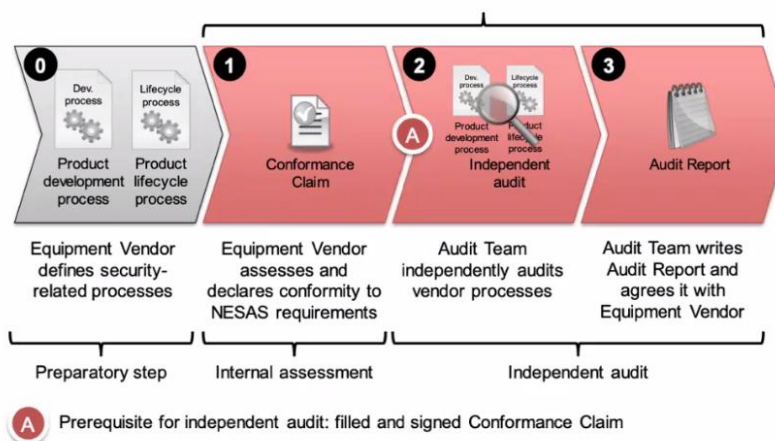


# NESAS audit

- An independent auditor follows the auditing methodology, defined by NESAS, and determines compliance of the Equipment Vendor to the NESAS requirements



© atsec information security, 2021

4

Mute Start video Share

Participants Chat

## The scope of the NESAS audit

- Focused on the Network vendor development and life-cycle process
- The NESAS audit can cover:
  - Different product and product lines
  - Different versions, releases of the product
  - Different tools (configuration management, build tools, etc.)



© atsec Information security, 2021

5



Mute



Start video



Share



Participants



Chat



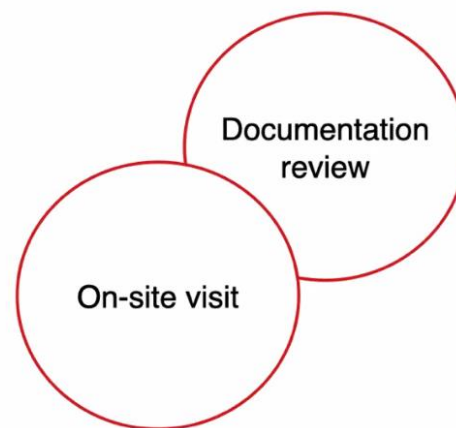
Type here to search





## How NESAS audit is performed?

- NESAS requirement implementation and associated security measures are assessed in terms of
  - coverage
  - effectiveness
  - efficiency
  - application



Mute Start video Share

Participants Chat

Windows taskbar with search bar, task icons, system tray, and date/time (9:22 AM 10/13/2021)

# Schedule

Preparation

Inform GSMA

Documentation review (1)

Intermediate audit result

Documentation review (2)

On-site audit

Audit report



The entire audit needs to be completed in max. 3 months



## On-site audit

- The goal is to verify:
  - If the processes are **actively applied** in the day-to-day business
  - If the Equipment Vendor has the **staff, skills, equipment, working practices and resources** to follow the processes
  - If the staff is **sufficiently trained** on the processes
- NESAS expects an on-site audit period of 4 days under average conditions
- Originally planned to be performed as an on-site activity, due to COVID-19 and travel restrictions performed as a virtual audit



Unmute

Start video

Share



Participants

Chat



## Comparison to other assessment schemes

- Similar to activities performed in CC ALC activities, but focused on the development processes rather than specific version of the TOE
- Two-part assessment approach with separate execution of NESAS audit and Network Equipment evaluation
  - Audit Reports written by auditors are expected to contain relevant information for evaluators
  - Auditors and evaluators may belong to different organisations
- Limited duration of the audit
- No official international recognition
- No certificate







Viewing Monique Bakker SGS...

Layout

Speaking: Monique Bakker SGS Brightsigl

# EUROSMART

The Voice of the Digital Security Industry

## Introducing the methodology and guidance for Secure-SubSystem evaluations using Eurosmart's 3S in SoC PP (PP-0117)

CCUF 2021

Monique Bakker, SGS-Brightsigl, ISCI-WG1 Subgroup Chair  
Markus Hinkelmann, NXP Semiconductors, JHAS Subgroup Chair

**Disclaimer:** This document is provided for internal information purposes only. It does not reflect any opinion or position of EUROSMART.

