CERTIFICATION AND STANDARDS

EU CYBERSECURITY ACT: THE TOUGH PART IS YET TO COME!

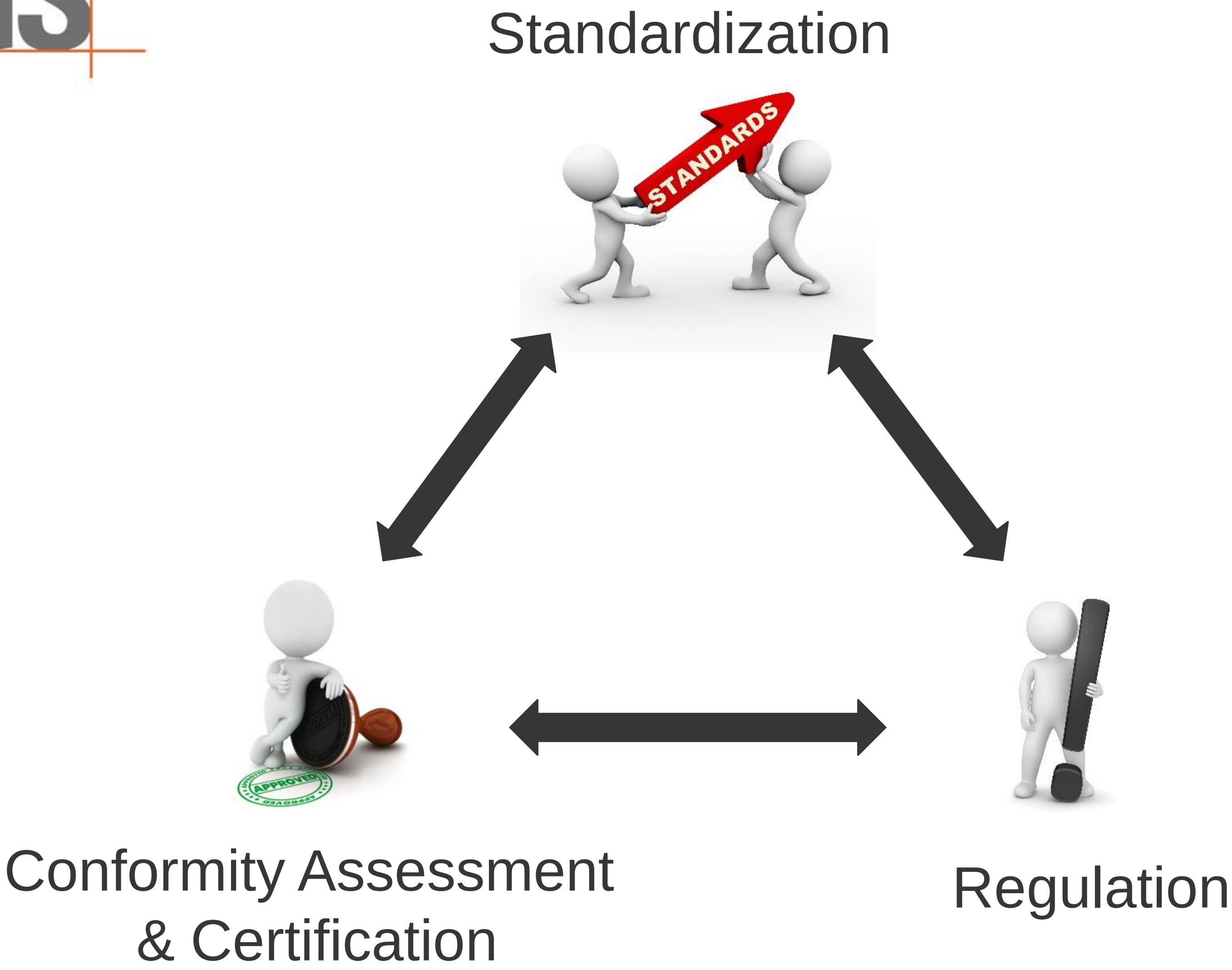
Dr. Martin Schaffer
Global Head of Secure Products & Systems
SGS DIGITAL TRUST SERVICES

European Cyber Security Organisation (ECSO) Working Group 1 Chair
Member of ENISA's Permanent Stakeholders Group
Member of the Eurosmart Board

Aligning and prioritizing EU & international Cybersecurity & Privacy
Cyberwatching.eu – Annual Workshop, Cybersec Forum
Krakow, Poland 08.10.2018

WHEN YOU NEED TO BE SURE

SGS



Standardization

Conformity Assessment
& Certification

Regulation

The EU Cybersecurity Act is a good start, but the tough work is yet to come!

