DIN INS Contribution
to ETSI/MTS Meeting Berlin

GI/ASQF Regional Group Berlin-Brandenburg

„Certification and Ealuation of security-critical Systems by unified means of ISO/IEC standards CC/FIPS and ETSI TVRA Method“

Jan deMeer
smartspacelab.eu GmbH
University of Technology and Economy

December, 14.-15.2010 @ FhG FOKUS, erlinB

This work is supported by the
German Standardization Institute DIN

INS INNOVATION MIT NORMEN UND STANDARDS

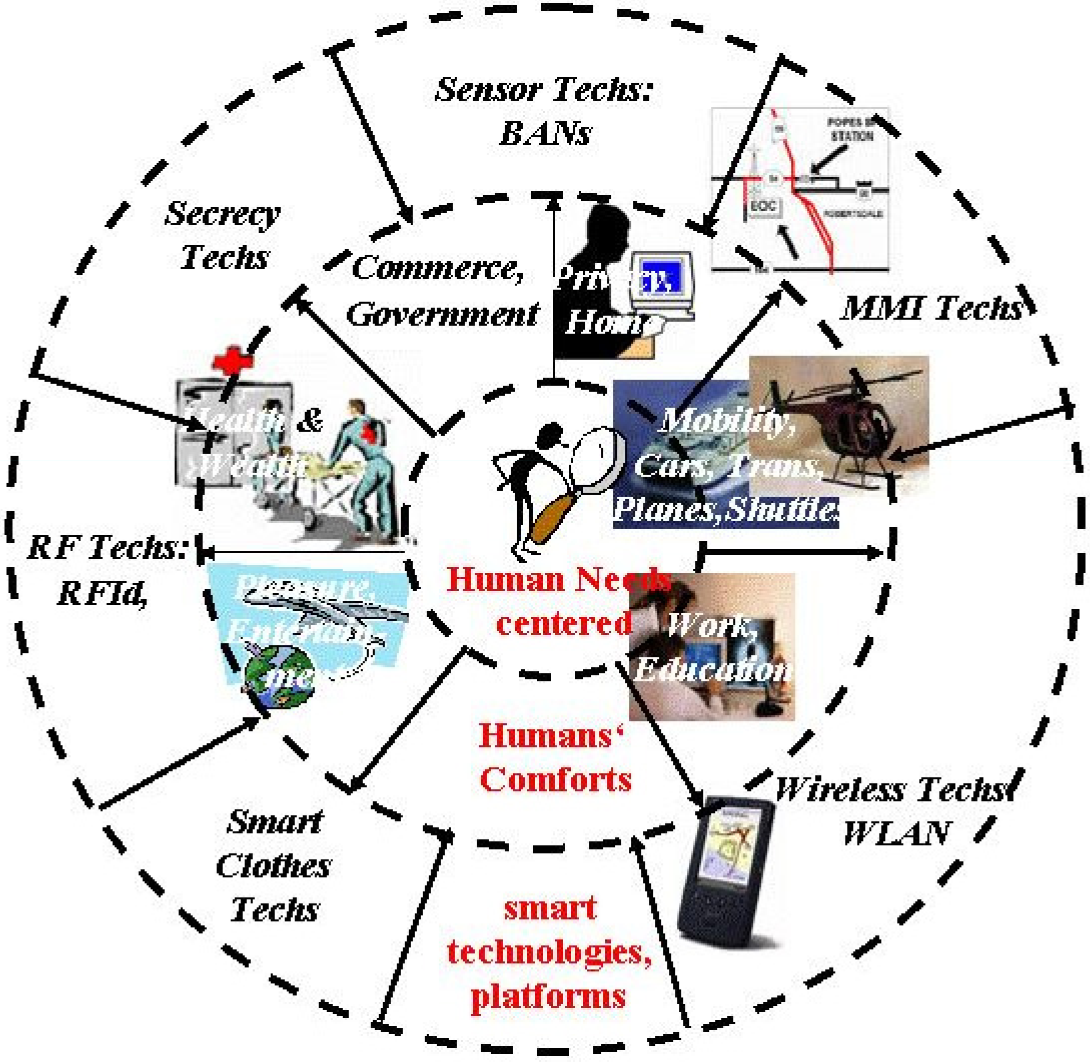
smartspace

ATEM$^{A/R/M}$ –**A**utomatized **T**est- and **E**valuation Platfor**M**,

Feasible for the Evaluation, Test and Certification of Complex (Traffic and Transportation) Systems and Components, so-called **U**ltra-**L**arge **S**caled (Eternal) Systems

Especially Of
Luftfahrt – **A**ir-borne,
Schienenverkehr – **R**ail-borne,
Straßenverkehr – Auto**M**otive-borne

smartspace®
yields Ambient Intelligence to your Business



Industrial Standards determine safety & security critical Systems

- Motivation:
  - Quality Management of safety & security critical industrial systems is determined by Industrial Standards:
    - Air-borne Standards
      - E.g. RTCA DO 178B, MIL-STD-498, …
    - Rail-borneStandards
      - E.g. EATCS, IRIS 01,
      - CEN/CENELEC standards EN 50126 / EN 50128 / EN 50129, …
    - Automotive-borne Standards
      - E.g. IEEE Intelligent Transportation System Committee
      - IEEE 1609-1-2-3-4 Wireless Access in Vehicular Environments Standard:
        - » 1609-2: methods to secure WAVE msgs against attacks from outside

Security Certification of SW Systems – Motivations

- Vendor-neutral Information Security Certification Landscape [E.Tittel, K.Lindros ISM 5.8.2008]:

- „Security Certification Ladder“ to climb depending on individuals‘ knowledge, skills, experience to provide knowledge in Computer Security Theory, Operations, Practices, Policies:

  - CompTIA‘s Security+ is on entry-level IT SecCert
  - ISC^2‘s System Security Certified Practinoner is on senior-level IT SecCert
  - SANS GIAC Security Essentials Certification is on intermediate and senior credentials
  - ISC^2‘s Certified Information Systems Security Professional is on premium level (>3years on-job experience, scientific papers, specific classes etc.)

  - SANS GIAC Security Specialist Certifications is on Premium Level
    - to extend GSEC, including firewalls, incident handling, intrusion analysis, OS Administration, information security officer, system/network auditor certification
    - To be examined to earn GIAC Security Engineer Certification

Security Certification of SW Systems – Motivations

- „Security School“ on CISSP® Certification Training in 10 lessons [SearchSecurity.com]:
  - Securing Data
    1. Security Management Practices, including Risk Analysis, Data Classification, Security Roles
    2. Access Control, including identification methods; biometrics; authentication tools; accountability, monitoring, auditing pracices; emanation technologies (Wirksamkeit); possible threats
    3. Cryptography, including PKI concepts, hashing, types of attack on Cryptosystems
  - Securing Infrastructure
    4. Security Models and Architecture, Trusted computing base, security models used in SW Development, Security Criterion and Ratings, Certifcation and accreditation
    5. Telecommunication and Networking, TCP/IP, LAN, WAN technologies, Intranet, extranet, Remote Access Technologies;
    6. Application and System Development, Types of SW Controls and Implementation, Data Warehousing/Mining, SW Life Cycle, Change Control Concepts, Expert Systems/AI

Security Certification of SW Systems – Motivations

- „Security School" on CISSP® Certification Training in 10 lessons [SearchSecurity.com]:
  - To do „Business of Security"
    7. Business Continuity/Availability/Desaster Recovery, including Impact (Business, Operational, Financial) Analysis, Contingency & Disaster Plannings; Backup and Offsite Facilities
    8. Law, Investigation and Ethics (Fraud, Theft, Embezzlement) on understanding how to investigate a computer crime and gather evidence (Beweismittel)
    9. Physical Security, convergence of physical and logical systems, including administrative, technical controls; physical security risks, threats, countermeasures, fire prevention, detection and suppression; Authentication Individuals and Intrusion Detection.

Reliable Systems Development – Security Testing and Metrics [NIST-1]

- Governmental Agencies require tested and validated products;
  - Protection of information and communication by cryptography
  - Cryptographic Modules
    - provide Security Services such as confidentiality, integrity, authentication by cryptographic algorithms
    - Avoid rendering products insecure, because of Weaknesses in design and implemented algorithms which place highly sensitive information at risk
    - provide Security Assurance by testing and validation of cryptographic module interfaces against standards is essential

Reliable Systems Development – Security Testing and Metrics [NIST-2]

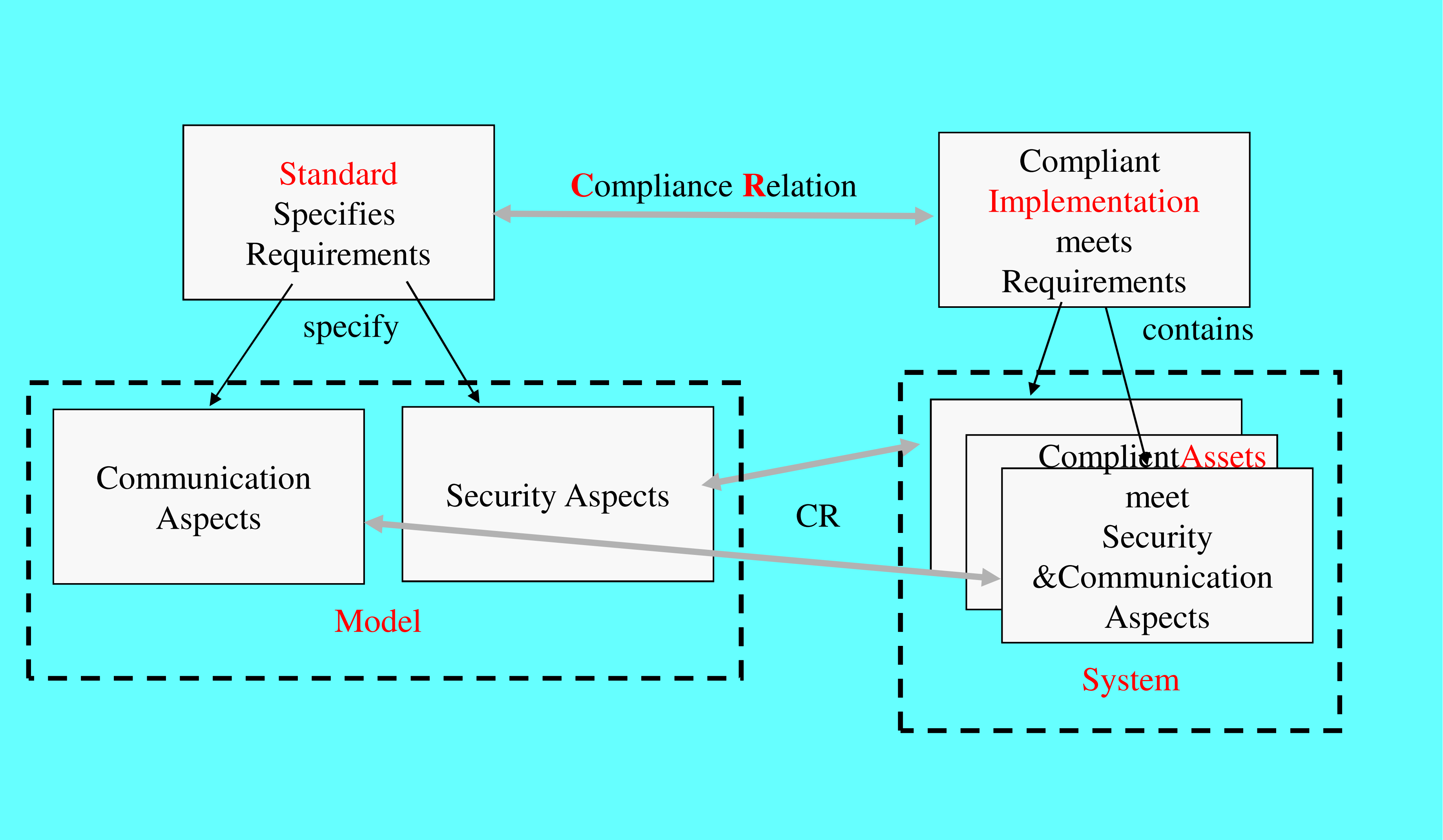
- Required STM Activities:
  - Validation of Cryptographic Modules,
    - of cryptographic Algorithm Implementation,
      - SMEs
  - Accreditation of Independent Testing labs
    - TÜV, VDI/VDE, …
  - Development of Test Suites
    - ISG ATEM
  - Providing Technical Support to Industry Forums
    - ISG ATEM
  - Conducting Education, Training, Outreach Programs (Überführungsprogramme)

