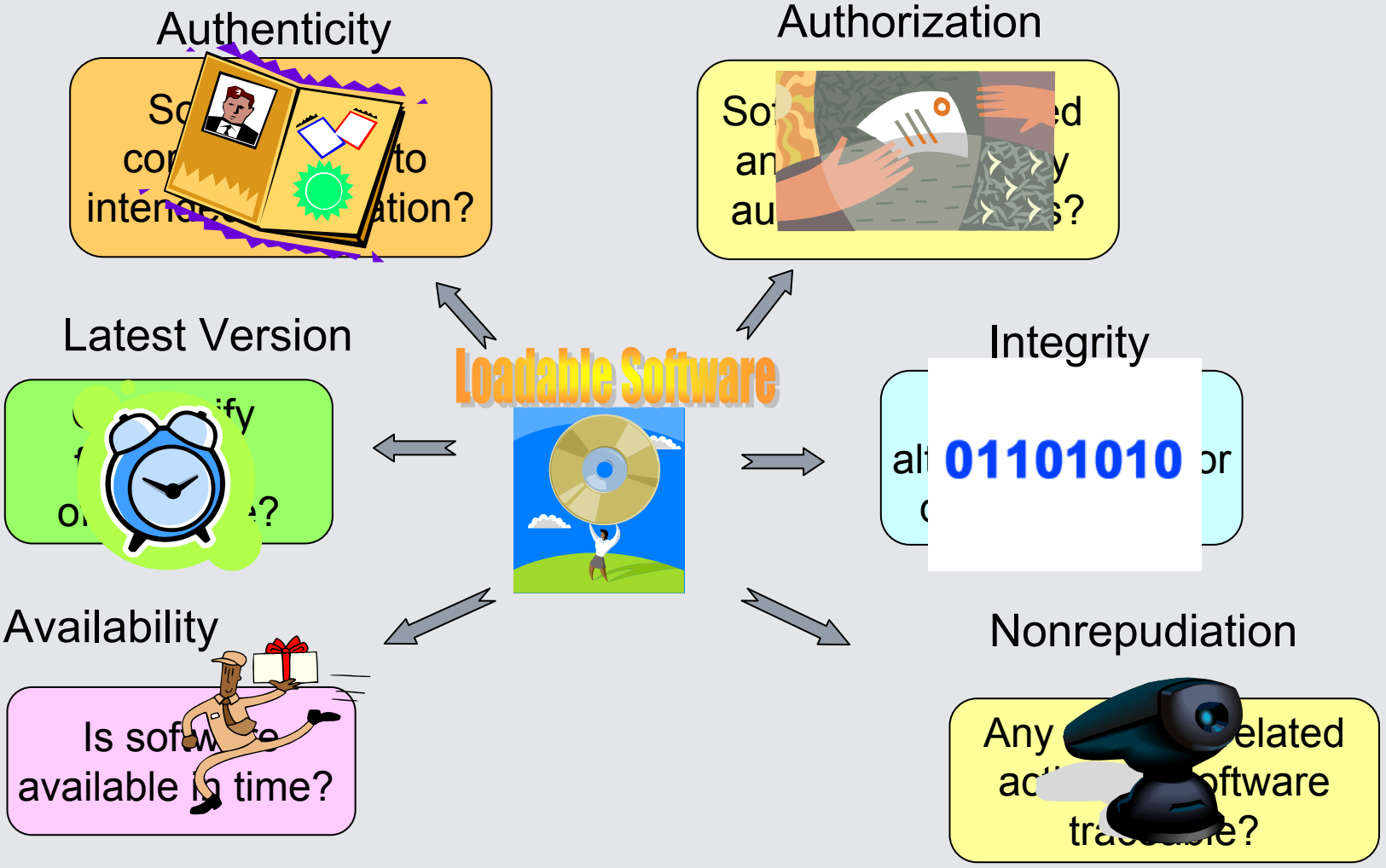
Certification according to the Common Criteria is a rather complex, time consuming and expensive process.

A successful, approved evaluation is awarded a certificate.

AADS Security Specification: CC Protection Profile (1)

1. Introduction
2. System Description
3. Security Environment
   - Assets and Related Actions
   - Threats
   - Required Assurance Level
   - Assumptions
4. Security Objectives
   - …
   - Rationale

Security Objectives for AADS



Threats Addressed by the AADS Security Objectives

Objectives	Threats	Safety-relevant				Business-relevant			
		Corruption	Misconfiguration	Diversion	Staleness	Unavailability	Late Detection	False Alarm	Repudiation
Safety-relevant	Integrity	√							
	Correct Destination			√					
	Latest Version				√				
	Authentication	√	√						√
	Authorization	√	√						
	Timeliness				√				
Business-Relevant	Availability					√			
	Early Detection						√		
	Correct Status							√	
	Traceability	√	√						√
	Nonrepudiation								√
Environment	Part_Coherence	√	√	√					
	Loading_Interlocks	√	√	√					
	Protective_Channels	√							
	Network_Protection				√	√			
	Host_Protection	√							√
Assumptions	Adequate_Signing	√							
	Configuration		√						
	Development	√	√	√	√	√	√	√	√
	Management	√	√						√

AADS Security Specification: CC Protection Profile (2)

1. Introduction
2. System Description
3. Security Environment
   - Assets and Related Actions
   - Threats
   - Required Assurance Level
   - Assumptions
4. Security Objectives
   - …
   - Rationale
5. Security Functional Requirements
   - …
   - Rationale

Selection of Evaluation Assurance Level (EAL) for AADS

	Flight safety	Airline business
Threat Level assume sophisticated adversary with moderate resources who is willing to take XXX risk	**T5**: XXX = significant e.g. intl. terrorists	**T4**: XXX = little e.g. organized crime, sophisticated hackers, intl. corporations
Information Value violation of the protection policy would cause YYY damage to the security, safety, financial posture, or infrastructure of the organization	**V5**: YYY= exceptionally grave Risk: loss of lives	**V4**: YYY = serious Risk: airplanes out of service, or damage airline reputation
Evaluation Assurance Level for the given Treat Level and Information Value	**EAL 6**: semiformally verified design and tested	**EAL 4**: methodically designed, tested, and reviewed

Evaluating the whole AADS at EAL 6 would be extremely costly.
Currently available Public Key Infrastructure (PKI) certified only at EAL 4.

Two-level approach: evaluate only LSAP integrity & authenticity at EAL6.

Overview

- Airplane Assets Distribution System
- Assessment according to the Common Criteria
- Conclusion

Conclusion

BOEING
UNIVERSITY OF WASHINGTON
SIEMENS

- Challenges for AADS development
  - pioneering system design and architecture
  - complex, heterogeneous, distributed system
  - security is critical for both safety and business
- Common Criteria offer adequate methodology for assessment
- Systematic approach, in particular formal analysis, enhances
  - understanding of the security issues
  - quality of specifications and documentation
  - confidence (of Boeing, customers, FAA, etc.) in the security solutions