Assessing Security Levels & Functional Interoperability

Cybersecurity Vehicle Forum

May 2025

WEI YUAN

PUBLIC

AGENDA

00

Context

01

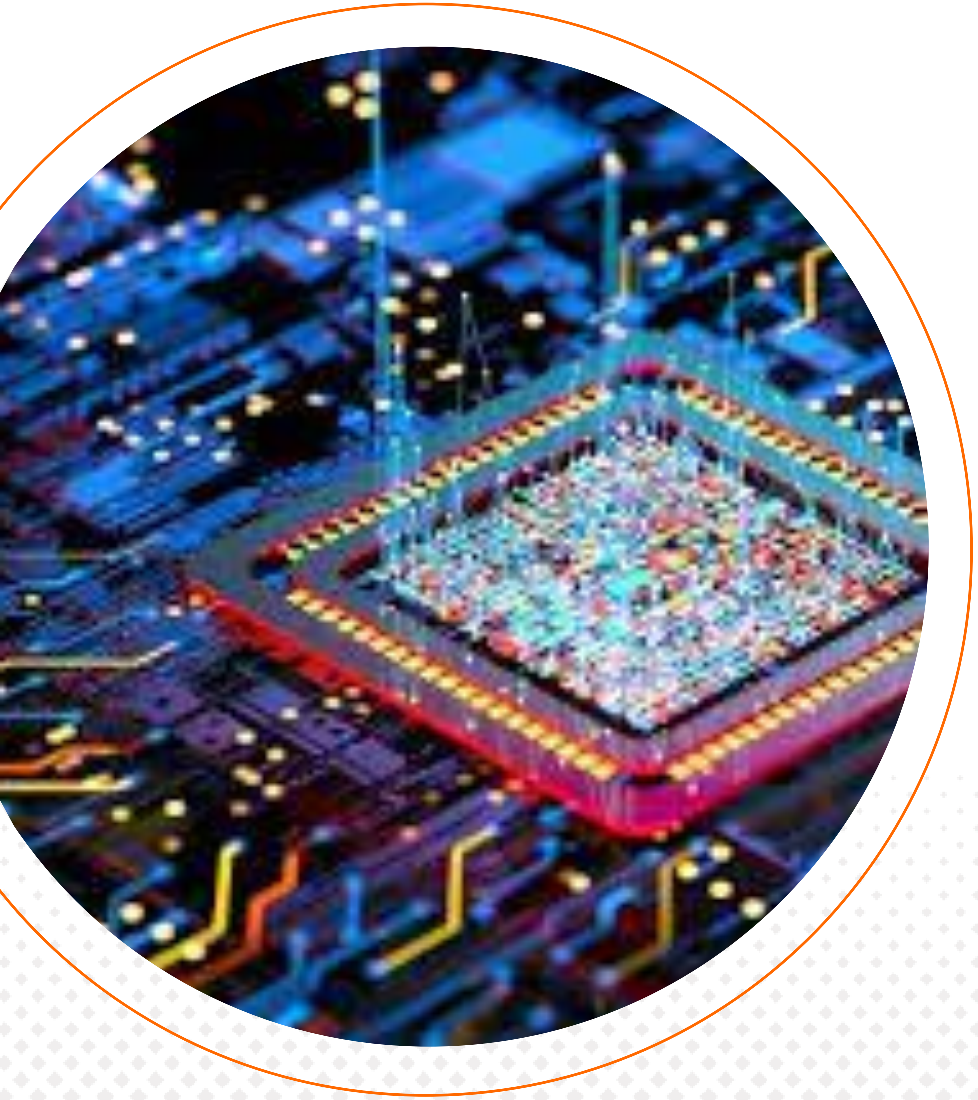
Attack Potential & Attack Methods

02

SESIP Assurance Levels & Protection Profiles

03

Final thoughts



Context

Automotive Security Today

Growth of Connected Vehicles

The number of connected vehicles is rapidly increasing.

Projections indicate that over **327 million connected vehicles will be in service by 2027**, encompassing advanced mobility platforms such as autonomous vehicles and electric vertical take-off and landing vehicles.

This surge significantly **expands the number of vehicle endpoints exposed** to potential cyberattacks.

Expanded Attack Surfaces

Modern vehicles integrate numerous electronic control units (ECUs) and communication interfaces, including Bluetooth, Wi-Fi, and cellular networks. This complexity introduces multiple potential entry points for cyberattacks.

•**Infotainment systems**: Vulnerable to control override and injection attacks.

•**Telematics units**: Susceptible to unauthorized remote access.

•**On-Board Diagnostics (OBD-II) ports**: Can be exploited for direct access to vehicle networks.

⚠ Escalating Cybersecurity Challenges

The automotive industry faces significant cybersecurity threats, including **compromised safety, privacy breaches, financial losses, and reputational damage**.

Automotive cybersecurity market is projected to grow from **$3.9 billion in 2023 to $5.9 billion by 2025**, reflecting the industry's response to these escalating threats.

Automotive Cybersecurity from a different view

ENISA's Attack Methodology

- EUCC Scheme and CC evaluation methodology.
- Experience in Technical Domains for SCSD and HWSB.
- Set of State of the Art (SoTA) documentation.

SESIP Methodology and Protection Profiles

- Pragmatic (and industry friendly) view of CC
- Granularity to reinforce Composition and Reusability
- Compliance demonstration (with requirements mappings) against industry proposals.

enisa

EUROPEAN UNION
CYBERSECURITY
CERTIFICATION

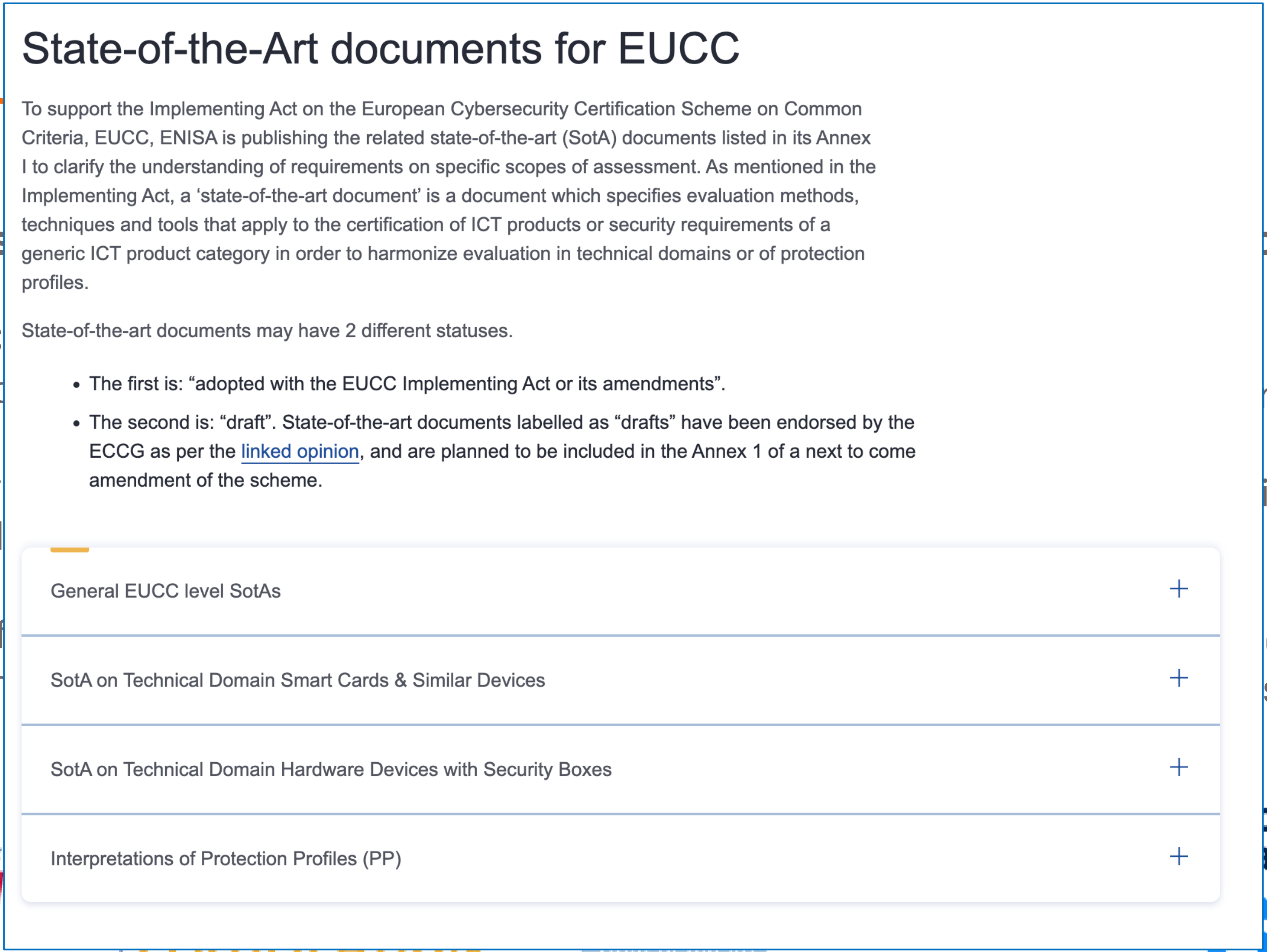
EUCC
State-of-the-Art

GlobalPlatform™
SESIP

Autom

ENISA's ogy and Protection

- EUCC ndustry friendly) view of CC metho
- Exper inforce Composition and and H
- Set of onstration (with requirements docur st industry proposals.



State-of-the-Art documents for EUCC

To support the Implementing Act on the European Cybersecurity Certification Scheme on Common Criteria, EUCC, ENISA is publishing the related state-of-the-art (SotA) documents listed in its Annex I to clarify the understanding of requirements on specific scopes of assessment. As mentioned in the Implementing Act, a 'state-of-the-art document' is a document which specifies evaluation methods, techniques and tools that apply to the certification of ICT products or security requirements of a generic ICT product category in order to harmonize evaluation in technical domains or of protection profiles.

State-of-the-art documents may have 2 different statuses.

- The first is: "adopted with the EUCC Implementing Act or its amendments".
- The second is: "draft". State-of-the-art documents labelled as "drafts" have been endorsed by the ECCG as per the linked opinion, and are planned to be included in the Annex 1 of a next to come amendment of the scheme.

General EUCC level SotAs +

SotA on Technical Domain Smart Cards & Similar Devices +

SotA on Technical Domain Hardware Devices with Security Boxes +

Interpretations of Protection Profiles (PP) +

https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

Automotive Cybersecurity from a different view

ENISA's Attack Methodology

- EUCC Scheme and CC evaluation methodology.
- Experience in Technical Domains for SCSD and HWSB.
- Set of State of the Art (SoTA) documentation.

SESIP Methodology and Protection Profiles

- Pragmatic (and industry friendly) view of CC
- Granularity to reinforce Composition and Reusability
- Compliance demonstration (with requirements mappings) against industry proposals.

Automotive Cybersecurity from a different view

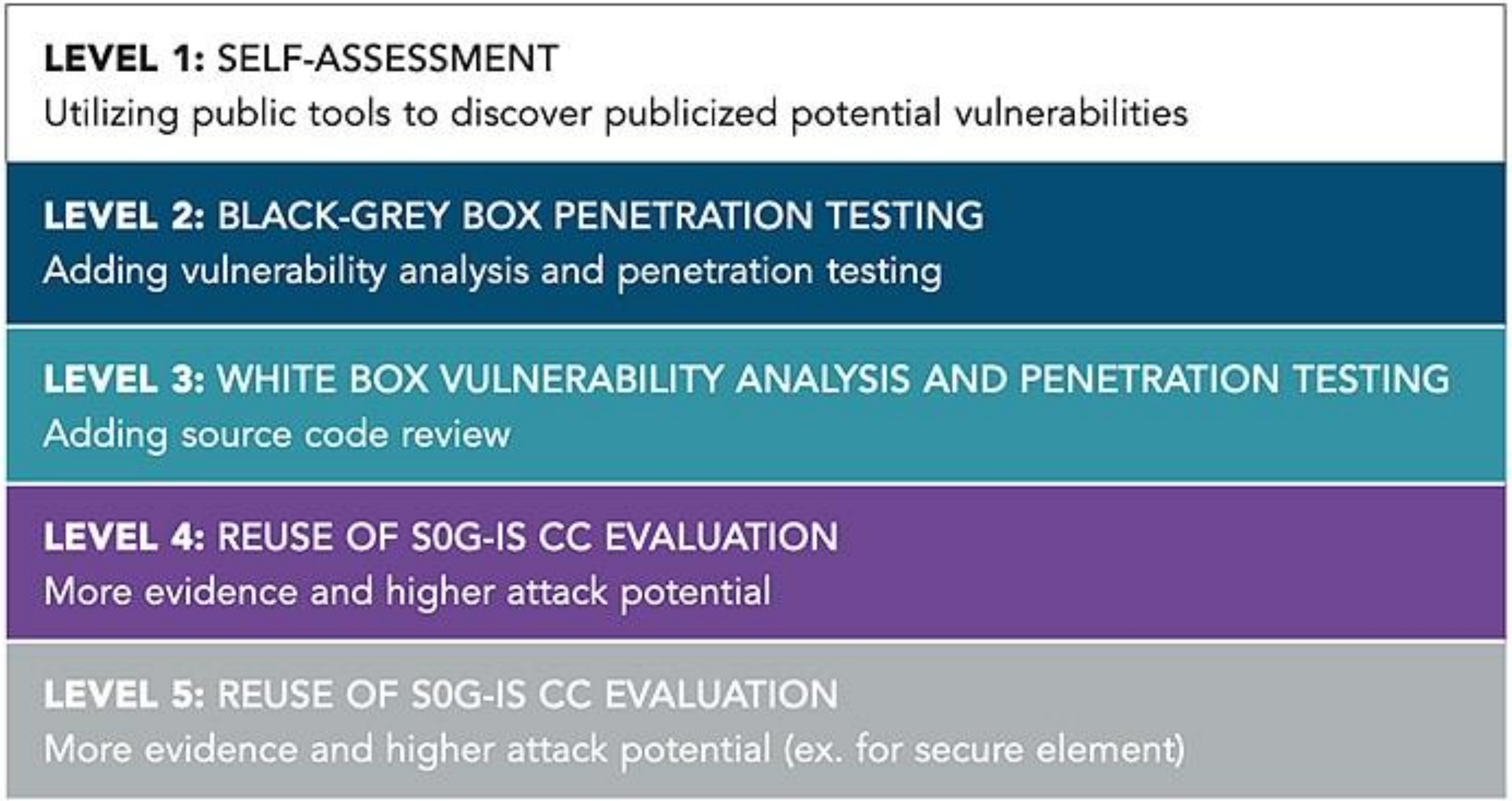
ENISA's Attack … on

- EUCC Scheme a… methodology.
- Experience in T… and HWSB.
- Set of State of … documentation.

