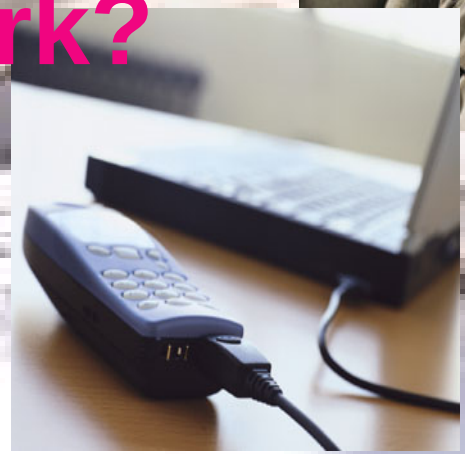
Security Certification and Common Criteria:

How does this Standard work?



Dr. Igor Furgel

T-Systems GEI GmbH
ICT Security

T · · Systems ·

What are we speaking about?

- Evaluation Philosophy
- Evaluation and Certification scheme
- Common Criteria within the Scheme
- Frame of Evaluation and Human Factor as the Anchor of Trust
- Digital Tachograph System and Security Evaluation
- Benefits and Restrictions of Security Certification

T Systems

Evaluation Philosophy

- Crucial objects
  - consumer's security needs, and
  - IT products/systems
- How can I gain the confidence in an IT product?
  - I trust in and rely on the developer (by my experience or his reputation) or
  - I investigate the product
- But how?
  - Can/shall I do it by myself?
  - Or is it more efficient to outsource this to an expert team due to special know-how and experiences.

T Systems

Evaluation Philosophy: Assurance, Correctness and Effectiveness

Assurance: the confidence in the security provided by a product.

Correctness: is the idea well implemented?

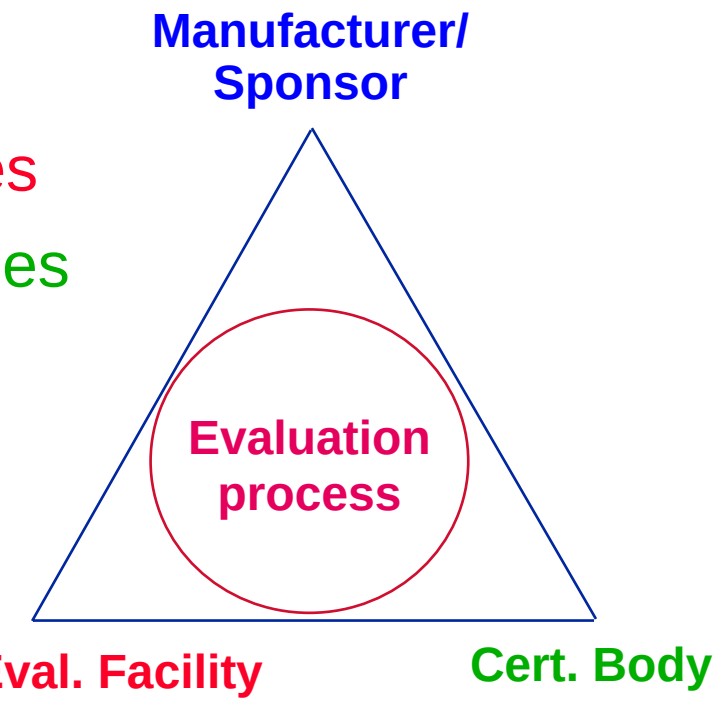
Effectiveness: is the idea appropriate to cope with the actual security situation?

Evaluation and Certification Scheme: Players

- Human players
- Technical players
- Common metric

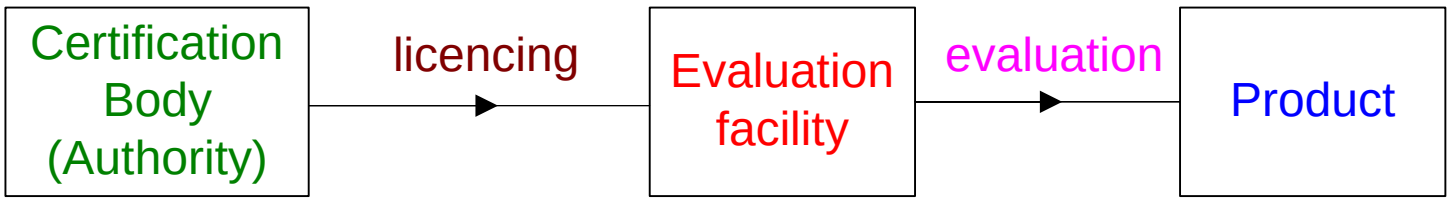
Evaluation and Certification Scheme: Human Players 1/2

- Human players:
  - –manufacturer/sponsor: provides
  - –evaluation facility (EF): examines
  - –certification body (CB): supervises



Evaluation and Certification Scheme: Human Players 2/2

- Certification Body is the anchor of trustworthiness



- Trust transition: If the consumer trusts in the CB, he can also trust in the product certified