CONFORMITY ASSESSMENT FOR SECURITY

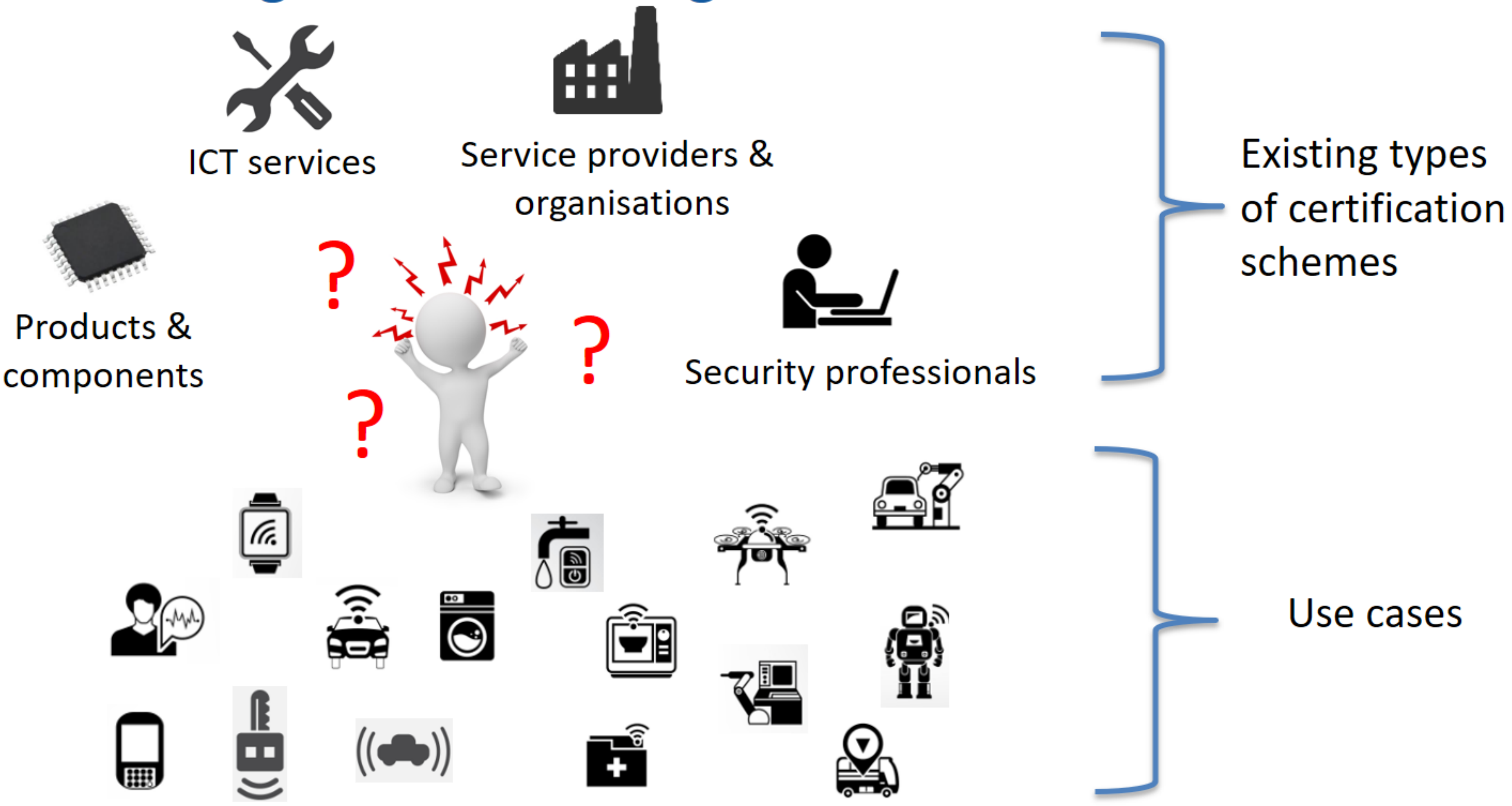
- Traditional conformity assessment
  - Criteria are usually static
  - physical laws do not change: „one kilogram is always one kilogram, also 1 day after getting the certificate“.

