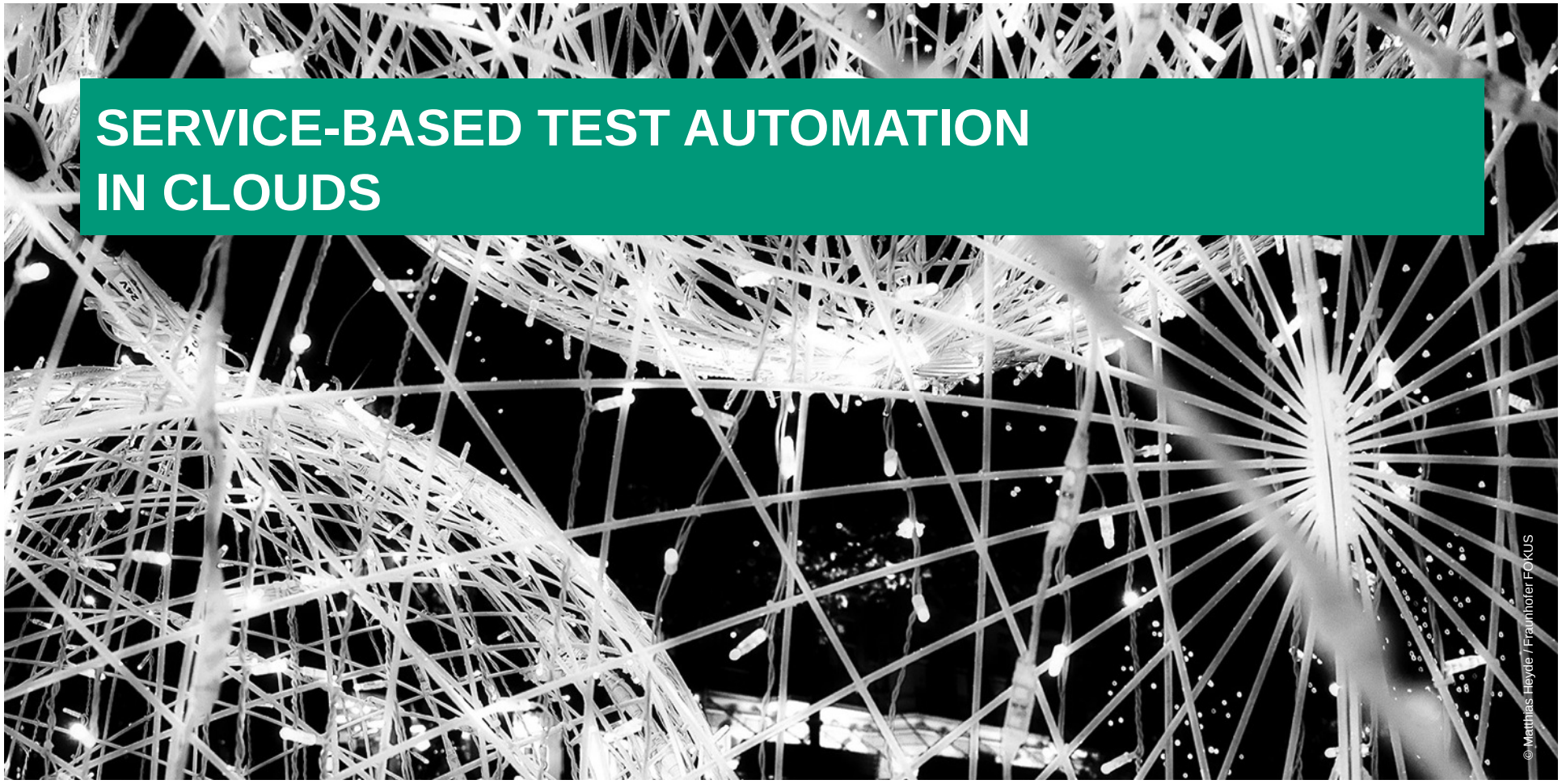
SERVICE-BASED TEST AUTOMATION IN CLOUDS



Prof. Dr.-Ing. Ina Schieferdecker

Secure Clouds Conference

Dublin, May 25, 2016

Fraunhofer FOKUS

Engineering a Connected World

SOFTWARE DEFECTS AND VULNERABILITIES

- Evelyn Labbate, SANS Institute, May 2016: Global Information Assurance Certification:
  poor software quality leads to security vulnerabilities; vulnerabilites as a function of software quality