Evaluation and Certification Scheme: Technical Players

- the product under evaluation

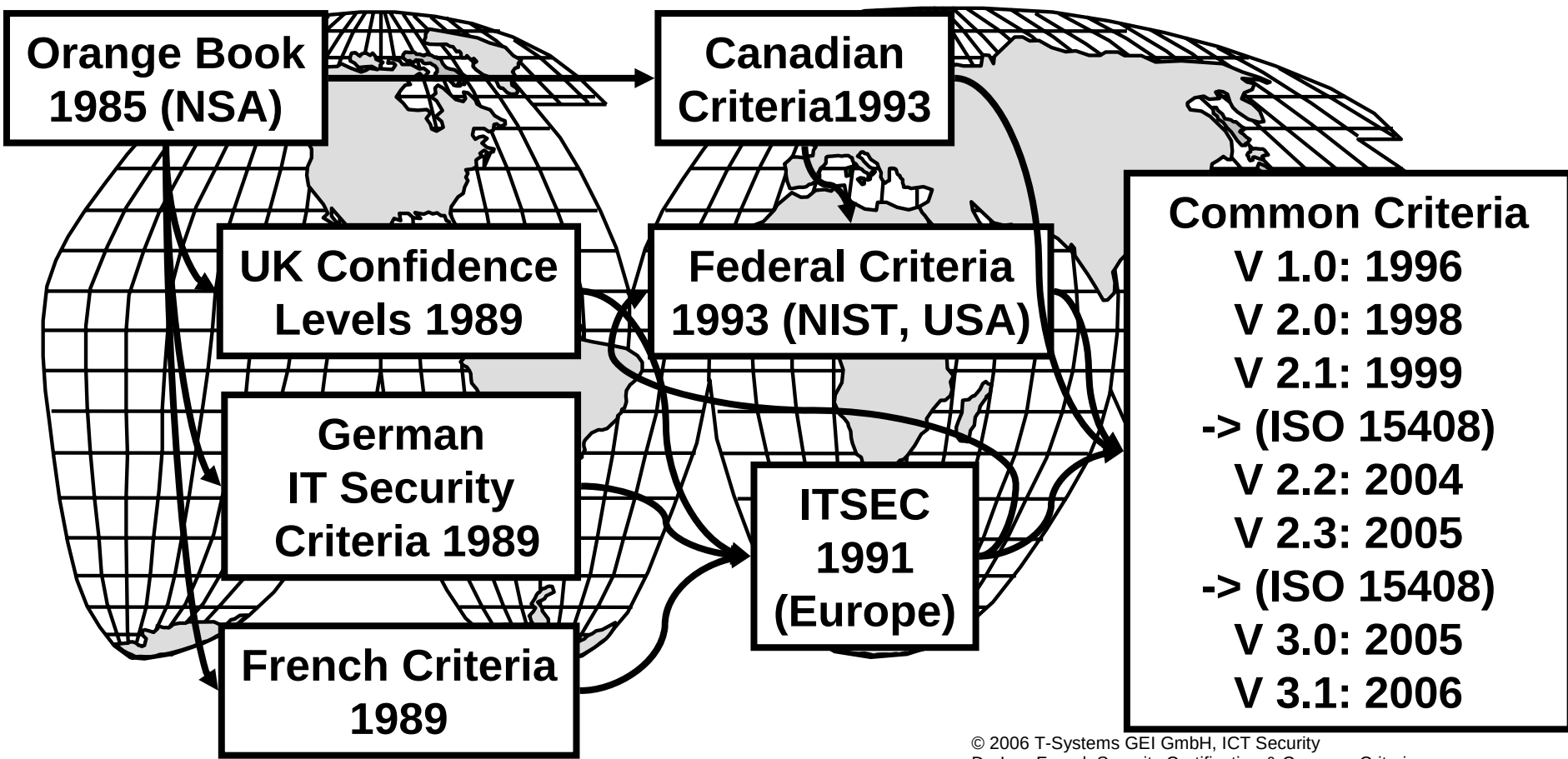
- evaluation tools

Evaluation and Certification Scheme: Common Metric

- The common metric of a contemporary evaluation comprises:
  - Criteria
    - Common Criteria (CC)
      - the current version of CCMB is 3.1 (since 18th Sept. 2006, www.commoncriteriaportal.org)
      - the official version within German National Scheme is 2.3 (BA 19.05.2006, www.bsi.de)
  - Methodology
    - CEM according to the relevant CC version
  - Interpretations
    - International: CCMB (CC Management Board)
    - European: JIL (Joint Interpretation Library)
    - National: Particular national interpretations of the evaluation scheme (e.g. AIS in Germany)

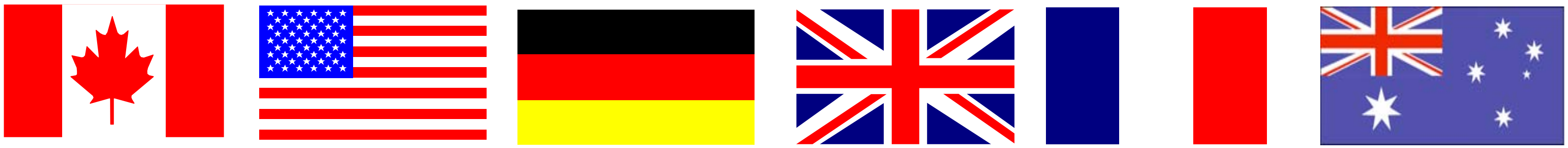
T · · Systems ·

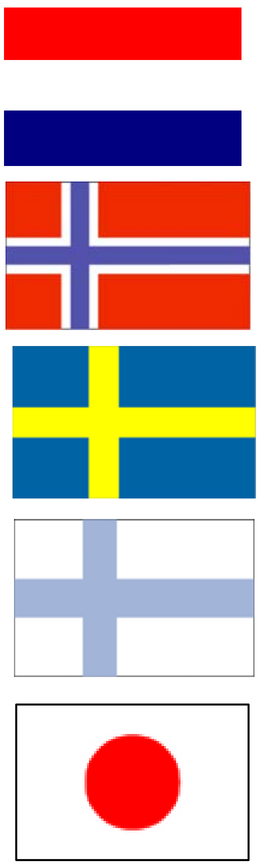
Common Criteria: History



T Systems

Common Criteria: Organisation
CCRA Members (some)

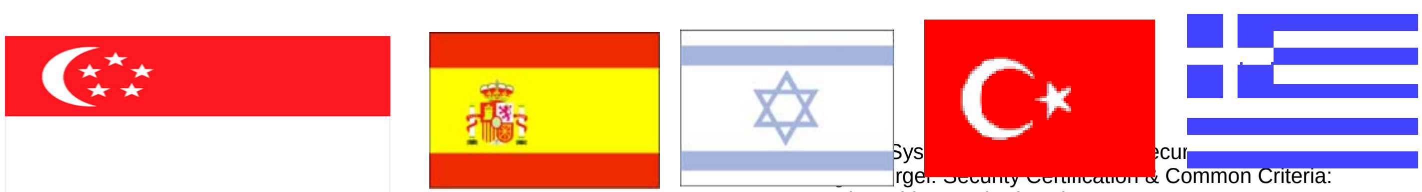




Common Criteria (CC)
CC Evaluation Methodology (CEM)

Common Criteria Organisation
(CCMB)

Common Criteria Recognition
Arrangement (CCRA)



Common Criteria: CCRA – Purpose 1/2

CCRA, Purpose

The Participants in this Arrangement share the following objectives:

a) to ensure that *evaluations* of *Information Technology (IT) products* and *protection profiles* are performed to **high and consistent standards**, and are seen to contribute significantly to confidence in the security of those products and profiles;

b) to **improve the availability of evaluated, security-enhanced IT** products and protection profiles;

T · · Systems ·

Common Criteria: CCRA – Purpose 2/2

CCRA, Purpose

The Participants in this Arrangement share the following objectives:

c) to **eliminate the burden of duplicating evaluations** of IT products and protection profiles;

d) to **continuously improve the efficiency and cost-effectiveness of the evaluation** and **certification/validation** process for IT products and protection profiles.

T · · Systems ·

Common Criteria:
CCRA – Recognition 1/2

CCRA, Article 5 Conditions for Recognition

- Except as otherwise provided in this Arrangement, each Participant should recognise applicable Common Criteria certificates authorised by any **certificate authorising Participant**.

- Such authorisation confirms that the evaluation and certification/validation processes have been carried out in a duly professional manner
  - a) **on the basis of accepted IT *security evaluation criteria***,
  - b) **using accepted IT *security evaluation methods***,

T · · Systems ·

Common Criteria:
CCRA – Recognition 2/2

CCRA, Article 5 Conditions for Recognition

– Such authorisation confirms that the evaluation and certification/validation processes have been carried out in a duly professional manner

- c) in the context of an ***Evaluation and Certification/Validation Scheme*** **managed by a** ***compliant CB*** in the authorising Participant's country,
- d) and that the Common Criteria certificates authorised and *Certification/Validation Reports* issued satisfy the objectives of this Arrangement.

