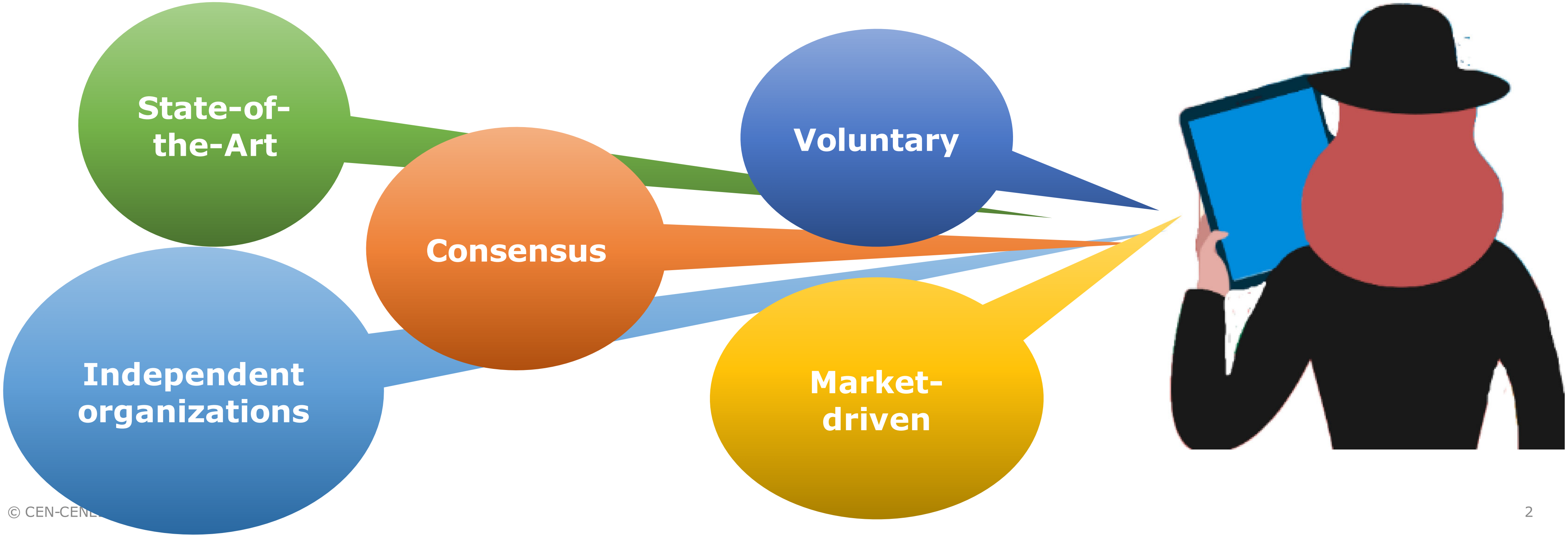
European Standardization Organizations

Setting the scene

Cinzia Missiroli – CEN-CENELEC
Director Standardization & Digital Solutions

European Standards

A key tool for the (security of the) **Single Market**



State-of-the-Art

Voluntary

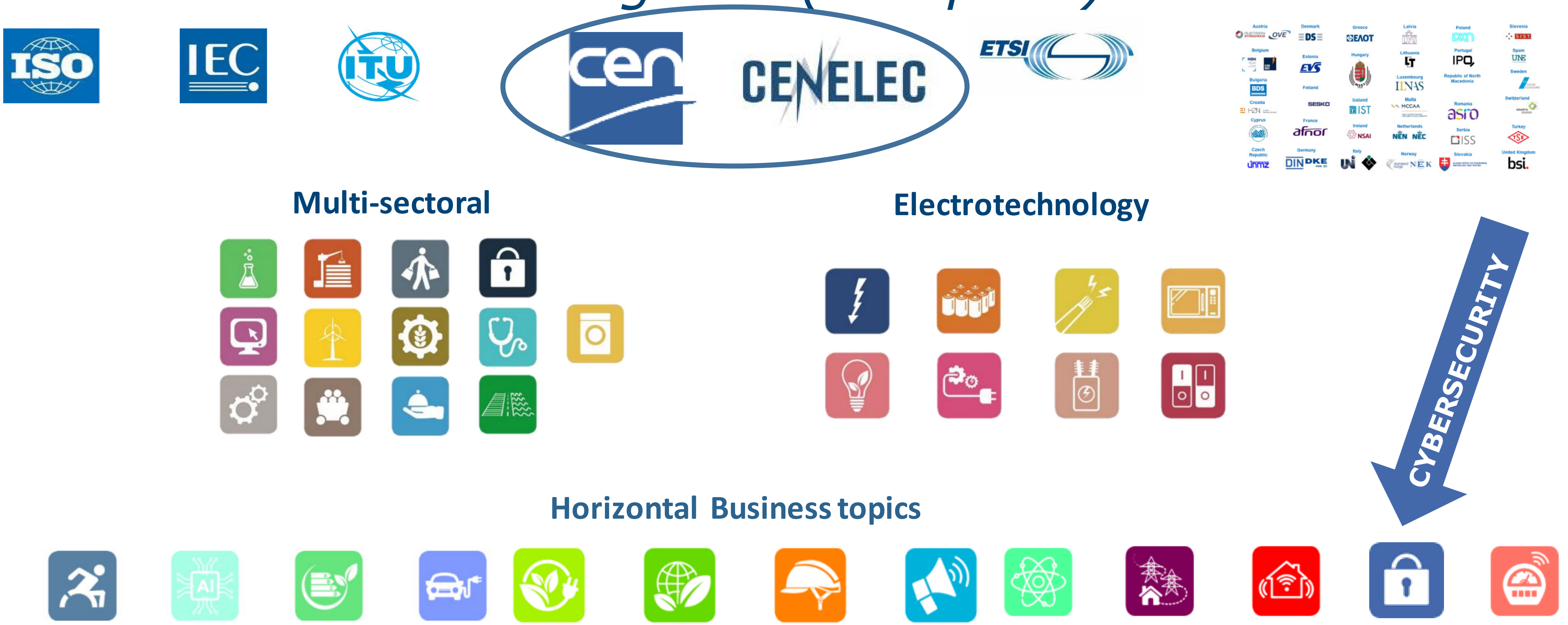
Consensus

Independent organizations

Market-driven

Making Standards for Europe

International → Regional (European) → National

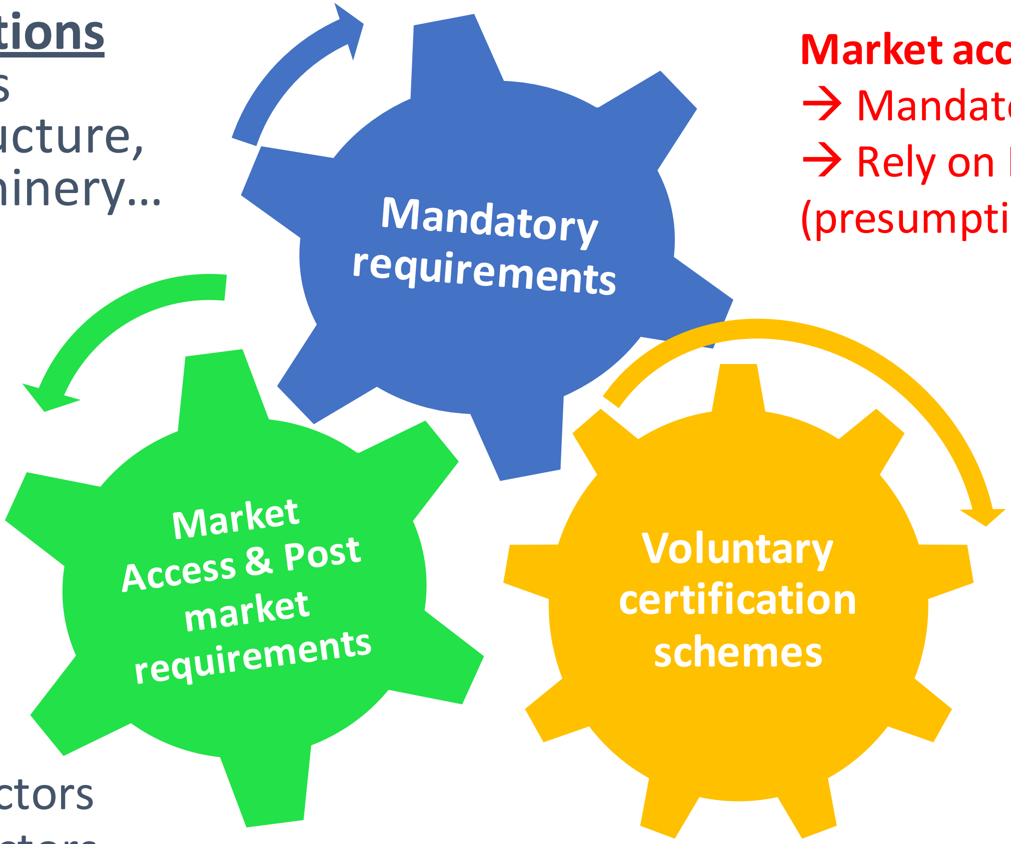


CEN and CENELEC at the interplay between legislation, standardization, conformity assessment and certification

cen CENELEC ETSI
EUROPEAN STANDARDIZATION ORGANIZATIONS
European Commission
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
IEC
ISO
Austria
Denmark
Greece
Latvia
Poland
Slovenia
Belgium
Estonia
Hungary
Lithuania
Portugal
Spain
Bulgaria
Finland
Luxembourg
Republic of North Macedonia
Sweden
Croatia
Iceland
Malta
Romania
Switzerland
Cyprus
France
Ireland
Netherlands
Serbia
Turkey
Czech Republic
Germany
Italy
Norway
Slovakia
United Kingdom

Intertwined European Regulatory Frameworks

Directives and Regulations
Essential requirements
RED, Network Infrastructure,
Medical Devices, Machinery…


Mandatory requirements
Market Access & Post market requirements
Voluntary certification schemes

Market access:
→ Mandatory essential requirements
→ Rely on Harmonized Standards (presumption of conformity)

Certification: market access + post market
→ Voluntary schemes (with different assurance levels)
→ Rely on ENISA/EC certification schemes

Standardization:
→Pre and post