Assurance Components/ EAL Assurance Class	EAL7	EAL6	EAL5	EAL4	EAL3	EAL2	EAL1
ADV Development	Formal TOE Sec Policy Model, Complete Mapping of Implementation to TSF	Semiformal specification, complete mapping of implementation to TSF Formal TOE security policy Model	Security Architecture description, semiformal functional specification	Security Architecture, functional and modular design	Security Architectdure Description, Arch Design	Sec Arch Descr. Sec-enforcing Func Spec	Basic Func Spec
AGD Guidance Documents	User guide, Preperative Procedures	User guide, prep. procedures	User guide, preperative procedures	User guide, Prep Procedures	UG, PP	UG, PP	UG, PP
ALC Life Cycle Support	Security Measures Measurable Life Cycle Model	Sufficiency of security measures, developer defined life-cycle model	Identificaton of Security measures, complinance with implementatin standards	Problem tracking CM Coverage, Security Measures, Developer-defined LCM	Authorization Conttrol, Id of Security Measures	Use of CM System, TOE CM Coverage	Labelling of TOE, TOE CM Coverage
ASE Security Target Evaluation	Conformance Claims, Security Objectives,	Conformance claims, Security Objekctives	Conformance claims, Security Objectives	Confirmation claims, Security Objectives, TOE spec	Conformance claims, Security Objectives, TOE Spec	Conformance claims, Security Objectives, TOE Spec	Ext. Comp Def., ST Description, Security Objectives
ATE Tests	Rigorous Analysis, complete independent testing	Rigorous analysis,independent testing	Analysis of Coverage, modular, functional testing	Analysis of cpoverage Security Enforcement Module Test	Analysis of Coverage, basic design & func test	Evidence of Coverage, func/indepent. test	Independent testing
Vulverability Assessment	Adv. Methodological VA	Advanced Methodological VA	Methodological VA	Focused VA	VA	VA	Vulnerability Survey

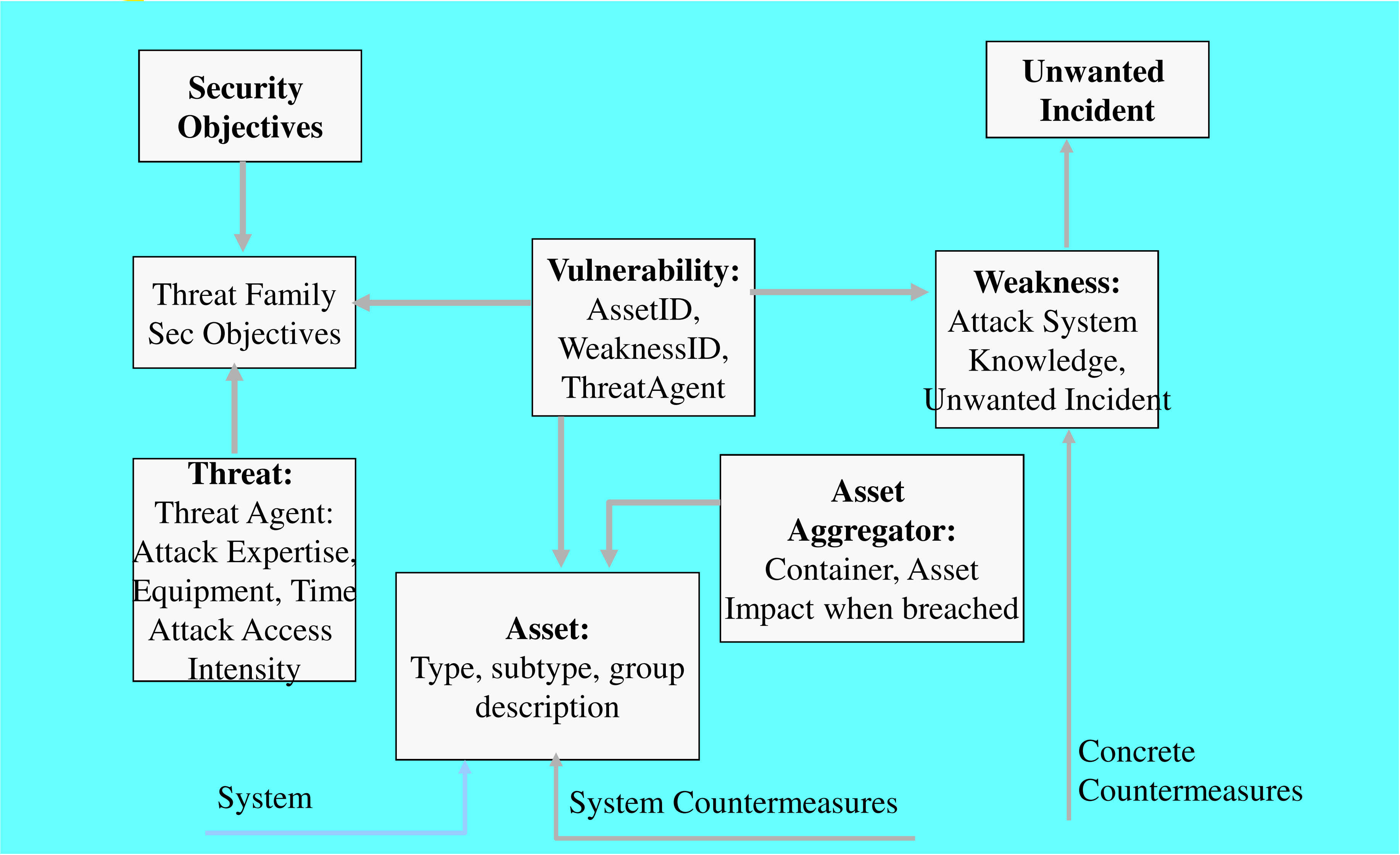
ETSI TVRA Method – 7 steps

- ETSI TISPAN WG7 (Security)
- Telecom and Internet-converged Services and Protocols for Advanced Networking
  - Threats – Vulnerability – Risk – Analysis Method
  - Tool/DB: http://portal.etsi.org/eTVRA/
  - To improve security of a system by
    - Understanding Security Threats
    - Specifying Countermeasures
  - TVRA methods provides 7 steps
    1. To identify Security Objectives
    2. To identify (functional) Security Requirements
    3. To produce Inventory of Assets
    4. To classify Vulnerabilities and Threats
    5. To quantify Likelihood and Impact of Threats
    6. To determine Risks
    7. To specify Countermeasures

ETSI TVRA Relationship: Standard - Model, Implementation - Assets



Class Structure of TVRA DB (1)



Security Objectives

Threat Family
Sec Objectives

Vulnerability:
AssetID,
WeaknessID,
ThreatAgent

Unwanted Incident

Weakness:
Attack System Knowledge,
Unwanted Incident

Threat:
Threat Agent:
Attack Expertise,
Equipment, Time
Attack Access
Intensity

Asset Aggregator:
Container, Asset
Impact when breached

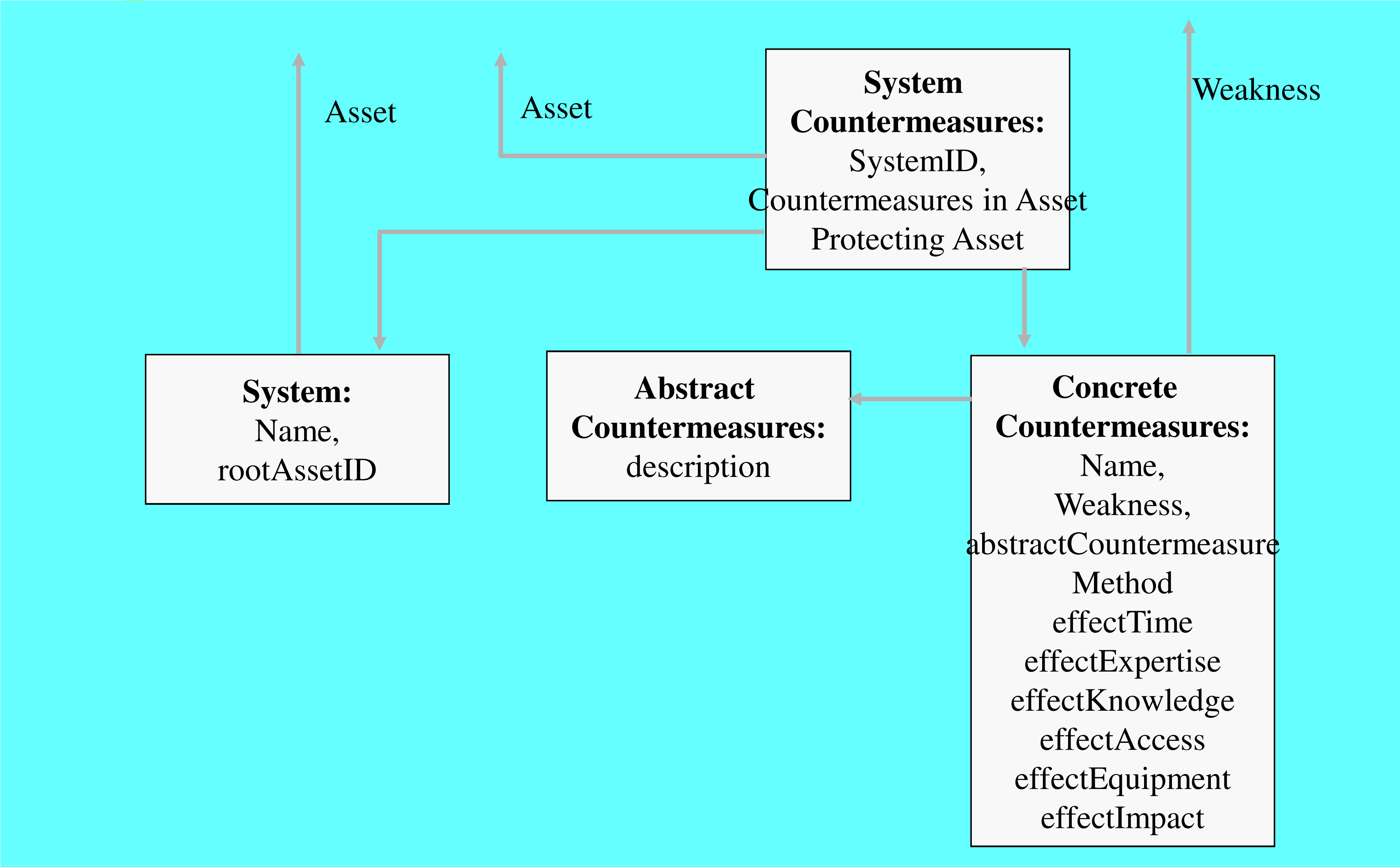
Asset:
Type, subtype, group
description

System

System Countermeasures

Concrete
Countermeasures

Class Structure of TVRA DB (2)



System Countermeasures: SystemID, Countermeasures in Asset Protecting Asset

System: Name, rootAssetID

Abstract Countermeasures: description

Concrete Countermeasures: Name, Weakness, abstractCountermeasure Method effectTime effectExpertise effectKnowledge effectAccess effectEquipment effectImpact