T · · Systems ·

Common Criteria: General Structure of CC

- Part 1: Introduction and general model (philosophy)
- Part 2: Security functional requirements (catalogue of functional requirements)
- Part 3: Security assurance requirements (catalogue of assurance requirements)
- CEM: Common Evaluation Methodology

T · · Systems ·

Common Criteria: Evaluation Assurance Levels (EAL)

- Functionally tested (EAL1)
- Structurally tested (EAL2)
- Methodically tested and checked (EAL3)
- Methodically designed, tested and reviewed (EAL4)
- Semi-formally designed and tested (EAL5)
- Semi-formally verified, designed and tested (EAL6)
- Formally verified, designed and tested (EAL7)

T · · Systems ·

Common Criteria: EAL Overview for CC v2.3

- EAL packages
  - EAL1: pure test, pre-evaluation
  - EAL2: obvious vulnerabilities assessed
  - EAL3: security assessment without specific efforts
  - EAL4: maximum assurance from positive security engineering based on good commercial development practices

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

T · · Systems ·

Limits of Evaluation: Back to the Consumer/Operator

- Now there are the product and the security certificate. What does the consumer (often the operator of the product/system) have to do else?

  - He has to decide, whether the security features of the product match his security needs.

- How can he do it?

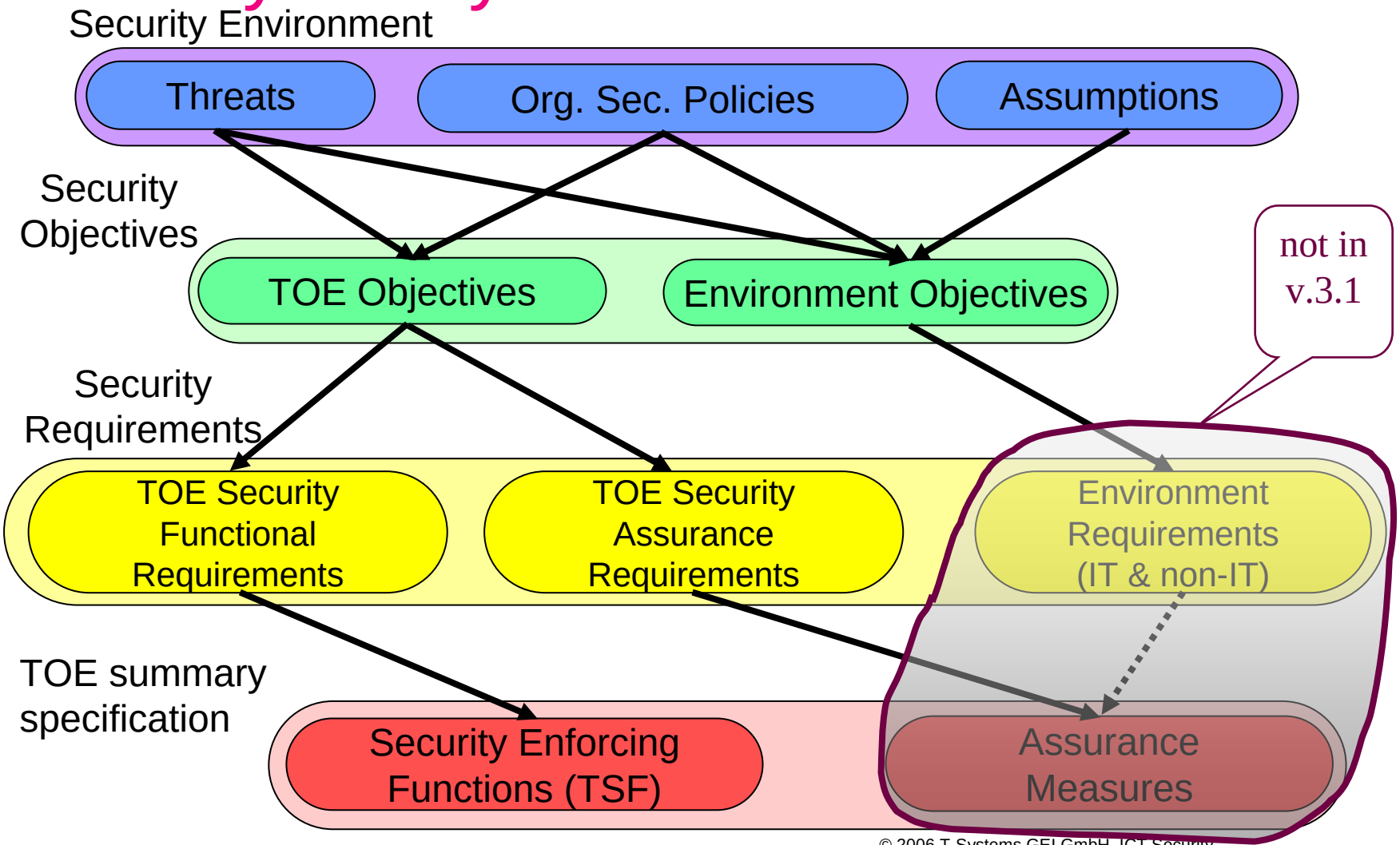
Limits of Evaluation: Scope

- The scope of a concrete evaluation is exactly defined in the product-specific Security Target.

- The Security Target declares:
  - a set of the security functionality being under evaluation
  - a set of the different configurations of the product having to be evaluated
  - environmental conditions (technical and organisational) being assumed and having to be fulfilled