…w of CC

… and

…uirements … ls.



LEVEL 1: SELF-ASSESSMENT
Utilizing public tools to discover publicized potential vulnerabilities

LEVEL 2: BLACK-GREY BOX PENETRATION TESTING
Adding vulnerability analysis and penetration testing

LEVEL 3: WHITE BOX VULNERABILITY ANALYSIS AND PENETRATION TESTING
Adding source code review

LEVEL 4: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential

LEVEL 5: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential (ex. for secure element)

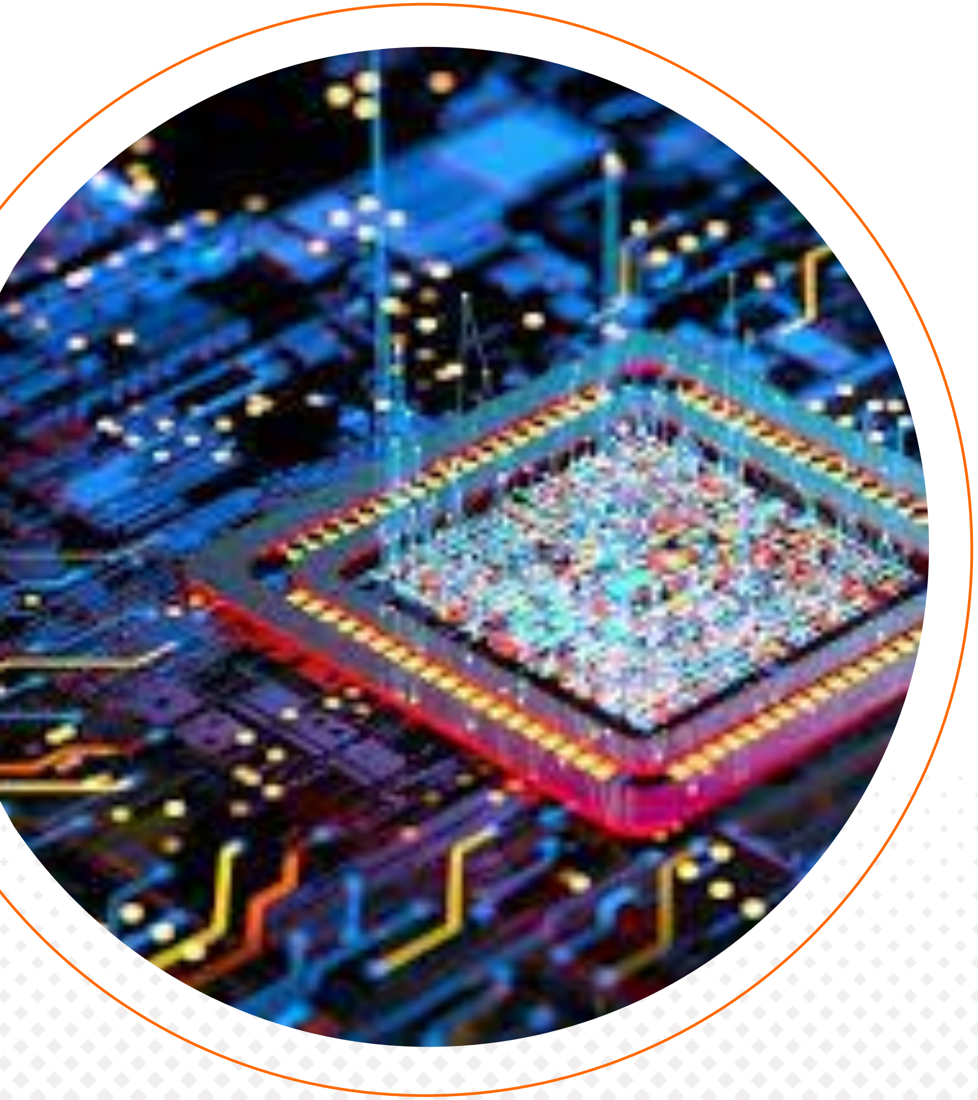
https://www.nxp.com/company/about-nxp/smarter-world-blog/BL-SESIP-SYSTEM

enisa

EU CY… CERTIFICATION

State-of-the-Art

SESIP



Attack Potential & Attack Methods

Applus+ experience on automotive penetration testing

Traditional pentest request:

- Typically, **software attacks methods in scope**
- Sometimes, **hardware attacks methods considered in TARAs**, but removed from scope
- **Very Limited budget** without priorization of attack vectors

Broken Access Control

Code Injection

Fuzzing

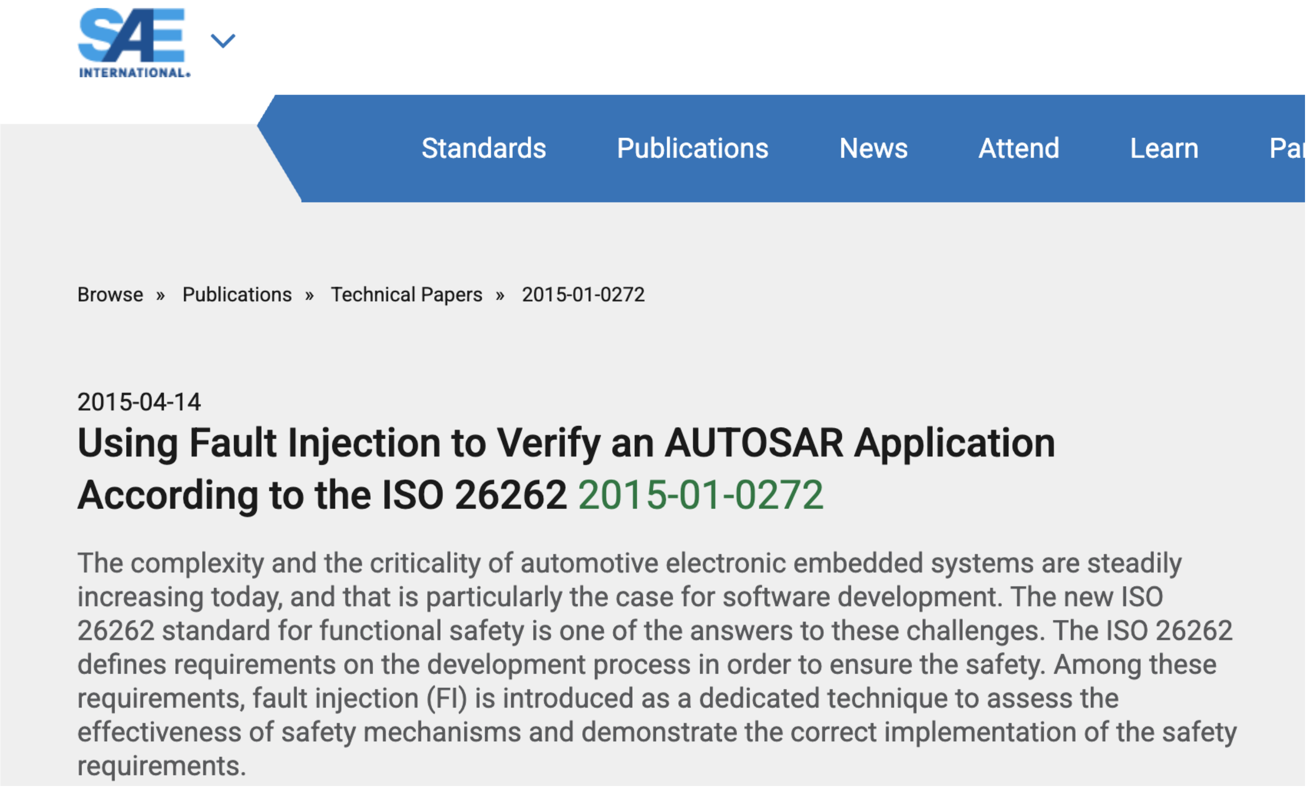
Cryptographic Failures

Vulnerable and Outdated Components

Security Misconfiguration

Code Review

Applus+ experience on automotive penetration testing

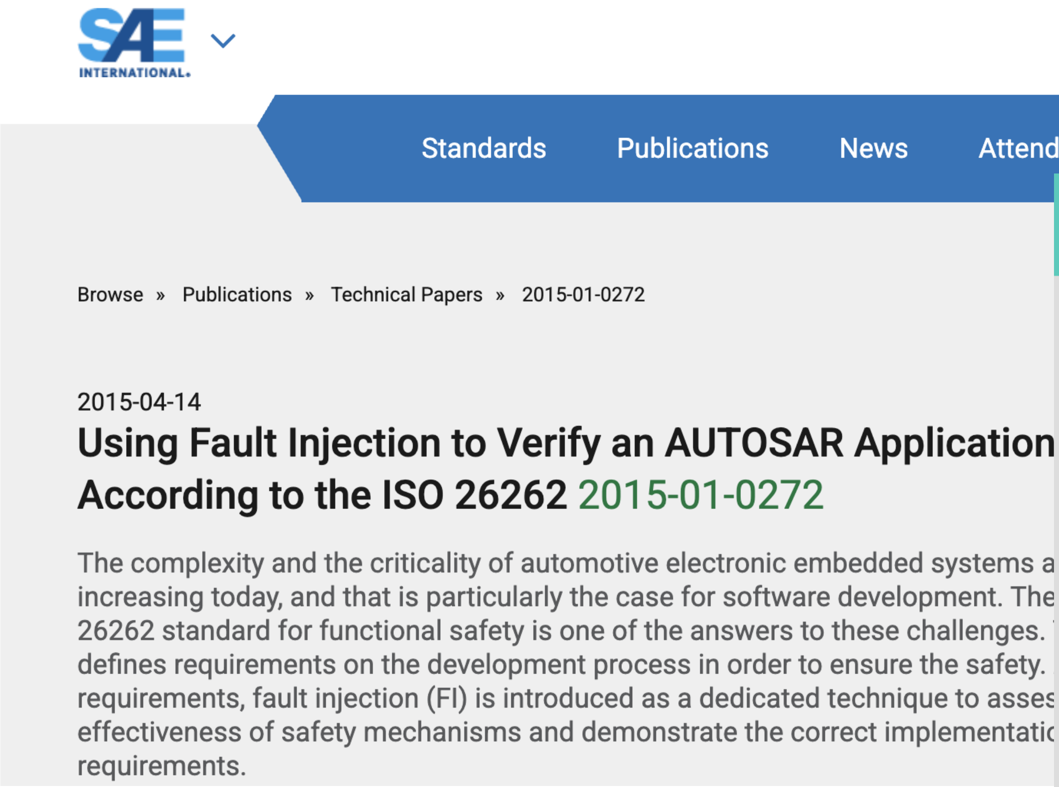


2015-04-14

Using Fault Injection to Verify an AUTOSAR Application According to the ISO 26262 2015-01-0272

The complexity and the criticality of automotive electronic embedded systems are steadily increasing today, and that is particularly the case for software development. The new ISO 26262 standard for functional safety is one of the answers to these challenges. The ISO 26262 defines requirements on the development process in order to ensure the safety. Among these requirements, fault injection (FI) is introduced as a dedicated technique to assess the effectiveness of safety mechanisms and demonstrate the correct implementation of the safety requirements.

