ILNAS/ETSI Breakfast

“Standardization of ICT, research and cybersecurity”

25.04.2024

Speakers

Dr. Jean-Philippe HUMBERT

ILNAS - Deputy Director

Mr. Nicolas DOMENJOUD

ILNAS/OLN - Responsible ICT & Technical Standardization

Ms. Claire D’ESCLERCS

ETSI - Director for Membership Development and Education

Mr. David BOSWARTHICK

ETSI - Director for New Technologies

Mr. Scott CADZOW

ETSI Chair of TC SAI, TC ITS WG5, ISG ETI and Vice-Chair of TC eHealth

Agenda

09h00 - 09h30	**Welcoming of participants**
09h30 - 09h45	**Introduction** *Dr. Jean-Philippe HUMBERT* *ILNAS – Deputy Director*
09h45 - 10h00	**Overview of ICT technical standardization - Standards Analysis of the ICT sector** *Mr. Nicolas DOMENJOUD* *ILNAS/OLN – Responsible ICT & Technical Standardization*
10h00 - 10h20	**An introduction to ETSI** *Ms. Claire D'ESCLERCS* *ETSI - Director for Membership Development and Education*
10h20 – 10h35	**Coffee Break**
10h35 – 10h55	**ETSI - Innovation and Research** *Mr. David BOSWARTHICK* *ETSI - Director for New Technologies*
10h55 - 11h15	**ETSI - Cyber Security and related topics** *Mr. Scott CADZOW* *ETSI Chair of TC SAI, TC ITS WG5, ISG ETI and Vice-Chair of TC eHealth*
11h15 - 11h45	**Q&A**

ILNAS/ETSI Breakfast “Standardization of ICT, research and cybersecurity”

Introduction

25 April 2024

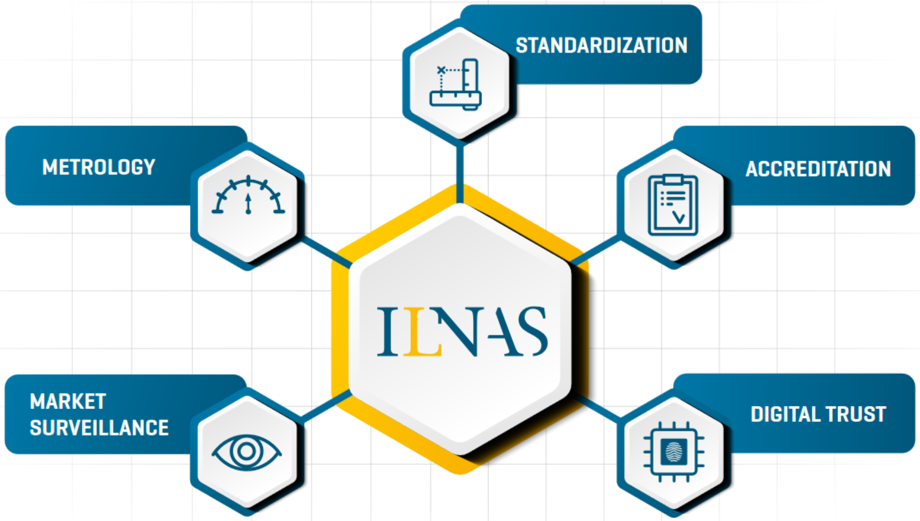
Jean-Philippe HUMBERT - Deputy Director, ILNAS

Presentation of ILNAS

- **ILNAS**
  - Public administration under the authority of the Minister of the Economy, SME, Energy and Tourism
  - Creation: Law of May 20, 2008
  - Legislation in force: amended Law of July 4, 2014 reorganizing ILNAS
  - Total staff: 62 (April 2024)
  - ISO 9001:2015 certification (Budget and administration department, OLN, Digital Trust department, Market surveillance department, BLM, OEC)

PORTAIL-QUALITE.LU
QUALITE·SECURITE·CONFORMITE
UNE INITIATIVE DE L'ILNAS

- **National Standards Body (OLN)**
  - Composed of 8 persons
  - Close collaboration with the E.I.G. ANEC-N



ILNAS

ANEC – Agency for standardization and knowledge-based economy

ANEC

- **Creation**: October 4, 2010
- **Status**: Economic Interest Group (EIG)
- **Objectives:** Promotion, awareness raising and training, applied research in the field of standardization and metrology in order to support companies' competitiveness in Luxembourg
- **Human resources**: 9 persons, including 4 employees in the standardization department (April 2024)
- **Partners** :

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

ILNAS

CHAMBRE
DES METIERS
Luxembourg

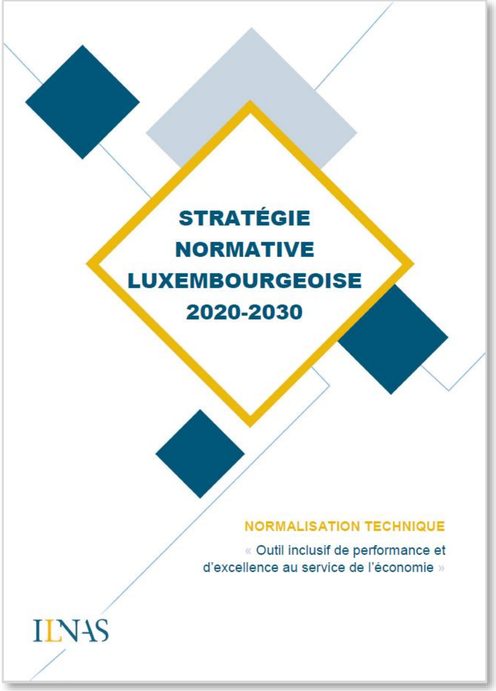
CHAMBRE DE
COMMERCE
LUXEMBOURG

➔ Support for the implementation of the Luxembourg standardization strategy

Luxembourg standardization strategy 2020-2030

Technical standardization

"Inclusive tool for performance and excellence to serve the economy"



STRATÉGIE NORMATIVE LUXEMBOURGEOISE 2020-2030

NORMALISATION TECHNIQUE

« Outil inclusif de performance et d'excellence au service de l'économie »