- Cybersecurity conformity assessment
  - Criteria are dynamic
  - Attacks are moving: 1 day after getting the certificate there might be a new attack breaking the certified product.

HANDLING THE COMPLEXITY

EUROPEAN CYBER SECURITY ORGANISATION

What to do?
There is not a single scheme fitting all needs!



ICT services

Service providers & organisations

Products & components

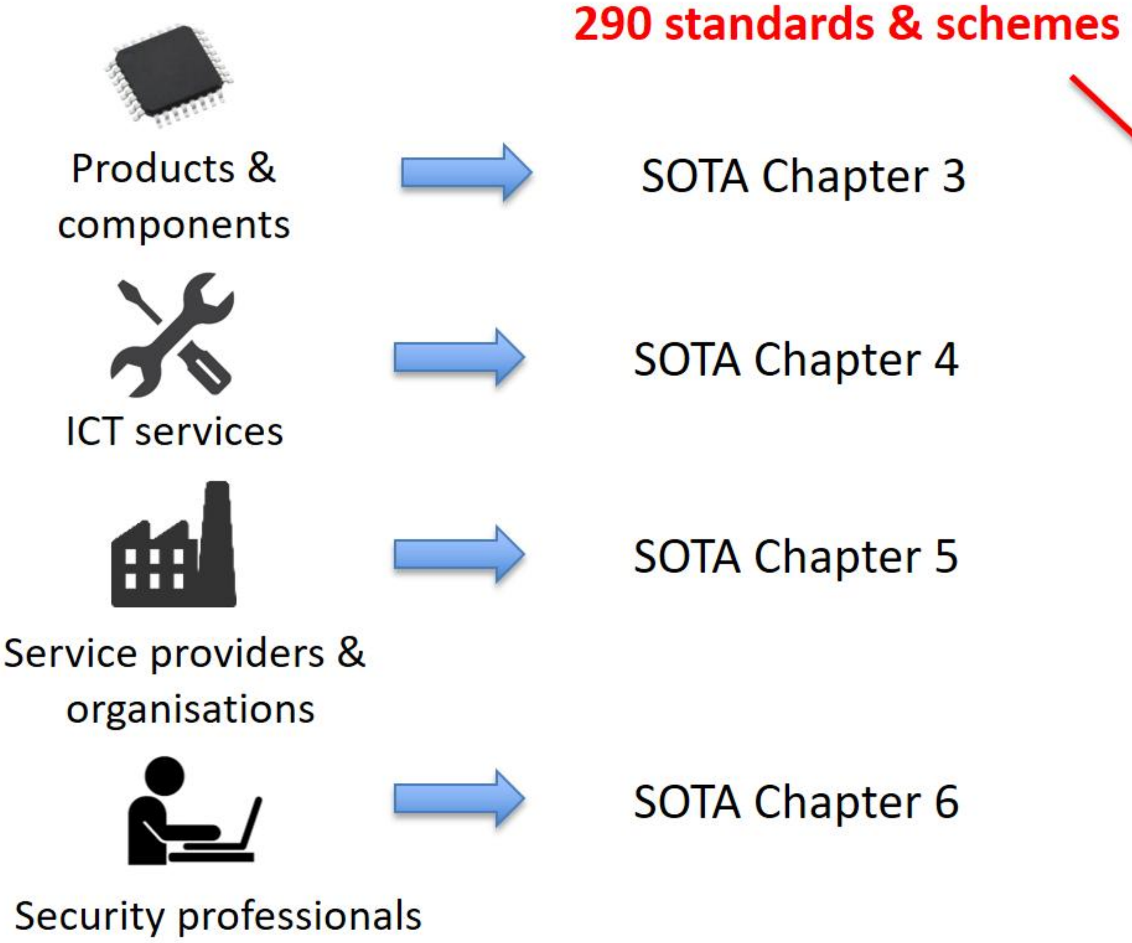
Security professionals

Existing types of certification schemes

Use cases

USING A STRUCTURED APPROACH

First of all: collection of what exists!