Applus+ experience on automotive penetration testing

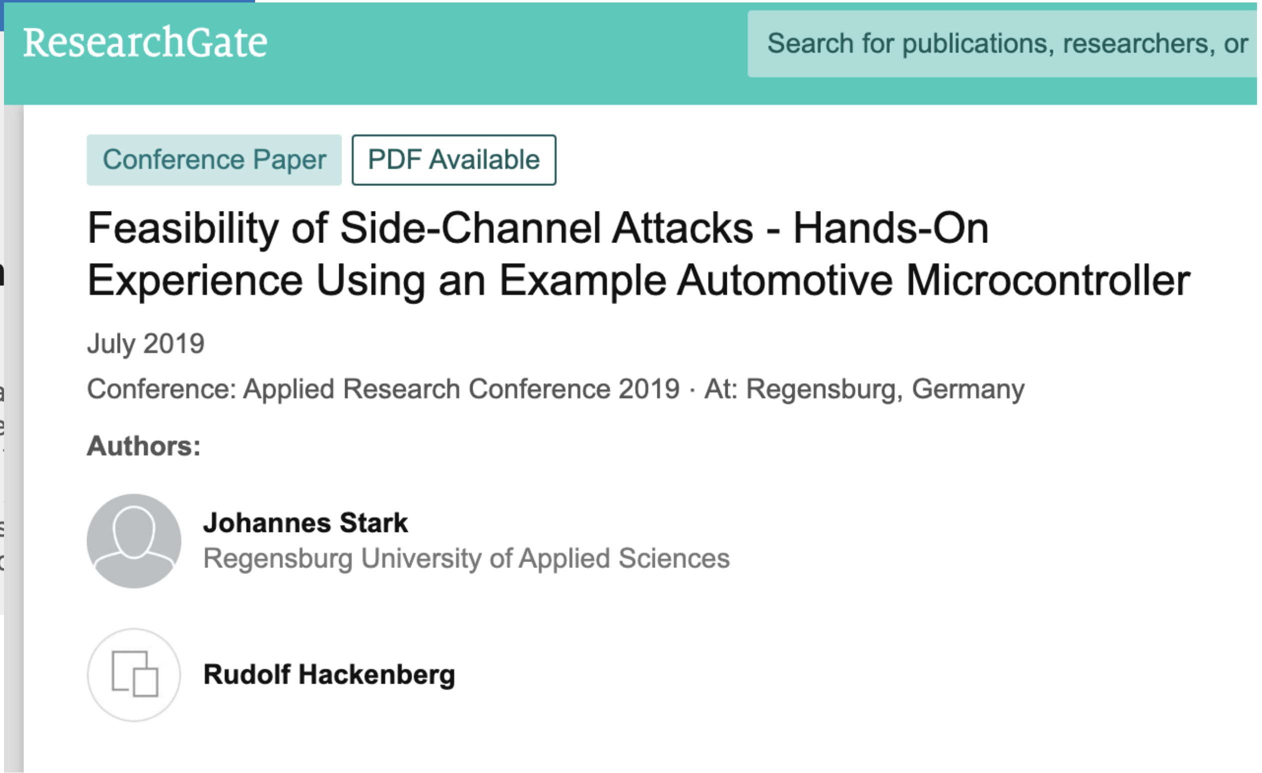


Browse » Publications » Technical Papers » 2015-01-0272

2015-04-14

Using Fault Injection to Verify an AUTOSAR Application According to the ISO 26262 2015-01-0272

The complexity and the criticality of automotive electronic embedded systems a increasing today, and that is particularly the case for software development. The 26262 standard for functional safety is one of the answers to these challenges. defines requirements on the development process in order to ensure the safety. requirements, fault injection (FI) is introduced as a dedicated technique to asses effectiveness of safety mechanisms and demonstrate the correct implementatic requirements.



Feasibility of Side-Channel Attacks - Hands-On Experience Using an Example Automotive Microcontroller

July 2019

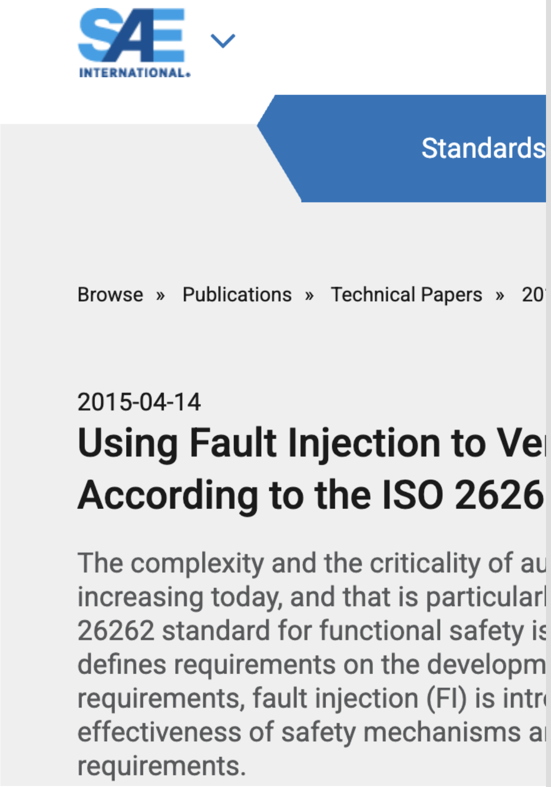
Conference: Applied Research Conference 2019 · At: Regensburg, Germany

Authors:

Johannes Stark
Regensburg University of Applied Sciences

Rudolf Hackenberg

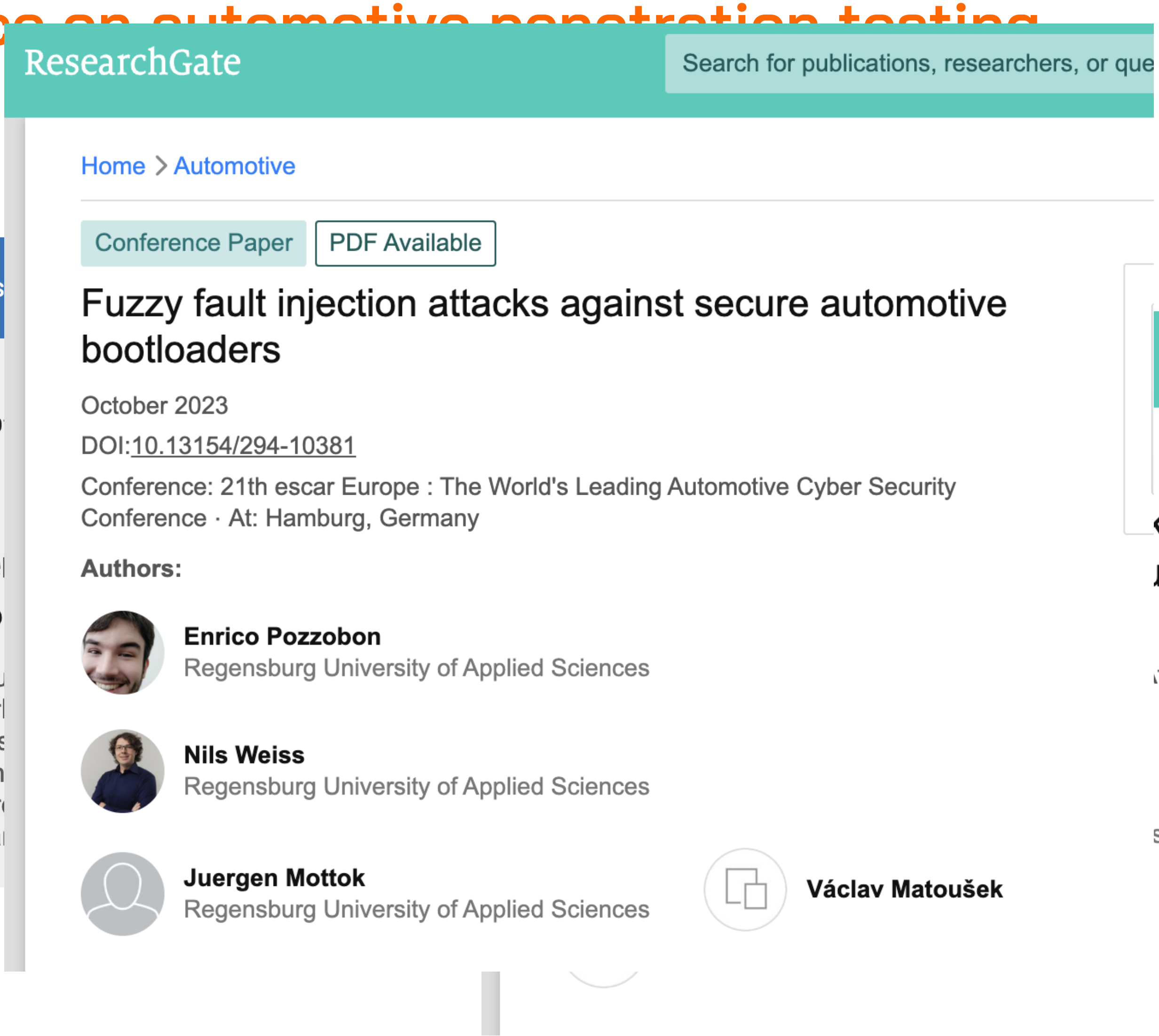
Applus+ experience on automotive penetration testing



2015-04-14

Using Fault Injection to Ve
According to the ISO 2626

The complexity and the criticality of au
increasing today, and that is particularl
26262 standard for functional safety is
defines requirements on the developm
requirements, fault injection (FI) is intr
effectiveness of safety mechanisms a
requirements.



Fuzzy fault injection attacks against secure automotive bootloaders

October 2023

DOI:10.13154/294-10381

Conference: 21th escar Europe : The World's Leading Automotive Cyber Security Conference · At: Hamburg, Germany

Authors:

Enrico Pozzobon
Regensburg University of Applied Sciences

Nils Weiss
Regensburg University of Applied Sciences

Juergen Mottok
Regensburg University of Applied Sciences

Václav Matoušek

‹s - Hands-On
ıtomotive Microcontroller

ıt: Regensburg, Germany

s

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Hardware Security Boxes and Automotive Parallels:

- Hardware security boxes and ECUs **share attack exposure definition**.
- ENISA attack potential model is mature and effective

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

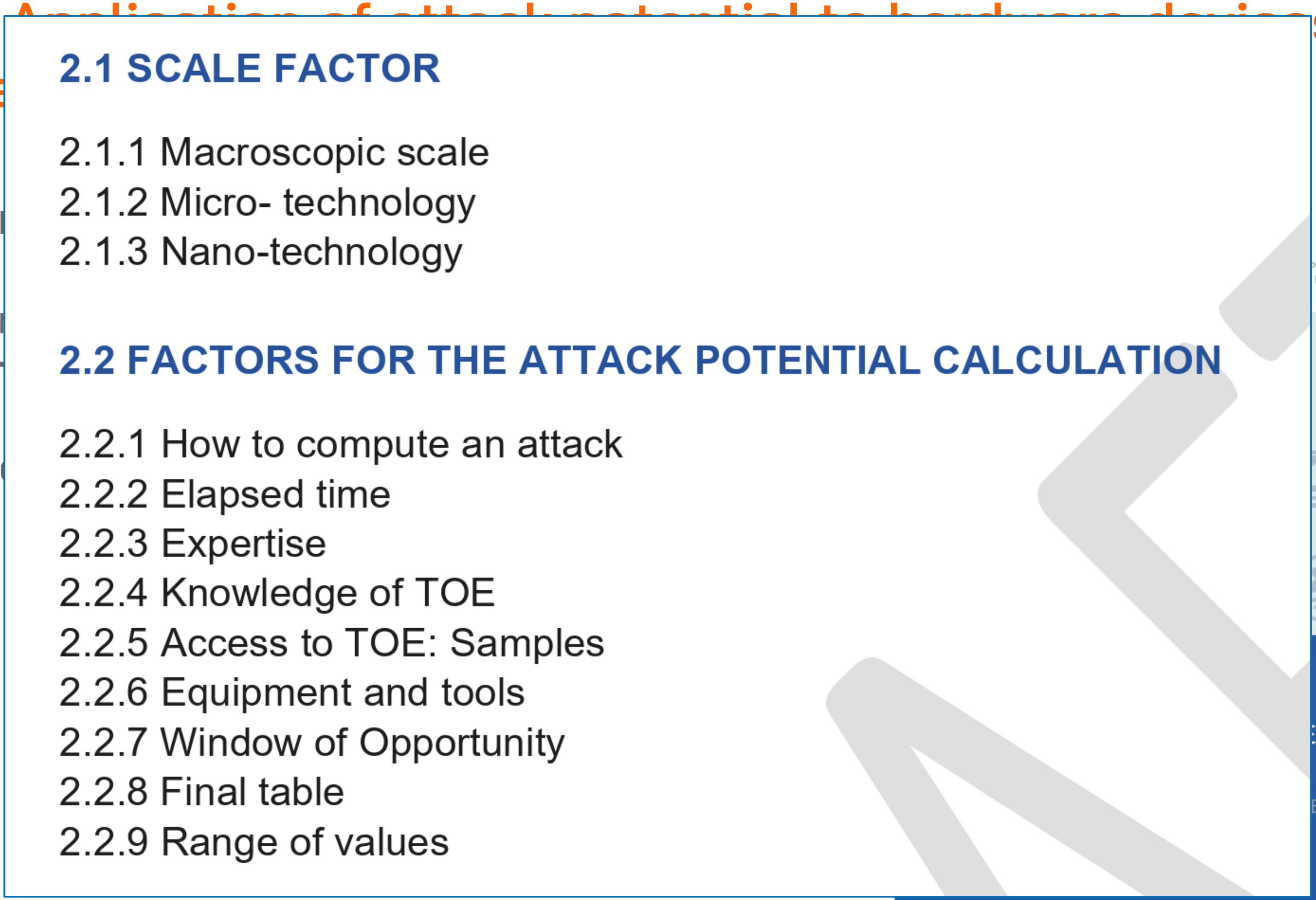
APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES

Version 2, February 2025

ENISA SoTA: s with security boxe

Hardware Secu

- Hardware secu **exposure defi**
- ENISA attack p

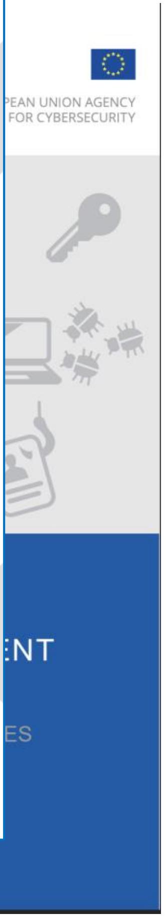


2.1 SCALE FACTOR

2.1.1 Macroscopic scale
2.1.2 Micro- technology
2.1.3 Nano-technology

2.2 FACTORS FOR THE ATTACK POTENTIAL CALCULATION

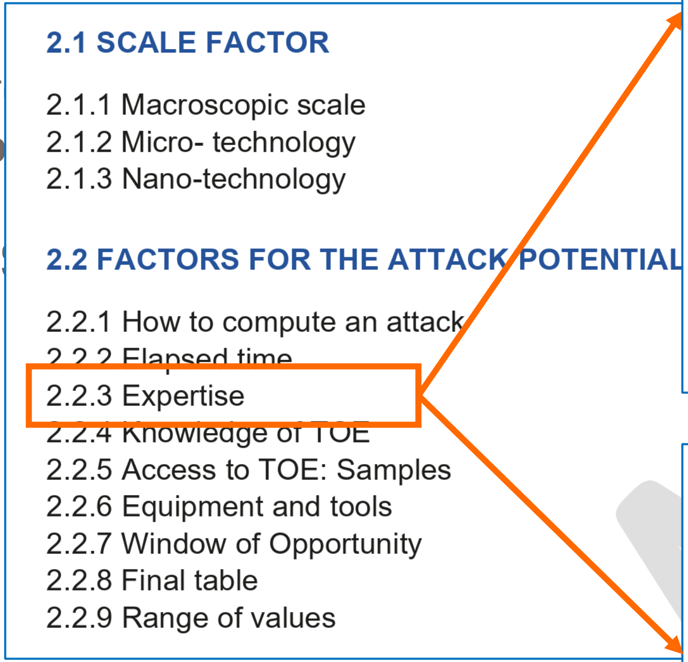
2.2.1 How to compute an attack
2.2.2 Elapsed time
2.2.3 Expertise
2.2.4 Knowledge of TOE
2.2.5 Access to TOE: Samples
2.2.6 Equipment and tools
2.2.7 Window of Opportunity
2.2.8 Final table
2.2.9 Range of values

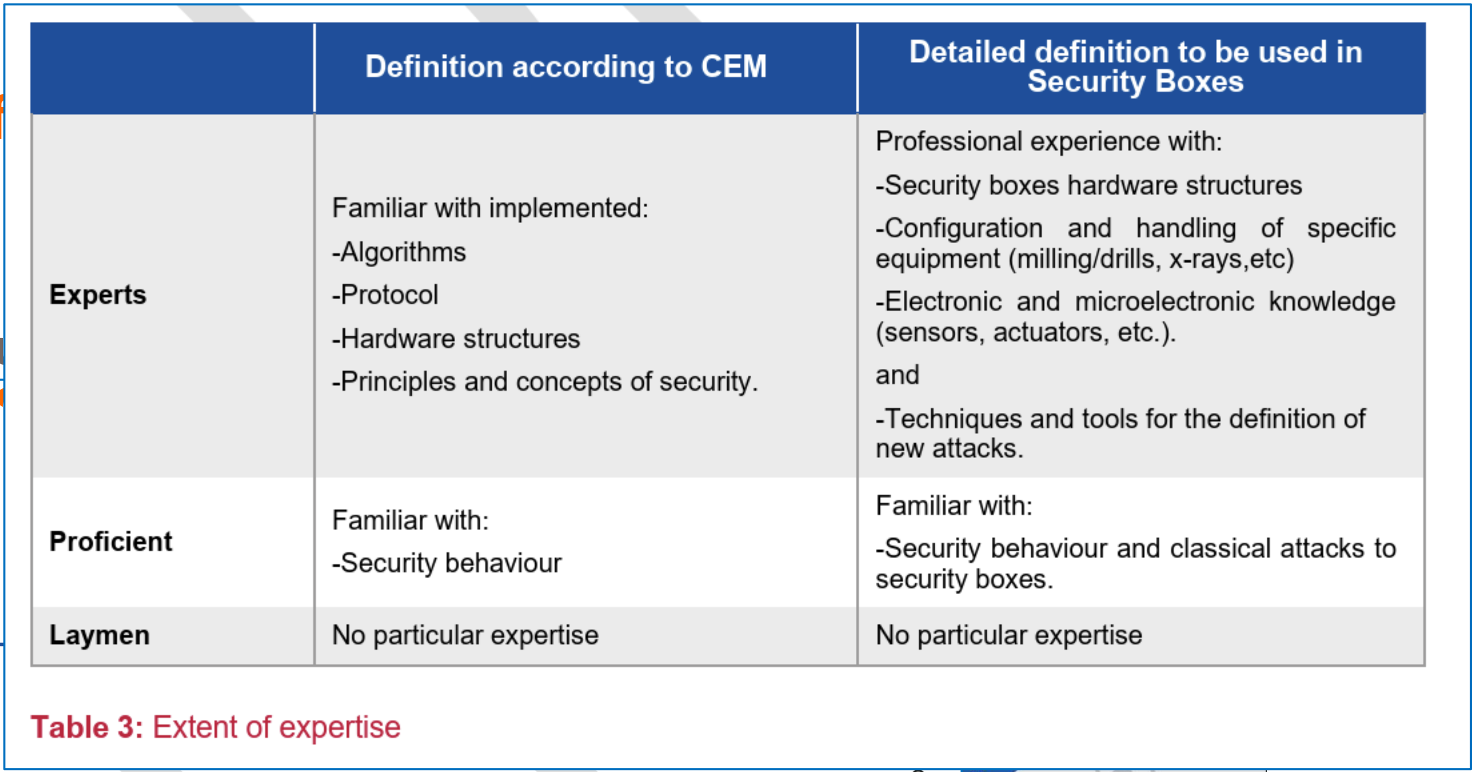


ENISA SoTA: Application of security boxes (HWSB)

Hardware Security Boxes and Au

- Har exp
- ENI





	Definition according to CEM	Detailed definition to be used in Security Boxes
Experts	Familiar with implemented: -Algorithms -Protocol -Hardware structures -Principles and concepts of security.	Professional experience with: -Security boxes hardware structures -Configuration and handling of specific equipment (milling/drills, x-rays,etc) -Electronic and microelectronic knowledge (sensors, actuators, etc.). and -Techniques and tools for the definition of new attacks.
Proficient	Familiar with: -Security behaviour	Familiar with: -Security behaviour and classical attacks to security boxes.
Laymen	No particular expertise	No particular expertise

Table 3: Extent of expertise

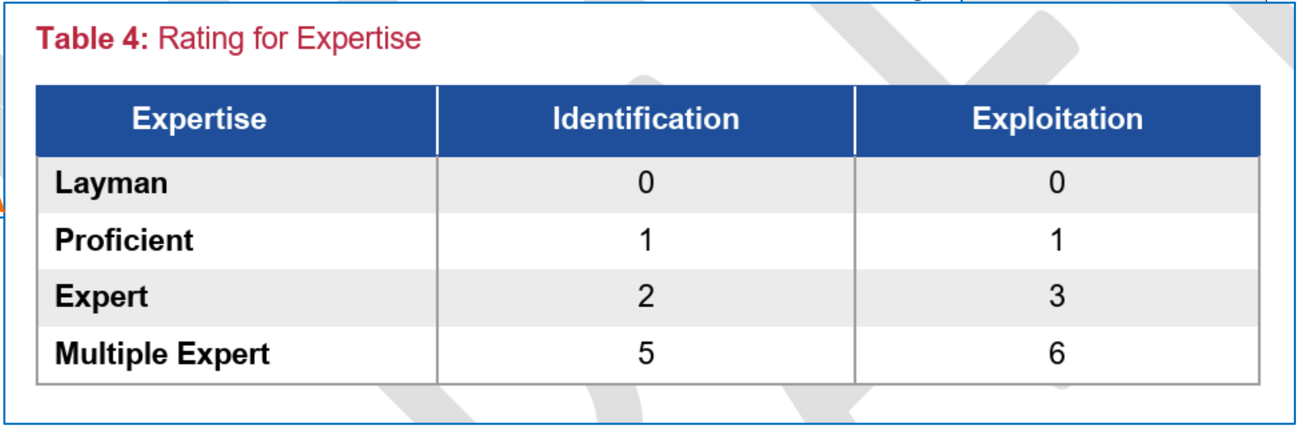


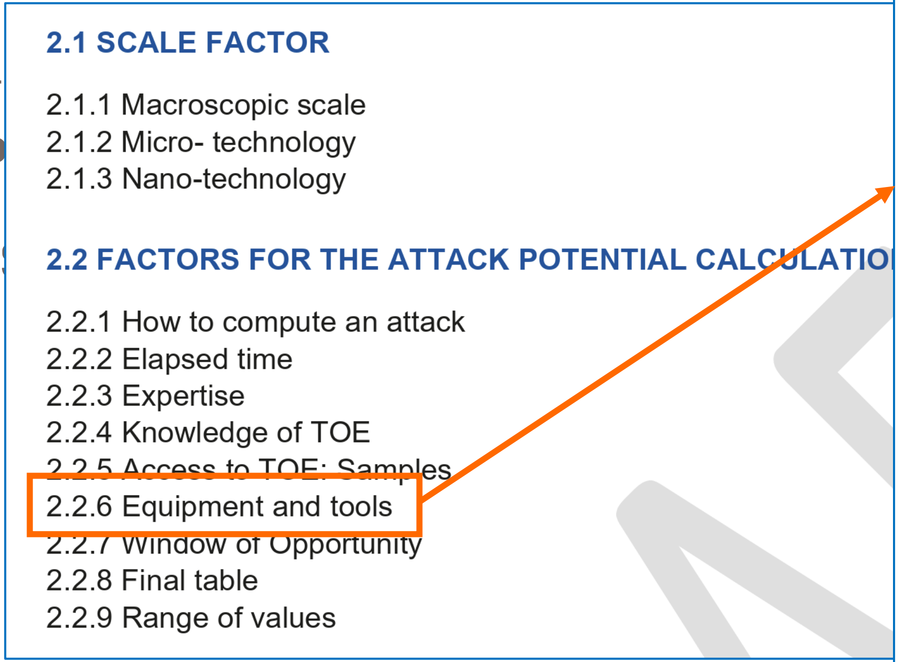
Table 4: Rating for Expertise

Expertise	Identification	Exploitation
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6

ENISA SoTA: Application of attack n security boxes (HWSB)

Hardware Security Boxes and Automotiv

- Har exp
- ENI

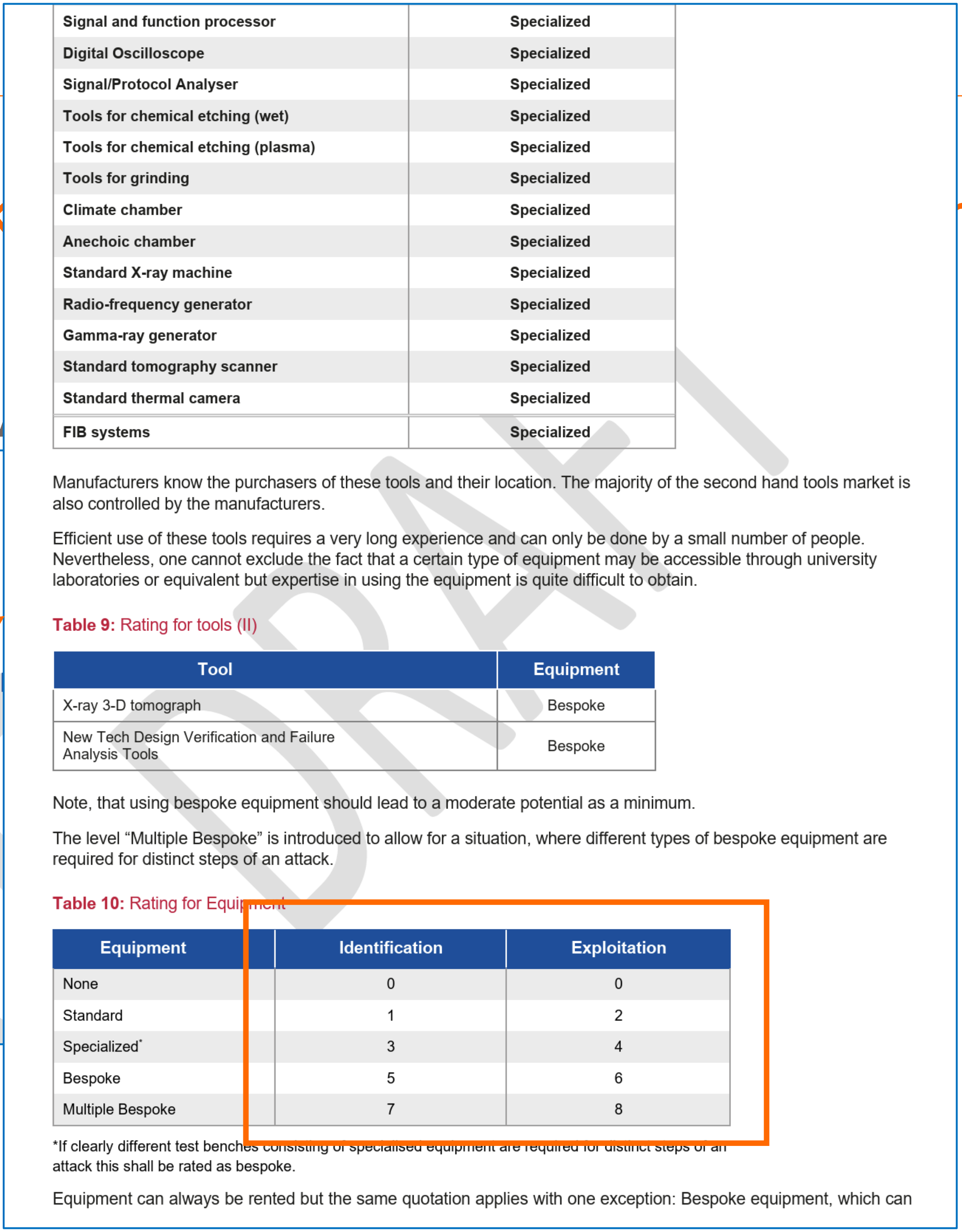


2.1 SCALE FACTOR

2.1.1 Macroscopic scale
2.1.2 Micro- technology
2.1.3 Nano-technology

2.2 FACTORS FOR THE ATTACK POTENTIAL CALCULATIO

2.2.1 How to compute an attack
2.2.2 Elapsed time
2.2.3 Expertise
2.2.4 Knowledge of TOE
2.2.5 Access to TOE: Samples
2.2.6 Equipment and tools
2.2.7 Window of Opportunity
2.2.8 Final table
2.2.9 Range of values



Signal and function processor	Specialized
Digital Oscilloscope	Specialized
Signal/Protocol Analyser	Specialized
Tools for chemical etching (wet)	Specialized
Tools for chemical etching (plasma)	Specialized
Tools for grinding	Specialized
Climate chamber	Specialized
Anechoic chamber	Specialized
Standard X-ray machine	Specialized
Radio-frequency generator	Specialized
Gamma-ray generator	Specialized
Standard tomography scanner	Specialized
Standard thermal camera	Specialized
FIB systems	Specialized

Manufacturers know the purchasers of these tools and their location. The majority of the second hand tools market is also controlled by the manufacturers.

