Formal models for high assurance: why and how

Carolina Lavatelli, Internet of Trust

Guillaume Tétu, ANSSI

18 November 2020

ICCC 2020

EAL6 certifications have recently gained terrain.

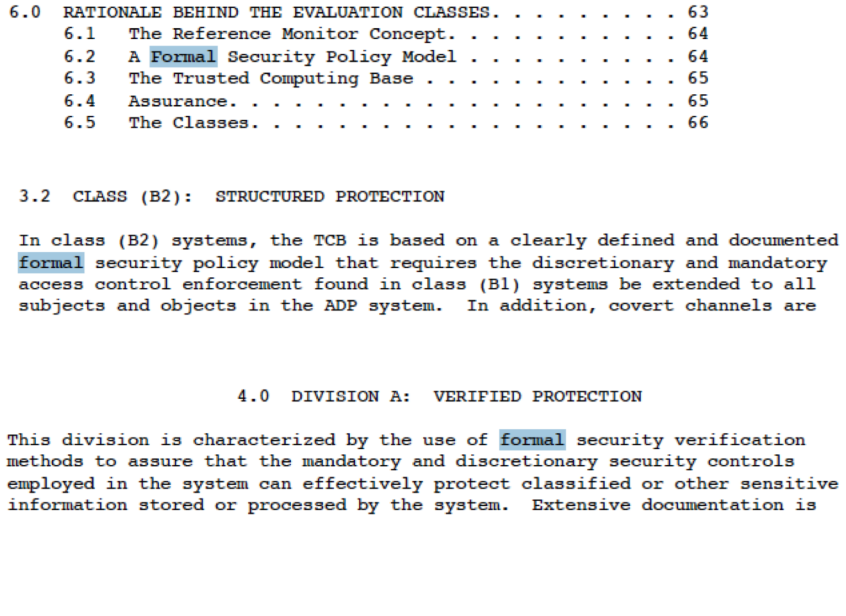
With CCv4 within reach and with an extensive experience in formal evaluations, we are proposing a formal methods usage approach that is clearly articulated around the SPM and the developer's claims about the TOE and the TSF. This leads to more flexibility, increased comprehension and decreased subjectivity for evaluators and CBs.

The presentation covers the definition of the formal assurance components and the impact on current practices.

Contents

- Formal methods from the origins to CC v3.1
- Evolution of concepts
- Impact of changes
- Relevance
- Conclusion

From the origins ...



6.0 RATIONALE BEHIND THE EVALUATION CLASSES. 63
6.1 The Reference Monitor Concept. 64
6.2 A Formal Security Policy Model 64
6.3 The Trusted Computing Base 65
6.4 Assurance. 65
6.5 The Classes. 66