- U.S. Department of Homeland Security (DHS), March 2013:
  90 percent of security incidents result from exploits against defects in software

- Steve Morgan, Cybersecurity Ventures, Sept. 2015: Is poor software development the biggest cyber threat?
  cyber industry over-focused on network security, while applications are the real weak spot; disconnect between software development and security

- Cisco 2015 Annual Security Report, Jan. 2015
  rise of cloud apps … has created a landscape of vulnerable websites and SaaS offerings

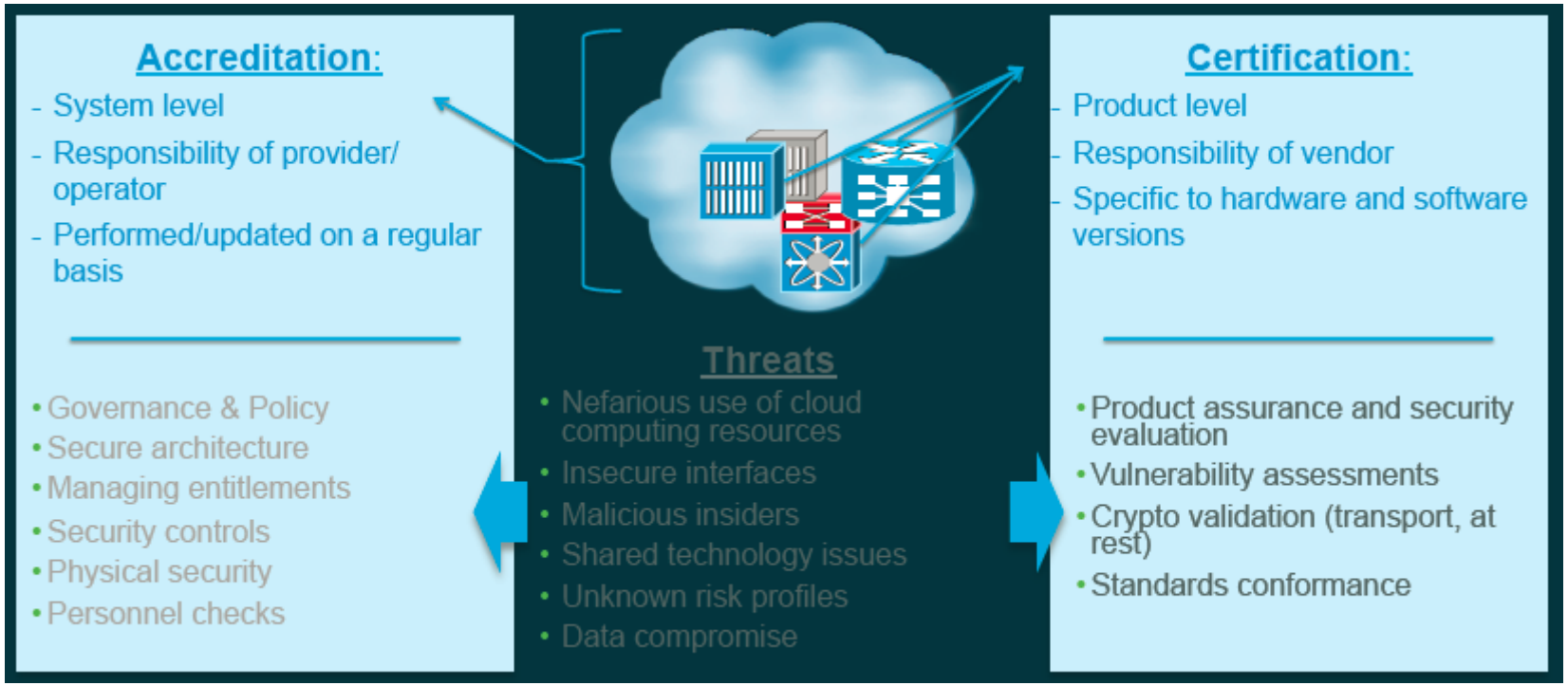
CLOUD SOFTWARE AND SECURITY