ILNAS

PERFORMANCE

- □ Pillar 1 – Use of relevant technical standards
- □ Pillar 2 – Involvement in the standardization process

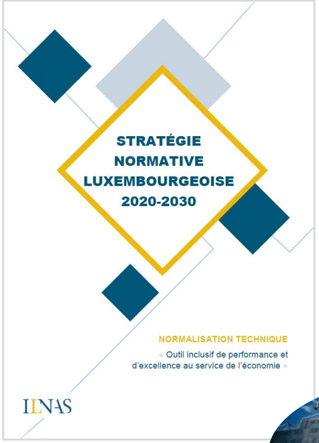
EXCELLENCE

- □ Pillar 3 – Active participation of the NSB in the European and international standardization organizations
- □ Pillar 4 – Development of research and education about standardization

https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

ILNAS

Luxembourg standardization strategy 2020-2030



STRATÉGIE NORMATIVE LUXEMBOURGEOISE 2020-2030

NORMALISATION TECHNIQUE

« Outil inclusif de performance et d'excellence au service de l'économie »

ILNAS

Technical standardization

"Inclusive tool for performance and excellence to serve the economy"

3 growth sectors identified

CONSTRUCTION

Politique pour la normalisation technique du secteur de la construction (2020-2025)

ILNAS

INFORMATION AND COMMUNICATION TECHNOLOGIES

Policy on ICT Technical Standardization (2020-2025)

ILNAS

AEROSPACE

Policy on Aerospace Technical Standardization (2021-2025)

ILNAS

- ➢ Computer Aided Design (CAD)
- ➢ Building Information Modelling (BIM)
- ➢ 3D printing
- ➢ …

- ➢ Space data processing
- ➢ Space traffic management
- ➢ Smart Mobility
- ➢ …

Identification of trans-sectoral standardization interactions

CONFORMITY

Politique normative nationale « ISO CASCO » 2022-2030

ILNAS

SUSTAINABILITY

Politique pour la normalisation technique du domaine du développement durable (2024-2026)

ILNAS

Luxembourg’s policy on ICT technical standardization

“Foster and strengthen the national ICT sector involvement in standardization work”

→ **Three lead projects**

Policy on ICT Technical Standardization (2022-2025)

ILNAS

1. Promoting the ICT technical standardization to the market
2. Reinforcing the valorization and the involvement regarding ICT technical standardization
3. Supporting and strengthening the EaS and the related research activities

Politique pour la normalisation technique du secteur de la construction (2020-2025)

Politique normative nationale « ISO CASCO » 2022-2030

Policy on Aerospace Technical Standardization (2021-2025)

ILNAS

Policies for the Construction and Aerospace sectors, as well as for the “Conformity” domain are based on similar lead projects

Promoting the ICT technical standardization to the market

Standards Analysis

2024 - Standards Analysis

ILNAS

STANDARDS ANALYSIS

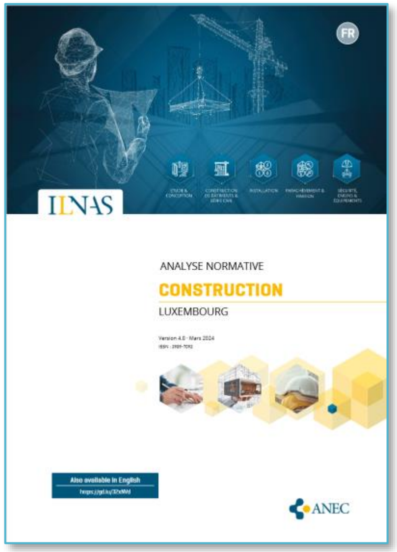
ICT SECTOR

LUXEMBOURG

Version 14.0 · April 2024

ISSN 2799-2411

ANEC


ILNAS

ANALYSE NORMATIVE

CONSTRUCTION

LUXEMBOURG

Version 4.0 · Mars 2024

ISSN : [illegible]

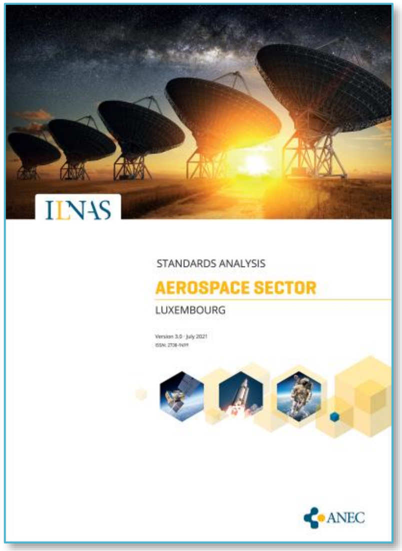
Also available in English

https://gd.lu/32xWd

ANEC

- **Content**
  - ○ Standardization context of the related sectors
  - ○ Presentation of European (CEN,CLC, ETSI) and international (ISO, IEC) technical committees active in the related sectors (distributed among subsectors relevant for the national economy)
  - ○ Offer guidance to national stakeholders for a potential future involvement in the standardization development process