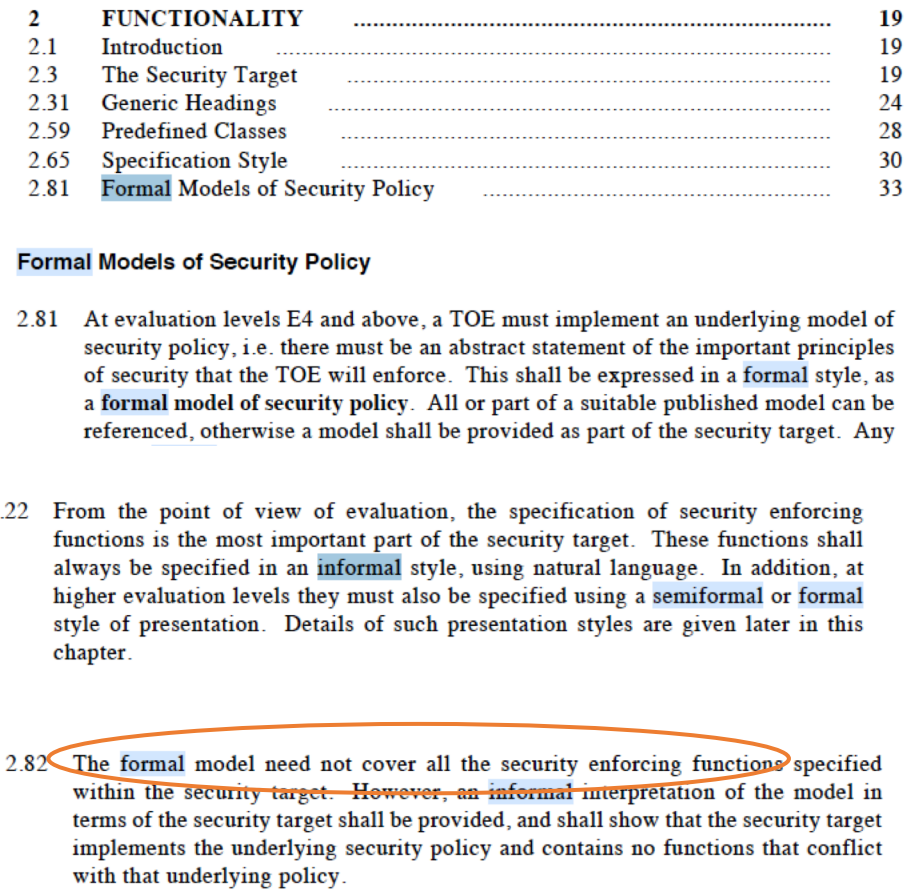
3.2 CLASS (B2): STRUCTURED PROTECTION

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are

4.0 DIVISION A: VERIFIED PROTECTION

This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is

TCSEC (1983-)



2 FUNCTIONALITY 19
2.1 Introduction 19
2.3 The Security Target 19
2.31 Generic Headings 24
2.59 Predefined Classes 28
2.65 Specification Style 30
2.81 Formal Models of Security Policy 33

Formal Models of Security Policy

2.81 At evaluation levels E4 and above, a TOE must implement an underlying model of security policy, i.e. there must be an abstract statement of the important principles of security that the TOE will enforce. This shall be expressed in a formal style, as a **formal model of security policy**. All or part of a suitable published model can be referenced, otherwise a model shall be provided as part of the security target. Any

2.22 From the point of view of evaluation, the specification of security enforcing functions is the most important part of the security target. These functions shall always be specified in an informal style, using natural language. In addition, at higher evaluation levels they must also be specified using a semiformal or formal style of presentation. Details of such presentation styles are given later in this chapter.

2.82 The formal model need not cover all the security enforcing functions specified within the security target. However, an informal interpretation of the model in terms of the security target shall be provided, and shall show that the security target implements the underlying security policy and contains no functions that conflict with that underlying policy.

ITSEC (1991-)

… to CC v3.1

TCSEC (1980') ITSEC (1990')

CC v2.1 (ISO 1999)
CC v2.3 (ISO 2005)

ADV_SPM.1 Informal security policy model
ADV_SPM.2 semi-formal security policy model
ADV_SPM.3 Formal security policy model

367 While a TSP may include any policies, TSP models have traditionally represented only subsets of those policies, because modeling certain policies is currently beyond the state of the art. The current state of the art determines the policies that can be modeled, and the PP/ST author should identify specific functions and associated policies that can, and thus are required to be, modeled. At the very least, access control and information flow control policies are required to be modeled (if they are part of the TSP) since they are within the state of the art.

ADV_SPM.3.1C The TSP model shall be **formal.**

ADV_SPM.3.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

CC v3.1 R3 (ISO 2009)
CC v3.1 R5

ADV_SPM.1 Formal security policy model

273 While the term "formal security policy model" is used in academic circles, the CC's approach has no fixed definition of "security"; it would equate to whatever SFRs are being claimed. Therefore, the formal security policy model is merely a formal representation of the set of SFRs being claimed.

274 The term *security policy* has traditionally been associated with only access control policies, whether label-based (mandatory access control) or user-based (discretionary access control). However, a security policy is not limited to access control; there are also audit policies, identification policies, authentication policies, encryption policies, management policies, and any other security policies that are enforced by the TOE, as described in the PP/ST. ADV_SPM.1.1D contains an assignment for identifying these policies that are formally modelled.