1. ETSI TVRA Method – 1st step Objectives

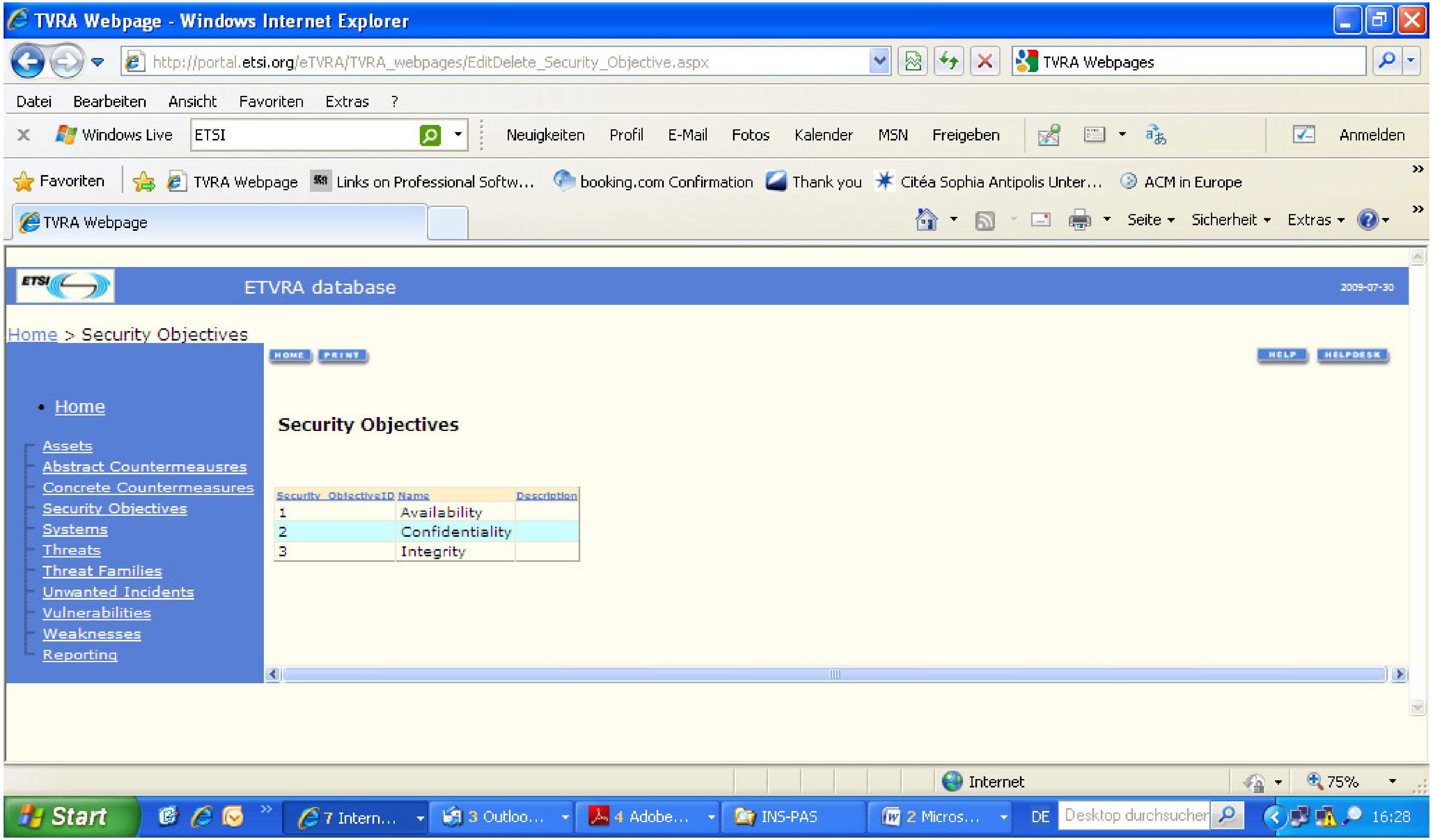
- To Identify **Security Objectives** diverse System Objectives into
  - Security Objectives
  - Assurance Objectives

- SOs in terms of Protection of Information refering to Security Attributes:
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability

- Breaking down to technical security issues, i.e. risks
  - Charging Fraud,
  - Protection of Privacy
  - Ensuring Availability of Offered Services

- being
  - Realistic – Achievable – Measurable – Relevant

ETSI TVRA Method - 1st step Objectives



ETVRA database

2009-07-30

Home > Security Objectives

- Home
  - Assets
  - Abstract Countermeausres
  - Concrete Countermeasures
  - Security Objectives
  - Systems
  - Threats
  - Threat Families
  - Unwanted Incidents
  - Vulnerabilities
  - Weaknesses
  - Reporting

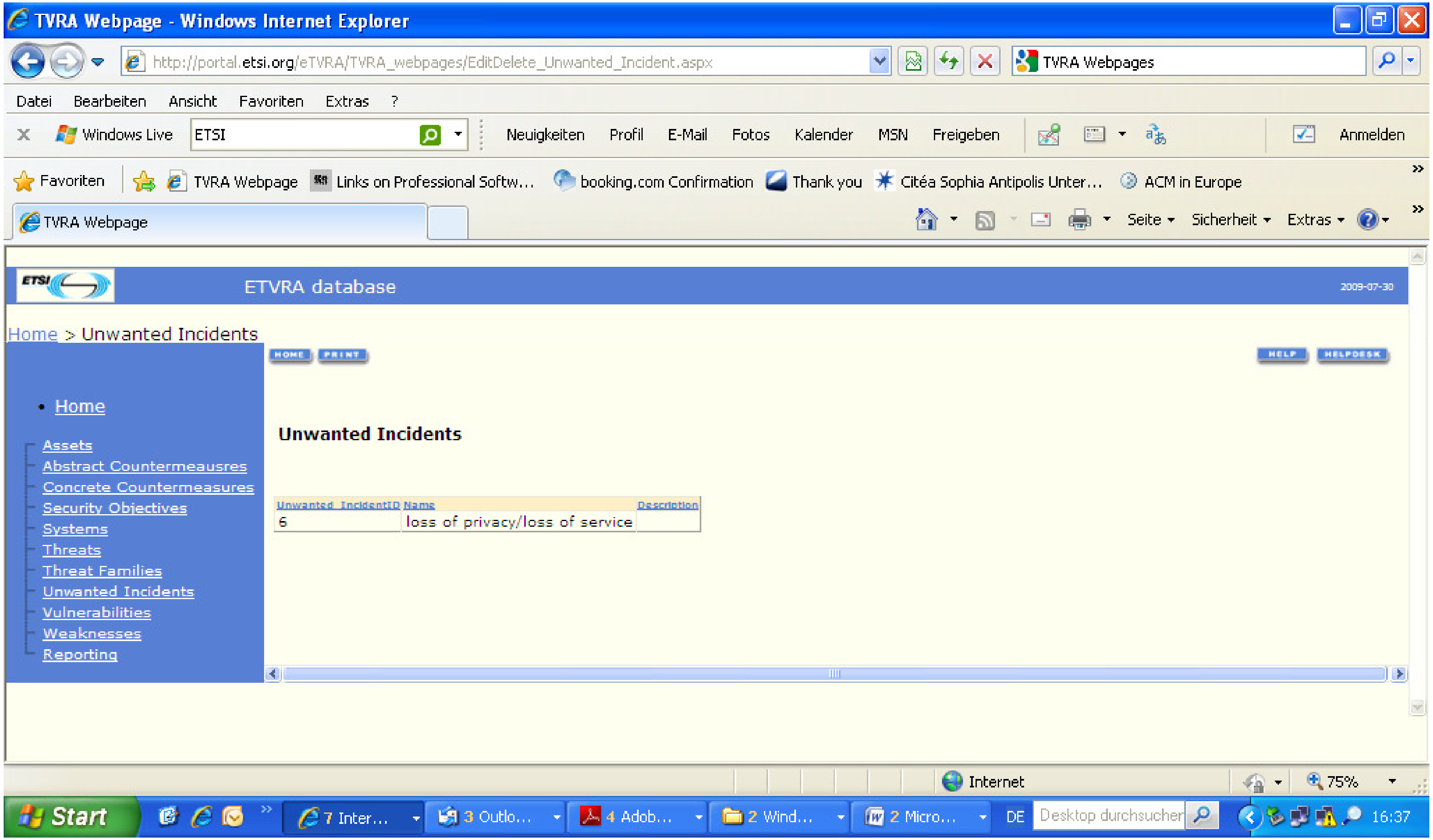
Security Objectives

Security_ObjectiveID	Name	Description
1	Availability	
2	Confidentiality	
3	Integrity	

ETSI TVRA Method – 1st step: Unwanted Incidents

- Disclosure of steering instructions u or signalling input r;
- Manipulation of steering instructions u;
- Unauthorized insertion of reference inputs r;
- Measurement and transmission failures of system variables y;
- Loss of Reliability of Bahn user services due to (G, H) malfunctioning or u- instruction, -attacks

ETSI TVRA Method - 1st step: Unwanted Incidents



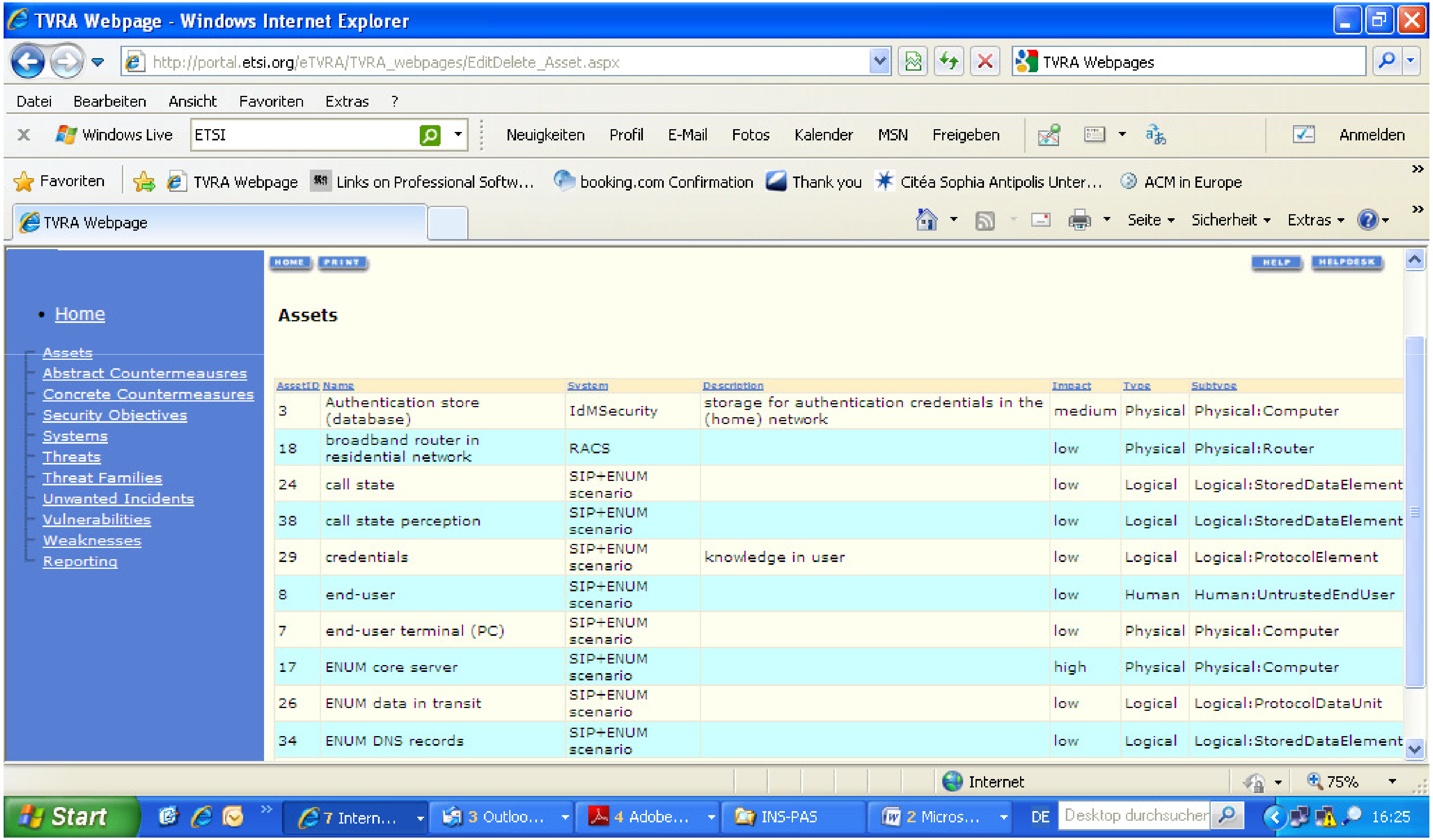
Unwanted Incidents

Unwanted_IncidentID	Name	Description
6	loss of privacy/loss of service	

2. ETSI TVRA Method – 2nd step Requirements

- To identify functional **Security Requirements**
  - Should specify higher level behaviour
  - May refer to protocol standards
  - Should map to ISO 15408-2 „Requirements“ capabilities, according to ETSI TR 187 011 „Guide, Method and Application“
  - Requirement Specification Conventions
    - Shall-means are mandatory
    - Should-means are recommended
    - May-means are optional