- **Updated annually (twice a year for ICT)**


ILNAS

STANDARDS ANALYSIS

AEROSPACE SECTOR

LUXEMBOURG

Version 3.0 · July 2021

ISSN: 2738-9499

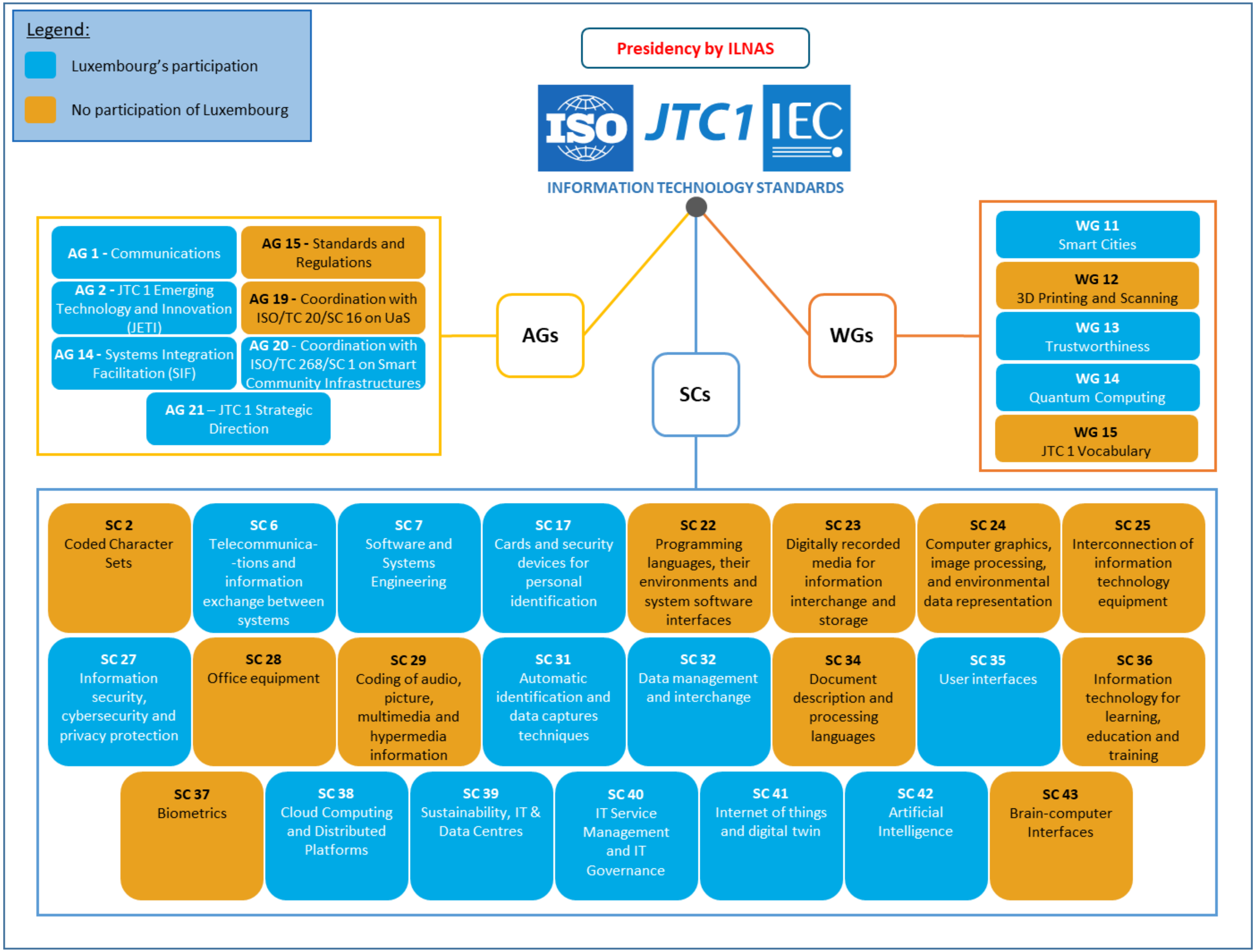
ANEC

Update planned in June 2024

ILNAS

Reinforcing the valorization and the involvement regarding ICT technical standardization

ISO/IEC JTC 1



Legend:

🟦 Luxembourg's participation

🟧 No participation of Luxembourg

Presidency by ILNAS

ISO JTC1 IEC

INFORMATION TECHNOLOGY STANDARDS

AGs

- 🟦 **AG 1 -** Communications
- 🟧 **AG 15 -** Standards and Regulations
- 🟦 **AG 2 -** JTC 1 Emerging Technology and Innovation (JETI)
- 🟧 **AG 19 -** Coordination with ISO/TC 20/SC 16 on UaS
- 🟦 **AG 14 -** Systems Integration Facilitation (SIF)
- 🟦 **AG 20** - Coordination with ISO/TC 268/SC 1 on Smart Community Infrastructures
- 🟦 **AG 21** – JTC 1 Strategic Direction

WGs

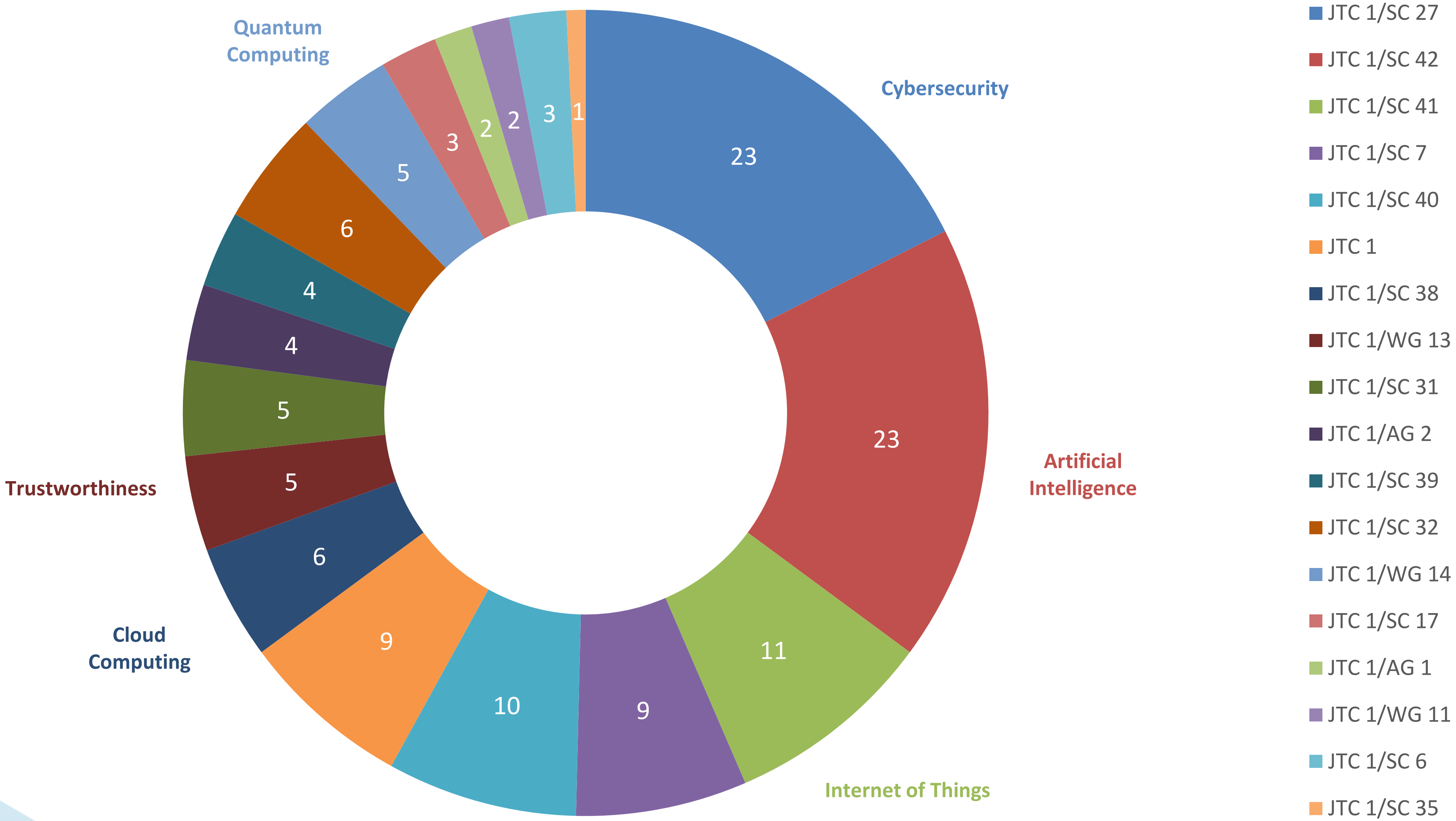
- 🟦 **WG 11** Smart Cities
- 🟧 **WG 12** 3D Printing and Scanning
- 🟦 **WG 13** Trustworthiness
- 🟦 **WG 14** Quantum Computing
- 🟧 **WG 15** JTC 1 Vocabulary