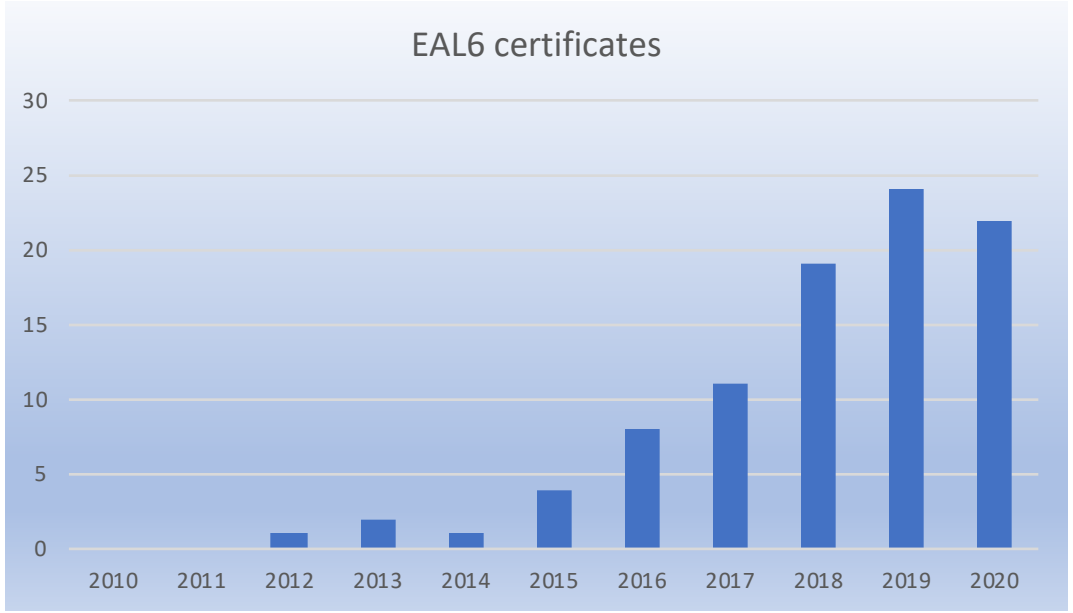
ADV_SPM.1.1D **The developer shall provide a formal security policy model for the [assignment: *list of policies that are formally modelled*].**

ADV_SPM.1.2D **For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.**

« state of the art » disappeared in CC v3.1 … but not the ambiguity on the scope

High EAL certificates in CC v3.1

- Formal methods are used mainly in the framework of SOG-IS
- Very few EAL7, which implies more than just a formal security policy model and proofs (formal design, implementation testing, etc.)
- Today high means essentially EAL6
- Figures for 2010-2020
  - For EAL7: 3 certificates
    - Virtual Machine (2)
    - Diode (1)
  - For EAL6: 92 certificates
    - Strictly increasing number in 2015-2019
    - Mainly ICs, Java Card , IP blocks
    - A variable scope



Source: Common Criteria portal, Nov 9th 2020

SPM in CC v3.1: a voluntary approach

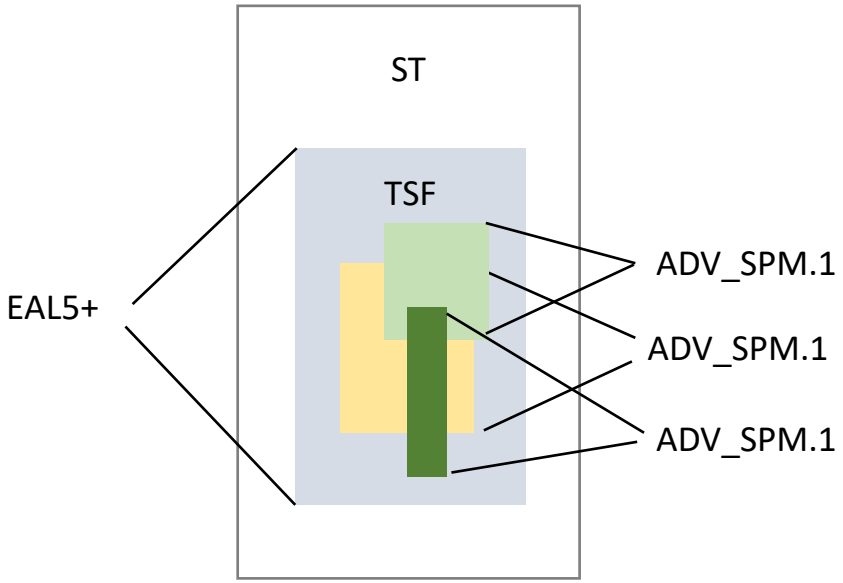
- CC v3.1 is ambiguous and does not provide the evaluation methodology
  - Allows for different interpretations of the underlying notions, in particular the scope of the formal model and properties and the characteristics of methods and tools