ETSI TVRA Method – 2nd step Requirements


TVRA Webpage - Windows Internet Explorer
http://portal.etsi.org/eTVRA/TVRA_webpages/EditDelete_Asset.aspx
TVRA Webpages
Datei Bearbeiten Ansicht Favoriten Extras ?
Windows Live ETSI Neuigkeiten Profil E-Mail Fotos Kalender MSN Freigeben Anmelden
Favoriten TVRA Webpage Links on Professional Softw... booking.com Confirmation Thank you Citéa Sophia Antipolis Unter... ACM in Europe
TVRA Webpage
Seite Sicherheit Extras
HOME PRINT
HELP HELPDESK
Home
Assets
Abstract Countermeausres
Concrete Countermeasures
Security Objectives
Systems
Threats
Threat Families
Unwanted Incidents
Vulnerabilities
Weaknesses
Reporting
Internet
75%
Start
7 Intern...
3 Outloo...
4 Adobe...
INS-PAS
2 Micros...
DE
Desktop durchsuchen
16:25

Assets

AssetID	Name	System	Description	Impact	Type	Subtype
3	Authentication store (database)	IdMSecurity	storage for authentication credentials in the (home) network	medium	Physical	Physical:Computer
18	broadband router in residential network	RACS		low	Physical	Physical:Router
24	call state	SIP+ENUM scenario		low	Logical	Logical:StoredDataElement
38	call state perception	SIP+ENUM scenario		low	Logical	Logical:StoredDataElement
29	credentials	SIP+ENUM scenario	knowledge in user	low	Logical	Logical:ProtocolElement
8	end-user	SIP+ENUM scenario		low	Human	Human:UntrustedEndUser
7	end-user terminal (PC)	SIP+ENUM scenario		low	Physical	Physical:Computer
17	ENUM core server	SIP+ENUM scenario		high	Physical	Physical:Computer
26	ENUM data in transit	SIP+ENUM scenario		low	Logical	Logical:ProtocolDataUnit
34	ENUM DNS records	SIP+ENUM scenario		low	Logical	Logical:StoredDataElement

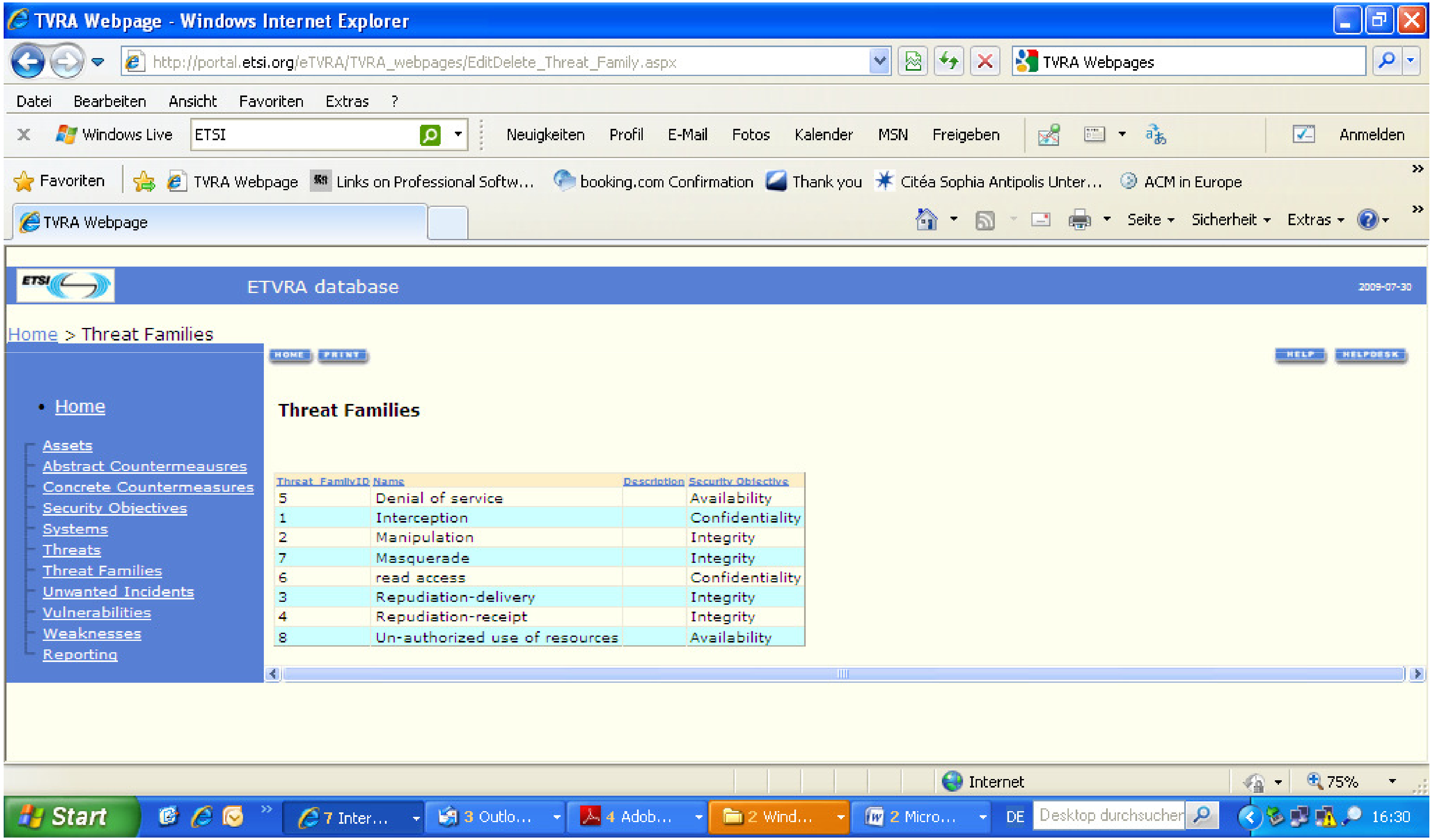
3. ETSI TVRA Method – 3rd step Cataloguing of Assets

- To produce inventory of assets
  - Use of UML Use Case Diagrams to assist System Analysis in order to identify assets
  - Identification of Attributes and Relationships
    - Systems in which assets reside (many-to-many Relationship)
    - Asset Parent-Child-Sibling Relationship (one-to-many, peer-to-peer)
  - Communication systems comprise number of assets
    - HW – SW – Humans
  - Impact of attack on asset is classified, thus
    - Low -> possible damage is slight
    - Medium -> potential threats cannot be neglected
    - High -> severer damage to business

4. ETSI TVRA Method - 4th step Classify Vulnerability & Threats

- To classify vulnerabilities and threats
  - Weaknesses are identified by systematic scrutiny of a specification
    - Weakness leads to unwanted incident (step2) and requires certain system knowledge
  - Identification of Attack Method
    - Threat Agent
      - models behaviour of Attacker
      - Exploits vulnerability through ports or interface
      - Threatens one of security objectives from step1
  - Aspects of weaknesses as a vulnerability
    - Availability of knowledge of assets
    - Ability of threat agent to mount attack in terms of
      - Time – expertise – opportunity – availability – complexity of essential equipment
    - Ratings in vulnerability range from „no-rating“ to „beyond-high“

ETSI TVRA Method - 4th step
Classify Vulnerability & Threats


TVRA Webpage - Windows Internet Explorer
http://portal.etsi.org/eTVRA/TVRA_webpages/EditDelete_Threat_Family.aspx
TVRA Webpages
Datei Bearbeiten Ansicht Favoriten Extras ?
Windows Live
ETSI
Neuigkeiten Profil E-Mail Fotos Kalender MSN Freigeben
Anmelden
Favoriten
TVRA Webpage
Links on Professional Softw...
booking.com Confirmation
Thank you
Citéa Sophia Antipolis Unter...
ACM in Europe
Seite Sicherheit Extras
HOME PRINT
HELP HELPDESK
Internet
75%
Start
7 Inter...
3 Outlo...
4 Adob...
2 Wind...
2 Micro...
DE
Desktop durchsuchen
16:30

ETVRA database

2009-07-30

Home > Threat Families

- Home
- Assets
- Abstract Countermeausres
- Concrete Countermeasures
- Security Objectives
- Systems
- Threats
- Threat Families
- Unwanted Incidents
- Vulnerabilities
- Weaknesses
- Reporting

Threat Families

Threat_FamilyID	Name	Description	Security Objective
5	Denial of service		Availability
1	Interception		Confidentiality
2	Manipulation		Integrity
7	Masquerade		Integrity
6	read access		Confidentiality
3	Repudiation-delivery		Integrity
4	Repudiation-receipt		Integrity
8	Un-authorized use of resources		Availability

5. ETSI TVRA Method - 5th step quantify Likelihood, Impact of Threats

- To quantify likelihood, impacts of threats by using vulnerabilty rating

Vulnerability Rating	Likelihood of Attack	Value
Beyond High	Unlikely	1
High		
Moderate	Possible	2
Basic	Likely	3
No Rating		

6. ETSI TVRA Method - 6th step
Determine Risks

- To determine risks by classification of attack intensity expected
  - 0 -> single instance of attack
  - 1 -> moderate intensity of attack
  - 2 -> high intensity of attack

