First Results from the Developer Site Certification / ALC-Reusability-Project

Frank Sonnenberg

Bundesamt für Sicherheit in der Informationstechnik /
Federal Office for Information Security

6th ICCC / 2005-09-29

Presentation Content

- Motivation for the Project
- Overview of possible concepts
- Project Roadmap
- Summary

Background

Certification of a development site

would be a significant benefit for developers who develop multiple products

at one or more sites,

particularly under the same procedures

Motivation

- Increasing demand for development site certificates coming from different developers
- Reduce time and money for evaluations which will be performed within a short time frame under the same product development conditions
- Extention of the CC to ISMS aspects which become more and more important
- Improvement of the acceptance and opening of new markets for the Common Criteria

Project Goal

Development, Validation & Documentation

of practical

Criteria and/or Procedures

to perform

Comprehensible, Comparable & Re-Useable

evaluations of development sites

Two possible Strategies

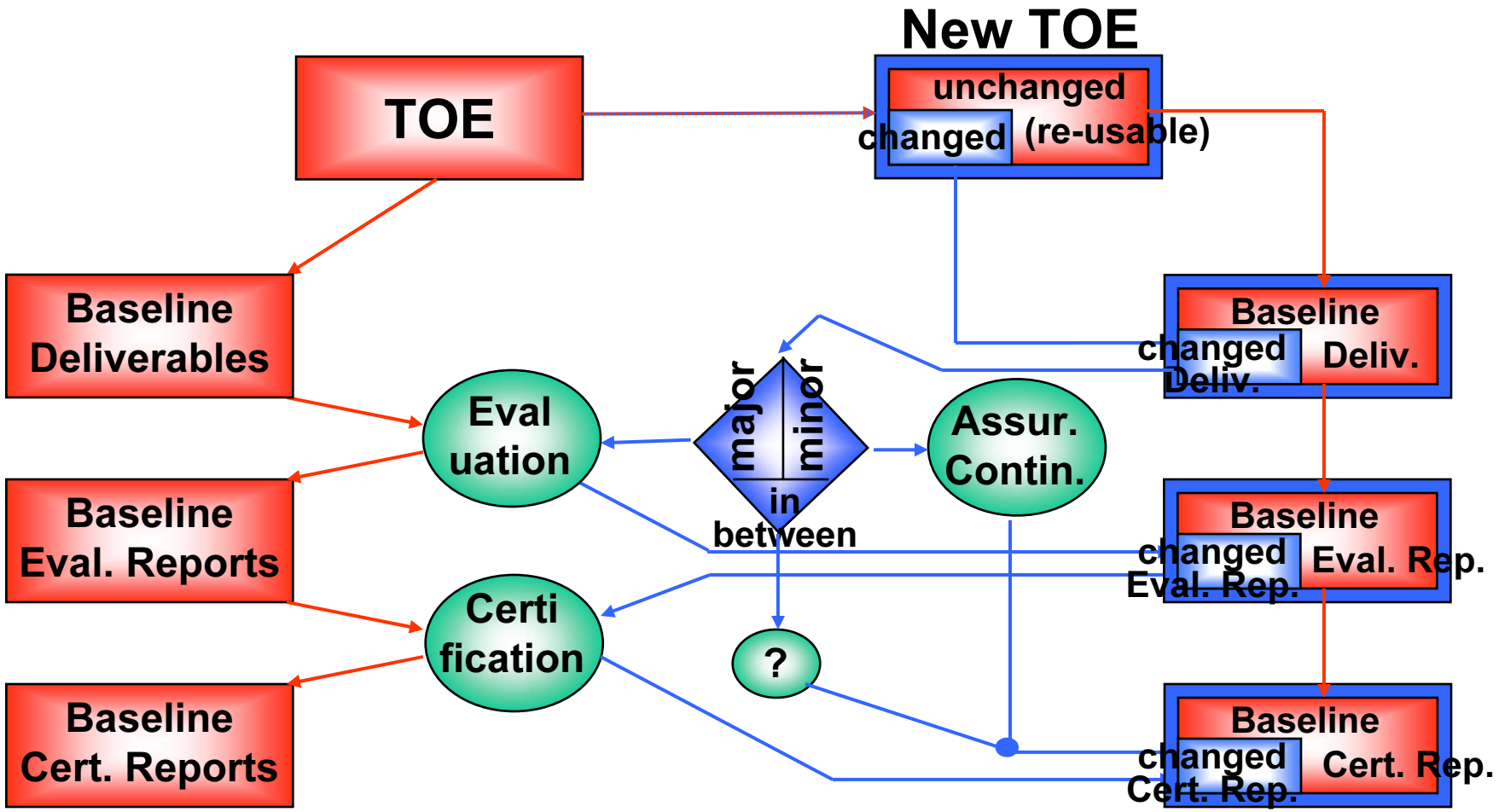
1. Re-Use of ALC material

Within a specific TOE evaluation references to previous TOE evaluation(s) will be made in order to re-use already certified CM system related aspects.

2. Developer Site Certification

A separate CC certificate will be issued to confirm that a specific development environment fulfils the CC requirements regarding the related ALC class.
This can be seen independently from a TOE evaluation.
Special ISMS definitions may be taken into account.

What is Re-Use?