1. No matter if IaaS, PaaS, SaaS, etc. – ***there is no defect-free software***

2. Pre-deployment testing and certification can secure parts of the cloud offers – ***but not completely***

3. Configurations, updates, surrounding processes have essential impacts on the security of cloud offers – ***but are assessed in auditing also partially only***

ACCREDITATION/AUDITING VS. CERTIFICATION



Ashit Vora, Cloud Security and Common Criteria, ICCC13, Sept. 2012

CLOUD AND COMMON CRITERIA

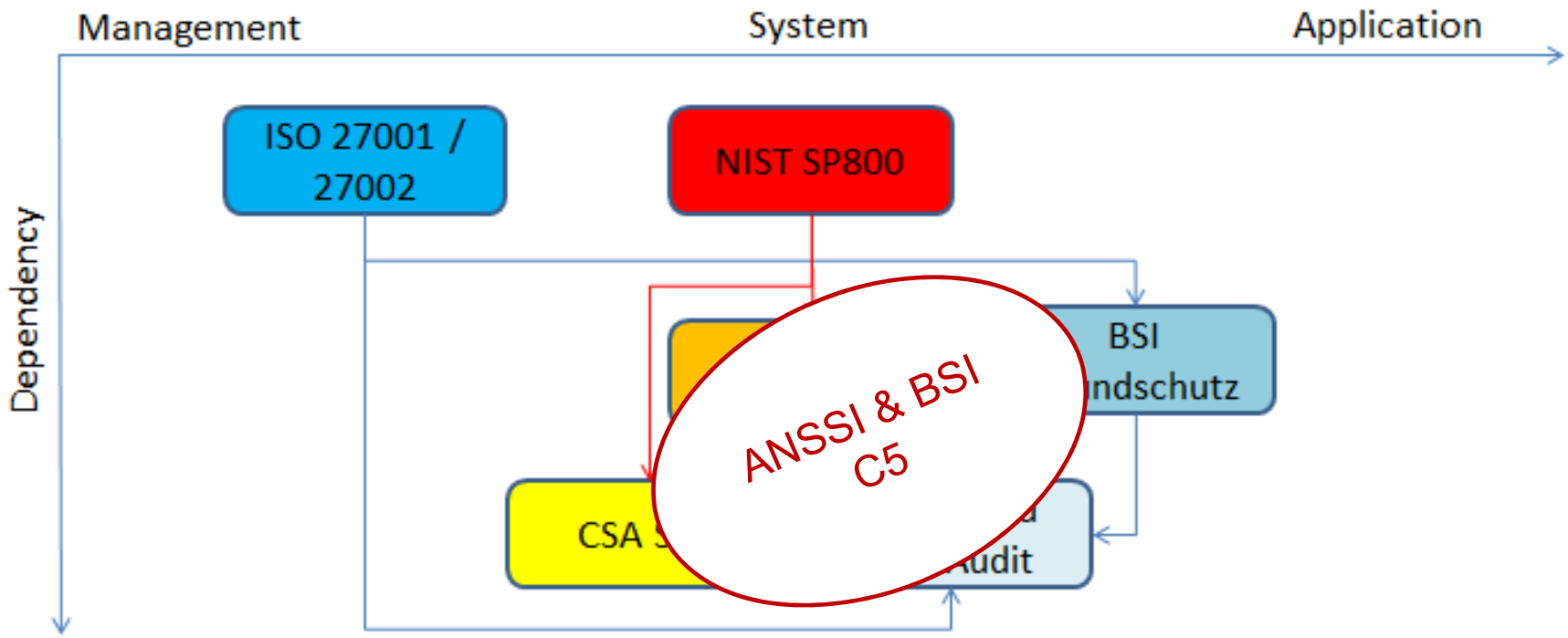
1. Trusted Cloud, April 2015: Trusted Cloud Data Protection Profile (TCDP), v0.9