Unmute

Start video

Share

Smiley

More

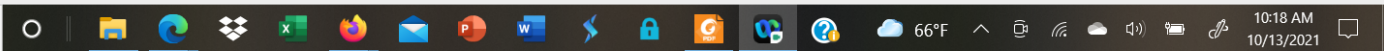


Participants

Chat

More

Type here to search



10:18 AM  
10/13/2021





## Overview

- The trend in modern Systems on Chip (SoC) and Microcontrollers (MCU) is the integration of advanced security functions.
- In particular, the secure element / UICC is being integrated into the SoC
- Main motivations for this integration are reduced system cost, enhanced performance and added-value functionality
- The challenge is lack of a Protection Profile (PP) which defines all aspects of using and protecting the security functions being integrated into the SoC
- Eurosmart took this challenge and established the 3S in SoC PP subgroup for developing this PP

13-Oct-2021

CCUF

2



Unmute

Start video

Share



Participants

Chat



Type here to search



10:19 AM  
10/13/2021

## Overview (cont.)

- Developing and certifying a PP is a starting point
- To allow the use of the PP and perform efficient evaluations, the PP will be accompanied by the publication of a number of guidance/methodology documents:
- To support vulnerability testing of a 3S embedded in a SoC
- To support evaluation of a complex life-cycle model
- Re-use of results gained during the first 3S in SoC during consecutive 3S in SoC evaluation.

13-Oct-2021

CCUF

3



Unmute

Start video

Share



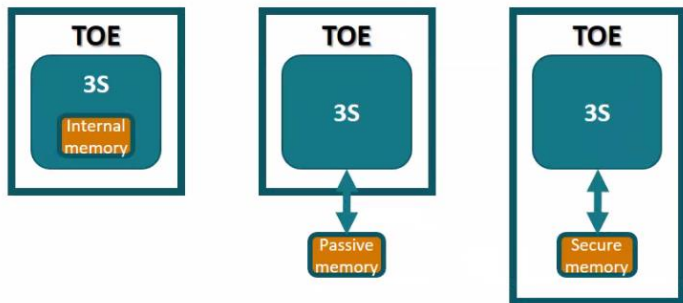
Participants

Chat



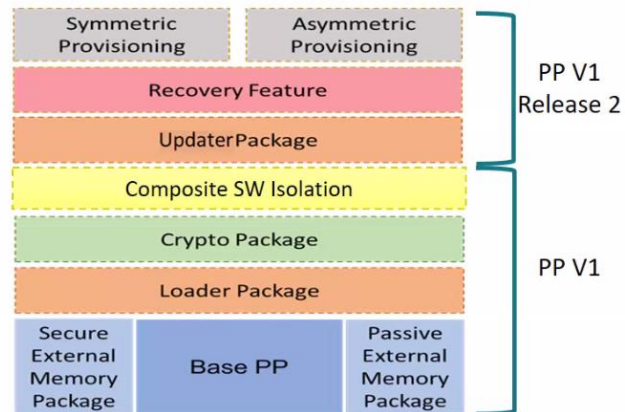
## Security Sub-System in System-on-Chip Protection Profile (PP-0117)

- Three external memory configurations are supported:



- External memory can be volatile and/or non-volatile

- Functional packages:



13-Oct-2021

CCUF

5

Unmute

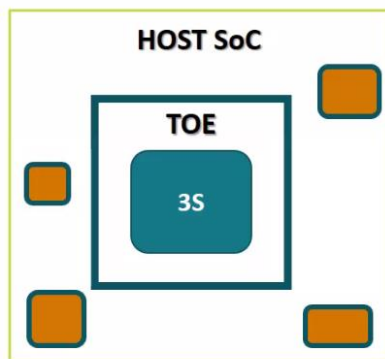
Start video

Share

Participants

Chat

# Security Sub-System in System-on-Chip Protection Profile (PP-0117) vs the Secure IC PP (PP-0084)



- A PP-0117 compliant TOE is tested embedded in its Host SoC.
- A PP-0084 compliant TOE is tested stand alone