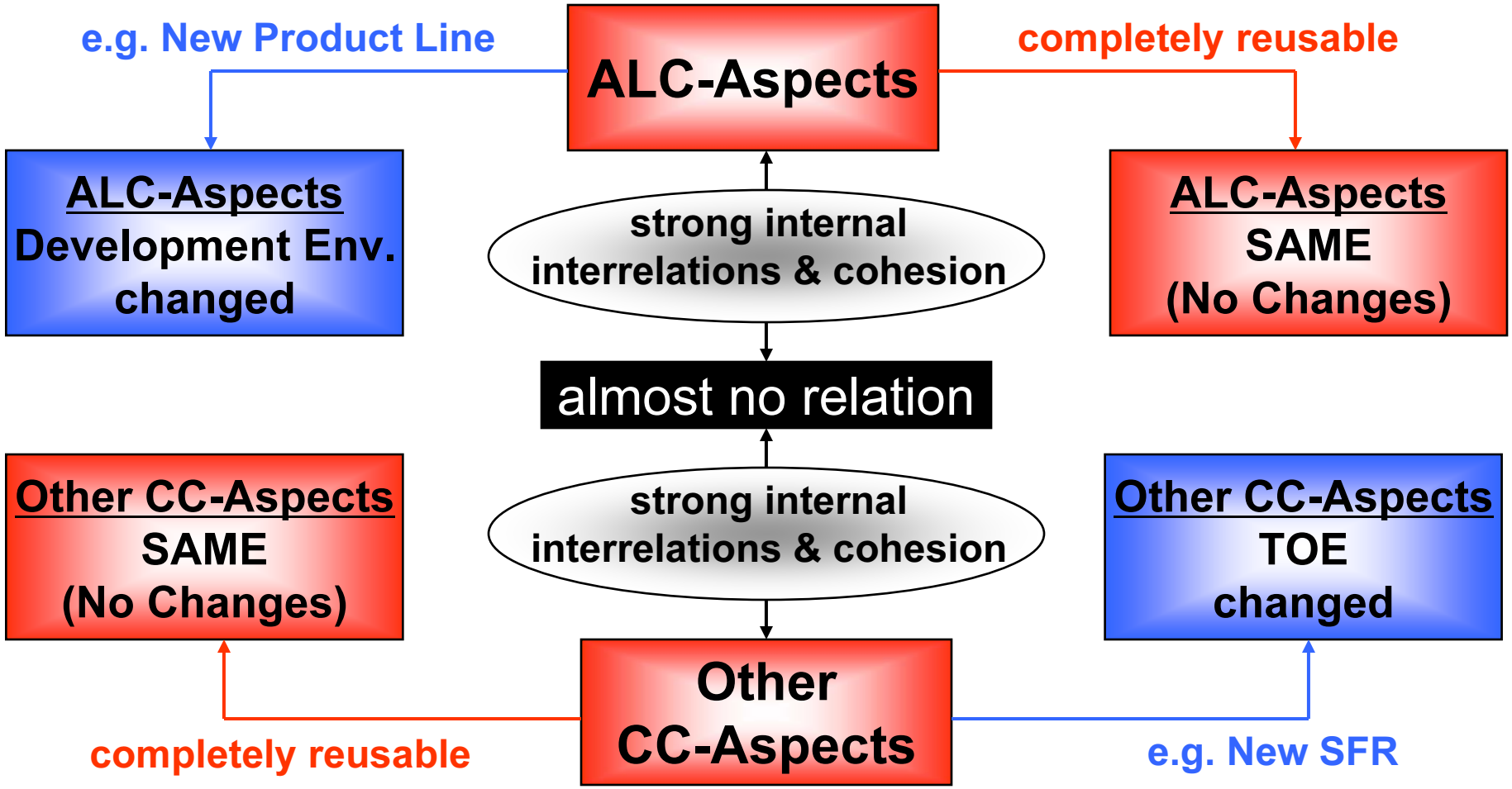


The Goal of Re-Use is ...

... to spend fewer resources on creating new results
than
the resources that would be spent
if the new items were created from scratch

$$\sum_{\text{Developer, Evaluator, Certifier}} \text{Efforts with Re-use} \;<\; \sum_{\text{Developer, Evaluator, Certifier}} \text{Efforts without Re-use}$$

Re-use in ALC


e.g. New Product Line
ALC-Aspects
completely reusable
ALC-Aspects
Development Env.
changed
strong internal
interrelations & cohesion
ALC-Aspects
SAME
(No Changes)
almost no relation
Other CC-Aspects
SAME
(No Changes)
strong internal
interrelations & cohesion
Other CC-Aspects
TOE
changed
completely reusable
Other
CC-Aspects
e.g. New SFR

ALC-Reusability Levels

- **The „Identical“ Case:**
  - Updated TOE same Develop. Environment
  - New TOE same Development Environment
- **The „Site-Evolution“ Case**
  - A Development Environment evolves in time under the same Evaluation Lab and Certification Body
- **The „Lab/Scheme-Change“ Case**
  - Identical Case and Site-Evolution Case under different Evaluation Lab / Certification Body

Reusability-Problems

- A catastrophe occurs when an expensive Site Visit has to be reperformed in the case of Minor Changes of the Development Site
- How to handle Reusability if the Developer changes the Evaluation Lab or the Certification Body
- How can ALC be classified into reusable and not reusable parts and how can the reusable parts be claimed in an evaluation?

Further Development of the Reusability Approach

We have added flexibility and efficiency by:

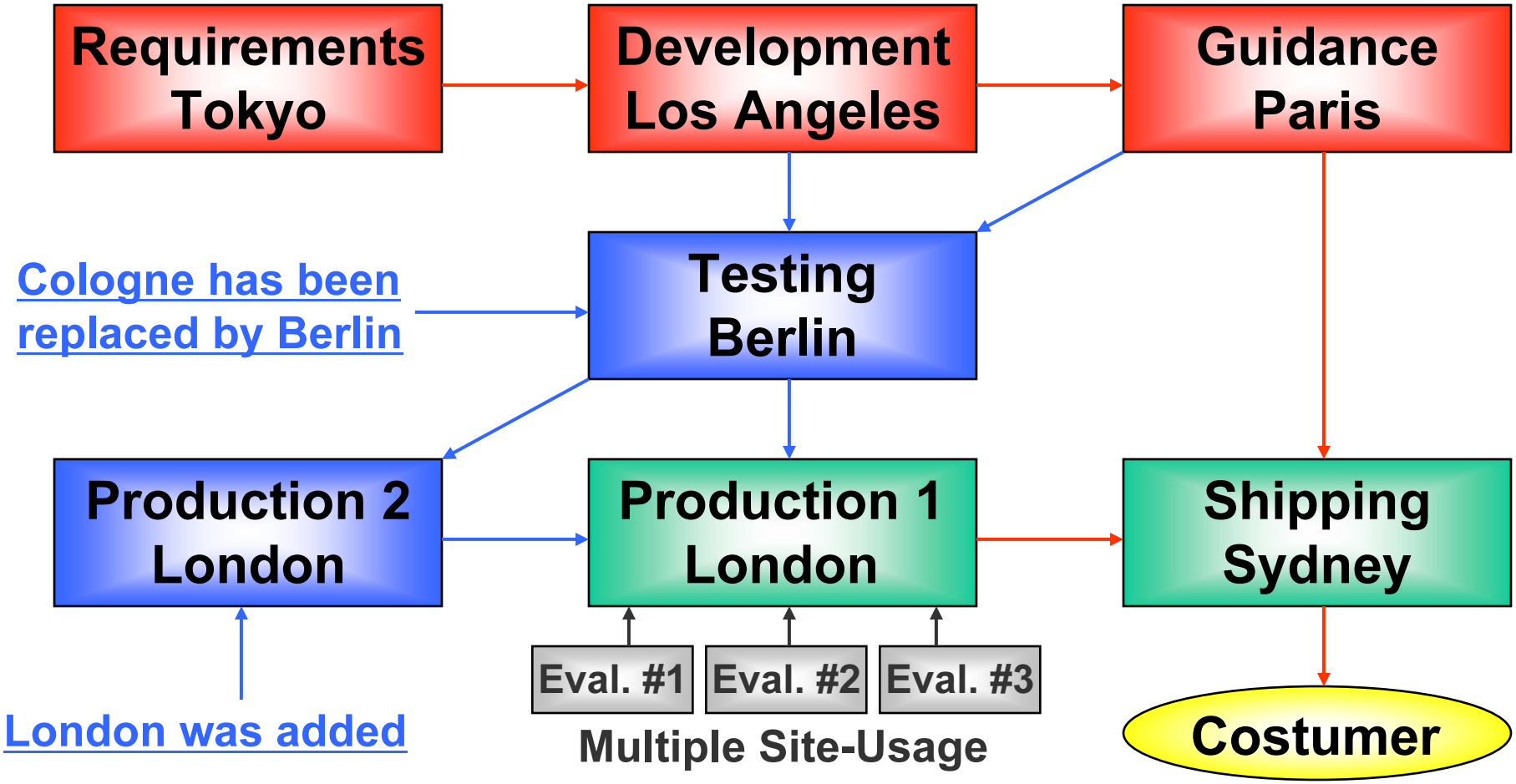
- Noting that ALC is independent to other CC-Aspects
- Splitting the evaluation between them

The same goes for complex evaluations where:

- parts of the site" may be relatively independent

Splitting the site may therefore also help

Example: A Complex TOE



Dividing the Site into „Splices“

In Site Splicing, a developer can choose to divide his site into ”Subsites” called ”Splices”.

- A splice can be the whole site
- A splice may consist of one physical location,
  may span multiple physical locations,
  or a splice may be a part of a physical location
- A splice may consist of one organizational unit,
  may span multiple organizational units,
  or a splice may be a part of an organizational unit.

Site/Splice Certification (I)

- Splice Certificate can be completely separated from the TOE certificate.
- A customer can now require a site certificate from a developer before actually giving him an assignment to develop something.
- An organization can obtain and maintain its own certificate and provide this to any developer who wants it.

Site/Splice Certification (II)

- An organisation can also maintain its own certificate, and does not have to give any information to the other developers.
- It provides an easy entry into the CC market for a developer.
  First get a site certificate, then a TOE certificate.
- A ”certificate to hang on the wall” would indicate the developer’s effort that some of their splices had to do a lot of work for a site evaluation.

Site/Splice Certification (III)