SCs

- 🟧 **SC 2** Coded Character Sets
- 🟦 **SC 6** Telecommunica--tions and information exchange between systems
- 🟦 **SC 7** Software and Systems Engineering
- 🟦 **SC 17** Cards and security devices for personal identification
- 🟧 **SC 22** Programming languages, their environments and system software interfaces
- 🟧 **SC 23** Digitally recorded media for information interchange and storage
- 🟧 **SC 24** Computer graphics, image processing, and environmental data representation
- 🟧 **SC 25** Interconnection of information technology equipment
- 🟦 **SC 27** Information security, cybersecurity and privacy protection
- 🟧 **SC 28** Office equipment
- 🟧 **SC 29** Coding of audio, picture, multimedia and hypermedia information
- 🟦 **SC 31** Automatic identification and data captures techniques
- 🟦 **SC 32** Data management and interchange
- 🟧 **SC 34** Document description and processing languages
- 🟦 **SC 35** User interfaces
- 🟧 **SC 36** Information technology for learning, education and training
- 🟧 **SC 37** Biometrics
- 🟦 **SC 38** Cloud Computing and Distributed Platforms
- 🟦 **SC 39** Sustainability, IT & Data Centres
- 🟦 **SC 40** IT Service Management and IT Governance
- 🟦 **SC 41** Internet of things and digital twin
- 🟦 **SC 42** Artificial Intelligence
- 🟧 **SC 43** Brain-computer Interfaces

Reinforcing the valorization and the involvement regarding ICT technical standardization