- Provides overall measurement of risk

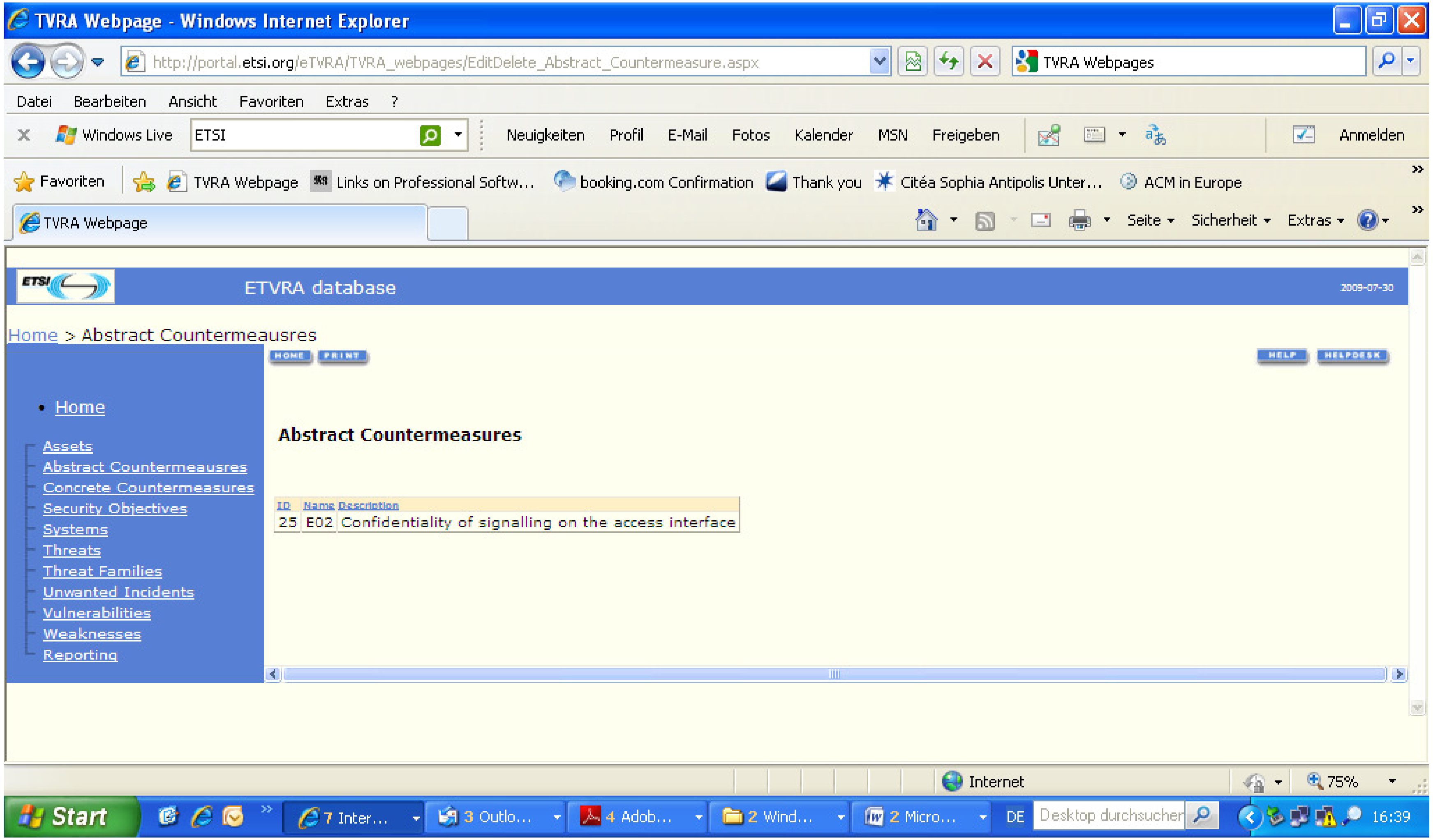
Asset Impact	Attack Likelihood		
	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

Risk		
Value	Classification	Explanation
1, 2, 3	Minor	No essential assets concerned; the attack is unlikely; minor risks; no need for countermeasures
4	Major	Threats on relevant assets likely; impact unlikely to be fatal; risks should be minimized by the appropriate use of countermeasures.
6, 9	Critical	Primary interests of the providers/subscribers threatened; effort required for potential attacker is not high; critical risks should be minimized.

7. ETSI TVRA Method - 7th step to specify detailed Countermeasures

- To Specify detailled requirements (countermeasures)
  - Which reduce
    - likelihood of attack,
    - impact of attack
  - Being determined by inspection and experience
  - TVRA to be iterated after countermeasures have been specified
  - Countermeasures include
    - Explicitly in security spec
    - by reference in another spec
    - implicitly in base spec

ETSI TVRA Method - 7th step to specify abstract Countermeasures


TVRA Webpage - Windows Internet Explorer
http://portal.etsi.org/eTVRA/TVRA_webpages/EditDelete_Abstract_Countermeasure.aspx
TVRA Webpages
Datei Bearbeiten Ansicht Favoriten Extras ?
Windows Live
ETSI
Neuigkeiten Profil E-Mail Fotos Kalender MSN Freigeben
Anmelden
Favoriten
TVRA Webpage
Links on Professional Softw...
booking.com Confirmation
Thank you
Citéa Sophia Antipolis Unter...
ACM in Europe
TVRA Webpage
Seite Sicherheit Extras
HOME PRINT
HELP HELPDESK
Internet
75%
Start
7 Inter...
3 Outlo...
4 Adob...
2 Wind...
2 Micro...
DE
Desktop durchsuchen
16:39

ETVRA database

2009-07-30

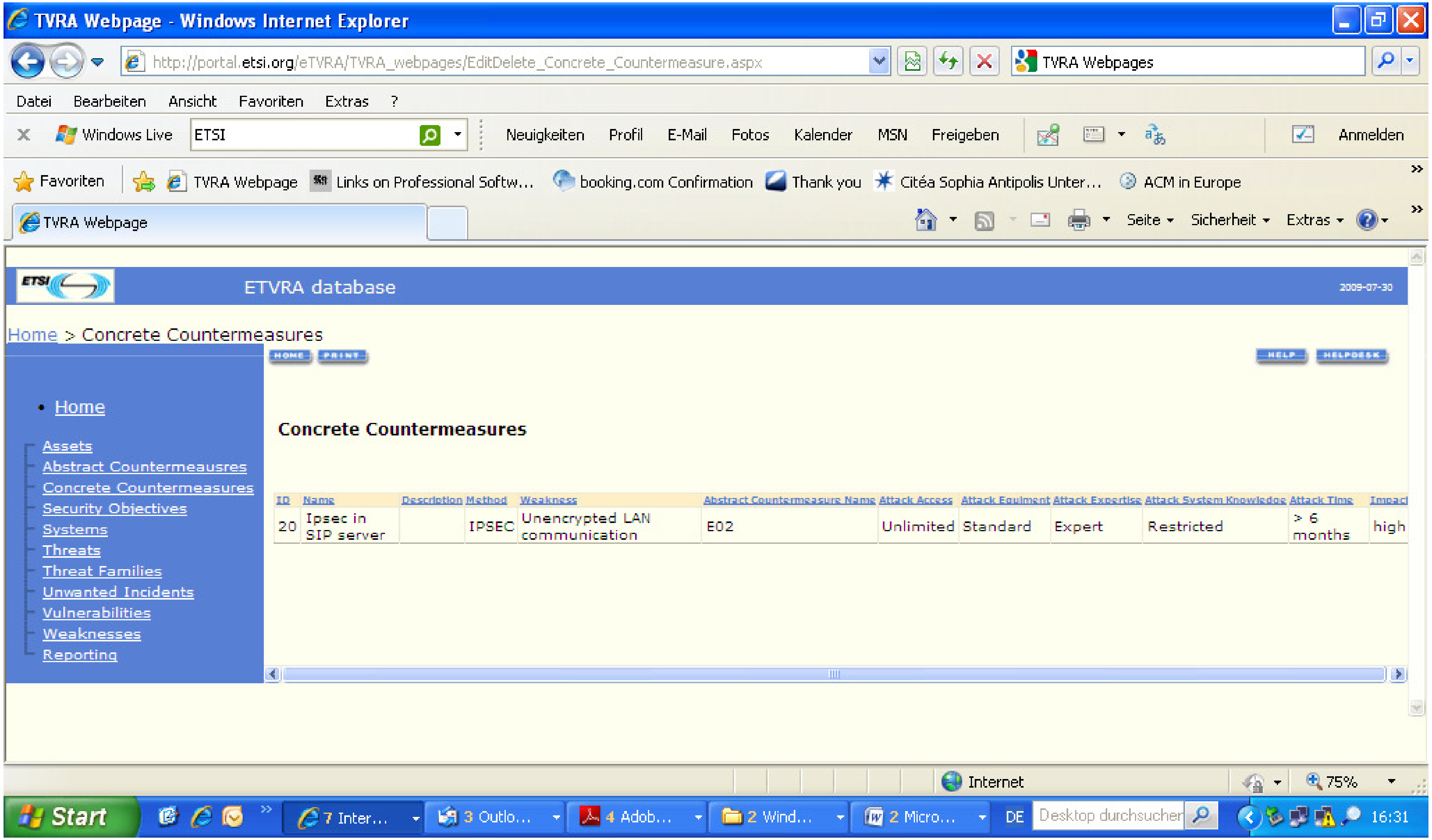
Home > Abstract Countermeausres

- Home
  - Assets
  - Abstract Countermeausres
  - Concrete Countermeasures
  - Security Objectives
  - Systems
  - Threats
  - Threat Families
  - Unwanted Incidents
  - Vulnerabilities
  - Weaknesses
  - Reporting

Abstract Countermeasures

ID	Name	Description
25	E02	Confidentiality of signalling on the access interface

ETSI TVRA Method - 7th step to specify detailled Countermeasures


TVRA Webpage - Windows Internet Explorer
http://portal.etsi.org/eTVRA/TVRA_webpages/EditDelete_Concrete_Countermeasure.aspx
TVRA Webpages
Datei Bearbeiten Ansicht Favoriten Extras ?
Windows Live ETSI Neuigkeiten Profil E-Mail Fotos Kalender MSN Freigeben Anmelden
Favoriten TVRA Webpage Links on Professional Softw... booking.com Confirmation Thank you Citéa Sophia Antipolis Unter... ACM in Europe
TVRA Webpage
Seite Sicherheit Extras
HOME PRINT HELP HELPDESK
Internet 75%
Start 7 Inter... 3 Outlo... 4 Adob... 2 Wind... 2 Micro... DE Desktop durchsuchen 16:31

ETVRA database 2009-07-30

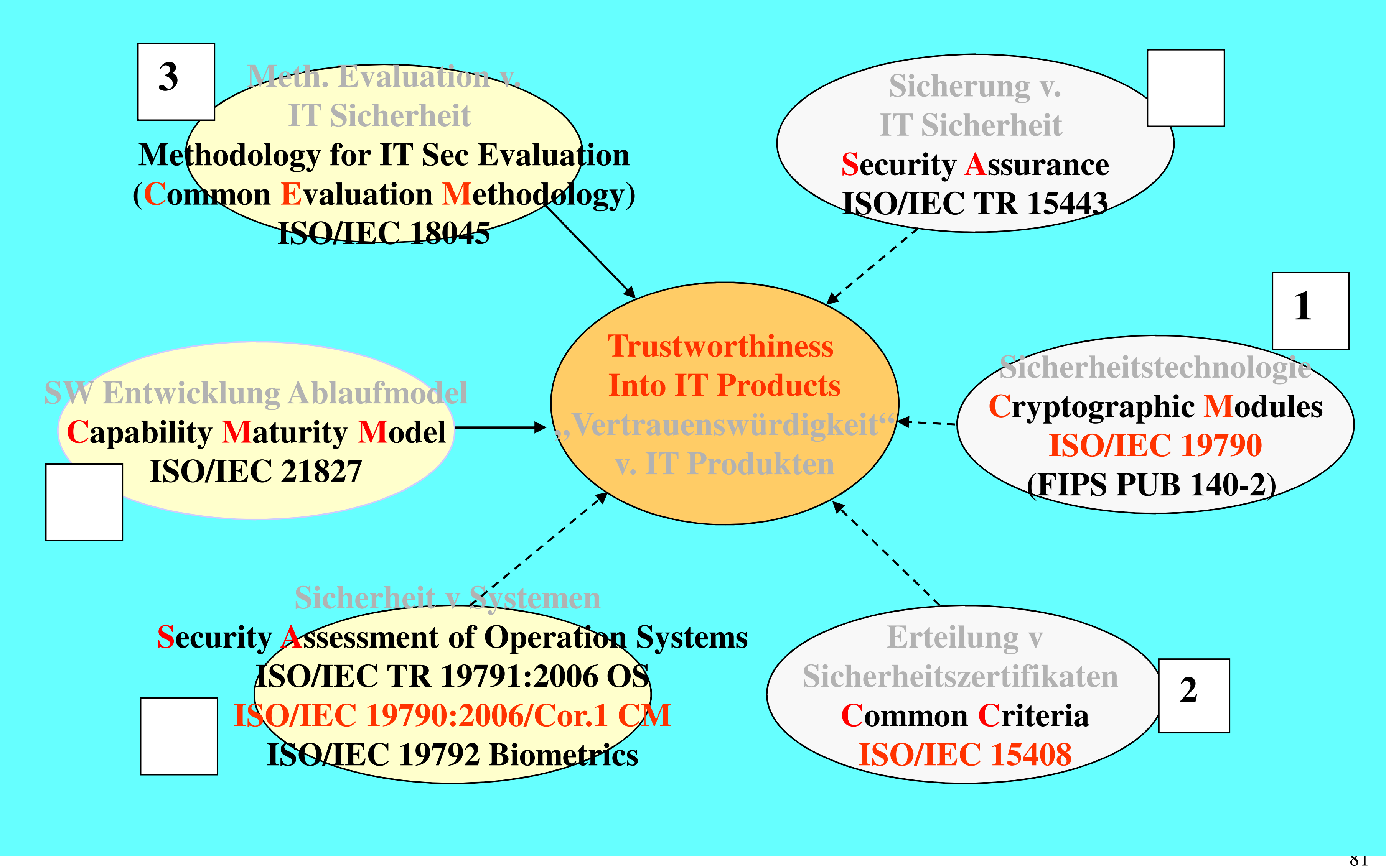
Home > Concrete Countermeasures

- Home
  - Assets
  - Abstract Countermeausres
  - Concrete Countermeasures
  - Security Objectives
  - Systems
  - Threats
  - Threat Families
  - Unwanted Incidents
  - Vulnerabilities
  - Weaknesses
  - Reporting