13-Oct-2021

CCUF

	Internal Memory	Passive Memory	Secure Memory
T.Leak-Inherent	✓	✓	✓
T.Phys-Probing	✓	✓	✓
T.Malfunction	✓	✓	✓
T.Phys-Manipulation	✓	✓	✓
T.Leak-Forced	✓	✓	✓
T.Abuse-Func	✓	✓	✓
T.RND	✓	✓	✓
T.Insecure-State	✓	✓	✓
T.Mem-Content-Abuse		✓	✓
T.Mem-Clone-Replace		✓	✓
T.Mem-Cmd-Replay		✓	✓
T.Mem-Unauth-Rollback		✓	✓
T.Mem-Abuse-Interface			✓

Threats covered by PP-0084

Additional threats in PP-0117

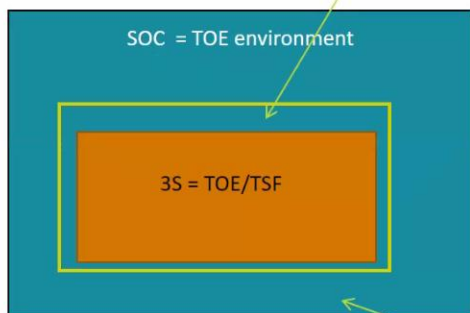


Unmute Start video Share Participants Chat

Windows taskbar with search bar, task icons, system tray, and clock (10:24 AM 10/13/2021)

## The role of integration guidance (I)

Integration Guidance requirements applied by the integrator



Part of development at SoC developer

- The integrator is a user of the TOE but not the end user. The integrator embeds the 3S in the SoC
- The 3S is delivered with integration guidance to the integrator. Integration guidance is seen as part of the TOE
- This guidance does not only contain ALC related requirements, but also:
  - requirements on terminating TSFI,
  - use of capacitors,
  - placement (metal layers), etc.
- in short requirements relevant for the design of the SoC

13-Oct-2021

CCUF

7



Unmute

Start video

Share



Participants

Chat





## Role of integration guidance (2)

- The integration guidance provides requirements that must be followed up by the SoC that embeds the 3S.
- It may cover objectives for the environment specifically applicable for the SoC that must be covered with security measures in the guidance
- The integration guidance must have the 'quality' of end user guidance and therefore is evaluated using the AGD SAR.

13-Oct-2021

CCUF

8



Unmute

Start video

Share



Participants

Chat



Type here to search



10:26 AM  
10/13/2021

## Role of integration guidance (3)

- The solution chosen by the SoC developer may have an impact on Self-protection and non-bypassability properties of the 3S
- As a result the ADV\_ARC is extended with a rationale explaining in what way the integration guidance is followed up.
- The evaluator will examine this rationale and possibly also request to investigate parts of the implementation representation of the SoC

13-Oct-2021

CCUF

9



Unmute

Start video

Share



Participants

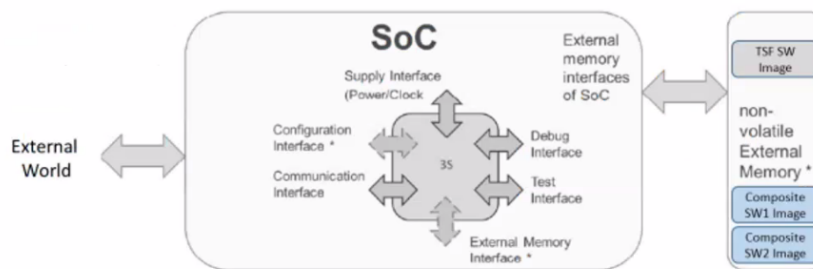
Chat





## ADV ARC Security Architecture update (JIL interpretation)

- To cover the rationale for the integration guidance
- Cover new properties as result of use of external memories for
  - self-protection,
  - domain separation,
  - initialization
  - non-bypassability



*Relevant for AVA\_VAN.5*

13-Oct-2021

CCUF

10




Unmute Start video Share

Participants Chat

Viewing Robert Hörr (Guest)...

Speaking: Mike Grimm (Guest)


Layout




**MAGENTA SECURITY**

# MODERN SOFTWARE TESTING WITH OUR NEW APPROACH: *FAST*


Author: Robert Hörr (robert.hoerr@t-systems.com)  
Job: Penetration Tester & Security Evaluator & Security Administrator



ERLEBEN, WAS VERBINDET.