   data protection certification of cloud computing services

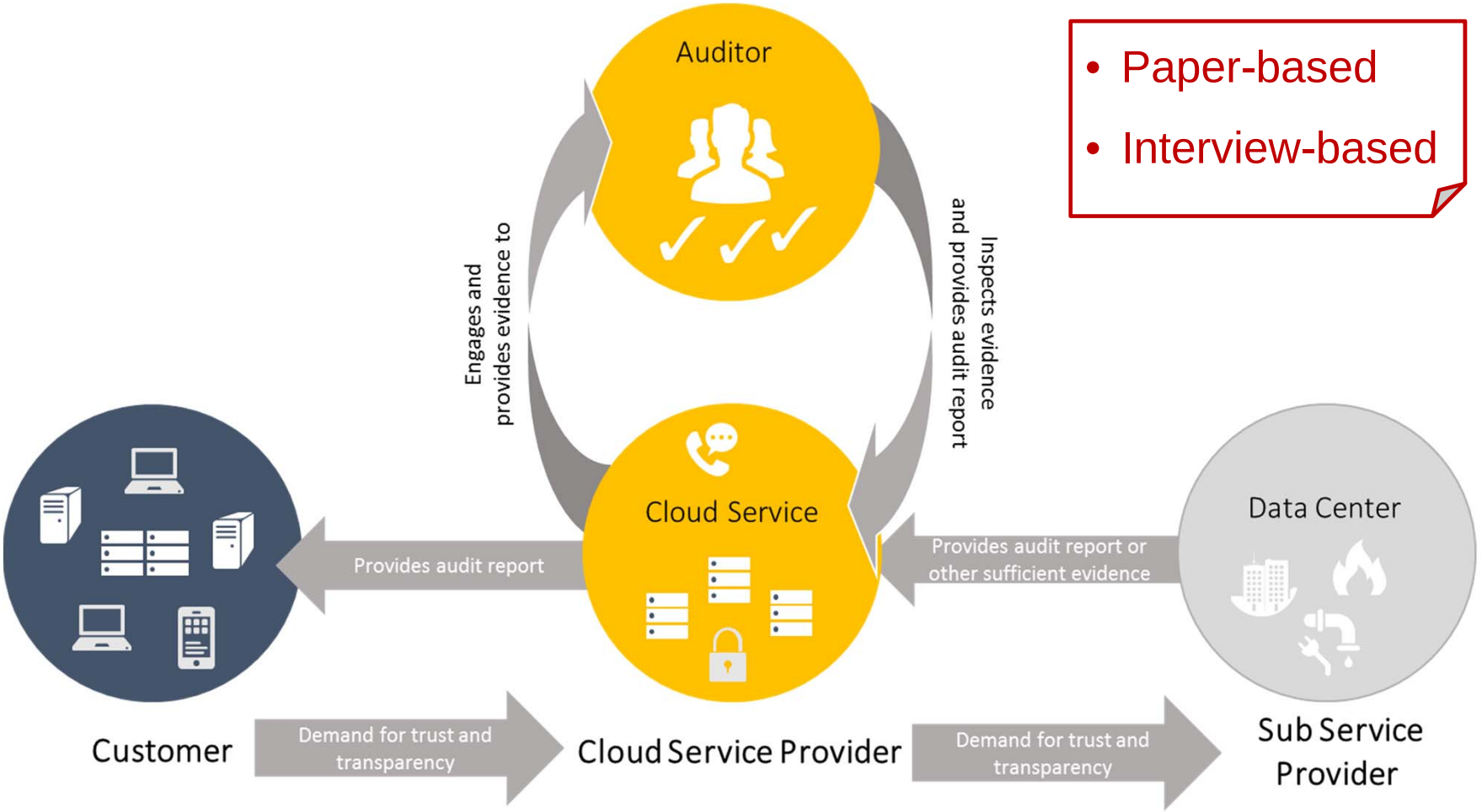
2. DMTF, Oct. 2014: Virtualization Protection Profile (VPP), v1.0

   security requirements for server virtualization

CLOUD AUDITING



CERTIFICATION BASED ON AUDITING



- Paper-based
- Interview-based

CERTIFICATION EXTENDED WITH CONTINUOUS MONITORING

1. Continuous monitoring inputs

   - observable information of a cloud service
   - operational monitoring data
   - server error logs
   - business process logs