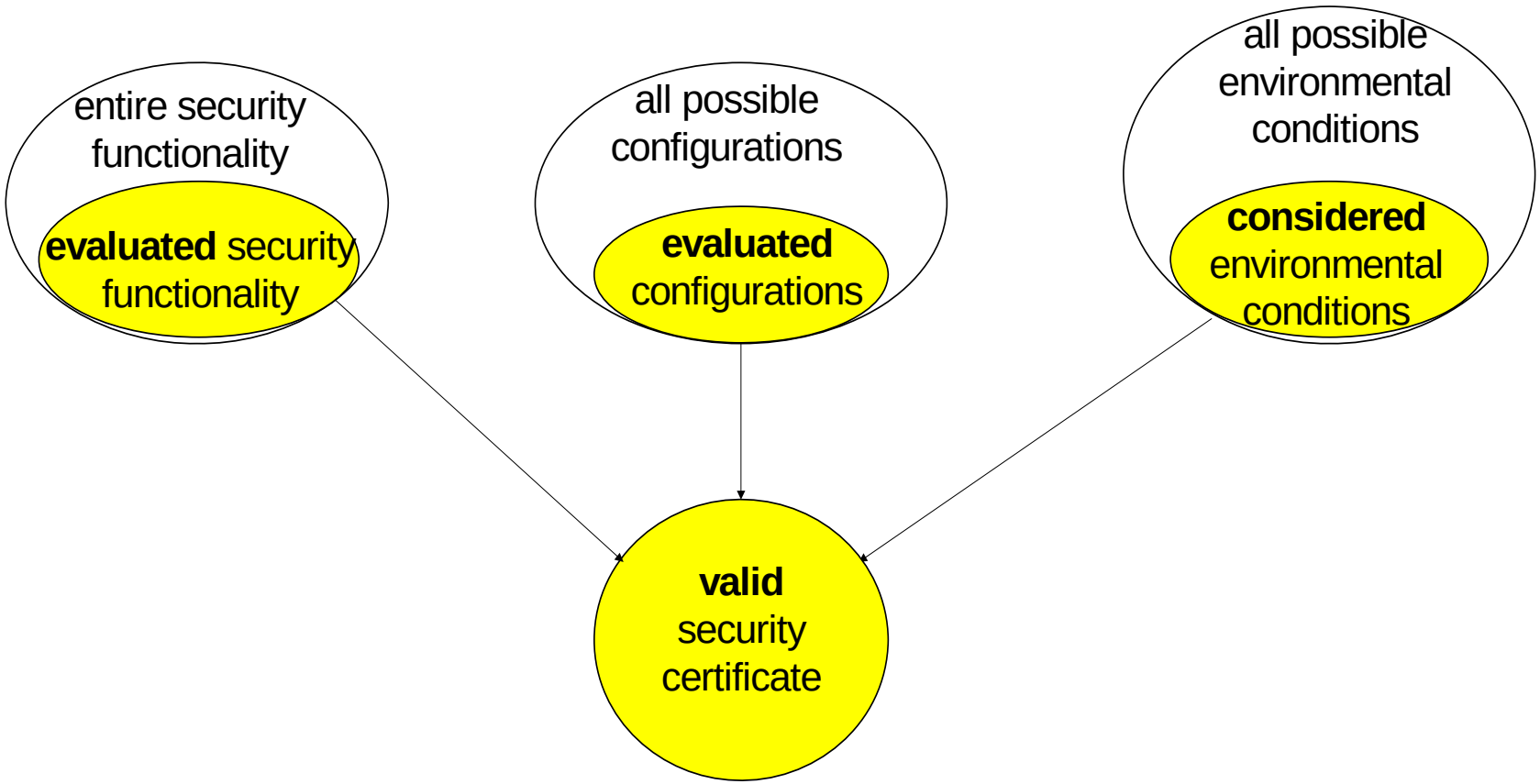
T · · Systems ·

Limits of Evaluation: Security Policy and its Formal Structure



T · · Systems ·

Limits of Evaluation: Certificate Validity

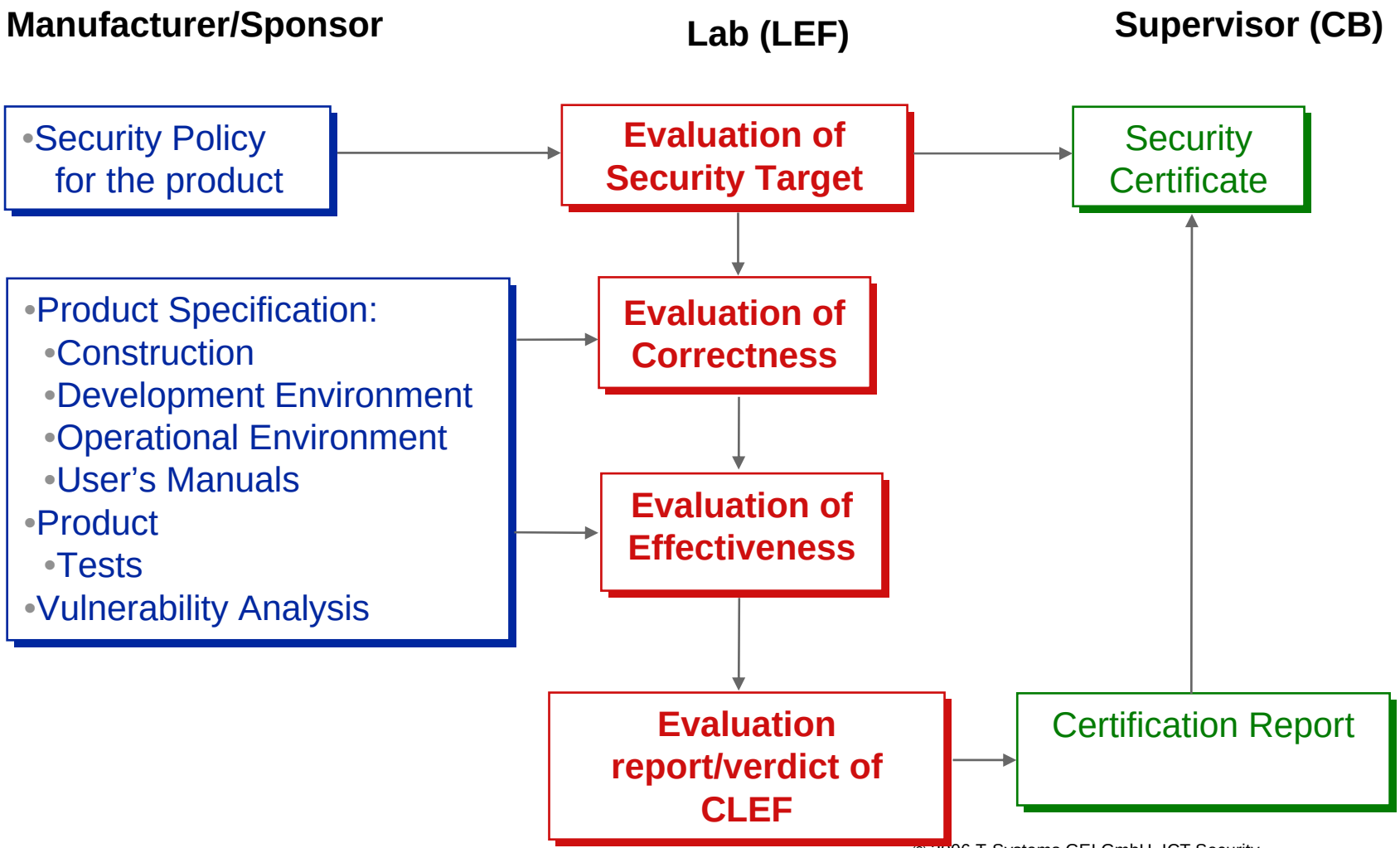


Limits of evaluation: Certificate Validity

- **Very important for consumer/operator: A security certificate is valid only for the scope of evaluation defined in the Security Target.**
  - The consumer shall compare the information delivered by the ST with his security needs and merely after having done it decide on using the product.
  - He shall operate the product/system only under conditions having been in the scope of evaluation. Else he operates the product **out of validity of the security certificate**. The question of liability should not be underestimated in this case.