- ANSSI and BSI have driven the use of formal methods in CC evaluations and published guidance for developers and evaluators (Note-12 and AIS34)
  - Insufficient to harmonise the use of ADV_SPM and henceforth EAL6

A direct consequence

EAL6 = {EAL5+, ADV_SPM.1}

In CC v3.1



Nobody knows what SPM
and therefore EAL6 mean, even
for a PP-conformant product

The aim is to repair the anomaly with a clear
set of requirements and evaluation methodology for ADV_SPM

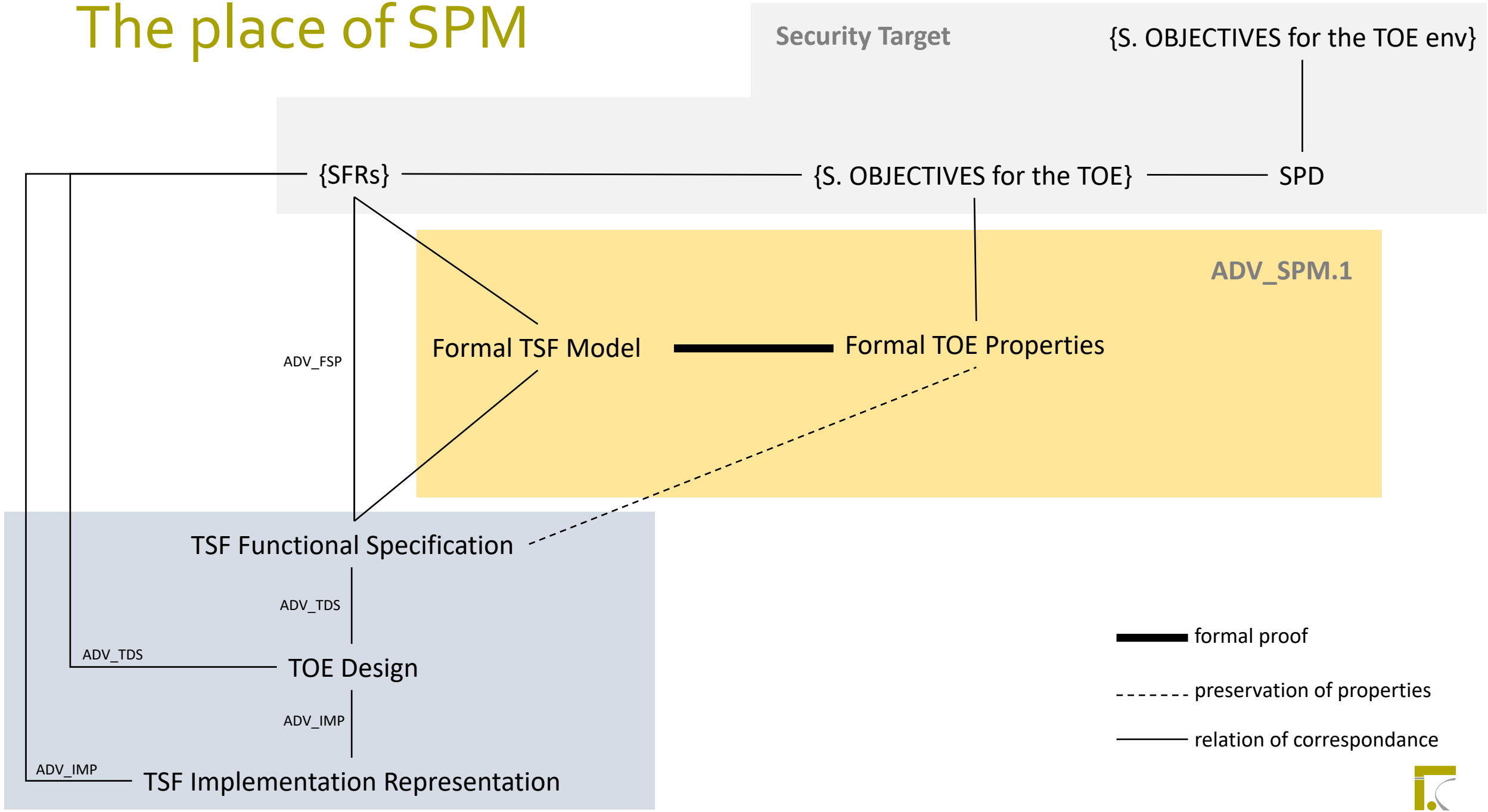
Momentum

- The revision of CC – the first good opportunity in 10 years