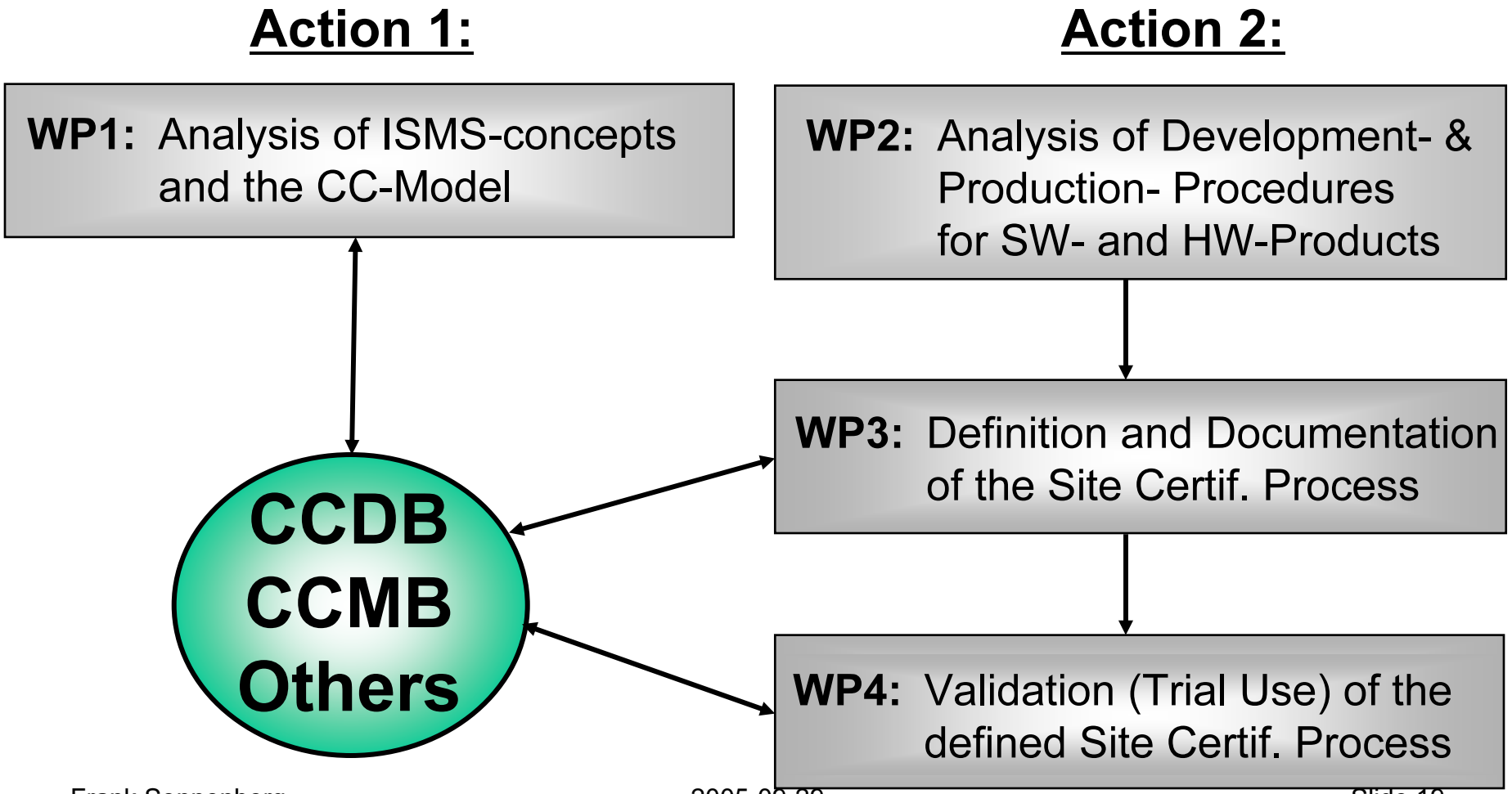
- Certain developers indicated that they had to undergo up to 15 different types of site certifications per year.

  Having a single all-encompassing site certificate would help them a lot, and they feel that the CC-certificate has the best chance of being accepted for this, as this standard is flexible/tailorable and recognized worldwide.

Questions to be solved

- What are the minimum requirements which have to be fulfilled by each Splice?
- Which criteria must each Splice meet, such that all Splices together meet ALC?
- How to handle changes of splices which occur all the time?
- Is it necessary to add Splice Certification to the CCRA?