ISO/IEC JTC 1

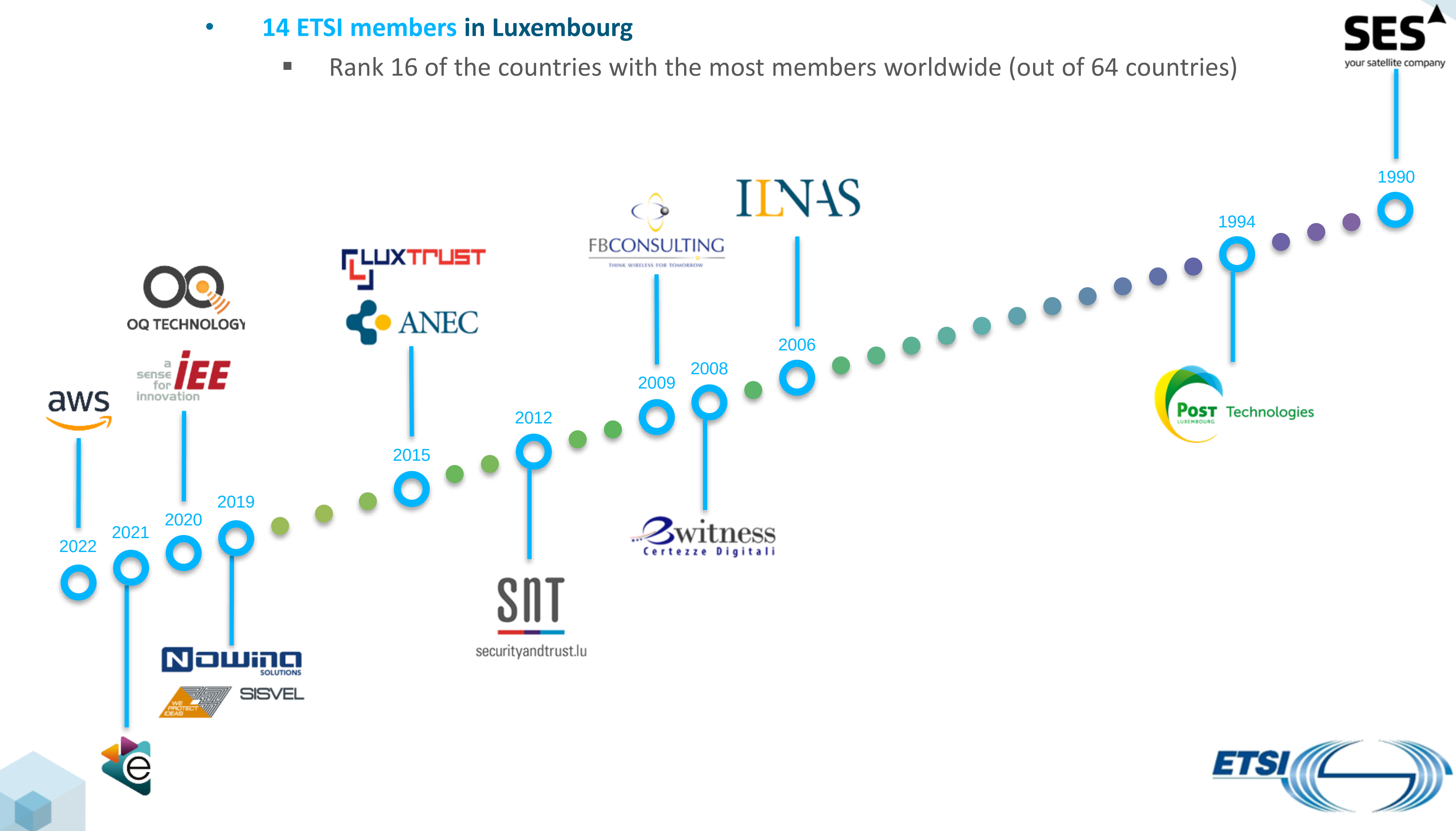


→ 67 national delegates registered in ISO/IEC JTC 1 (92 in total for the ICT sector)

Reinforcing the valorization and the involvement regarding ICT technical standardization

ETSI

- **14 ETSI members in Luxembourg**
  - Rank 16 of the countries with the most members worldwide (out of 64 countries)

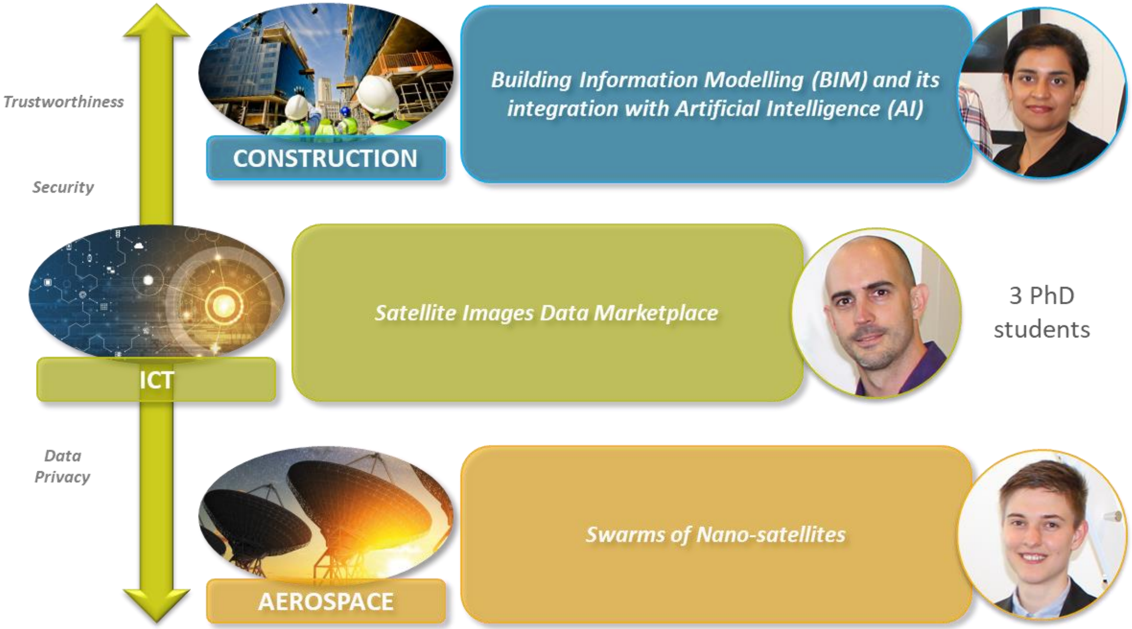


ETSI

Supporting and strengthening the EaS and the related research activities

Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024)

Research program “Technical Standardisation for Trustworthy ICT, Aerospace, and Construction” (2021-2024) in collaboration with the University of Luxembourg



Trustworthiness

Security

Data Privacy

CONSTRUCTION

Building Information Modelling (BIM) and its integration with Artificial Intelligence (AI)

ICT

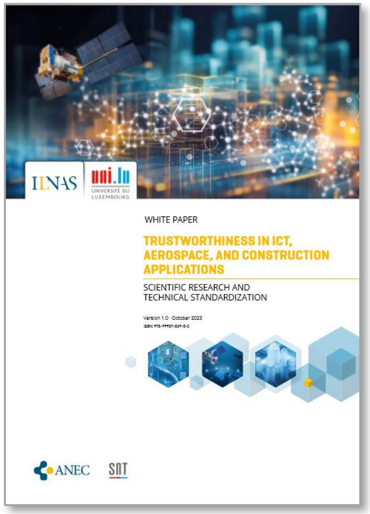
Satellite Images Data Marketplace

AEROSPACE

Swarms of Nano-satellites

3 PhD students

1 postdoc



ILNAS | uni.lu UNIVERSITÉ DU LUXEMBOURG

WHITE PAPER

TRUSTWORTHINESS IN ICT, AEROSPACE, AND CONSTRUCTION APPLICATIONS

SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION

Version 1.0 · October 2023

ISBN 978-99987-869-8-0

ANEC SnT

https://ilnas-snt.uni.lu/

ILNAS

Supporting and strengthening the EaS and the related research activities

Research project CORAL - cybersecurity Certification based On Risk evALuation and treatment

CORAL

Luxembourg House of Cybersecurity

ILNAS

ANEC

CORAL - cybersecurity Certification based On Risk evALuation and treatment

Co-financed by the Connecting Europe Facility of the European Union

The European CORAL project
Copier le li...
CORAL
cybersecurity Certification based On Risk evALuation
Regarder sur YouTube
ILNAS
ANEC

https://youtu.be/kmMHJ-lj4FY

Overview

CORAL is a European Union-funded project under CEF Telecom Call, that **aims to elaborate a toolkit and methodology to speed up the certification process in line with the EU Cybersecurity Act** or CSA (Regulation EU 2019/881). The project aims to address challenges concerning self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with the CSA.