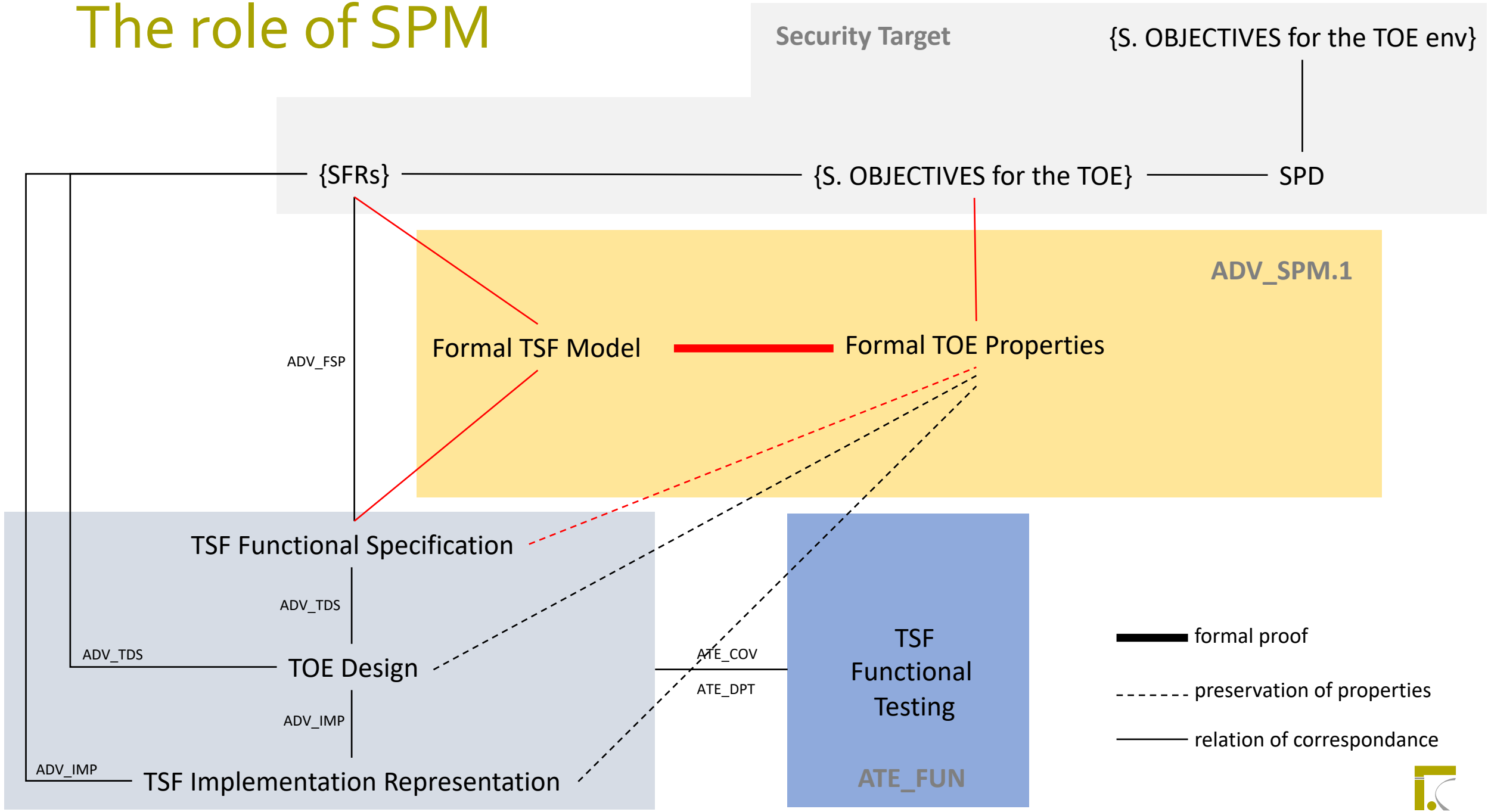
- CC v4 as a tool-box for specifying and evaluating security
  - Exact conformance and constructs for specifying evaluation methods
  - Enhanced notion of packages with SPD and objectives for easier and more structured specifications
  - Enhanced notions of PP-Modules and PP-Configurations
  - Introduction of multi-assurance for combining different assurance packages for different parts within a single evaluation
  - Introduction of composite evaluation for reusing evaluation results in complex supply/development chains