Efficient use of these tools requires a very long experience and can only be done by a small number of people. Nevertheless, one cannot exclude the fact that a certain type of equipment may be accessible through university laboratories or equivalent but expertise in using the equipment is quite difficult to obtain.

Table 9: Rating for tools (II)

Tool	Equipment
X-ray 3-D tomograph	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke

Note, that using bespoke equipment should lead to a moderate potential as a minimum.

The level "Multiple Bespoke" is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Table 10: Rating for Equipment

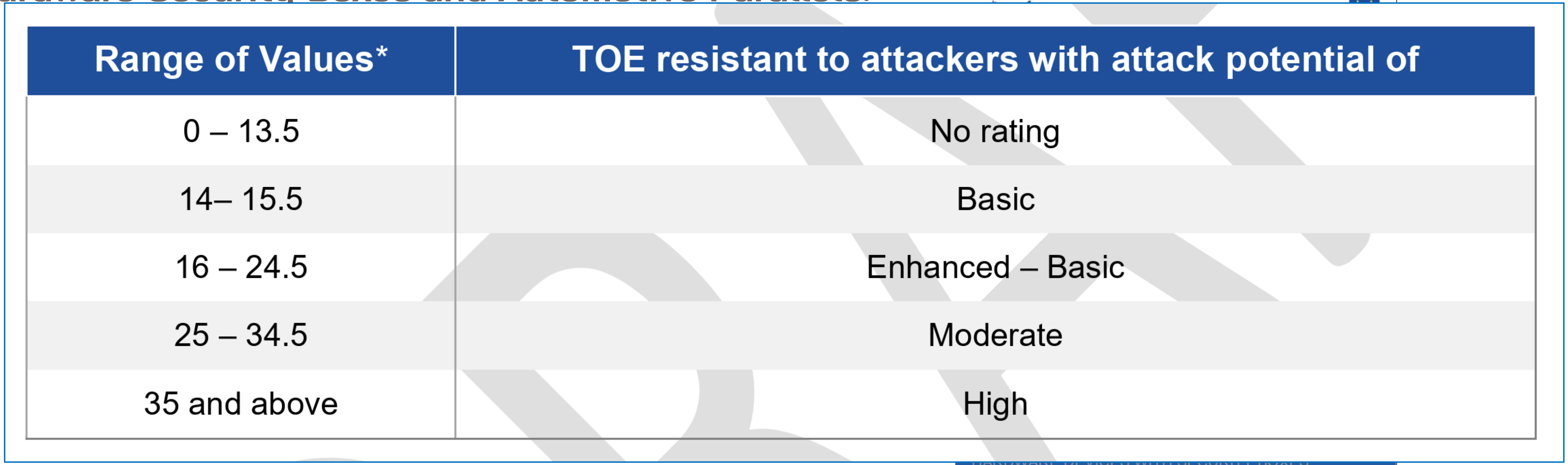
Equipment	Identification	Exploitation
None	0	0
Standard	1	2
Specialized*	3	4
Bespoke	5	6
Multiple Bespoke	7	8

*If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.

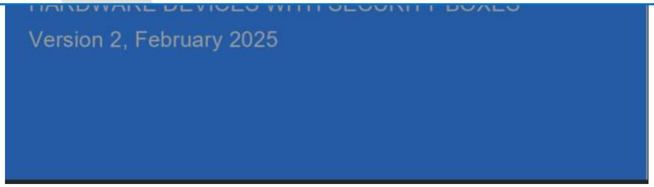
Equipment can always be rented but the same quotation applies with one exception: Bespoke equipment, which can

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Hardware Security Boxes and Automotive Parallels:



Range of Values*	TOE resistant to attackers with attack potential of
0 – 13.5	No rating
14– 15.5	Basic
16 – 24.5	Enhanced – Basic
25 – 34.5	Moderate
35 and above	High



HARDWARE DEVICES WITH SECURITY BOXES

Version 2, February 2025

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

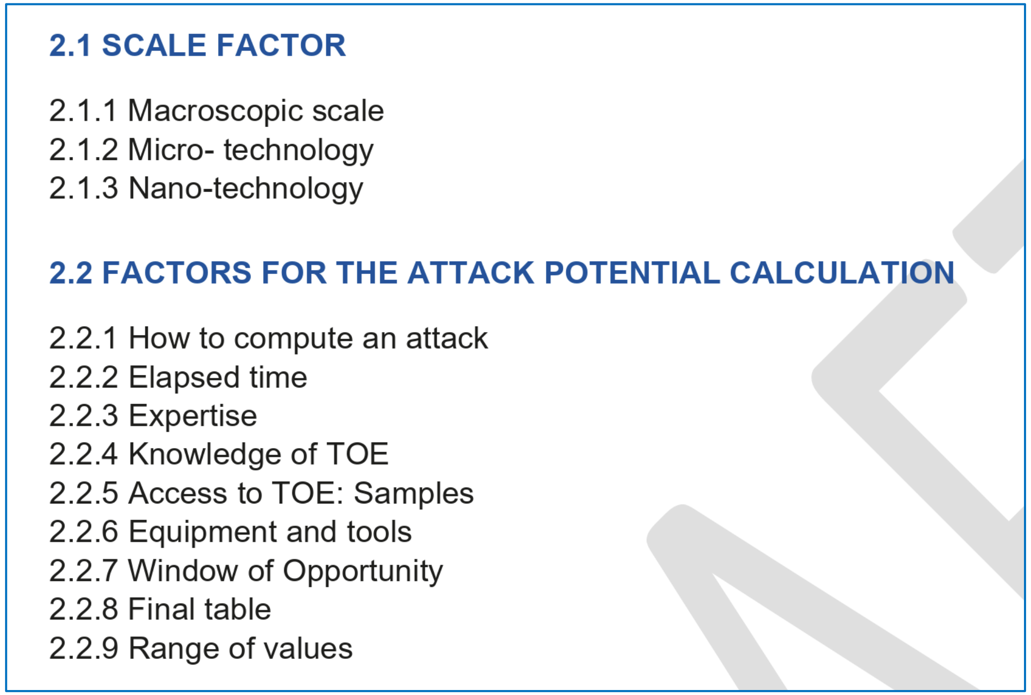
Attack potential rating example

Attack scenario:

- **Target:**
  - Bypass FW signature verification during FW update process with the target to load a forged FW with malicious code.

- **Identification of (potential) vulnerability:**
  - When wrong FW is processed, different error messages are received.
  - The verification of the FW might not be protected against faults.

- **Attack method:**
  - Perturbation attack using Voltage glitch



ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE		
Access to TOE: Samples		
Equipment and tools		
Windows of Opportunity		
Final table		

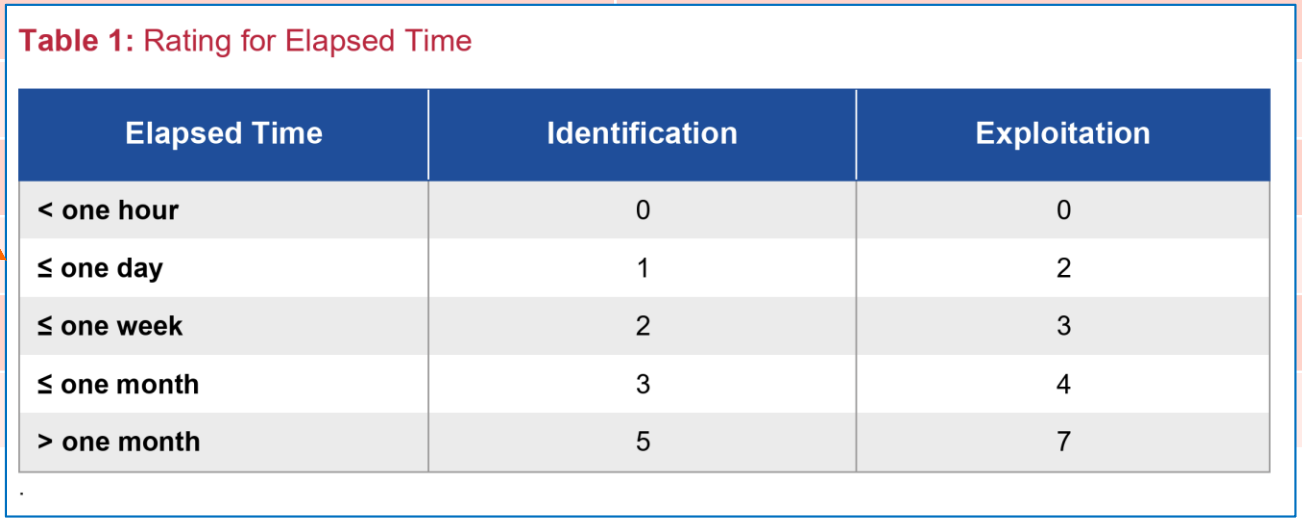


Table 1: Rating for Elapsed Time

Elapsed Time	Identification	Exploitation
< one hour	0	0
≤ one day	1	2
≤ one week	2	3
≤ one month	3	4
> one month	5	7

.

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	[illegible]	[illegible]
Access to TOE: Samples	[illegible]	[illegible]
Equipment and tools	[illegible]	[illegible]
Windows of Opportunity	[illegible]	[illegible]
Final table	[illegible]	[illegible]

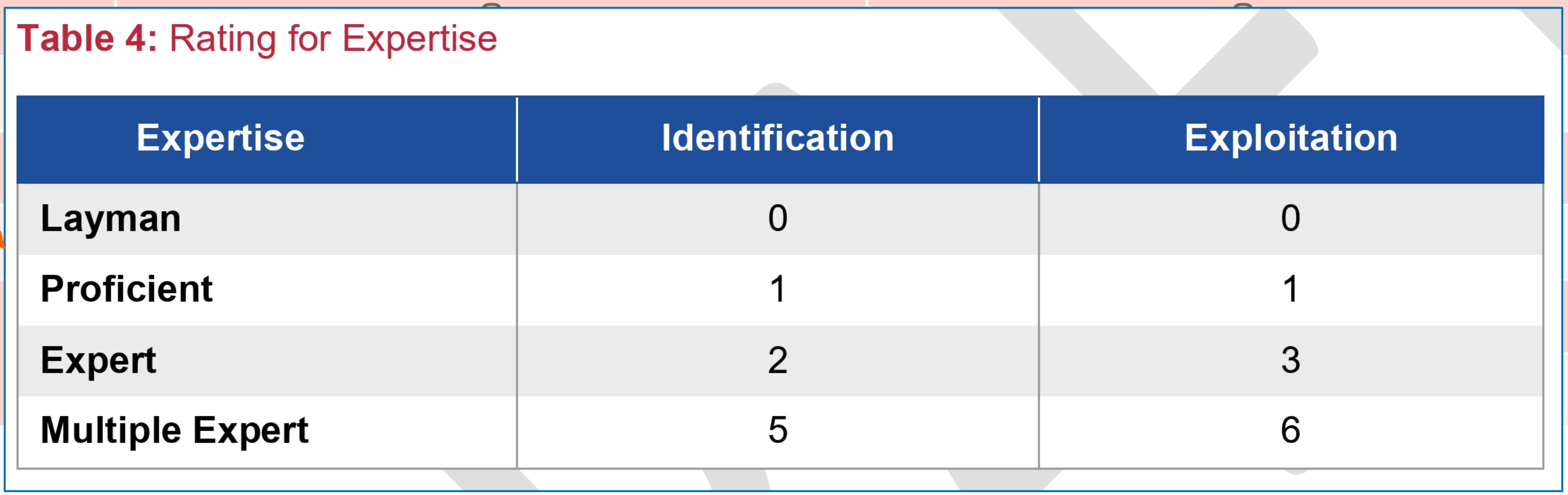


Table 4: Rating for Expertise

Expertise	Identification	Exploitation
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	[illegible]	[illegible]
Equipment and tools		
Windows of Opportunity		
Final table		