Concrete Countermeasures

ID	Name	Description	Method	Weakness	Abstract Countermeasure Name	Attack Access	Attack Equipment	Attack Expertise	Attack System Knowledge	Attack Time	Impact
20	Ipsec in SIP server		IPSEC	Unencrypted LAN communication	E02	Unlimited	Standard	Expert	Restricted	> 6 months	high

European Information Technology Security Evaluation Criteria (ISO WG3)



3

Meth. Evaluation v. IT Sicherheit

Methodology for IT Sec Evaluation (Common Evaluation Methodology) ISO/IEC 18045

Sicherung v. IT Sicherheit

Security Assurance ISO/IEC TR 15443

SW Entwicklung Ablaufmodel

Capability Maturity Model ISO/IEC 21827

Trustworthiness Into IT Products

„Vertrauenswürdigkeit“ v. IT Produkten

1

Sicherheitstechnologie

Cryptographic Modules ISO/IEC 19790 (FIPS PUB 140-2)

Sicherheit v Systemen

Security Assessment of Operation Systems

ISO/IEC TR 19791:2006 OS

ISO/IEC 19790:2006/Cor.1 CM

ISO/IEC 19792 Biometrics

Erteilung v Sicherheitszertifikaten

Common Criteria ISO/IEC 15408

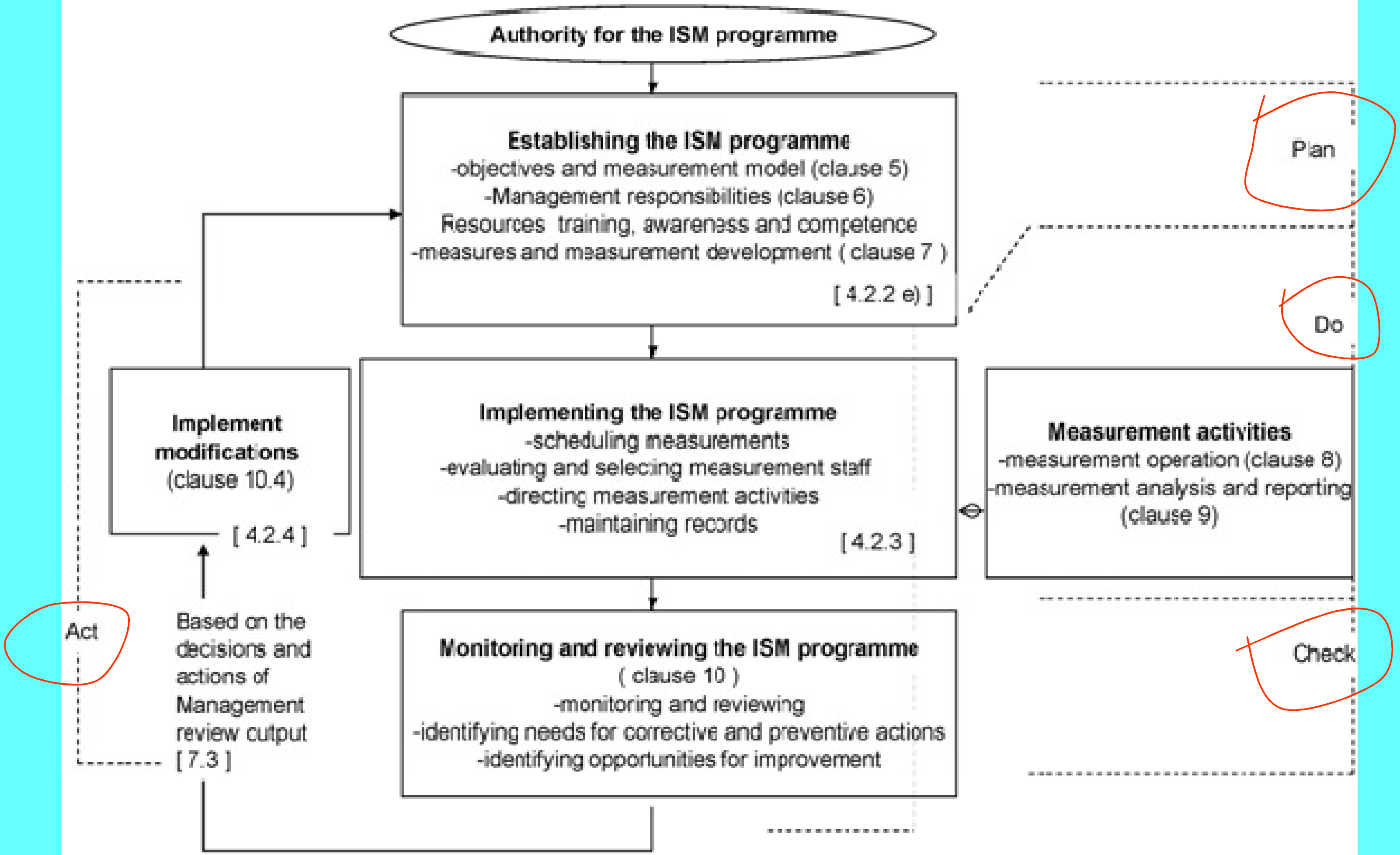
2

ISO/IEC Security Evaluation Criteria – Cryptographic Module Test Requirements (FCD24759:2007)

1. Assertions and Security Requirements
    1. **General Test Requirements**
    2. **CM Specification**
    3. **CM Ports and Interfaces**
    4. **Roles, Services, and Authentication**
    5. Finite State Model
    6. Physical Security
    7. Operational Environment
    8. Cryptographic Key Management
    9. Self-Tests (Power-up, Conditional)
    10. Design Assurance
    11. Mitigation of other Attacks
    12. Documentation Requirements
    13. CM Security Policies
    14. Approved Protection Profiles
    15. Approved Security Functions
    16. Recommended SW Development Practices
    17. Examples of Mitigation of other Attacks

ISO/IEC Security Evaluation Criteria – CM Test Requirements (FCD24759:2007)

- **Process Flow for Information Security Measurement Programs**



Authority for the ISM programme

Establishing the ISM programme
-objectives and measurement model (clause 5)
-Management responsibilities (clause 6)
Resources training, awareness and competence
-measures and measurement development (clause 7)
[4.2.2 e)]

Implement modifications
(clause 10.4)
[4.2.4]

Implementing the ISM programme
-scheduling measurements
-evaluating and selecing measurement staff
-directing measurement activities
-maintaining records
[4.2.3]

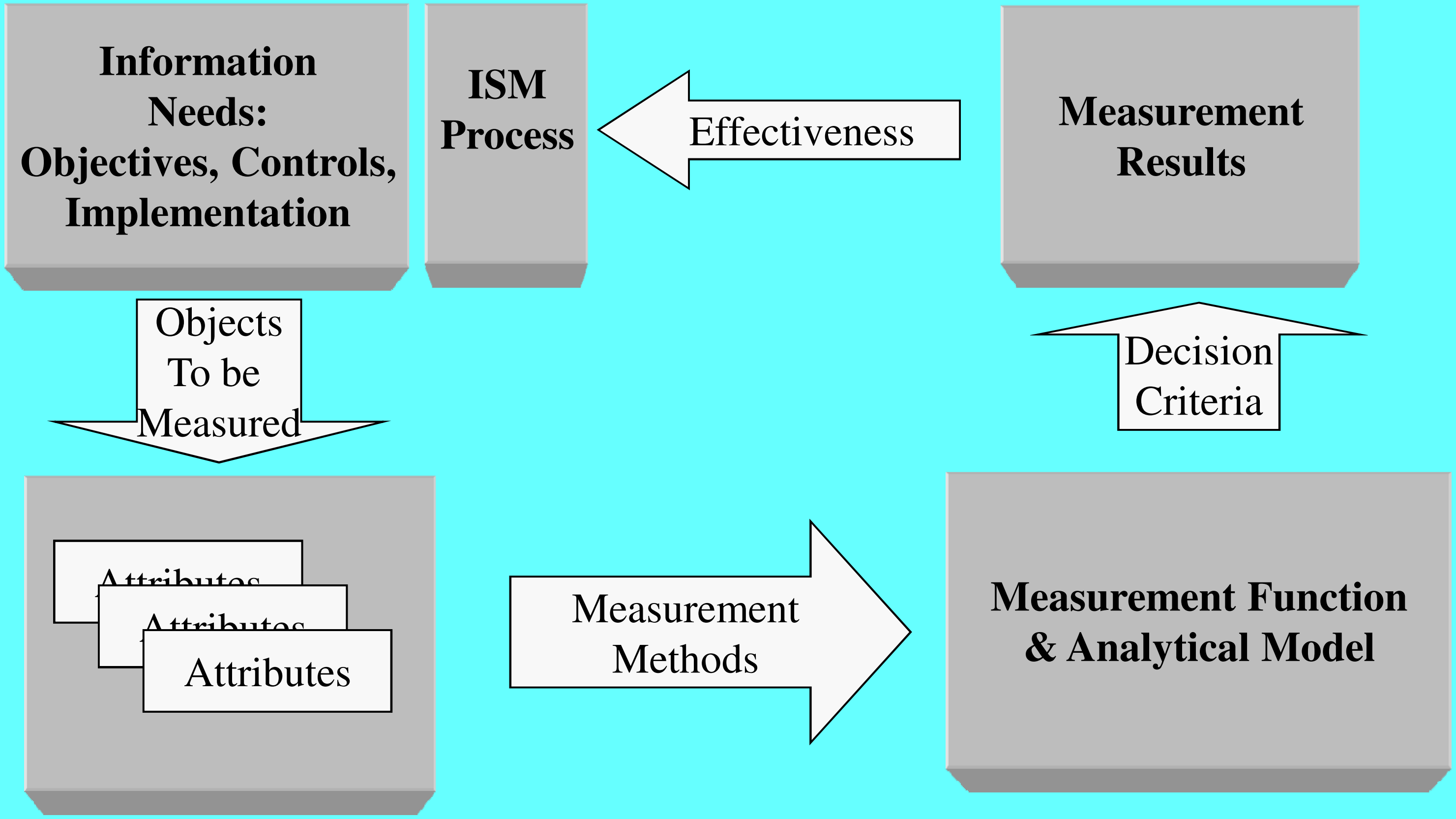
Measurement activities
-measurement operation (clause 8)
-measurement analysis and reporting (clause 9)

Based on the decisions and actions of Management review output [7.3]

Monitoring and reviewing the ISM programme
(clause 10)
-monitoring and reviewing
-identifying needs for corrective and preventive actions
-identifying opportunities for improvement

ISO/IEC Security Evaluation Criteria - CM Test Requirements (FCD24759:2007)