## DEUTSCHE TELEKOM SECURITY GMBH



Participants Chat

Viewing Robert Hörr (Guest)...

## WHAT ARE THE TESTS REQUIREMENTS?

Goal: To detect „all“ errors (known, unknown) on all „paths“ efficiently

- **Executer (*Path finder*)**
  - To execute all „paths“
  - Tests (QoS)
  - Metric
  - Open source
- **Efficiency (*Scalability*)**
  - Costs
  - Think like a Hacker
  - Automation
  - Tests (QoS)
  - Source source
  - Metric
- **Execution auditor (*Path discoverer*)**
  - All „paths“ are executed?
  - Feedback
  - Tests (QoS)
  - Open source
  - Metric
- **Error detection (*Error discoverer*)**
  - To detect „all“ errors
  - Tests (QoS)
  - Reproducibility
  - Open source
  - Metric



6



Unmute

Start video

Share



Participants

Chat



Type here to search

10:52 AM  
10/13/2021

## WHAT IS MODERN TESTING?

- **Information level**
  - Blackbox
  - Whitebox (Open Source, EAL4+)
  - Greybox
- **Testing methods**
  - Dynamic (execution)
    - Mutator (path finder)
    - Code coverage (path discoverer)
    - AddressSanitizer (error discoverer)
  - Static (no execution)
    - Review
    - Source code analysis
  - Combination
- **Test levels (V - model)**
  - Unit tests
  - Integration tests
  - System tests
  - Public API tests (external interfaces)
- **Test execution**
  - Automatically (parallel)
  - Manually
  - Combination
- **Test metrics**
  - Lines of code
  - Cyclomatic complexity (CyCo)
  - Code coverage (CoCo)
  - Executions per second



7



Unmute Start video Share

Participants Chat

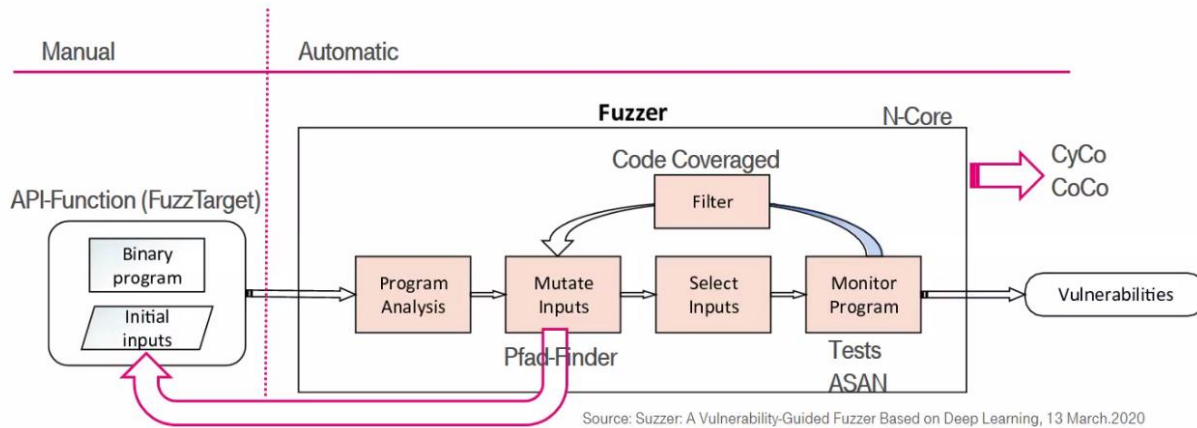
Type here to search



10:53 AM  
10/13/2021

# WHAT IS MODERN TESTING?

Goal: To detect „all“ errors (known, unknown) on all „paths“ efficiently



Speaking: Robert Hörr (Guest)