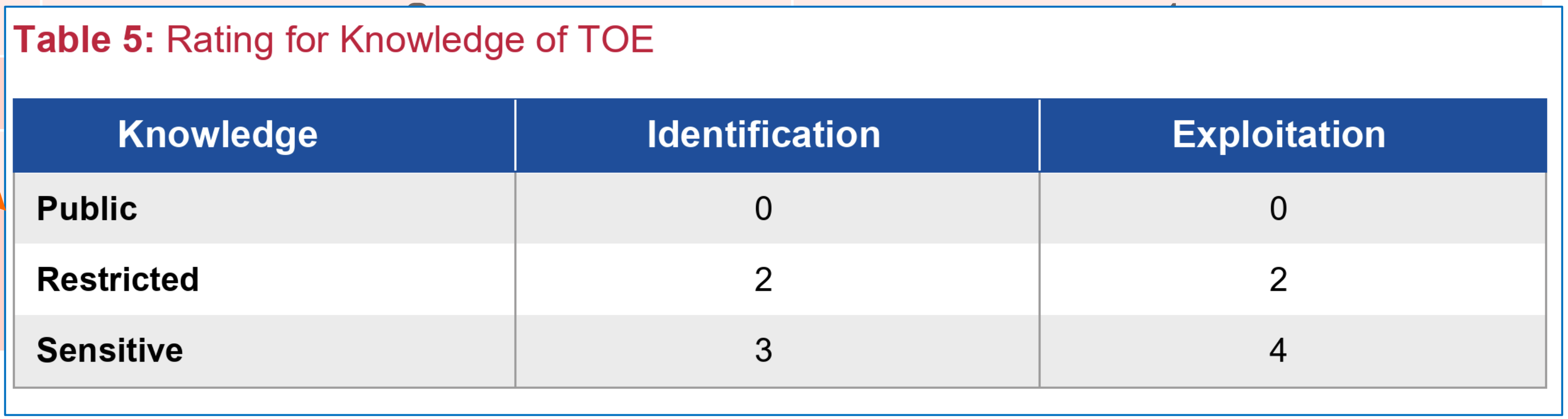


Table 5: Rating for Knowledge of TOE

Knowledge	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	3	4

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identifi
Elapsed time	
Expertise	
Knowledge of TOE	
Access to TOE: Samples	
Equipment and tools	
Windows of Opportunity	
Final table	

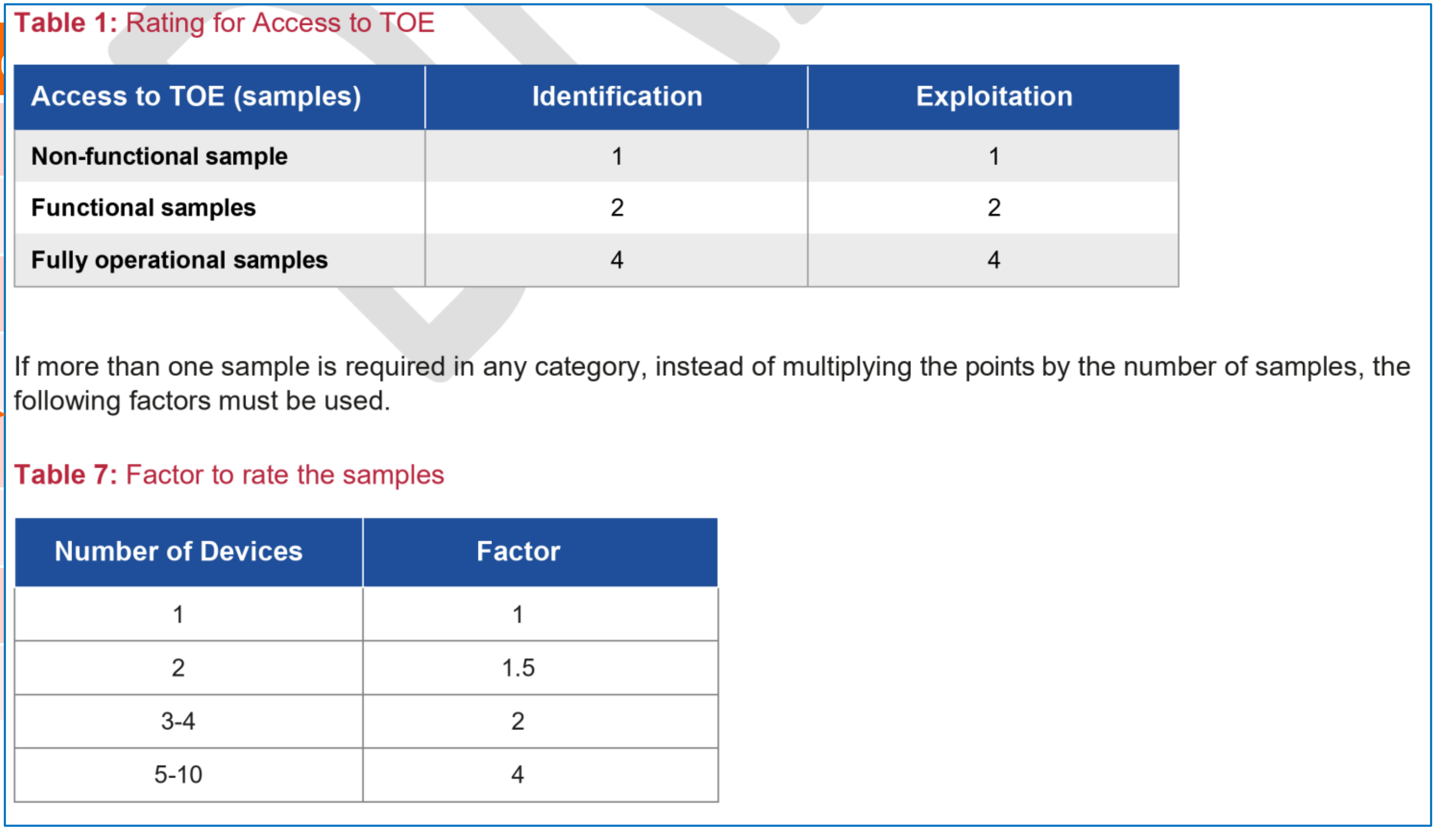


Table 1: Rating for Access to TOE

Access to TOE (samples)	Identification	Exploitation
Non-functional sample	1	1
Functional samples	2	2
Fully operational samples	4	4

If more than one sample is required in any category, instead of multiplying the points by the number of samples, the following factors must be used.

Table 7: Factor to rate the samples

Number of Devices	Factor
1	1
2	1.5
3-4	2
5-10	4

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

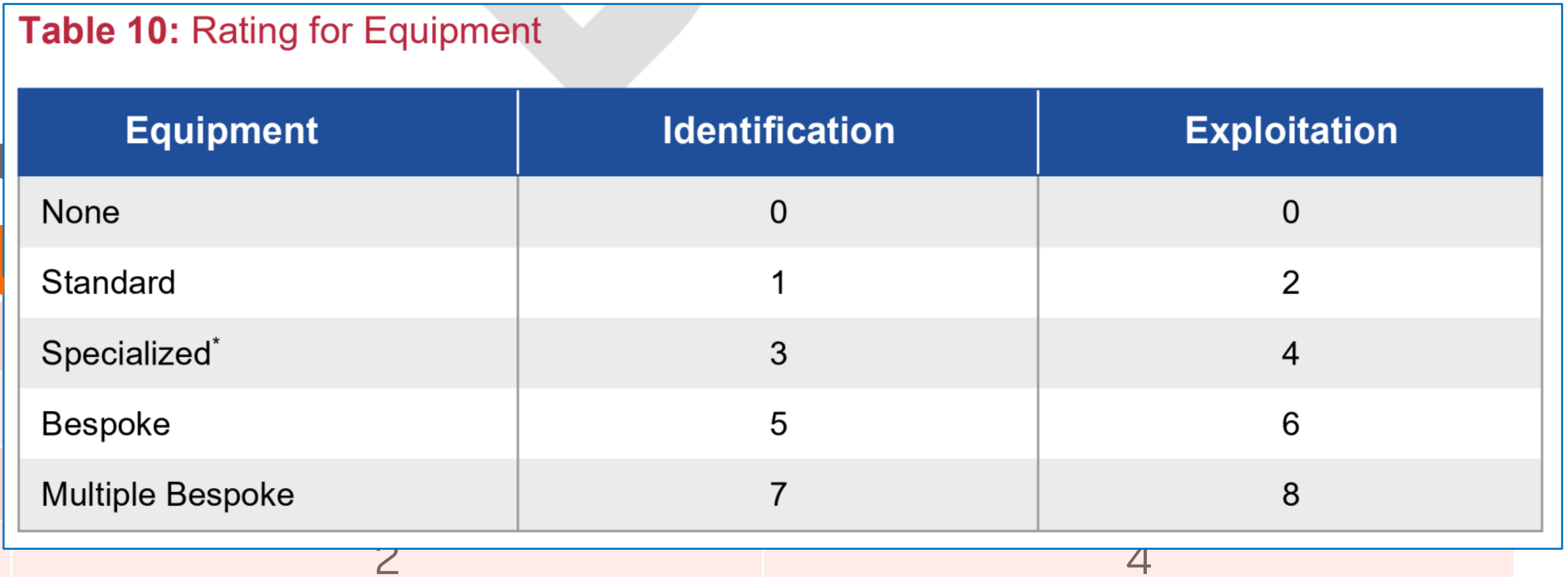


Table 10: Rating for Equipment

Equipment	Identification	Exploitation
None	0	0
Standard	1	2
Specialized*	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Attack potential rating exampl

Elapsed time		
Expertise		
Knowledge of TOE		
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identi	
Elapsed time		
Expertise		
Knowledge of TOE		
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

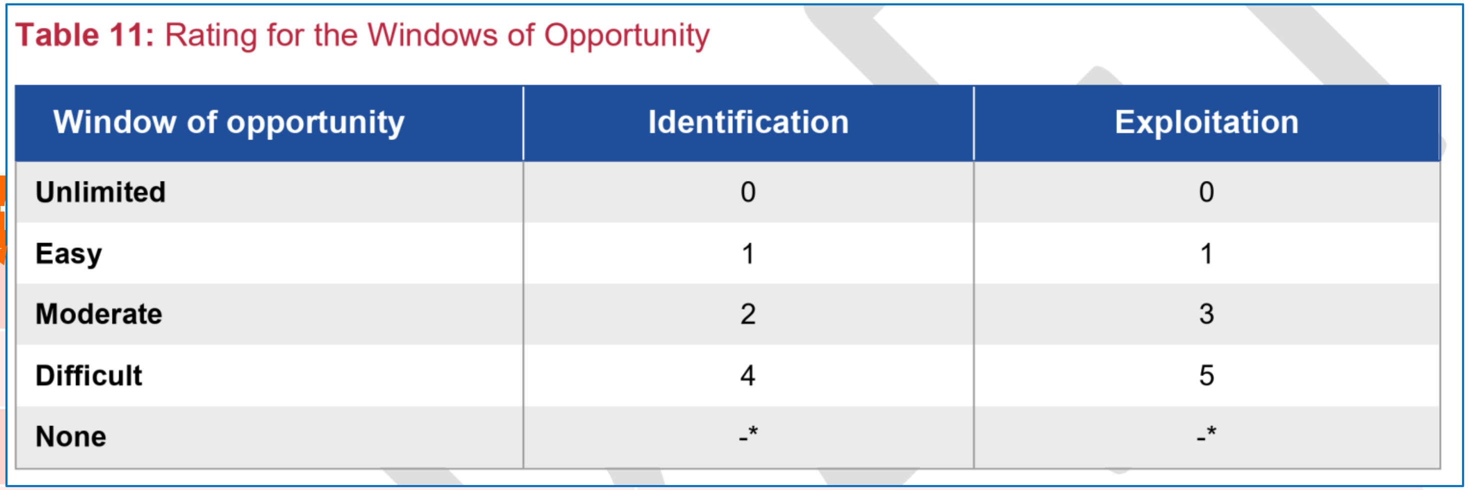


Table 11: Rating for the Windows of Opportunity

Window of opportunity	Identification	Exploitation
Unlimited	0	0
Easy	1	1
Moderate	2	3
Difficult	4	5
None	-*	-*

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed time	5	2
Expertise	2	2
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**14**	**14**
	28 (Moderate resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