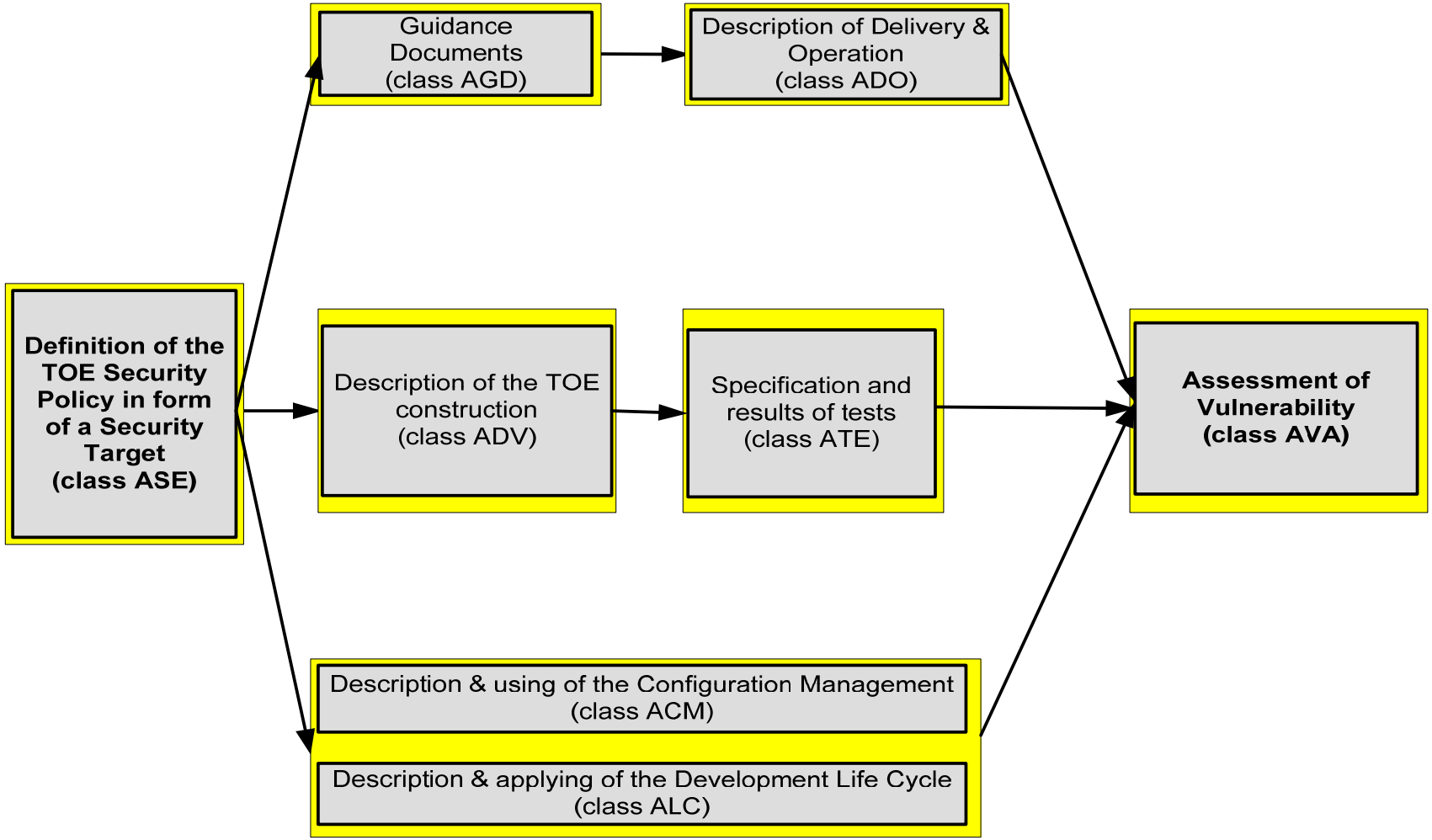
T · · Systems ·

Frame of Evaluation: Succession - Players & Tasks



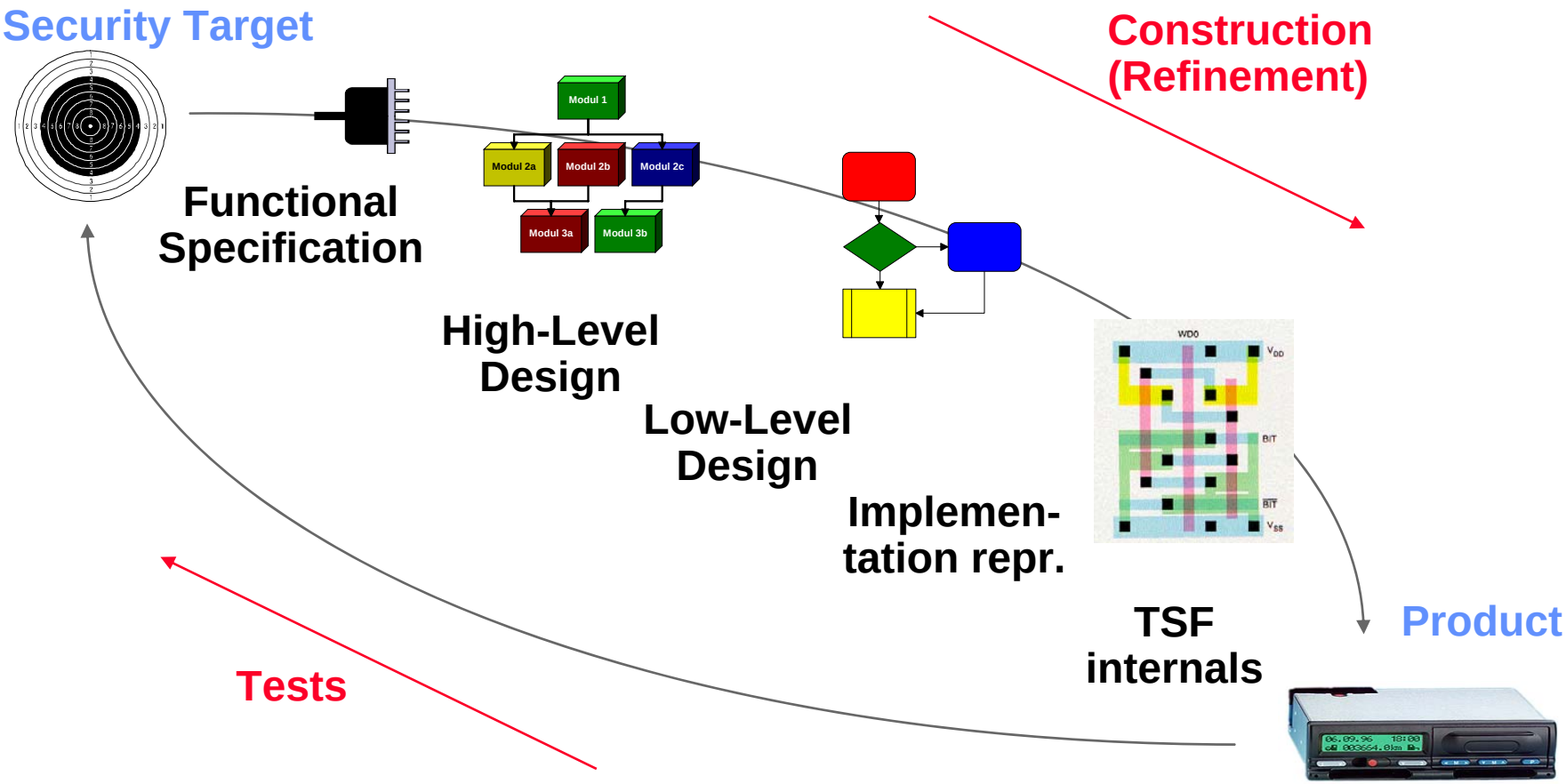
T · · Systems