8

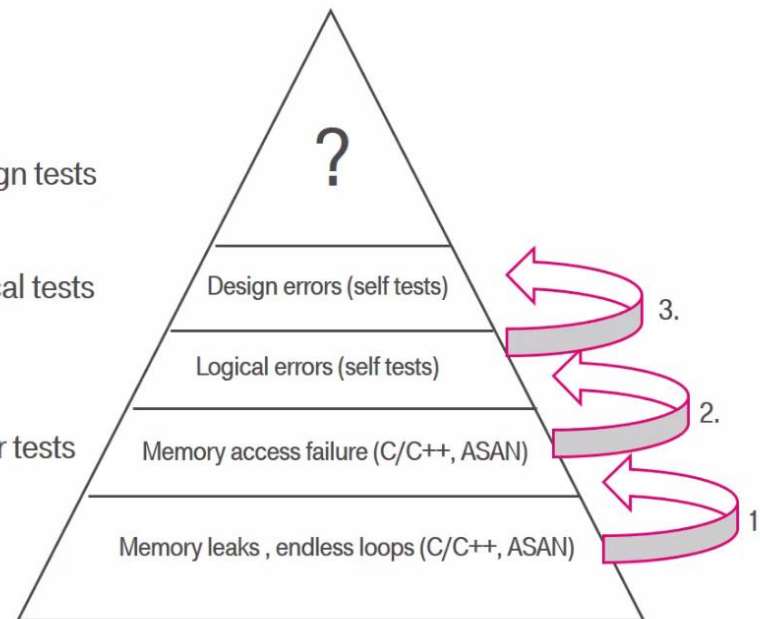


Unmute Start video Share Participants Chat

Windows taskbar with search bar, task icons, and system tray (67°F, 10:56 AM 10/13/2021)

## WHAT IS MODERN TESTING?

- **Strategy:**
  - Bottom up
  - Discovered error : wait for fix
  - „Zero Bug Policy“
- **Logical errors:**
  - Must be fixed to perform design tests
- **Memory access failure:**
  - Must be fixed to perform logical tests
- **Memory leaks:**
  - Costs RAM (stopped testing)
  - Must be fixed to perform other tests



T...

12

Speaking: Robert Hörr (Guest)

Unmute

Start video

Share

...



Participants

Chat

...

Type here to search

Taskbar icons: File Explorer, Edge, Teams, Excel, Firefox, Mail, PowerPoint, Word, OneDrive, Outlook, Settings, Network, Volume, Battery, 67°F, 11:00 AM 10/13/2021



## TEST-METRIC: EXECUTIONS PER SECOND

- Goal: To detect „all“ errors on all „paths“ efficiently
- Test execution: M x test iterations
  - Mutator
  - API execution
  - Self tests
- Test performance:
  - Test iterations per second
    - Min: 500 execs/sec per core
  - Parallelization of the test execution
    - No dependencies between test iterations
    - N x Cores => N x 500 execs/s (linear scaling)
    - e.g. 100 cores, one month running time => 120.960.000.000 execs (total)
    - Costs: 1000 Euro per month



15



Speaking: Robert Hörr (Guest)

Unmute

Start video

Share



Participants

Chat



Type here to search



11:03 AM  
10/13/2021

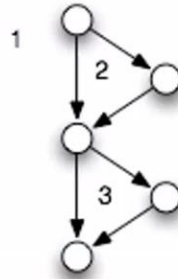


## TEST-METRICS: CYCO AND COCO

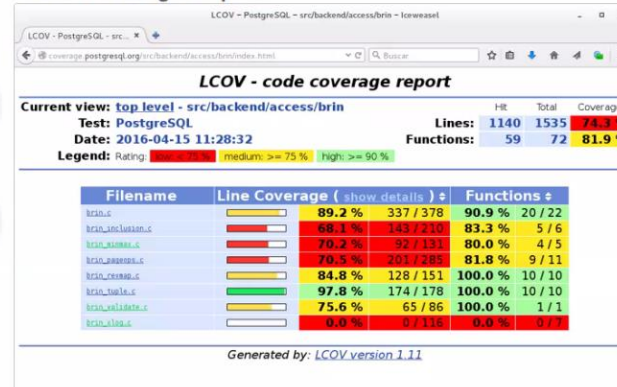
- Cyclomatic complexity (CyCo)
  - Number of independent execution paths, e.g. CyCo = 30
- Code coverage (CoCo)
  - Number of executed independent execution paths, e.g. CoCo = 30%

CyCo = 3

```
def my_method (x, y)
  r = x
  if x > 5
    r = 5
  end
  if y < 5
    r = y
  end
  r
end
```



### Code Coverage Report



16



Unmute Start video Share

Participants Chat

Viewing Kwangwoo Lee (Gue...