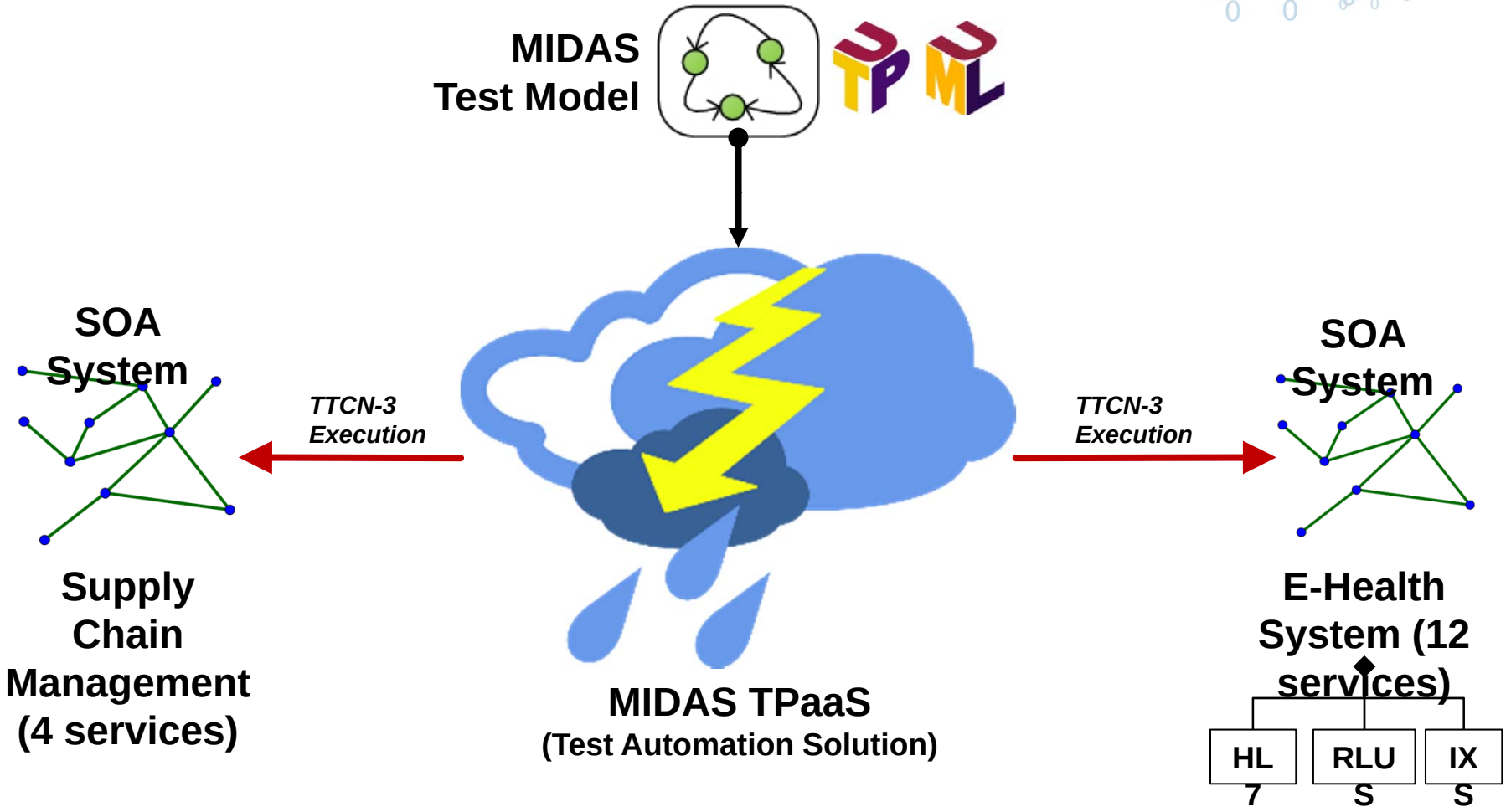
2. Reliably produce trustworthy evidence in real-time