Frame of Evaluation: Succession - Workflow



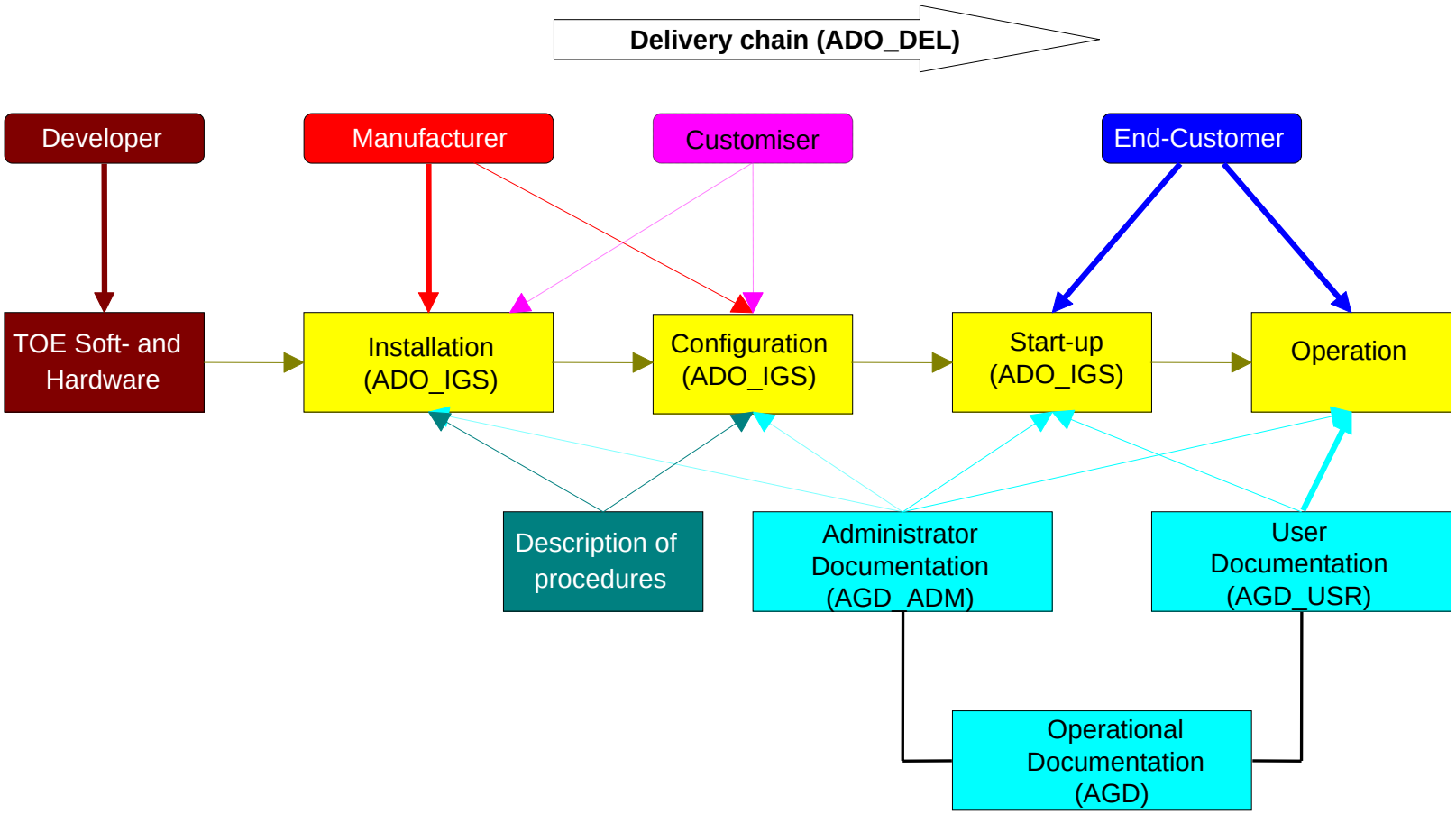
T Systems

Frame of Evaluation: Development and Tests (ADV + ATE)