- Information Security Measurement Model



Common Criteria – ISO/IEC 15408 Overview

Common Criteria

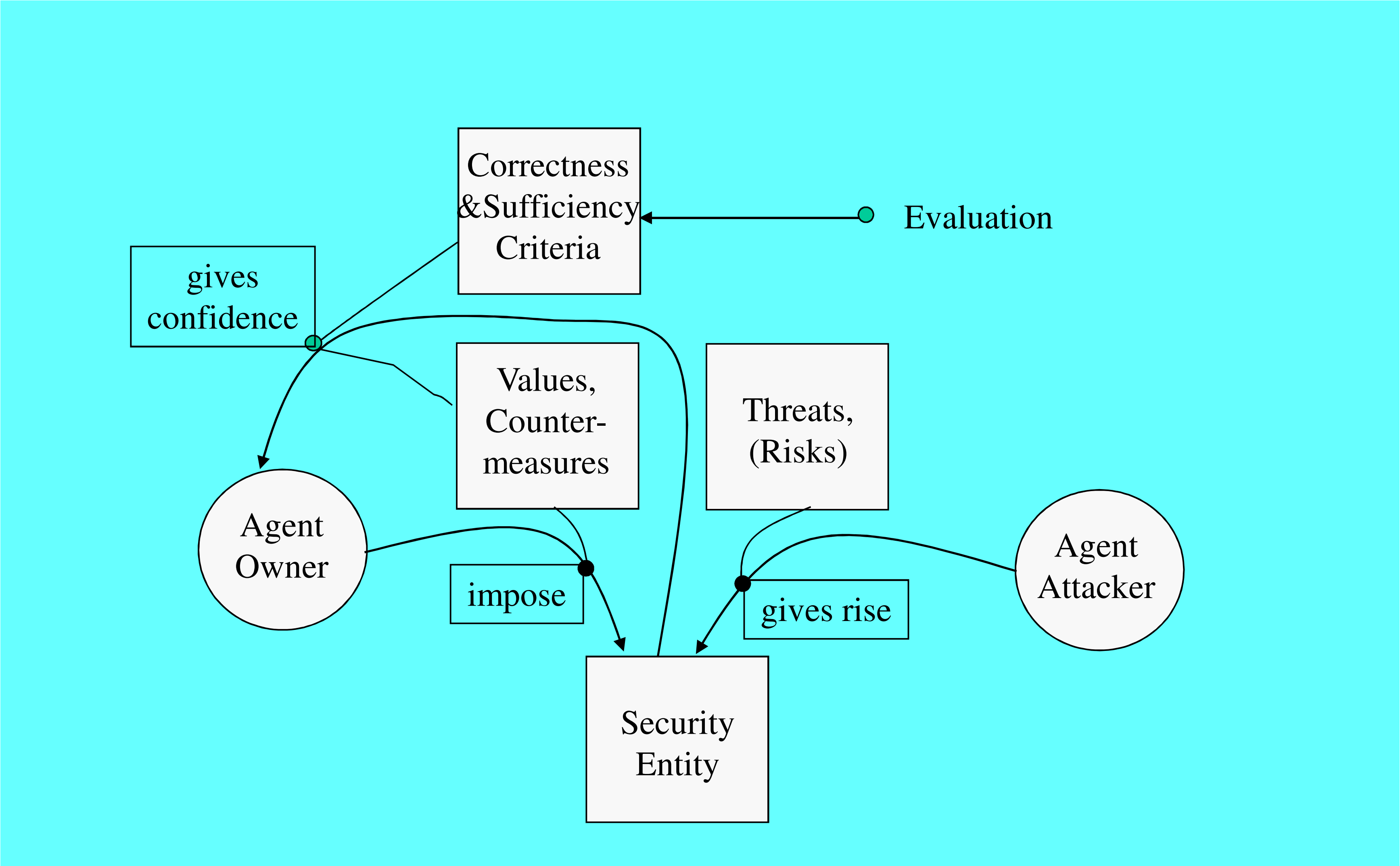
Common Criteria – ISO/IEC 15408 Overview

- CC Part 1: General Model
  - Concepts & Principles of IT Security Evaluation
- CC Part 2: Security Functional Components
  - Set of Functional Components serving as templates on which Functional Requirements for „Target-of-Evaluations" based upon, and
  - Organizes functional components into families and classes
- CC Part 3: Security Assurance Components
  - Set of Assurance Components serving as templates on which Assurance Requirements for ToEs based upon, and
  - Defines Evaluation Criteria for „Protection Profiles" and „Security Targets", and
  - Present 7 pre-defined Assurance Packages, called „Evaluation Assurance Levels".

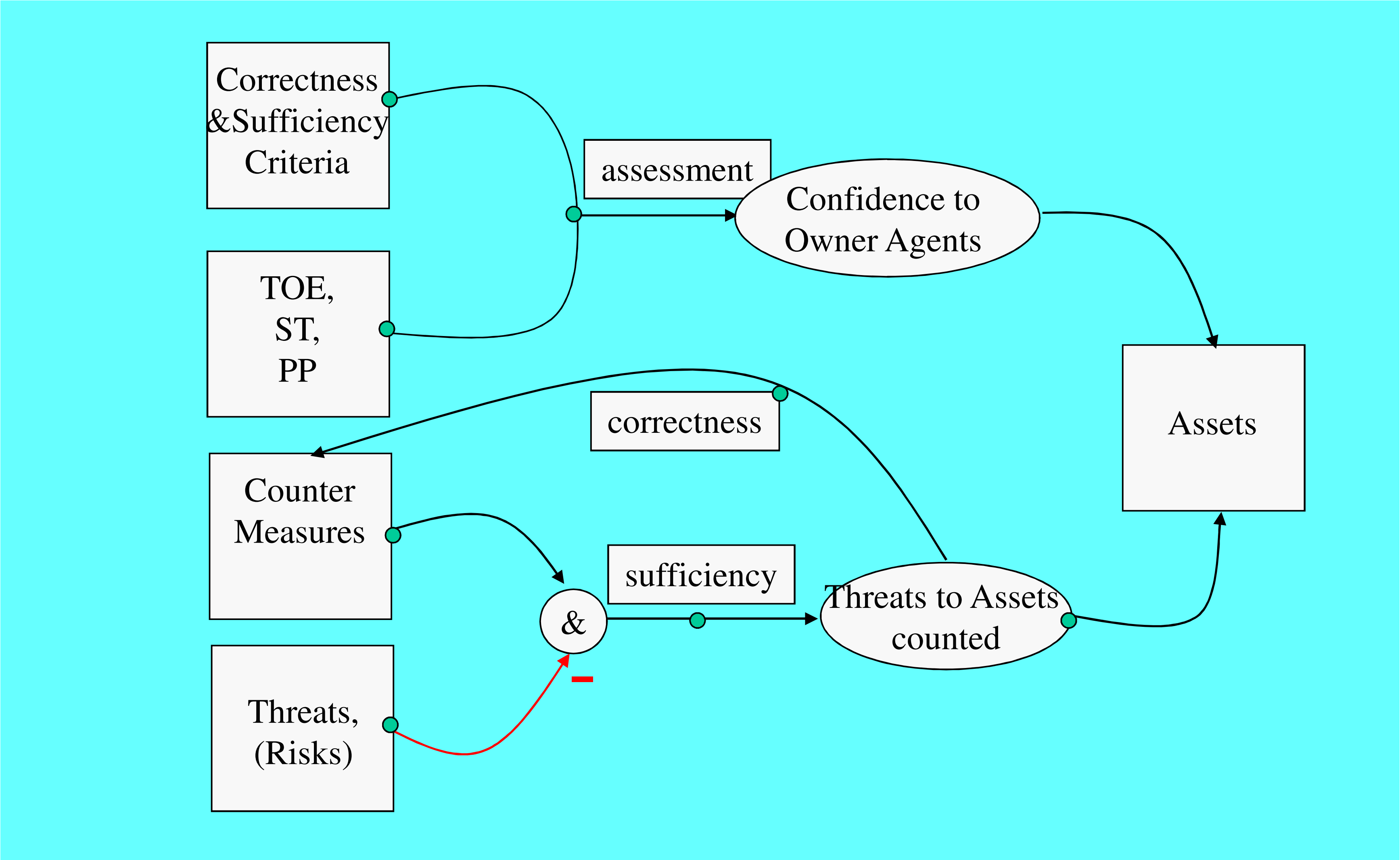
Common Criteria - ISO/IEC 15408 Overview

	Consumer‘s Interest	Developer‘s Interest	Evaluator‘s Interest
P1: GM	guidance to structure PPs	Reference to develop security specs fo ToEs	guidance to structure PP, STs
P2: SFC	guidance to state Reqs on (TOE) SecFuncs	Reference to interprete statements of FuncReqs on ToEs	Mandatory Evaluation Criteria on ToE‘s SecFunc claims
P3: SAC	guidance to determine required level of assurance	Reference to interprete assurance requirements, approaches of ToEs	Mandatory evaluation criteria on ToE‘s assurance, PP‘s, ST‘s evaluations

Common Criteria – ISO/IEC 15408-1: General Model: Agent – Entity - Relationship

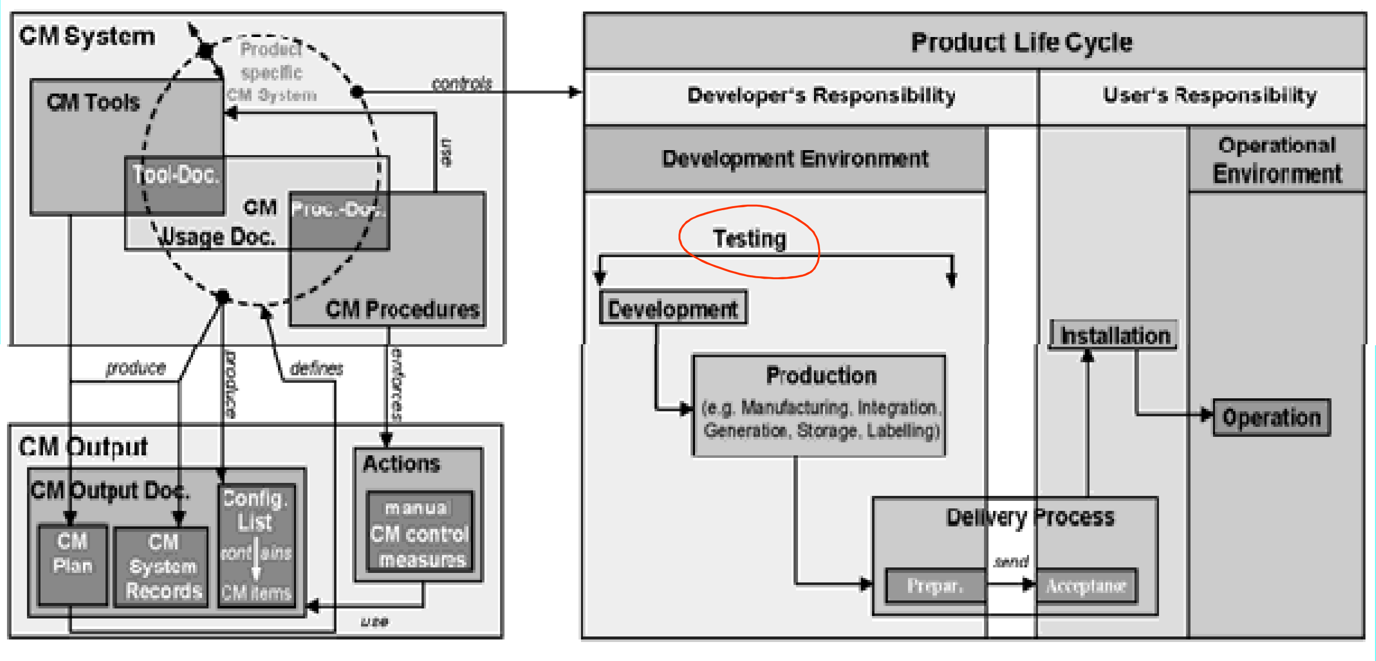


Common Criteria - ISO/IEC 15408-1: General Model: Concept of Evaluation


Correctness &Sufficiency Criteria
TOE, ST, PP
assessment
Confidence to Owner Agents
Assets
correctness
Counter Measures
&
sufficiency
Threats to Assets counted
Threats, (Risks)
–