   - collect and maintain security controls and associated requirements (including risk profiles)

3. Monitoring-based audit methods

   - controlling some input to the cloud service and evaluating the output

ONLINE TESTING AND MONITORING



SERVICE-ORIENTED TEST AUTOMATION

TTCN-3

- TTCN-3 is the Testing and Test Control Notation
- Internationally standardized testing language for formally defining test scenarios. Designed purely for active and passive testing

```
testcase Hello_Bob () {
        p.send("How do you do?");
        alt {
        []p.receive("Fine!");
                {setverdict( pass )};
        [else]
                {setverdict( inconc )}  //Bob asleep!
        }
}
```

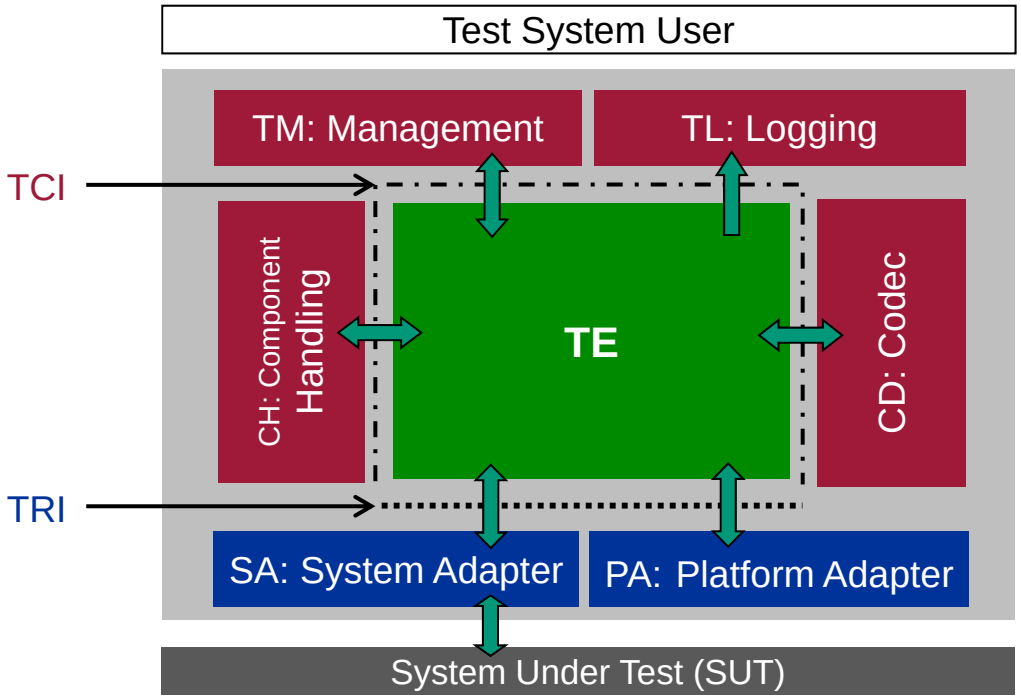
DESIGN PRINCIPLES OF TTCN-3

- One test technology for different tests
  - Distributed, platform-independent testing
  - Integrated graphical test development, documentation and analysis
  - Adaptable, open test environment

- Areas of Testing
  - Regression testing
  - Conformance and functional testing
  - Interoperability and integration testing
  - Real-time, performance, load and stress testing
  - Security testing

- Used for system and product qualification and certification, for example for GCF/PTCRB certification of handsets