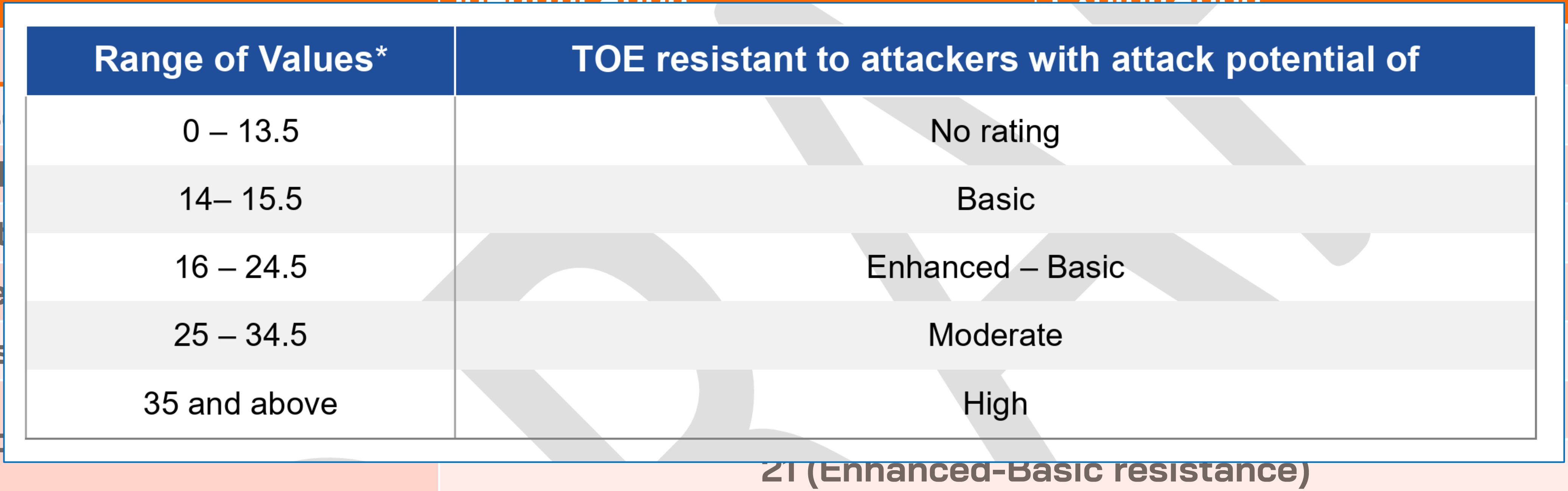
Attack potential rating example

	Identification	Exploitation
Elapsed time	3	2
Expertise	2	0
Knowledge of TOE	2	2
Access to TOE: Samples	2	4
Equipment and tools	3	4
Windows of Opportunity	0	0
Final table	**11**	**12**
	21 (Enhanced-Basic resistance)	

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Attack potential rating example

	Identification	Exploitation
Elapsed		
Expertis		
Knowled		
Access t		
Equipme		
Windows		
Final tab	21 (Enhanced-Basic resistance)	



Range of Values*	TOE resistant to attackers with attack potential of
0 – 13.5	No rating
14– 15.5	Basic
16 – 24.5	Enhanced – Basic
25 – 34.5	Moderate
35 and above	High

ENISA SoTA: Application of attack potential to hardware devices with security boxes (HWSB)

Harmonized criteria to rate attack difficulty:

- **Supports layered defense strategy** helping to prioritize testing investment
- Easier **quantification of cost of the attacks (in USD)**
- Promotes **budget-efficiency** while clarifying criteria for laboratories.

enisa

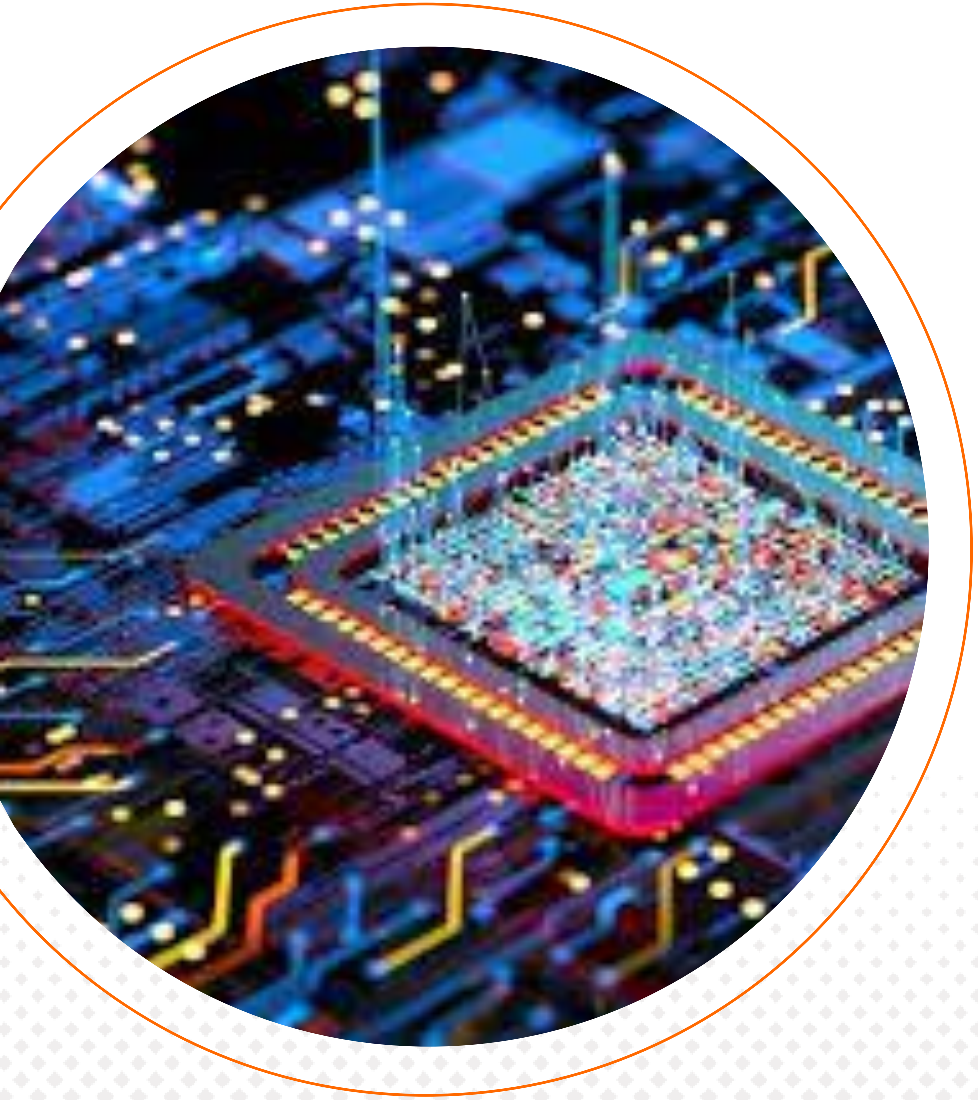
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES

Version 2, February 2025



SESIP Assurance Levels & Protection Profiles

SESIP contribution for Automotive sector

- Objective to reduce the cost, complexity, and effort associated with security evaluations.
- Emphasis on modularity and the reuse of certified components.

Modular Evaluation:

Automotive systems comprise various components like ECUs, telematics units, and infotainment systems. SESIP allows for individual evaluation of these components, facilitating targeted security assessments.

Reuse of Certified Components:

Manufacturers can integrate previously certified components into new systems without re-evaluating the entire system, saving time and resources.

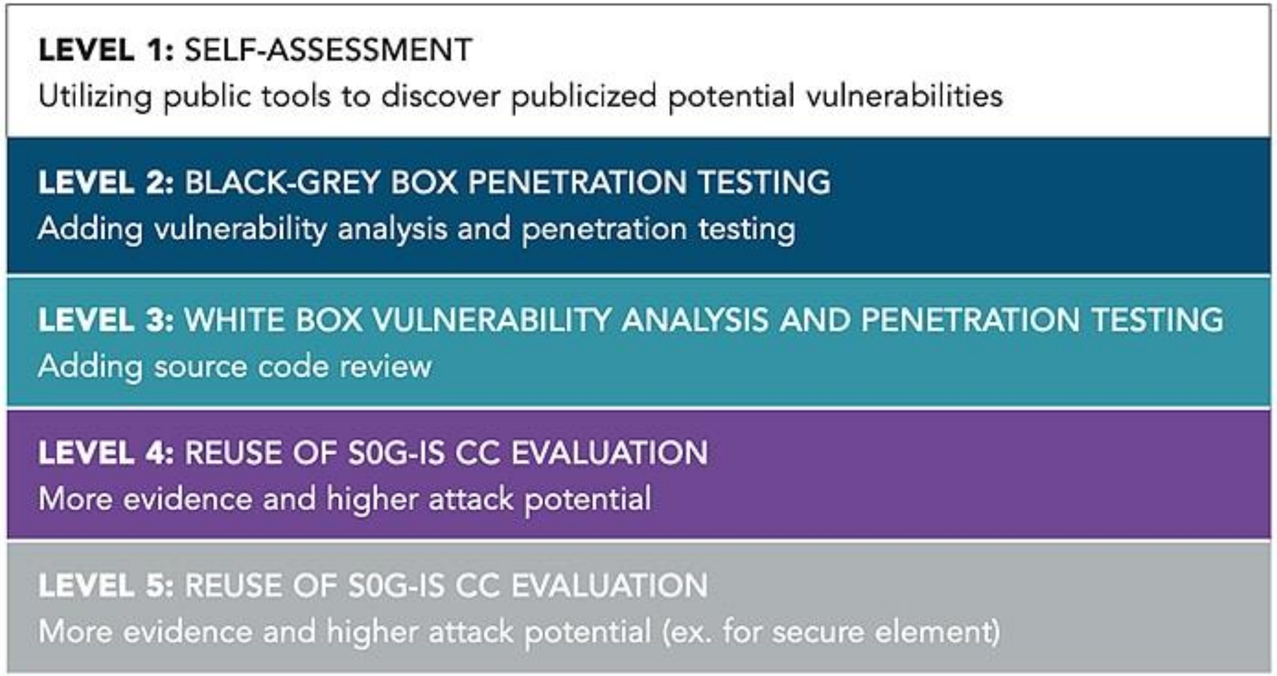
Support for ISO/SAE 21434 Compliance:

SESIP's methodology supports compliance with ISO/SAE 21434, the international standard for automotive cybersecurity risk management.

SESIP Assurance Levels

Adapt SESIP to your risk assessment:

- SESIP levels let you tailor assurance to risk
- Avoid overengineering: not every ECU needs SESIP 5
- Enables scalable security investment based on product criticality



LEVEL 1: SELF-ASSESSMENT
Utilizing public tools to discover publicized potential vulnerabilities

LEVEL 2: BLACK-GREY BOX PENETRATION TESTING
Adding vulnerability analysis and penetration testing

LEVEL 3: WHITE BOX VULNERABILITY ANALYSIS AND PENETRATION TESTING
Adding source code review

LEVEL 4: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential

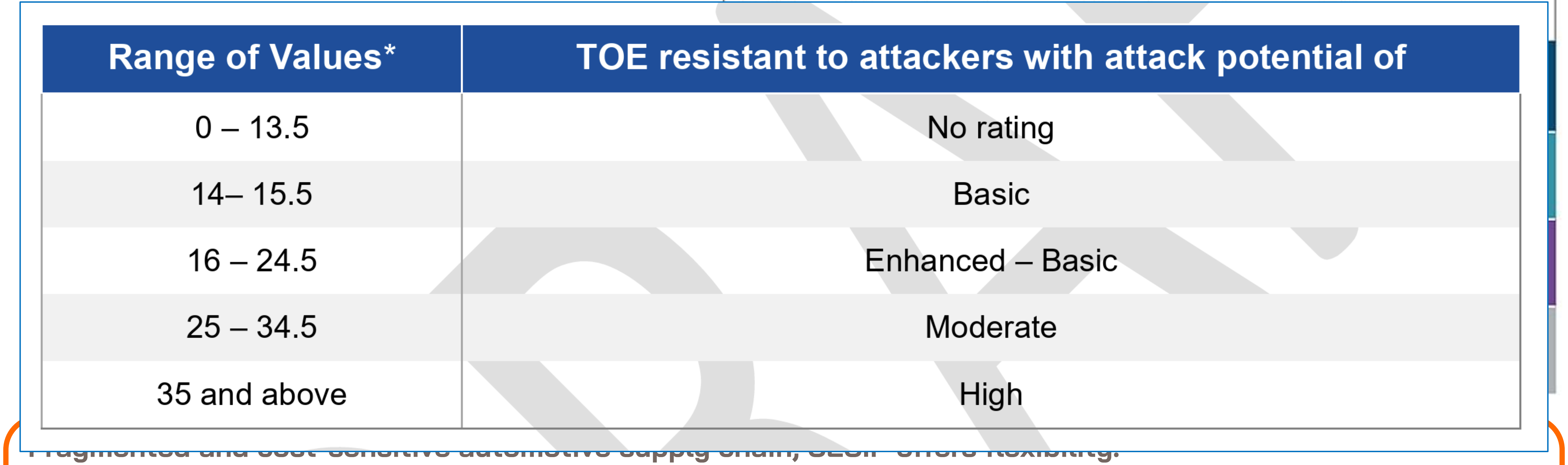
LEVEL 5: REUSE OF S0G-IS CC EVALUATION
More evidence and higher attack potential (ex. for secure element)

Fragmented and cost-sensitive automotive supply chain, SESIP offers flexibility.
For example, you can assign SESIP 2 for a temperature sensor, and SESIP 3 for a gateway that handles over-the-air (OTA) updates.
This ensures resources are focused where they yield the highest security value. The SESIP model supports iterative and modular certification, reducing total cost of ownership.