Project Structure



Estimated Time Schedule

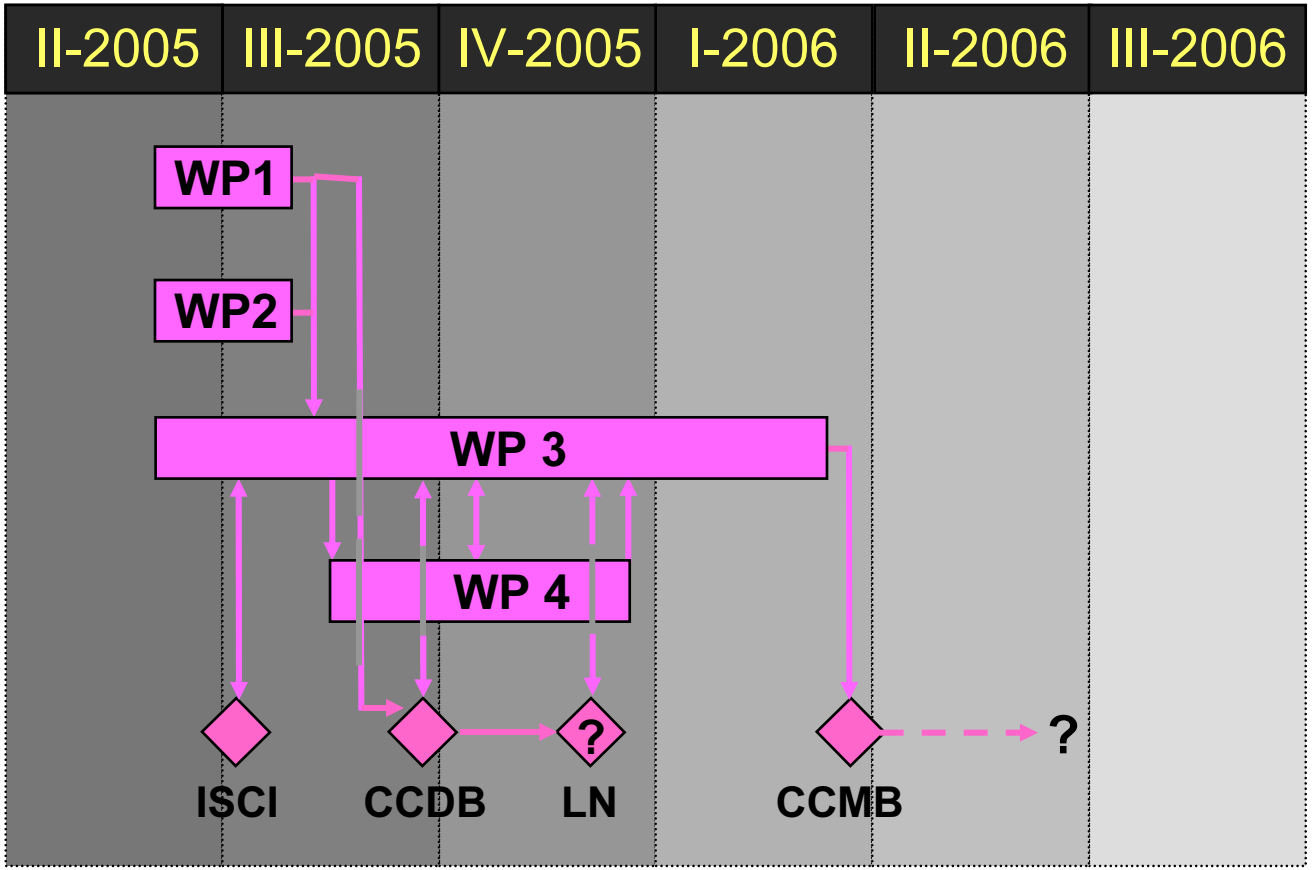
ISMS-CC Comparison

SW- & HW-Production Analysis

Site Certif. Process Definition

Validation by Trial-Use

Special Meetings



Summary

- The ALC-Reusability-Approach can be seen as a first step in saving Evaluation Efforts
- Reusability does only have a limited Applicability since several Technical Problems remain
- Site/Splice Certification can solve all these Technical Problems and will save an considerable amount of Evaluation Efforts
- There is an actual need and a new market for the CC to issue Site/Sdlice Certificates

Contact Information

Bundesamt für Sicherheit in der
Informationstechnik (BSI) /
Federal Office for Information Security

Dr. Frank Sonnenberg
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888-9582-470
Fax: +49 (0)1888-10-9582-470

frank.sonnenberg@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de