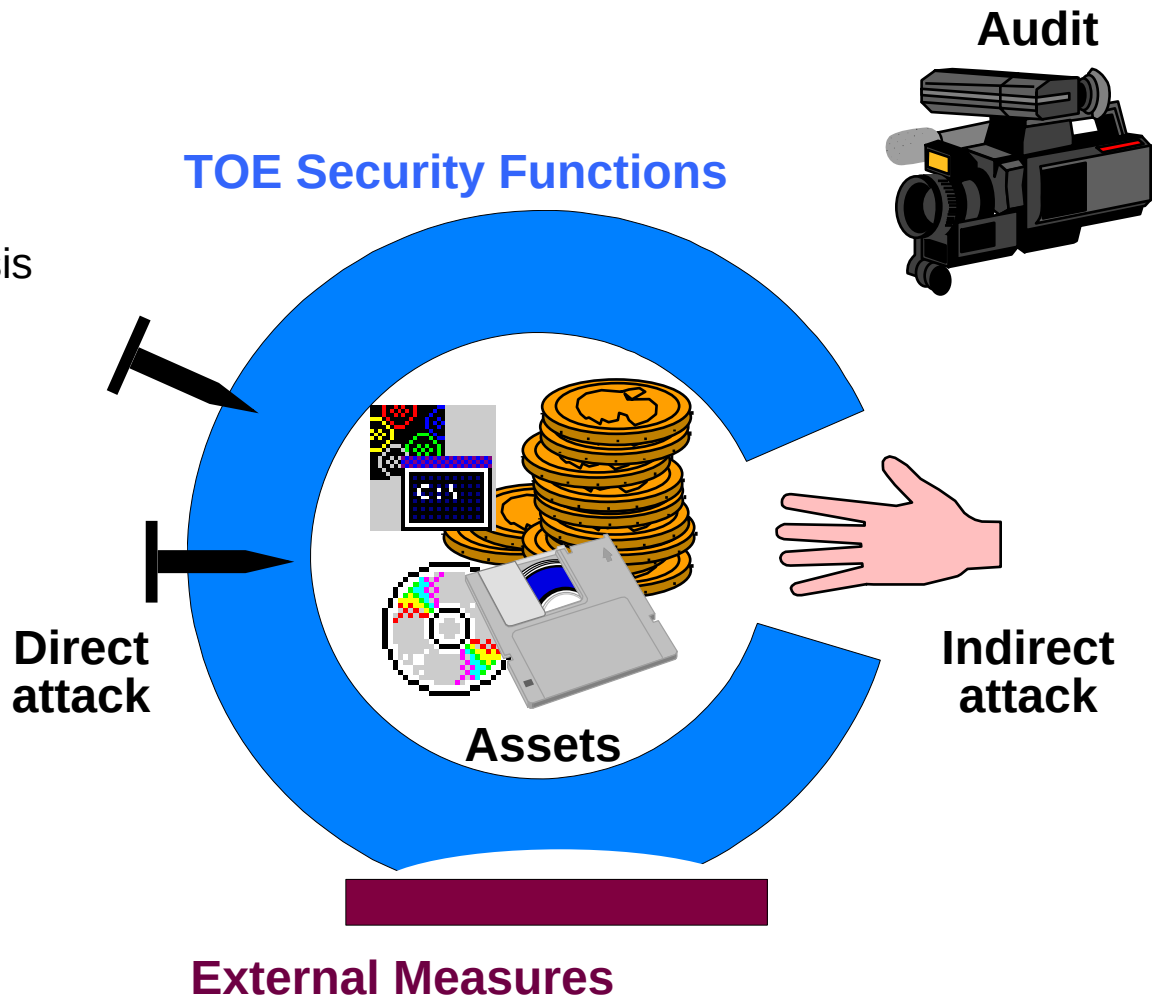
T · · Systems ·

Frame of Evaluation: Delivery and Operation (ADO + AGD)



Frame of Evaluation:
Attacks & Assessment of Effectiveness (AVA)

- Direct Attacks
  - suitability analysis
  - strength of security functions analysis
- Indirect Attacks
  - binding analysis
  - vulnerabilities analysis
- Misuse
- Side channels
- Audit and Alarms
- External Measures



T Systems

Vulnerability Analysis: Assessment of Effectiveness

- The assessment of effectiveness is not 'black-white' (security can be – cannot be undermined), but with a specific metric based on **resources** needed for an attack scenario.

- The Common Criteria use the following assessment metric for a general case (CEM, Annex B.8.2):

T · · Systems ·

Vulnerability Analysis: Assessment of Effectiveness (v.2.3)

Factor	Range	Identifying value	Exploiting value
Elapsed Time	< 0.5 hour	0	0
	< 1 day	2	3
	< 1 month	3	5
	> 1 month	5	8
	Not practical	*	*
Expertise	Layman	0	0
	Proficient	2	2
	Expert	5	4
Knowledge of TOE	None	0	0
	Public	2	2
	Sensitive	5	4
Access to TOE	< 0.5 hour, or access undetectable	0	0
	< 1 day	2	4
	< 1 month	3	6
	> 1 month	4	9
	Not practical	*	*
Equipment	None	0	0
	Standard	1	2
	Specialised	3	4
	Bespoke	5	6

T Systems

Vulnerability Analysis: Assessment of Effectiveness (v.2.3)

Range of values of the attack potential of an attack scenario **breaking** the TOE's security	Attack potential of the attack scenario	TOE is resistant to attacker with attack potential of:
0 – 9	Basic	No rating
10 – 17	Moderate	Low
18 – 24	High	Moderate
> 24 or "not practical"	Beyond normal practicability	High

- Cryptographic algorithms need a special assessment: usually there are relevant guidelines of national authorities

T Systems

Human Factor as the Anchor of Trust

- An IT product/system
  - offers different configuration options
  - shall be maintained, etc.

- We cannot gain assurance based only upon the technical measures: The organisational – **personal and procedural** – measures are important as well.

Human Factor as the Anchor of Trust: Organisational Measures: Operator

- The operator of a certified IT product/system shall run it under conditions having been in the scope of evaluation: **He shall also enforce each organisational measure!**

- **The question of plausibility of the assumptions defined in the Security Policy for a product/system can primarily be answered by the consumer/operator:**

  He shall know, whether he can implement and enforce the organisational measures assumed.