The CORAL project is being developed in a Luxembourgish context, but it aims to become known and used beyond the Luxembourg market and borders. Its target audience is primarily small and medium enterprises who have a product or service for which, they wish to assess the basic cybersecurity requirements.

Fit4CSA tool: https://fit4csa.nc3.lu/

CORAL website: https://coral-project.org/

Supporting and strengthening the EaS and the related research activities

White Papers & Technical Reports ILNAS

2020-2023 - ILNAS Research activities

1 White Paper published

ARTIFICIAL INTELLIGENCE

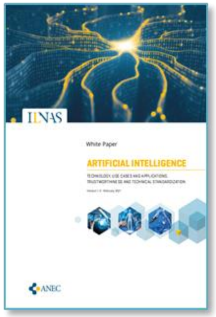
Technology review

Economic overview

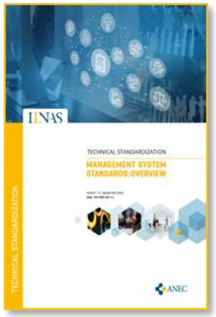
Challenges

Technical Standardization

...


ILNAS
White Paper
ARTIFICIAL INTELLIGENCE
TECHNOLOGY, USE CASES AND APPLICATIONS, TRUSTWORTHINESS AND TECHNICAL STANDARDIZATION
ANEC

ILNAS
TECHNICAL STANDARDIZATION
ADDRESSING CLOUD COMPUTING CHALLENGES AND SUPPORTING RELATED ICT DEVELOPMENT
TECHNICAL STANDARDIZATION
ANEC


ILNAS
TECHNICAL STANDARDIZATION
MANAGEMENT SYSTEM STANDARDS: OVERVIEW
TECHNICAL STANDARDIZATION
ANEC

BLOCKCHAIN

INTERNET OF THINGS

CLOUD COMPUTING

MSS

4 National Technical Standardization Reports published

(November 2023)

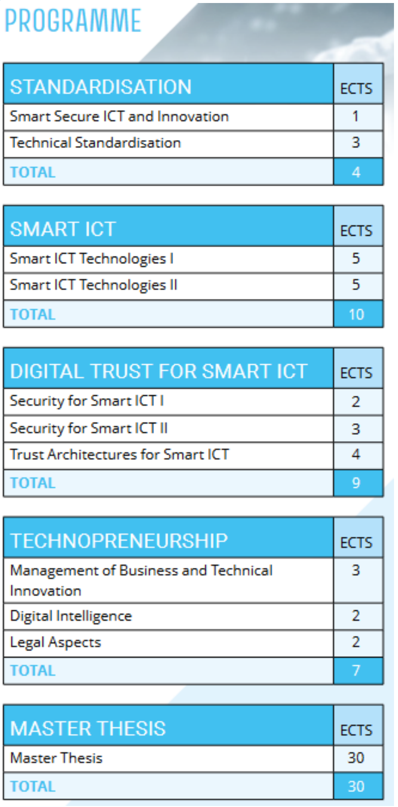
New Technical Standardization Report on Quantum Technologies

ILNAS

Supporting and strengthening the EaS and the related research activities

Master MTECH (second promotion)

Master MTECH (2023-2024) – ILNAS in collaboration with the University of Luxembourg and the Chamber of Employees



PROGRAMME

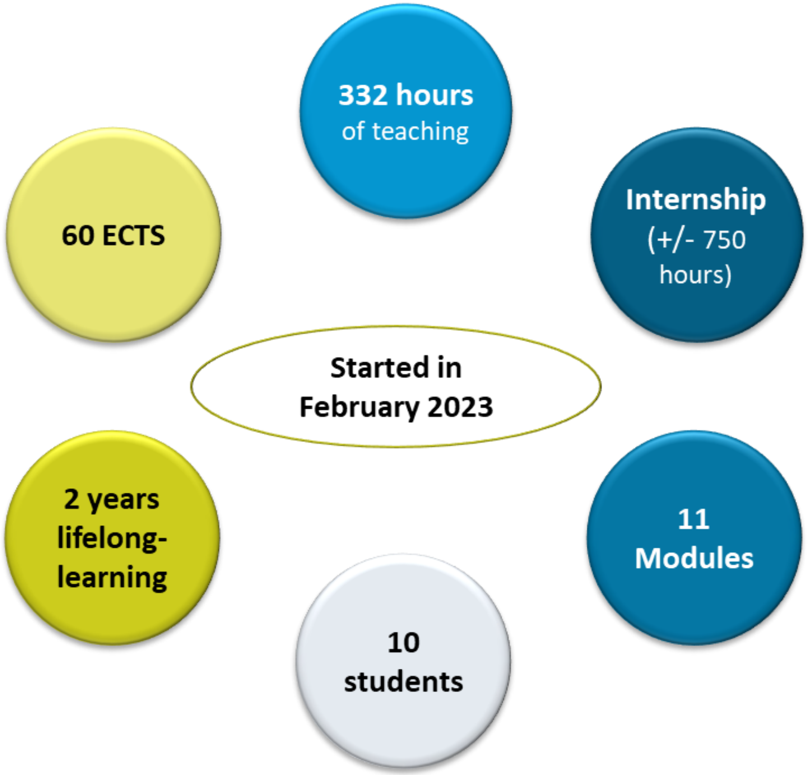
STANDARDISATION	ECTS
Smart Secure ICT and Innovation	1
Technical Standardisation	3
TOTAL	4

SMART ICT	ECTS
Smart ICT Technologies I	5
Smart ICT Technologies II	5
TOTAL	10

DIGITAL TRUST FOR SMART ICT	ECTS
Security for Smart ICT I	2
Security for Smart ICT II	3
Trust Architectures for Smart ICT	4
TOTAL	9

TECHNOPRENEURSHIP	ECTS
Management of Business and Technical Innovation	3
Digital Intelligence	2
Legal Aspects	2
TOTAL	7