- New ADV_SPM.1 for harmonising the use of formal methods in CC

The place of SPM



The role of SPM



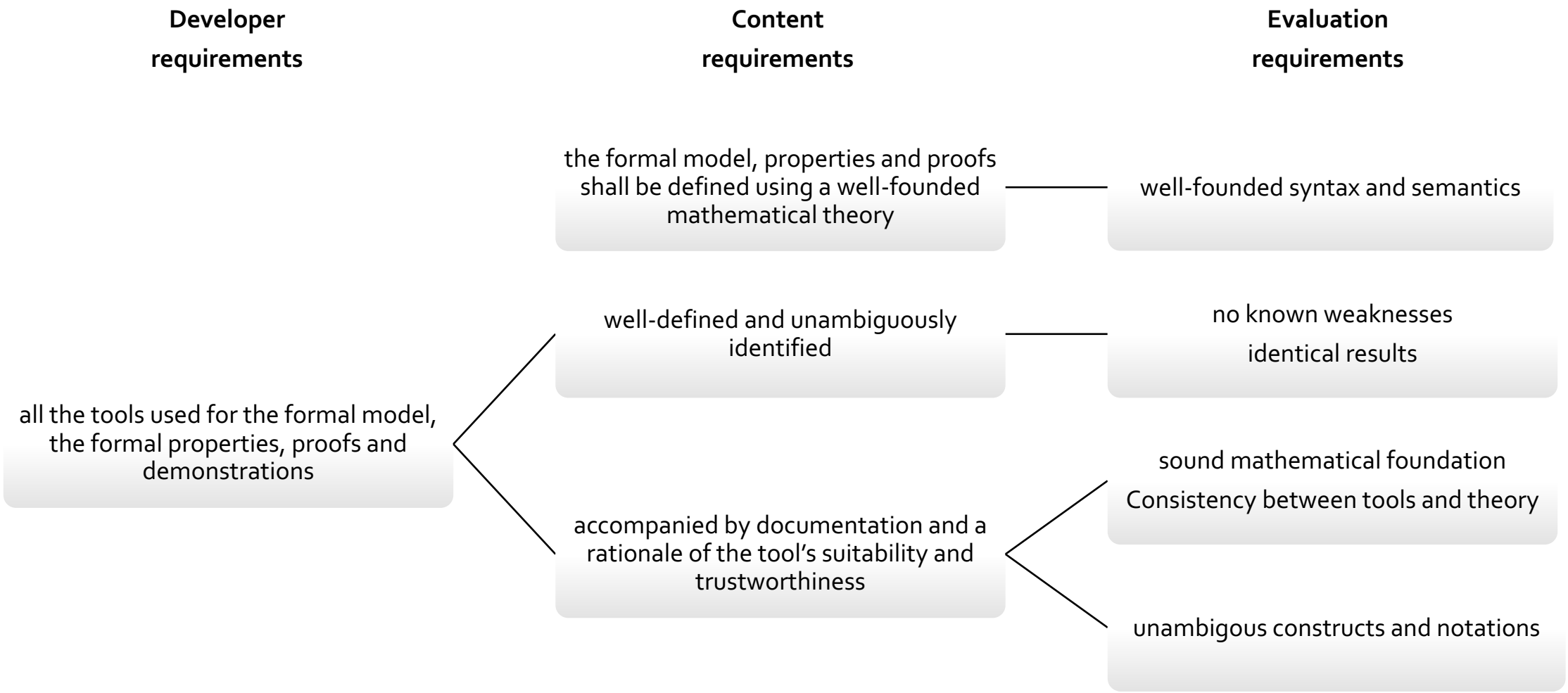
ADV_SPM.1 in CC-3 and CEM (1/3)