A TTCN-3 TEST SYSTEM



TE – TTCN-3 Executable
TM – Test Management
TL – Test Logging
CD – Codec
CH – Component Handling
SA – System Adapter
PA – Platform Adapter
SUT – System Under Test

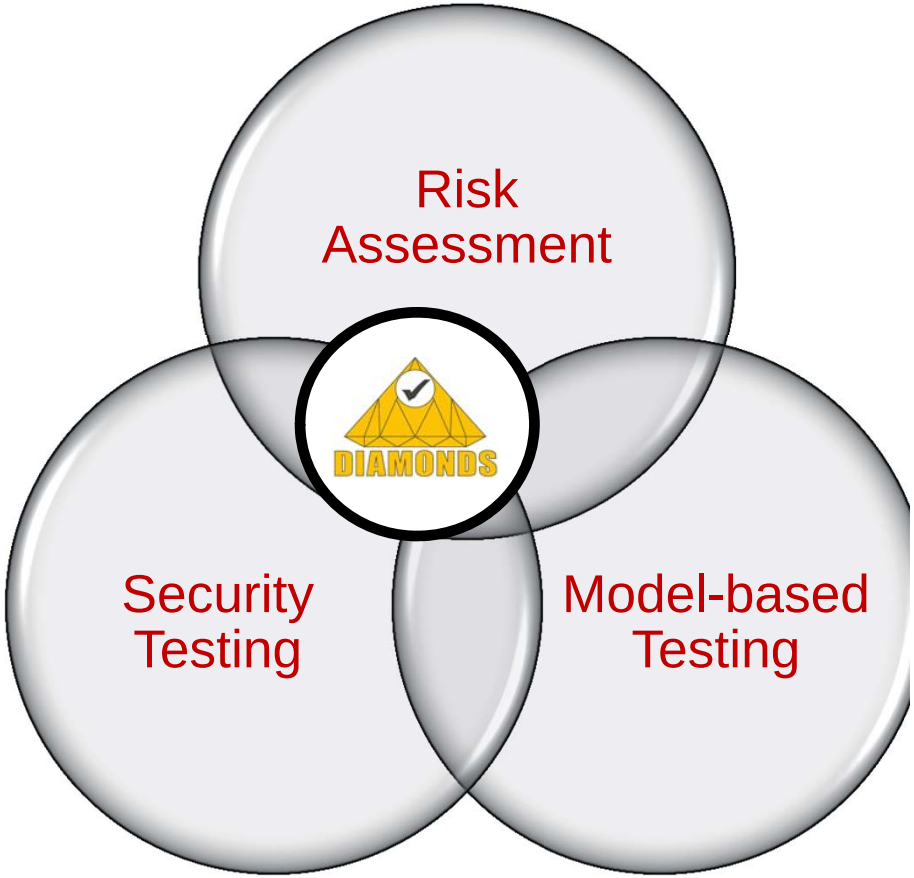
ETSI ES 201 873-1 TTCN-3 Core Language (CL)
ETSI ES 201 873-5 TTCN-3 Runtime Interface (TRI)
ETSI ES 201 873-6 TTCN-3 Control Interfaces (TCI)