MASTER THESIS	ECTS
Master Thesis	30
TOTAL	30



332 hours of teaching

60 ECTS

Internship (+/- 750 hours)

Started in February 2023

2 years lifelong-learning

11 Modules

10 students

Next promotion in September 2024

With the support of: THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy

cen CENELEC ETSI

Supporting and strengthening the EaS and the related research activities

Master MTECH – Profile of the students enrolled in the Master MTECH

WOMEN : MEN

30% 70%

3 : 7

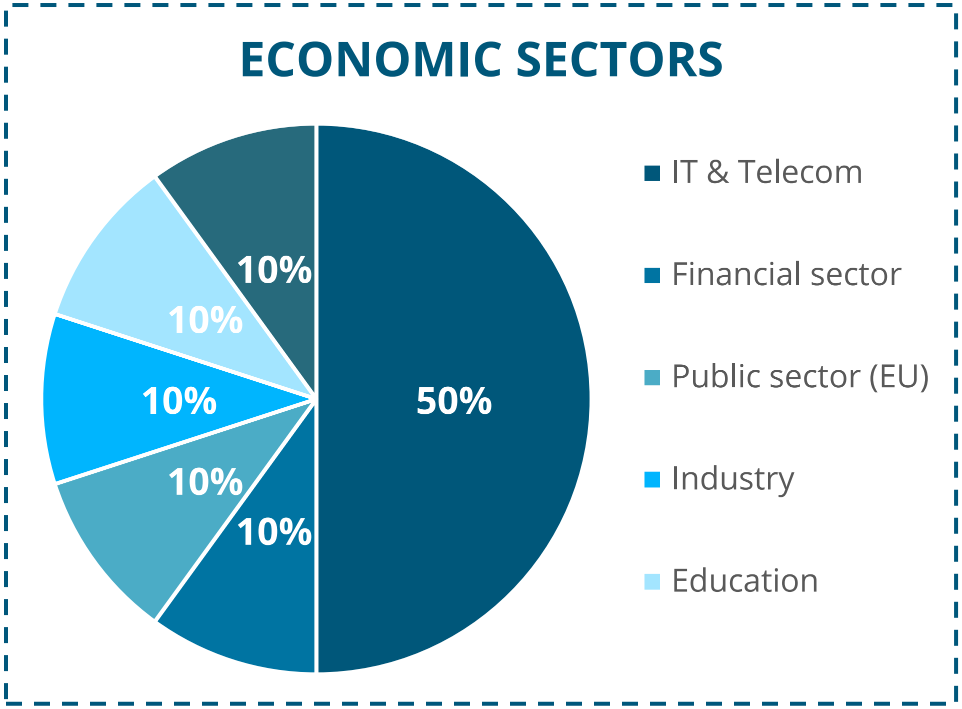
AGE

28 → 56

Average: 40

NATIONALITIES

9


ECONOMIC SECTORS

SAVE THE DATE

12/06/2024

ILNAS Breakfast

Presentation of the Technical Standardization Report on Conformity

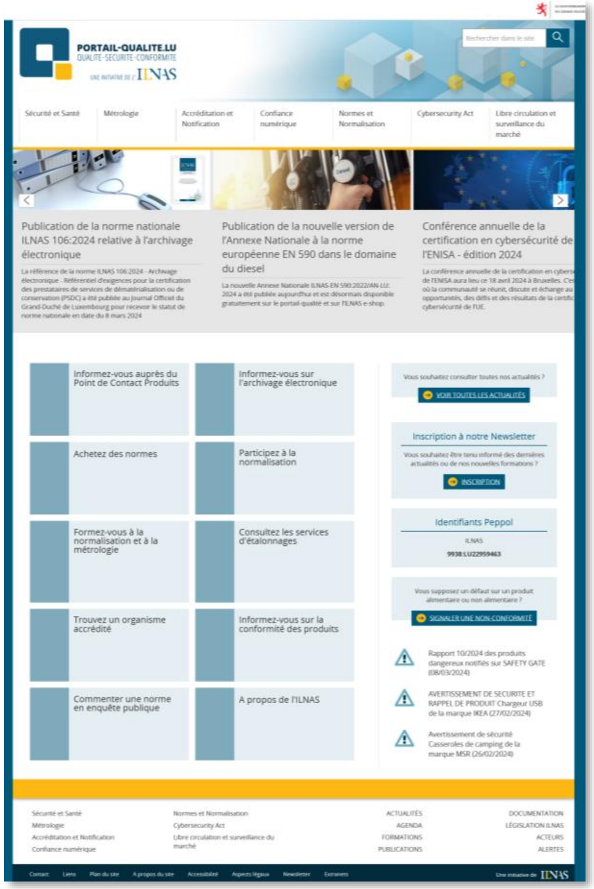
20/06/2024

Workshop ILNAS "Space & Technical Standardization

New version of the Standards Analysis of the space sector

STAY INFORMED ABOUT ILNAS ACTIVITIES

→ **Portail qualité:**
www.portail-qualite.lu



PORTAIL-QUALITE.LU
QUALITE-SECURITE-CONFORMITE
UNE INITIATIVE DE L'ILNAS

Rechercher dans le site

Sécurité et Santé | Métrologie | Accréditation et Notification | Confiance numérique | Normes et Normalisation | Cybersecurity Act | Libre circulation et surveillance du marché

Publication de la norme nationale ILNAS 106:2024 relative à l'archivage électronique

La référence de la norme ILNAS 106:2024 - Archivage électronique - Référentiel d'exigences pour la certification des prestataires de services de dématérialisation ou de conservation (PSDC) a été publiée au Journal Officiel du Grand-Duché de Luxembourg pour recevoir le statut de norme nationale en date du 8 mars 2024

Publication de la nouvelle version de l'Annexe Nationale à la norme européenne EN 590 dans le domaine du diesel

La nouvelle Annexe Nationale ILNAS-EN 590:2022/AN-LU: 2024 a été publiée aujourd'hui et est désormais disponible gratuitement sur le portail-qualité et sur l'ILNAS e-shop.