Common Criteria – ISO/IEC 15408-1: Terms & Definitions

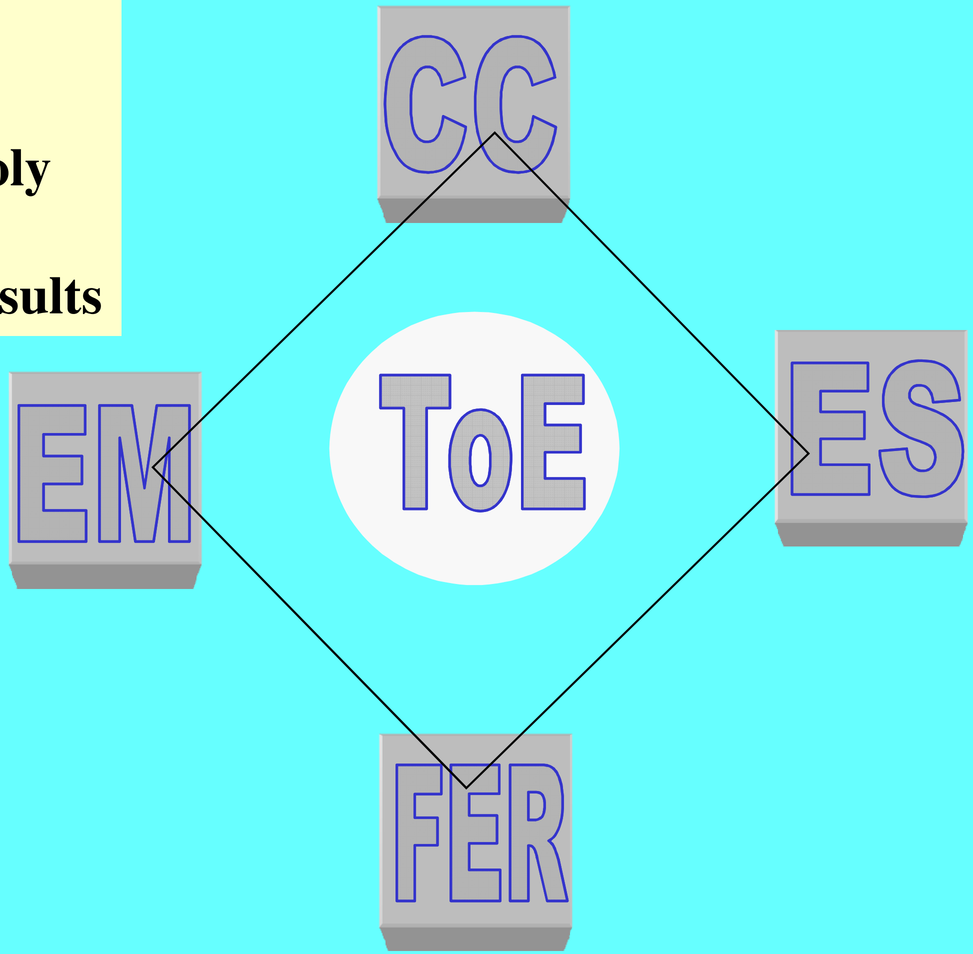
- Terminology in Configuration Management and Product Life-Cycle [CC Part 1 Figure 1]
  - Implementaton Transformation of a ToE into a state acceptable for delivery to customers
  - Comprises manufacturing, integration, generation, internal transport, storage, labelling of ToE



*CM Documentation = CM Usage Doc. + CM Output Doc.

Common Criteria - ISO/IEC 15408-1: Evaluation & Certification Contexts

Evaluation Context:
- **Common Criteria**
- **Evaluation Methodoly**
- **Evaluation Scheme**
- **Final Evaluation Results**



Common Criteria -ISO/IEC 15408-3:

CC Testing

Common Criteria –ISO/IEC 15408-3: Evaluation Assurance Level

- EALs balance level of assurance obtained with cost and feasibility of acquiring a certain degree of assurance
  - 7 hierarchical (inclusion) EALs defined for a ToE's assurance rating
    - Increase in assurance is accomplished by substitution of higher assurance componenet from same assurance family
    - Increase of rigour, scope, depth
  - Each EAL includes no more than 1 component of each assurance class resp. Family:
    - Development
    - Guidance Document
    - Life-cycle Support
    - Security Target Evaluation
    - Tests
    - Vulnerability Assessment

Common Criteria -ISO/IEC 15408-3: Evaluation Assurance Level

- Functional Testing of EAL1
- Structural Testing of EAL2
- Methodically Testing and Checks of EAL3
- Methodically Design, Testing and Reviewing of EAL4
- Semiformally Design and Testing of EAL5
- Semiformally Verified Design and Testing of EAL6
- Formally Verified Design and Testing of EAL7
- …

Conclusions

Conclusions
on SecCert

Requirements of Security Assurance

- What do we need?
  - A „trusted stack“ including „I&4A“, i.e.
    - Identity Claims, Authentication, Authorization, Access, Audit! [Jacques Stern, ANR Paris, ICST Dept.]
- What do we have currently?
  - Almost mature standards (CC)
    - FIPS PUB 140-2 (N.A.): Cryptographic Module
    - 3rd FCD15408-1:2008 : Target of Evaluation
    - 1st FCD 15408-2/3:2007: 2 Paradigms:
      Security Requirements(2) + Security Assurance(3)
- What do we miss?
    - A formal reasoning
    - Engineering platform, integrating test, V&V, Certification Guidlines Tools
- How to bridge the gap – future work?
    - Coordinated Approach including Industry, Research & Standardization Bodies on
    - Formal-based Test & Verification integrated Security Assurance Methodology, suitable for ULS Systems

Security Certification Features

- At time being, 5 stakeholder communities have vested interest in certifying (OSS) features by CCR-EAL:
  - **Common Criteria Recognition Evaluation Assertion Levels**
  - Charnes, Cooper Rhodes Model to evaluate I/O Efficiency of Decision-Making Units
  - ISO's Estimated Aggregate Liability, i.e. EAL financial liability estimation tool (SCALE)

- Target of Evaluation (EValuierungs-Gegenstand) is the part of an IT System which is subject of IT Security to be evaluated!
  - All possible configurations of ToE must meet requirements
  - Connection between security and configuration change view on ToE from certified product to certified configuration!
  - Moving from context-dependent test-based certifications to hybrid long-term certification (of OSS)!

Security Certification of Long-Lived Systems

- Long-lived Systems need development- and run-time techniques to certify security, safety and dependability properties.
  - LLS Communication Platforms need to be secure
    - Verifiably as opposed to informally claimed security
    - Measurably as opposed to vague best-effort security
    - Withstands not only threats but also context changes and aging
  - Behavior to be certified by modelling and test-based techniques
  - When the system context changes a runtime tool shall allow to re-check a system's (security and dependability) properties.
    - Dynamic re-checking is important when changes affect preserved functions but with different performance objectives, e.g. new HW technology,
      - Evolving Systems being for long-term service
      - Systems for emerging scenarios, i.e. ubiquitous computing, where it is not possible to overlook all possible arising computing situations

Long-Lived System Certification

- Changes in a system's overall context or execution environment may compromise reliabilty security and non-functional properties.
  - Dependability Characteristics of system modules should be certified by a verification and testing integrated technique!
  - LLCs rely on 3 categories of properties:
    - Abstract model-based specification
    - model, reversely engineered from code
    - Set of tests, acc. to „something good must happen"
  - By testing system properties are compared to desired security and dependability profiles.
  - LLC should allow fast re-evaluation of properties on demand, whenever system configuration evolves

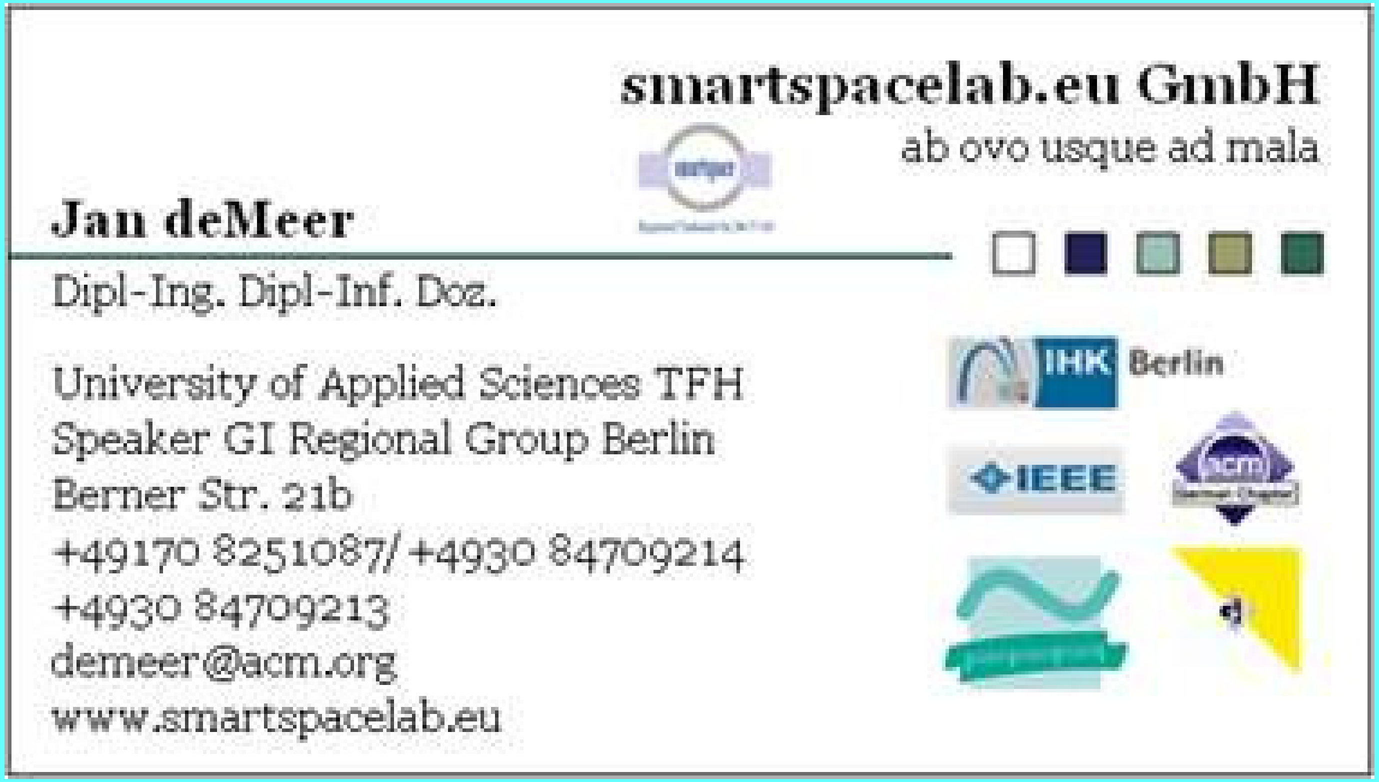
Integration of Test/Model-based Certification

- Research on Integration of
  - Predictable System Engineering by a development process integrating seemlessly Tb and Mb described system properties with emphasis on security and dependability
    - Need of formal methods with regard to model transformation, safety assessment, metrics, certification
  - Support for Dynamic System Evolution (time mobility) by mechanisms built-into systems and work throughout systems' life cycle.
    - Need of innovations with regard to semantic specification of security and dependability

On-demand Certificate Checking

- Distinction between long-lived certificates and proofs:
  - Proof designates a run-time demonstration of program code properties as counterpart to demonstrating the validity of certificate at a formal model, i.e. trial in a controlled executions environment, i.e. a sandbox test.
  - LLCertificate is demonstrated by tests, i.e. test-based certificate!
  - LLC Characteristics
    - Hybrid Nature by integrating Tb and Mb aspects to include properties to be proven on program source code or testing
    - Delayed Verification of proofs of assertions by trusted external entities.
  - Certification is the ability to enforce complex security policies while concilating other features to generate the certificate.

Contact Co-Ordinates



smartspacelab.eu GmbH
ab ovo usque ad mala

Jan deMeer

Dipl-Ing. Dipl-Inf. Doz.

University of Applied Sciences TFH
Speaker GI Regional Group Berlin
Berner Str. 21b
+49170 8251087/ +4930 84709214
+4930 84709213
demeer@acm.org
www.smartspacelab.eu

IHK Berlin
IEEE
acm