SESIP Assurance Levels

Adapt SESIP to your risk assessment:

LEVEL 1: SELF-ASSESSMENT



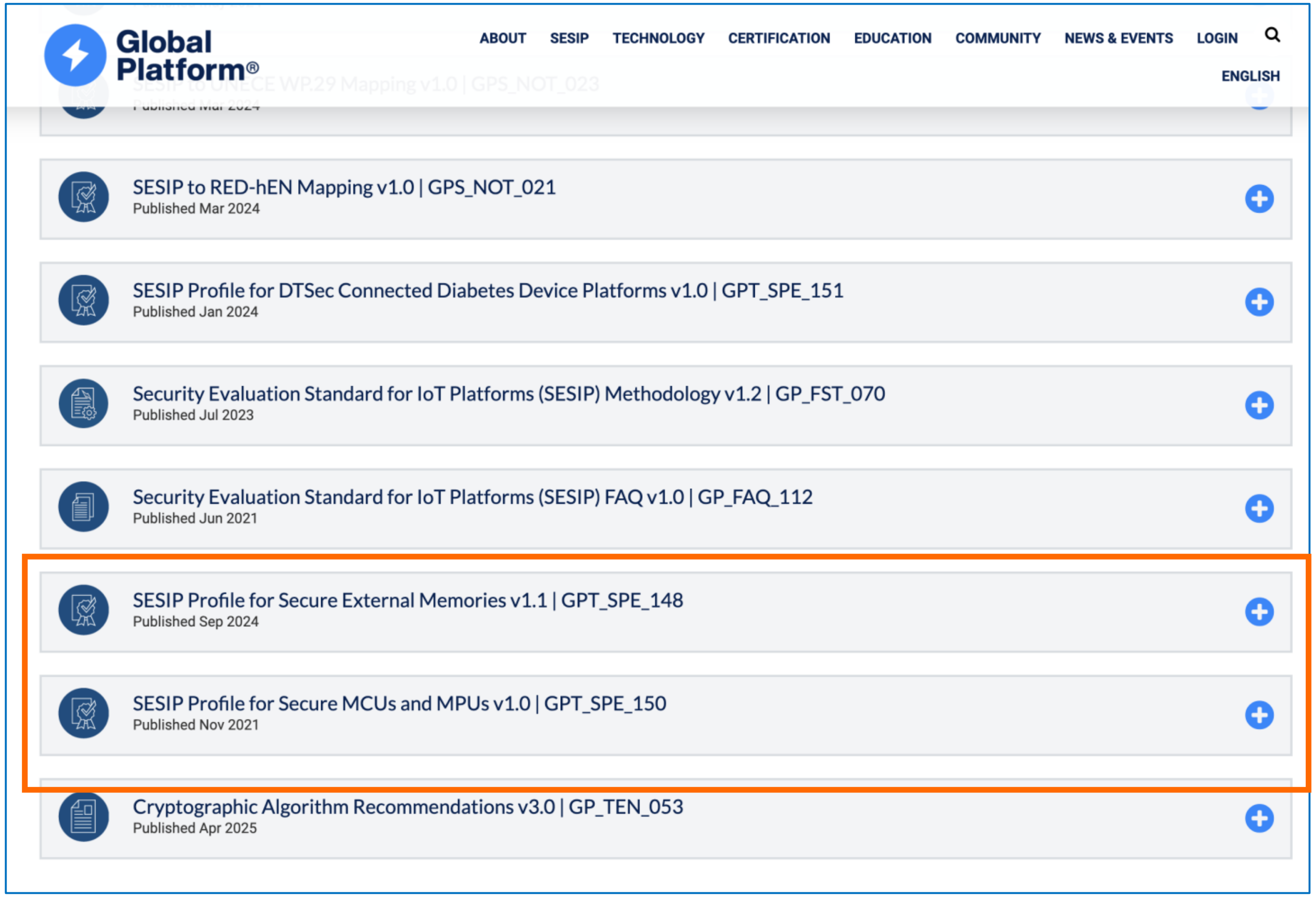
Range of Values*	TOE resistant to attackers with attack potential of
0 – 13.5	No rating
14– 15.5	Basic
16 – 24.5	Enhanced – Basic
25 – 34.5	Moderate
35 and above	High

Fragmented and cost-sensitive automotive supply chain, SESIP offers flexibility:
For example, you can assign SESIP 2 for a temperature sensor, and SESIP 3 for a gateway that handles over-the-air (OTA) updates.
This ensures resources are focused where they yield the highest security value. The SESIP model supports iterative and modular certification, reducing total cost of ownership.

SESIP Protection Profiles

Why Protection Profiles Matter

- Define security objectives and scope early
- Enable harmonization across the supply chain
- Lower certification cost



SESIP to UNECE WP.29 Mapping v1.0 | GPS_NOT_023
Published Mar 2024

SESIP to RED-hEN Mapping v1.0 | GPS_NOT_021
Published Mar 2024

SESIP Profile for DTSec Connected Diabetes Device Platforms v1.0 | GPT_SPE_151
Published Jan 2024

Security Evaluation Standard for IoT Platforms (SESIP) Methodology v1.2 | GP_FST_070
Published Jul 2023

Security Evaluation Standard for IoT Platforms (SESIP) FAQ v1.0 | GP_FAQ_112
Published Jun 2021

SESIP Profile for Secure External Memories v1.1 | GPT_SPE_148
Published Sep 2024

SESIP Profile for Secure MCUs and MPUs v1.0 | GPT_SPE_150
Published Nov 2021

Cryptographic Algorithm Recommendations v3.0 | GP_TEN_053
Published Apr 2025

SESIP Protection Profiles

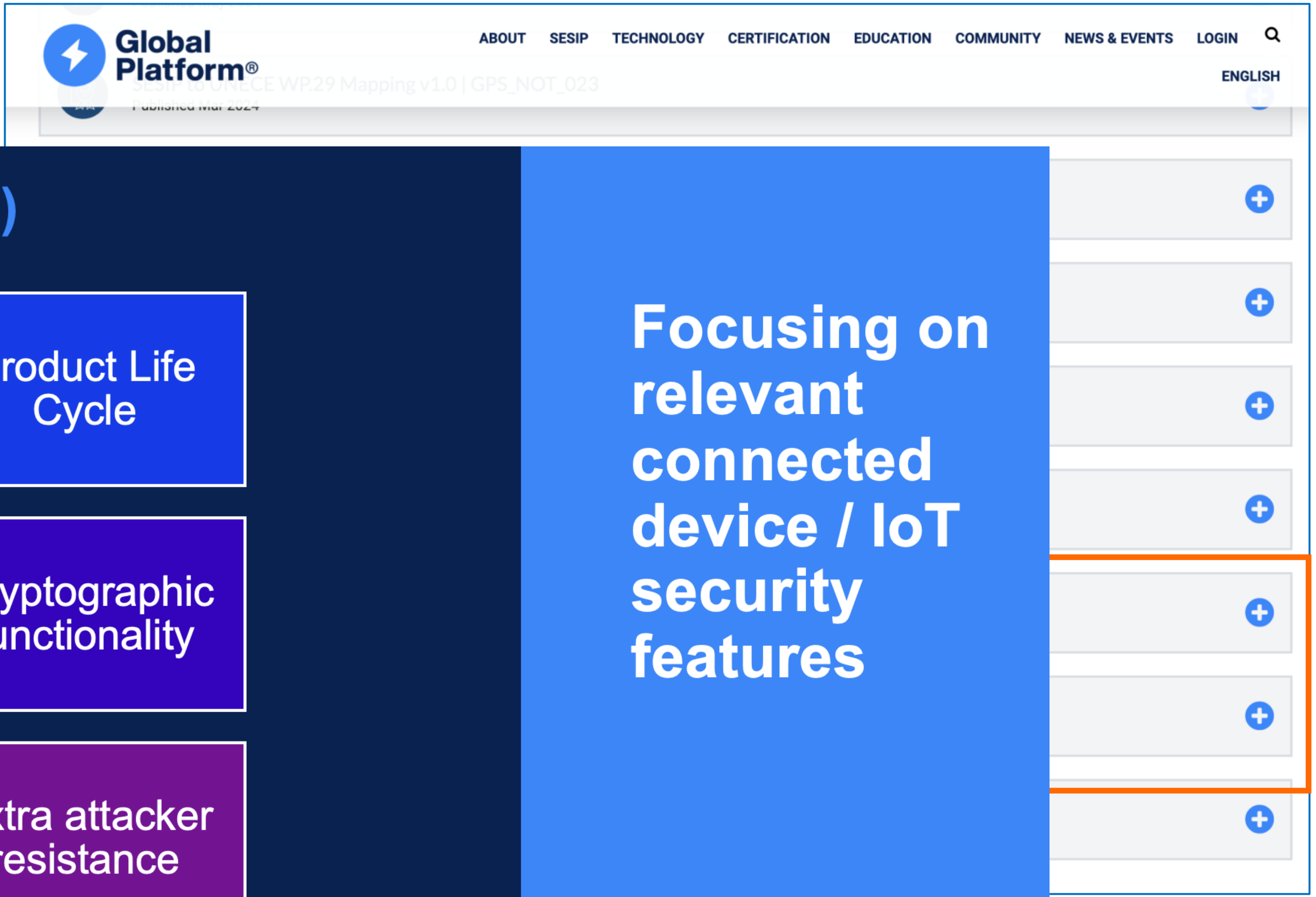
Why Protection Profiles Matter

- Define securi
- Enable harmo chain
- Lower certific

SESIP Efficiency (SFRs)

Identification and Attestation	Product Life Cycle
Secure Communication	Cryptographic functionality
Compliance functionality	Extra attacker resistance

Focusing on relevant connected device / IoT security features



SESIP to UNECE WP.29 Mapping v1.0 | GPS_NOT_023

Published Mar 2024

GlobalPlatform role within the certification ecosystem

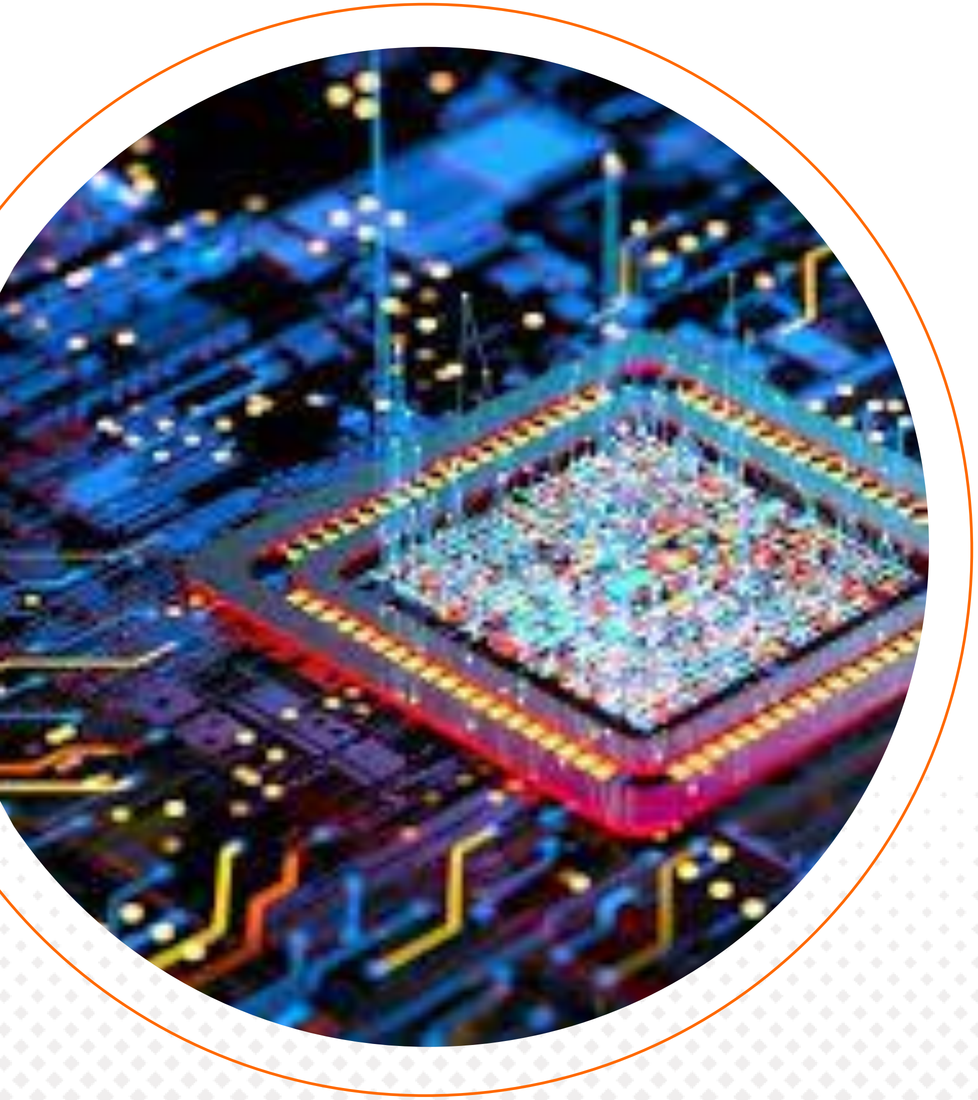
Continuous work to adapt to industry needs:

- **Technical working groups** to standardize criteria and requirements
  - Harmonize criteria for attacks (i.e., minimum/maximum attack scoring for specific attack scenarios)
  - Harmonize acceptance on ad-hoc approaches (i.e., test witnessing in vendor facilities)
- **ITSEFs** in alignment with certification bodies to adapt requirements to discuss ad-hoc approaches for specific use cases.
  - Workshop to go though implementation instead of in-house code review
  - Specific test-setups to facilities exposure of attack surface
  - Alternative functional test methods to demonstrate compliance

SESIP Assurance Levels and Protection Profiles

A common and optimized approach for evaluating the security of connected products:

- General model similar to CC
- Granularity
- Requirement hierarchy
- Profiles



Final thoughts

Key Takeaways

enisa
EUROPEAN UNION
CYBERSECURITY
CERTIFICATION

ENISA's Attack Potential Method:

Harmonized criteria to rate attack difficulty

SESIP Certification:

A common and optimized approach for evaluating the security of connected products

Global Platform™
SESIP

Thanks!

Applus laboratories

Join us on

TESTING AND CERTIFICATION CENTER

www.appluslaboratories.com