→Horizontal for all sectors
→Consistent for all sectors

High risks: protecting critical infrastructures

- **Critical infrastructure** (power plant, hospital) requires high level of protection
- It also requires strong **combination between IT and OT**: protect data flow and also apply security requirements that are part of the 'real' world
- Relying on Operational Technologies (OT) to ensure the **correct execution of automated actions** (e.g. shutting down a valve)
- OT includes both hardware and software to **keep systems working as intended**

With the emergence of IoT and the integration of physical machines with sensors and software, the lines between IT and OT are blurring

A key issue is that cyber security is commonly understood only in terms of IT

Linking IT with OT: example of the role of the EN IEC 62443 series

- Industrial systems depend on **Operational Technology** (OT), which must be taken into account to mitigate cyber risks

- The EN IEC 62443 series was developed to secure industrial communication network and industrial automation and control systems (IACS) through a systematic approach

- IACS also includes Supervisory Control and Data Acquisition (SCADA) systems that are used by organizations operating in critical infrastructure industries

Focus on EN IEC 62443-4-1 for secure product development lifecycle requirements:

- **Specifies process requirements**
- **Defines secure development life-cycle requirements**
- **Security requirements definitions**
- **Secure design, implementation, verification and validation**

EN IEC 62443 standards are the cornerstone for an industrial secure-by-design approach and provide the IT-OT integration

Some current focus and challenges...

Ensure transition based on requested **harmonized standards**

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Ensure the right ENs are available to support ENISA schemes

EUROPEAN NORM
EN

Address new technologies and trends in standards

Standards in support of the evolving framework

- Radio Equipment Directive (RED)
  - *First drafts will be made available in October for EC assessment in accordance with schedule*
  - *To address the transition with the Cyber Resilience Act*

- Work continues on the Technical Specifications in support of the **EUCS**:
  - *Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services*
  - *Requirements for Conformity Assessment Bodies certifying Cloud Services*

- EN 17640 "**Fixed time cybersecurity evaluation methodology for ICT products**" will be made available on October 19th

- **Upcoming Standardization Request on AI** calling for cybersecurity specifications for AI systems – basis for a future AI scheme?

- New technical activities:
  - **Quantum technologies**: standardization roadmap finalization (by November)
  - **Trusted & Secure Chips and semi-conductors –** stakeholders' workshops to be held in December

An evolving framework… that requires alignment and coordination between all the actors in the ecosystem

European Standards provide trust …a harmonized approach for cybersecurity in the EU market

European Standardization Organizations

Thank you

cmissiroli@cencenelec.eu
www.cencenelec.eu

Follow us