Developer requirements	Content requirements	Evaluation requirements
a formal model for the TSF	cover the complete set of SFRs	conceptual mapping and accurate representation
the set of formal properties for the TOE	cover the complete set of security objectives for the TOE	conceptual mapping and accurate representation
a formal proof that the model satisfies the formal properties	show that the formal model satisfies all the formal properties	reproduce formal proofs
	show that the consistency of the underlying mathematical theory is preserved	consistency of unproven assertions
all supported by explanatory text	include instructions for reproducing the proofs and the correspondence rationale, and a rationale for the modeling and verification choices	all parts covered and clarity of instructions

ADV_SPM.1 in CC-3 and CEM (2/3)

Developer requirements	Content requirements	Evaluation requirements
a correspondence rationale between the formal model and the functional specification	show that the formal properties proven for the formal model hold for the functional specification	relevant abstraction examine correspondence
a semi-formal demonstration of correspondence between the formal model and any semi-formal functional specification	show that the formal properties proven for the formal model hold for any semi-formal functional specification	(if applicable) examine demonstration
a formal proof of correspondence between the formal model and any formal functional specification	show that the properties proven for the formal model hold for any formal functional specification	(if applicable) reproduce proof

ADV_SPM.1 in CC-3 and CEM (3/3)



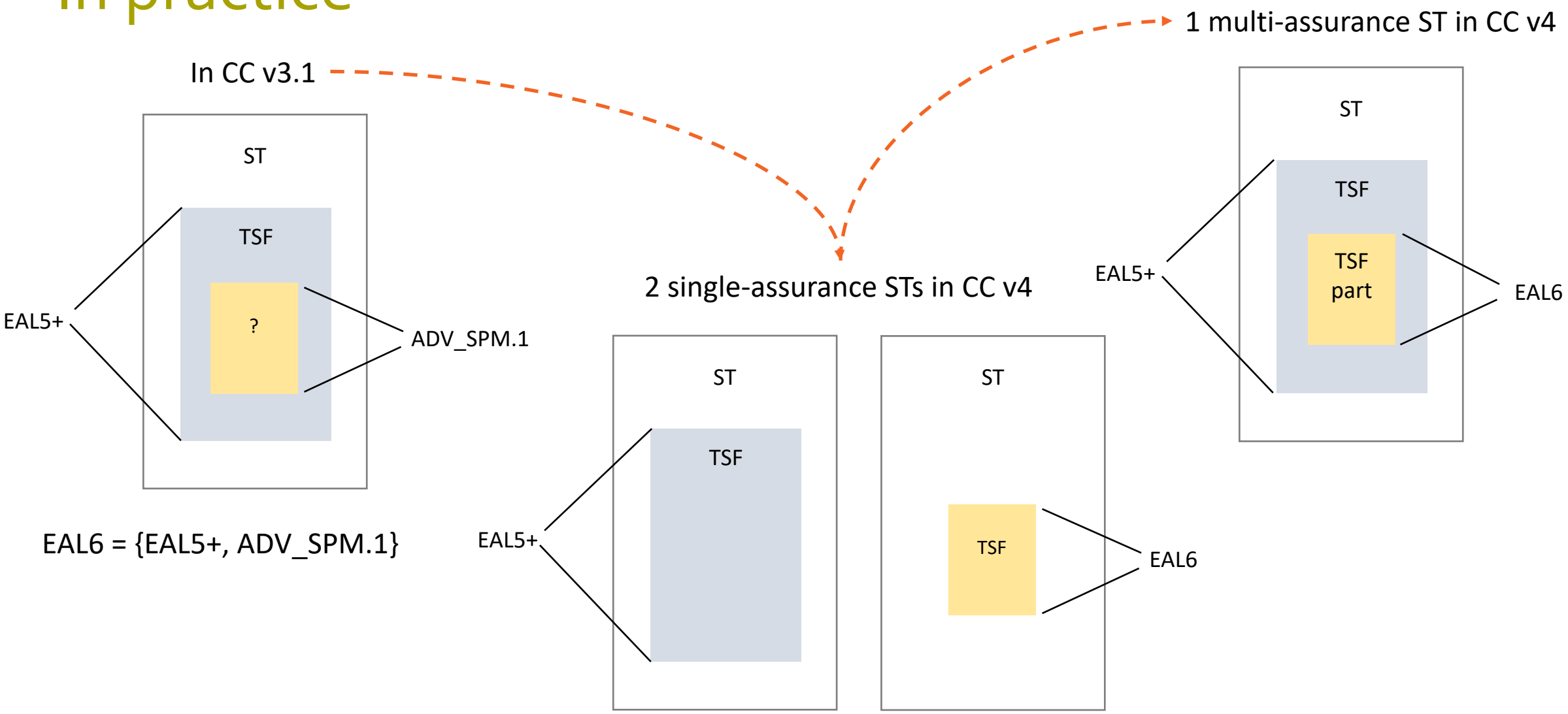
The impact of the changes

- ST-driven SPM with unambiguous scope
- Mathematical foundation for theory and tools
- Preservation of formal properties across different TOE/TSF representations

- As in CC v3.1 the developer decides the scope for which a formal model makes sense
  - Now the developer presents an ST and an SPM that match each other

- As in CCv3.1 the baseline is EAL4: ADV_SPM.1 has a dependency towards FSP.4 "Complete specification"
  - EAL4 augmented with ADV_SPM.1 still makes sense

In practice



Removed anomaly: ADV_SPM.1 applies to a well-defined TSF or TSF-part

This is not theory …

- Formal methods are behind the most fundamental principles for a controlled cybersecurity strategy