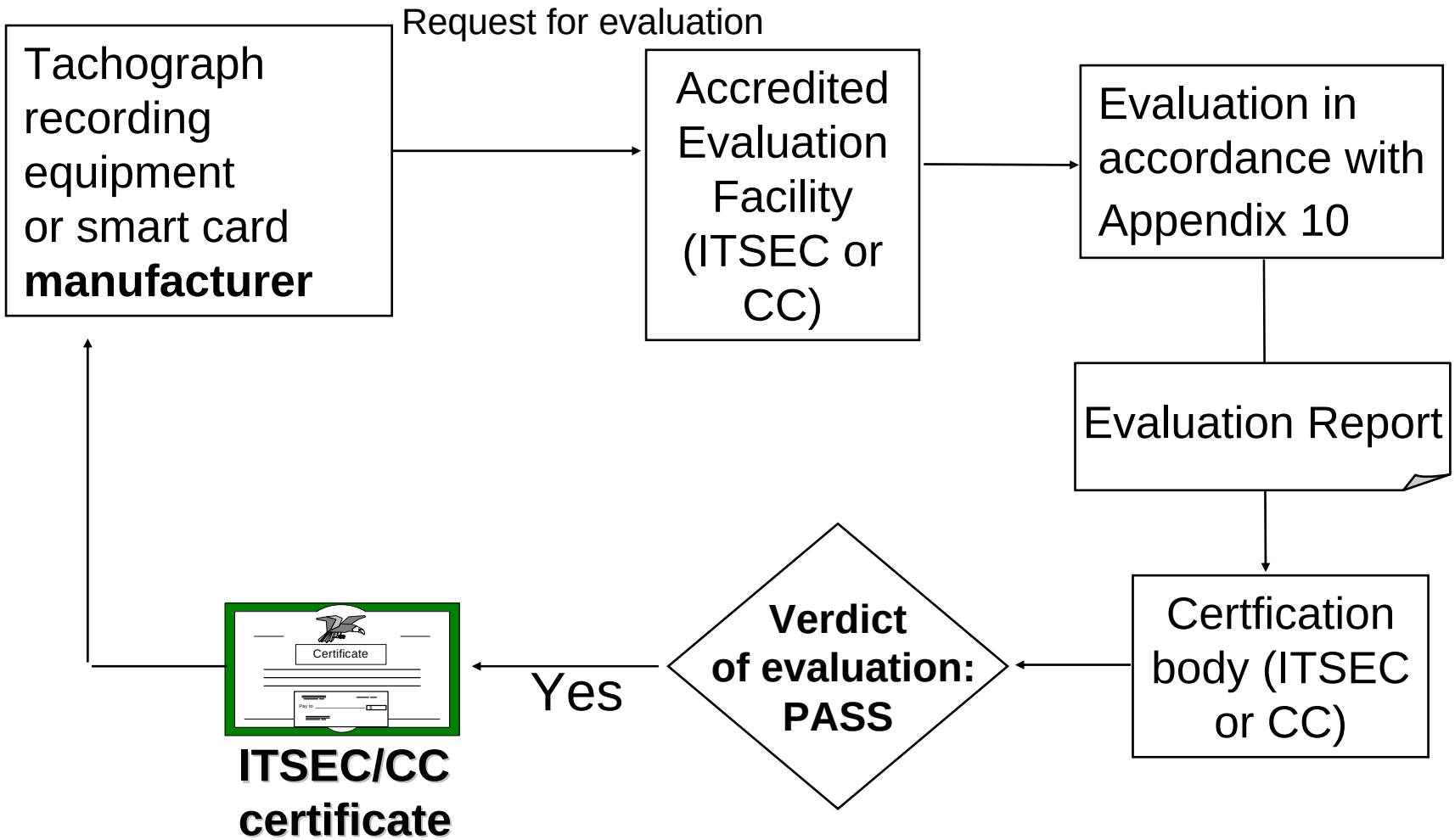
T · · Systems ·

Digital Tachograph: Type Approval

- The prescribed European type approval procedure concerns only three components of the tachograph system: the motion sensor, the vehicle unit and the tachograph card.

- Type approval steps are:
  - security certification,
  - functional certification,
  - interoperability certification,
  - type approval certification.

Digital Tachograph:
Type Approval - Security Certification



T · · Systems

Digital Tachograph:
Type Approval - Functional Certification

Test request

Tachograph recording equipment or smart card **manufacturer**

Accredited Laboratory

Functional tests in accordance with Appendix 9

Test Report

Type approval authority

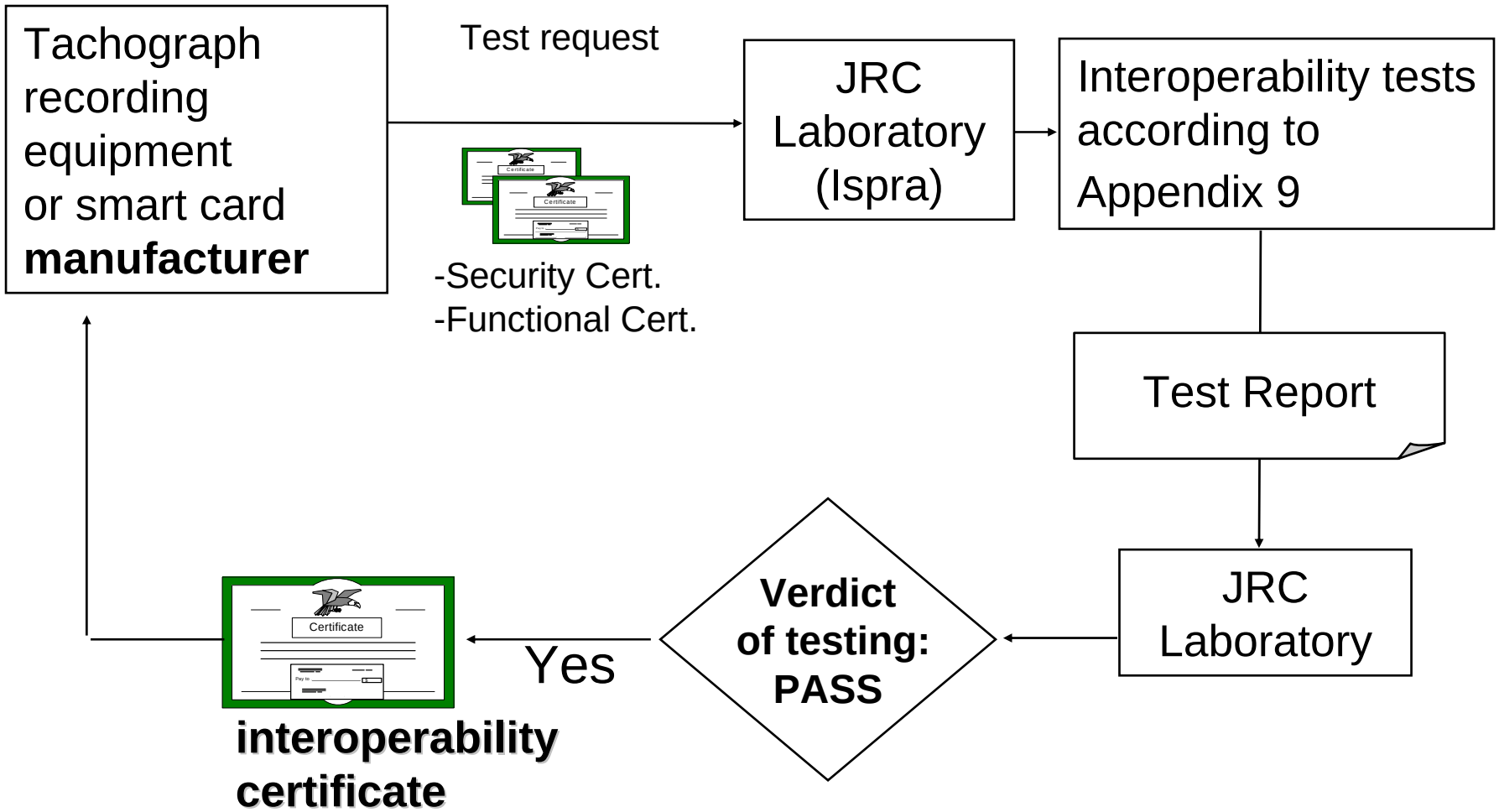
Verdict of testing: PASS

Yes

functional certificate

T Systems

Digital Tachograph:
Type Approval - Interoperability Certification



T Systems

Digital Tachograph: Type Approval Certification

Member State type approval authority

- ITSEC/CC certificate
- Functional certificate
- Interoperability certificate

Certificate of Type Approval

Digital Tachograph:
Type Approval Certification - Publishing

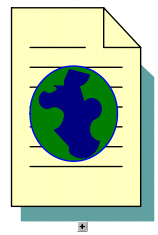
Member State
type approval authority

Copy of

Type Approval Certificate

JRC

http://dtc.jrc.it



Public web site
with list of the type
approved equipment

T · · Systems ·

Benefits and restrictions of evaluation

- **Benefits**:
  - clear alignment with the actual security needs
  - improve security
  - improve quality (clear concept; control, supervision)
  - eliminate flaws (independent opinion)
  - product documentation (keep Know-How)

  - **more confidence** in security capability of an IT product for its operator.
  - **more objectivity** because of independent evaluation and certification

T Systems

Benefits and restrictions of evaluation

- **Restrictions**:
  - Consumers will still need to review the information given by certification results carefully and assess its applicability to his special needs.
  - Consumer shall enforce the assumptions about the method of use of the product and its operating environment as well as other conditions confining the validity of the assurance assessment.

Dr. Igor Furgel

T-Systems GEI GmbH

ICT Security

Rabin Strasse 8
53111 Bonn, Germany

☎ +49 228 9841-512
🗎 +49 228 9841-60
💻 igor.furgel@t-systems.com

T · · Systems ·