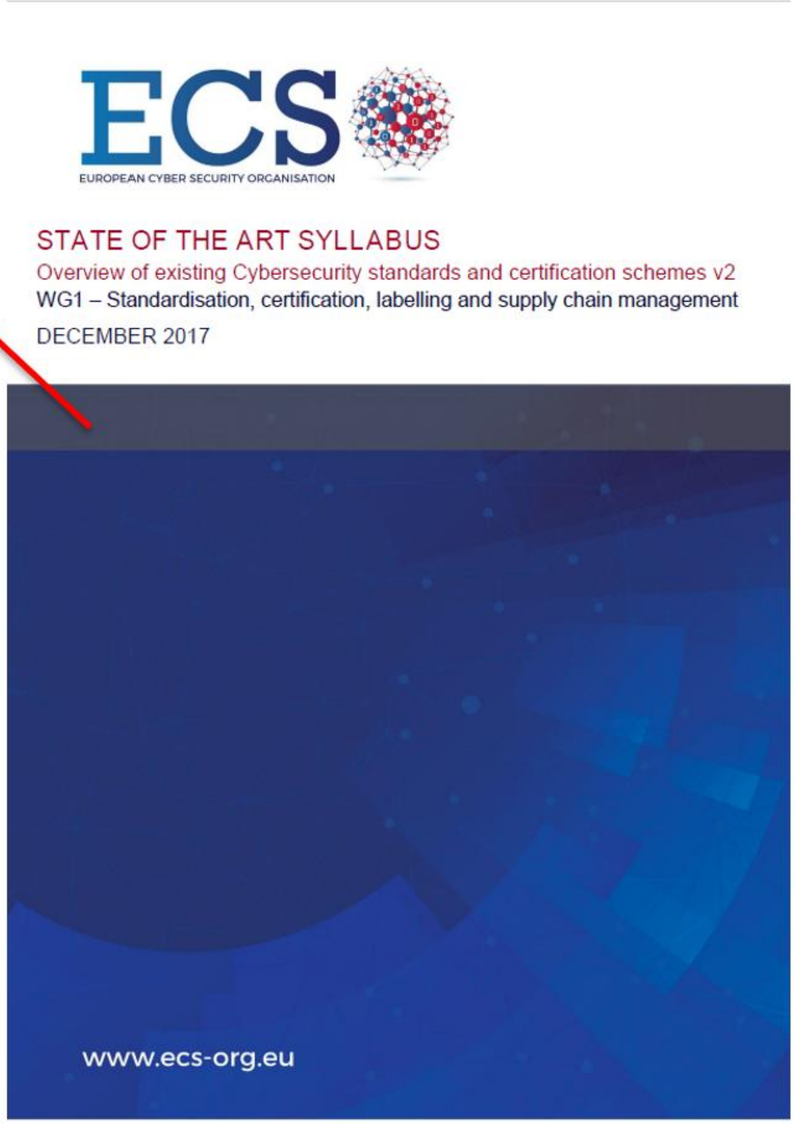
290 standards & schemes

Products & components → SOTA Chapter 3

ICT services → SOTA Chapter 4

Service providers & organisations → SOTA Chapter 5

Security professionals → SOTA Chapter 6



ECS

EUROPEAN CYBER SECURITY ORGANISATION

STATE OF THE ART SYLLABUS

Overview of existing Cybersecurity standards and certification schemes v2

WG1 – Standardisation, certification, labelling and supply chain management

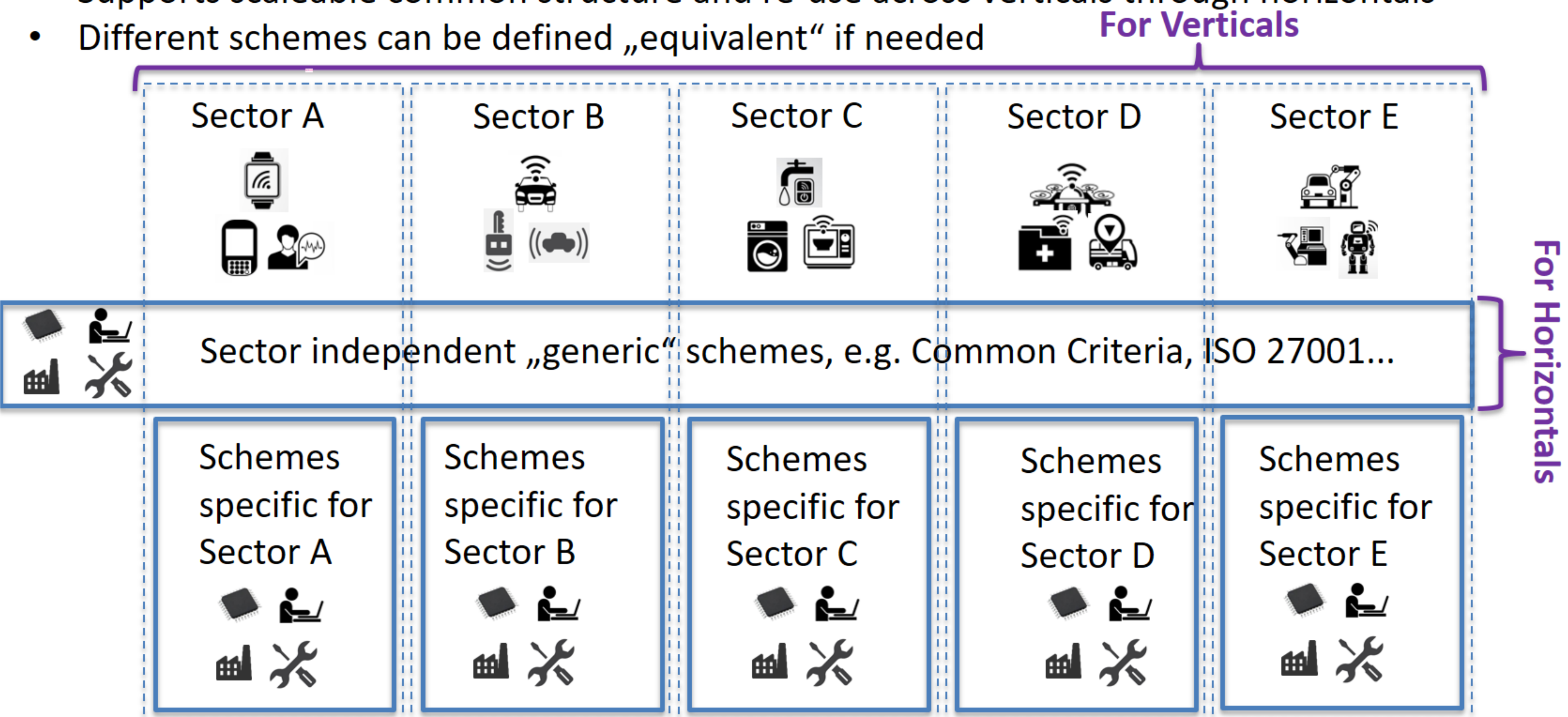
DECEMBER 2017

www.ecs-org.eu

CREATING A META-STRUCTURE

Then create a structure: Meta-Scheme Idea

- Allows composition across **different** schemes via a meta-language
- Supports scaleable common structure and re-use across verticals through horizontals
- Different schemes can be defined „equivalent“ if needed



For Verticals

Sector A

Sector B

Sector C

Sector D

Sector E

Sector independent „generic“ schemes, e.g. Common Criteria, ISO 27001...