MODEL-BASED SECURITY TESTING

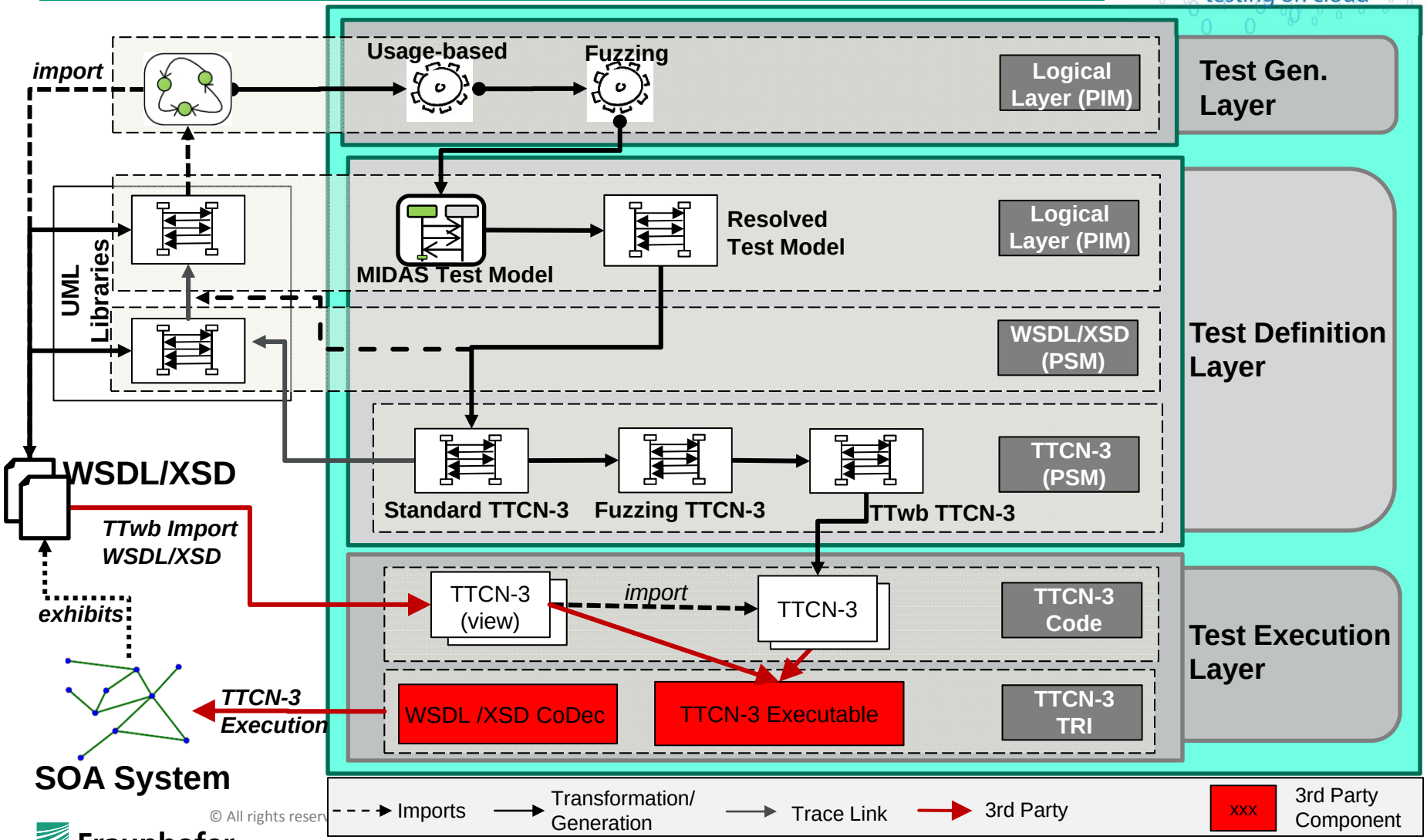
1. Fuzz testing extension for TTCN-3
2. Open source fuzzing library
3. Security test pattern catalog
4. Standardization

ETSI World Class Standards ITU ISO

5. EUREKA Innovation Award, 2016



MODEL-DRIVEN TEST AUTOMATION FRAMEWORK



Fraunhofer FOKUS

CONCLUSIONS

1. Auditing-based certification to be complemented by continous monitoring and online testing

2. Service-based test automation enables flexible online monitoring and test setups

3. TTCN-3 can analyse the functionality of security measures and the features of the cloud offer, but also do randomized penetration tests by its load and fuzzing concepts

4. TTCN-3 with its extensible adapter architecture provides a mature test and monitoring platform

CONTACT

Fraunhofer Institute for Open Communication Systems FOKUS

Kaiserin-Augusta-Allee 31
10589 Berlin, Germany

info@fokus.fraunhofer.de

www.fokus.fraunhofer.de

Director

Prof. Dr.-Ing Ina Schieferdecker
Tel. +49 (30) 34 63 -7241
ina.schieferdecker@fokus.fraunhofer.de

Fraunhofer FOKUS