Layout

## Specification-based approach

## Attack-based approach

Speaking: Kwangwoo Lee (Guest) (Cohost)

Keywords: exact conformance, direct rationale PPs, TOE-specific evaluation methods

Keywords: strict/demonstrable conformance, EALs, TOE type-specific evaluation methods

All evaluated TOEs are compliant to a given list of requirements: nothing more and nothing less

All evaluated TOEs are protected against a given set of threats

All tests are set and known beforehand

The attacker strength is set and known beforehand; the tests themselves may be fine-tuned (penetration testing)

Unmute

Start video

Share

😊

⋮

✖

Participants

Chat

⋮



Webex Meeting Info Meeting Info Hide Menu Bar ^

File Edit Share View Audio & Video Participant Meeting Help

Connected

PWG Chair Me Kwangwoo Lee Cohost Mike Grimm Cohost Brian Wood Cohost NL\_Rob Huisman [JP] Toru Hashimoto

Layout

Viewing Kwangwoo Lee (Gue...)

# What is new in the ISO 4<sup>th</sup> Edition? (1/2)

- Input from stakeholders for the 21<sup>st</sup> Century
  - ~~Terms and definitions consolidated, reviewed and revised~~
  - Security evaluation approaches allowing both:
    - Specification-based : Exact Conformance added
    - Attack-based : "Traditional EAL approach"
  - Addition of modularity and composition techniques to the model
  - Enhanced specification for packages
  - Updated Security Policy definition
  - Updated to include state-of-the art for the highest levels of evaluation (EAL 6 and EAL 7)

4<sup>th</sup> Ed transition Guidance describing the changes more fully is in ISO/IEC 22216

Unmute Start video Share

Participants Chat

Type here to search

9:21 AM 10/14/2021

# What is new in the ISO 4<sup>th</sup> Edition? (2/2)

Speaking: Kwangwoo Lee (Guest) (CoHost)

- The general model has been significantly revised (Part 1)
- New & changed security functional requirements (Part 2)
- Updated security assurance requirements (Part 3)
- Adds support in developing evaluation methodologies for specific technologies/product types (New part 4)
- All pre-defined packages of assurance packages moved to a (new) part 5
  - For example this is where the evaluation assurance level (EALs) are now found
  - (To facilitate use by scheme/MRA policies)
- Updated the common evaluation methodology (ISO/IEC 18045 aka “CEM”)



4<sup>th</sup> Ed transition Guidance describing the changes more fully is in ISO/IEC 22216



Unmute

Start video

Share



Participants

Chat



# Progress with the 4<sup>th</sup> Edition



> Expand panel to show video

- Draft International Standard (DIS) ballots completed
  - 27 nations approved. 5 nations had mostly editorial comments
- The Final Draft International Standard (FDIS) stage where nations indicate their Final Approval before publishing was initiated and approved by SC 27.
- The standards are expected be published before the end of 2021(?).

### WG Recommendation 19. Document for 1st FDIS

ISO/IEC JTC 1/SC 27/WG 3 resolves to request the SC 27 Secretariat to register the following documents as 1<sup>st</sup> FDIS to circulate for balloting.

Document	Project	Title
WG 3 N1958	15408-1	Evaluation criteria for IT security – Part 1: Vocabulary, introduction and general model #
WG 3 N1959	15408-2	Evaluation criteria for IT security – Part 2: Security functional components
WG 3 N1960	15408-3	Evaluation criteria for IT security – Part 3: Security assurance components
WG 3 N1961	15408-4	Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities
WG 3 N1962	15408-5	Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements
WG 3 N1963	18045	Methodology for IT security evaluation

# Subject to approval of WG Recommendation 13

Began	2017
Working Drafts (2)	2017
Committee Drafts (3)	2018-2019
Draft International Standard	2020 Spring
Final Draft International Standard	2021 Spring
Publish	2021 (?)



Unmute Start video Share

Participants Chat

Windows taskbar with search bar, icons for File Explorer, Edge, Teams, Word, PowerPoint, and system tray showing 63°F and date 10/14/2021.