For Horizontals

Schemes specific for Sector A

Schemes specific for Sector B

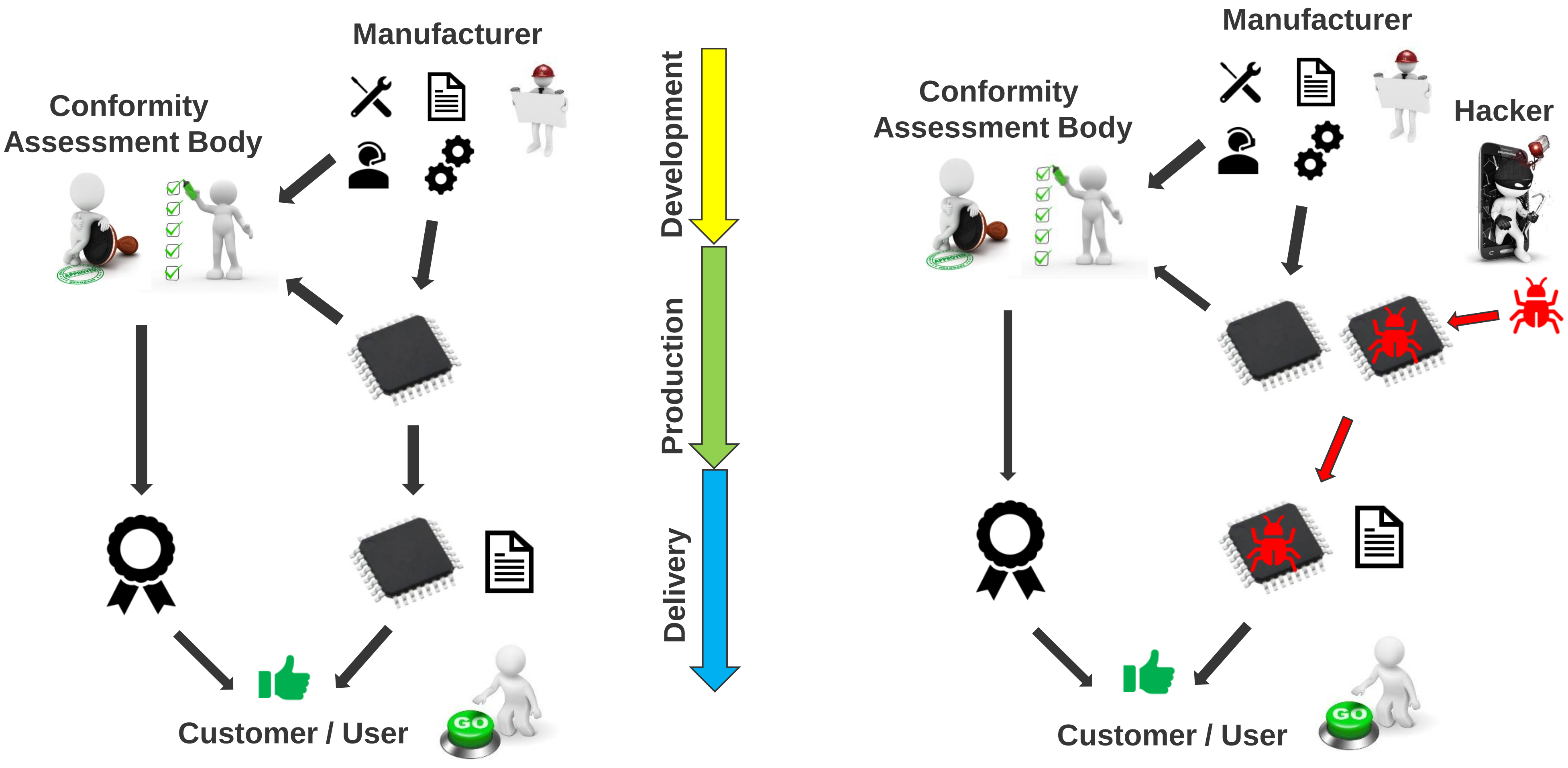
Schemes specific for Sector C

Schemes specific for Sector D

Schemes specific for Sector E

SUPPLY CHAIN INTEGRITY ISSUES

- Case A: integrity preserved
- Case B: integrity violated

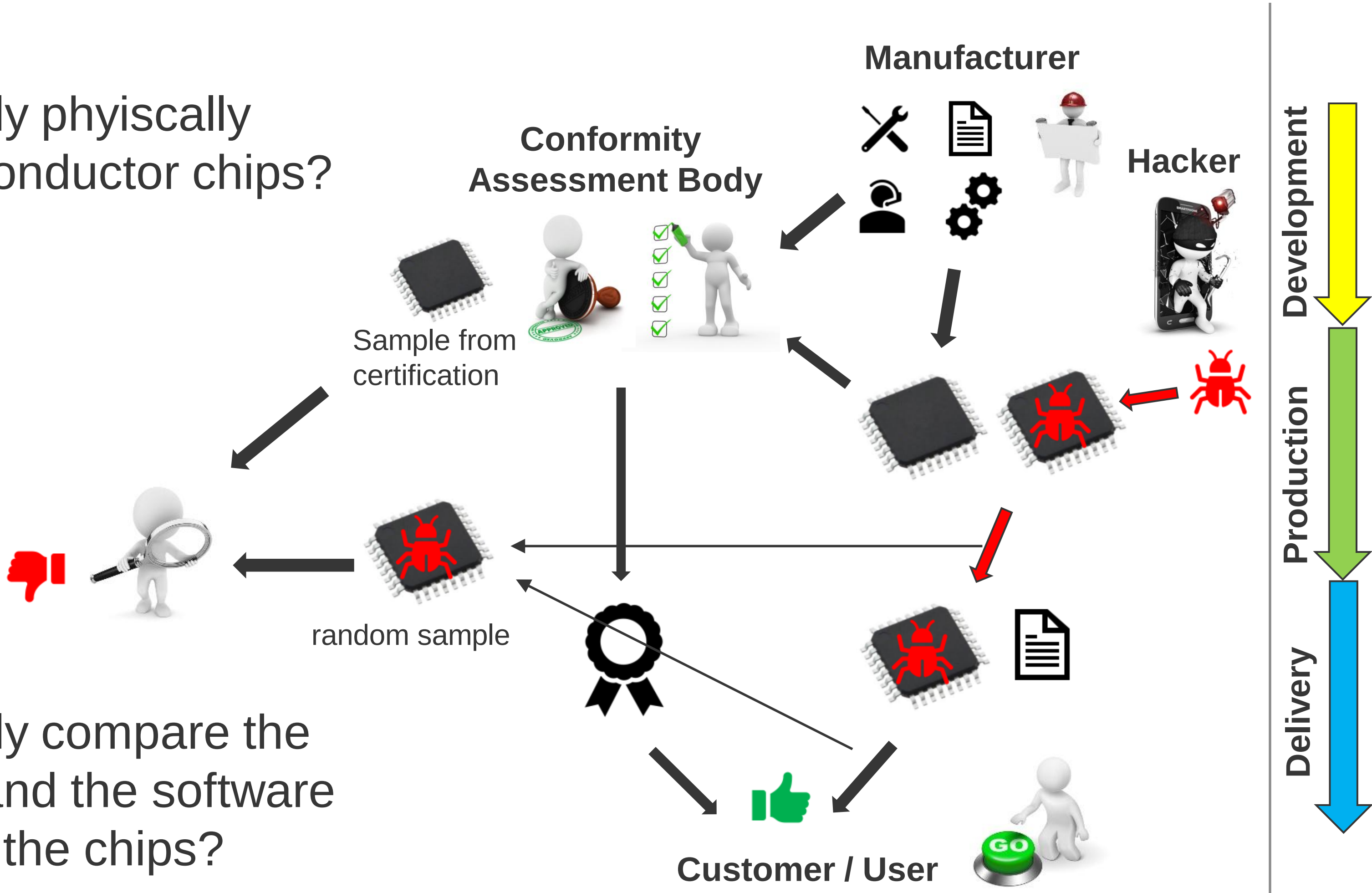


How can the customer know that the product at hand is the certified one?

MARKET SURVEILLANCE: SAMPLE CHECKS

The challenges

- How to efficiently phyiscally compare semiconductor chips?



- How to efficiently compare the configurations and the software stored inside of the chips?

CONCLUSION

- Security **standards** are crucial to have criteria as a basis for regultion and conformity assessment

- **Regulation** is essential to ensure products & services are only delivered if there is certain confidence that they are no harming the user

- **Conformity assessment & certification** are a useful instrument to get confidence about the security, but it must be able to handle the fact that attacks are moving

- **Market surveillance** is crucial to ensure that what has been delivered to a customer is consistent with what has been assessed

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

SGS