  - Security-by design, security-by-default, privacy- by-design, root-of-trust, least privilege, sandboxing, etc.

- Formal methods are used for
  - Deriving reliable conclusions about the possible behaviours of the system in normal conditions and as the adversary interacts with it
  - Proving that the system is resilient to entire classes of potential attacks
  - Informing implementers unambiguously concerning what to develop
  - Informing users of systems and integrators of components what exactly to rely on the system or component

Applications

- Formal methods are applied and/or standardised in many sectors, for instance
  - Aerospace, automotive, railway signalling, subway automation, cloud, cryptography, kernels, compilation, etc.

- Formal methods are called to be used more and more in the context of cyber-physical systems for ensuring safety and for control over AI applications
  - By developing new models or by relying on known, existing models

Conclusion

The new definition of ADV_SPM.1 fills the gap for
a formal methods-based assurance for IT products.
It provides a framework for leveraging and harmonizing
the use of formal models and proofs in CC.

"During the next decade, cybersecurity risks will become harder to assess & interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface." (Enisa report on Emerging Trends)

Acknowledgments

- Arnaud Fontaine and Thomas Letan, ANSSI, France
- Oana Andreescu, Internet of Trust, France
- Susanne Pingel, BSI, Germany
- Jörg Brauer, Verified Systems International GmbH, Germany
- CC v4 editors team

Final remarks

- ADV_SPM.1 does not prescribe the use of any particular formal method or tool

- If you are interested in Coq, we recommend the following recent paper and guidance written by ANSSI and INRIA research teams
  - *The use of Coq for Common Criteria Evaluations*, Yves Bertot, Maxime Dénès, Vincent Laporte, Arnaud Fontaine, Thomas Letan, POPL2020, https://popl20.sigplan.org/details/CoqPL-2020-papers/2/The-use-of-Coq-for-Common-Criteria-Evaluations
  - *Requirements on the Use of Coq in the Context of Common Criteria Evaluations*, 23/09/2020, https://www.ssi.gouv.fr/uploads/2014/11/anssi-requirements-on-the-use-of-coq-in-the-context-of-common-criteria-evaluations-v1.0-en.pdf

Thank you!

carolina.lavatelli@internetoftrust.com

guillaume.tetu@ssi.gouv.fr


INTERNET
OF TRUST