Conférence annuelle de la certification en cybersécurité de l'ENISA - édition 2024

La conférence annuelle de la certification en cybers
de l'ENISA aura lieu ce 18 avril 2024 à Bruxelles. C'e
où la communauté se réunit, discute et échange au
opportunités, des défis et des résultats de la certific
cybersécurité de l'UE.

- Informez-vous auprès du Point de Contact Produits
- Informez-vous sur l'archivage électronique
- Achetez des normes
- Participez à la normalisation
- Formez-vous à la normalisation et à la métrologie
- Consultez les services d'étalonnages
- Trouvez un organisme accrédité
- Informez-vous sur la conformité des produits
- Commenter une norme en enquête publique
- A propos de l'ILNAS

Vous souhaitez consulter toutes nos actualités ?
VOIR TOUTES LES ACTUALITÉS

Inscription à notre Newsletter
Vous souhaitez être tenu informé des dernières actualités ou de nos nouvelles formations ?
INSCRIPTION

Identifiants Peppol
ILNAS
9938:LU22959463

Vous supposez un défaut sur un produit alimentaire ou non alimentaire ?
SIGNALER UNE NON-CONFORMITÉ

Rapport 10/2024 des produits dangereux notifiés sur SAFETY GATE (08/03/2024)

AVERTISSEMENT DE SECURITE ET RAPPEL DE PRODUIT Chargeur USB de la marque IKEA (27/02/2024)

Avertissement de sécurité Casseroles de camping de la marque MSR (26/02/2024)

Sécurité et Santé
Métrologie
Accréditation et Notification
Confiance numérique

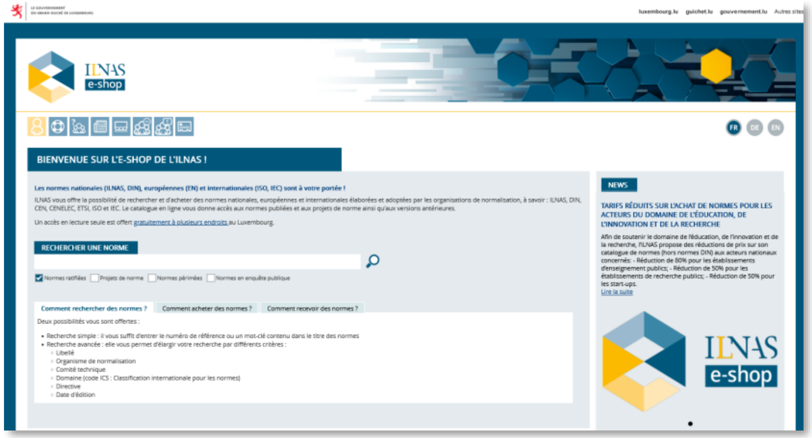
Normes et Normalisation
Cybersecurity Act
Libre circulation et surveillance du marché

ACTUALITÉS
AGENDA
FORMATIONS
PUBLICATIONS

DOCUMENTATION
LÉGISLATION ILNAS
ACTEURS
ALERTES

Contact | Liens | Plan du site | A propos du site | Accessibilité | Aspects légaux | Newsletter | Extranets | Une initiative de ILNAS

→ **ILNAS e-shop:**
https://ilnas.services-publics.lu/



LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

luxembourg.lu | guichet.lu | gouvernement.lu | Autres sites

ILNAS e-shop

FR | DE | EN

BIENVENUE SUR L'E-SHOP DE L'ILNAS !

Les normes nationales (ILNAS, DIN), européennes (EN) et internationales (ISO, IEC) sont à votre portée !

ILNAS vous offre la possibilité de rechercher et d'acheter des normes nationales, européennes et internationales élaborées et adoptées par les organisations de normalisation, à savoir : ILNAS, DIN, CEN, CENELEC, ETSI, ISO et IEC. Le catalogue en ligne vous donne accès aux normes publiées et aux projets de norme ainsi qu'aux versions antérieures.

Un accès en lecture seule est offert gratuitement à plusieurs endroits au Luxembourg.

RECHERCHER UNE NORME

☑ Normes ratifiées ☐ Projets de norme ☐ Normes périmées ☐ Normes en enquête publique

Comment rechercher des normes ? | Comment acheter des normes ? | Comment recevoir des normes ?

Deux possibilités vous sont offertes :

- Recherche simple : il vous suffit d'entrer le numéro de référence ou un mot-clé contenu dans le titre des normes
- Recherche avancée : elle vous permet d'élargir votre recherche par différents critères :
  - Libellé
  - Organisme de normalisation
  - Comité technique
  - Domaine (code ICS : Classification internationale pour les normes)
  - Directive
  - Date d'édition

NEWS

TARIFS RÉDUITS SUR L'ACHAT DE NORMES POUR LES ACTEURS DU DOMAINE DE L'ÉDUCATION, DE L'INNOVATION ET DE LA RECHERCHE

Afin de soutenir le domaine de l'éducation, de l'innovation et de la recherche, l'ILNAS propose des réductions de prix sur son catalogue de normes (hors normes DIN) aux acteurs nationaux concernés: - Réduction de 80% pour les établissements d'enseignement publics; - Réduction de 50% pour les établissements de recherche publics; - Réduction de 50% pour les start-ups.
Lire la suite

ILNAS e-shop

→ **Newsletters:** https://portail-qualite.public.lu/fr/support/newsletter.html

→ **Social Networks:**

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10

E-mail: info@ilnas.etat.lu

www.portail-qualite.lu

ACCRÉDITATION

CONFIANCE NUMÉRIQUE

SURVEILLANCE DU MARCHÉ

MÉTROLOGIE

NORMALISATION

ILNAS

ILNAS/ETSI Breakfast “Standardization of ICT, research and cybersecurity”

Standards Analysis ICT – Luxembourg - V14.0

25 April 2024

Nicolas DOMENJOUD - Responsible ICT & Technical Standardization, ILNAS

ILNAS

What is this document?

Policy on ICT Technical Standardization (2022-2025)

ILNAS

1. Promoting the ICT technical standardization to the market
2. Reinforcing the valorization and the involvement regarding ICT technical standardization
3. Supporting and strengthening the EaS and the related research activities

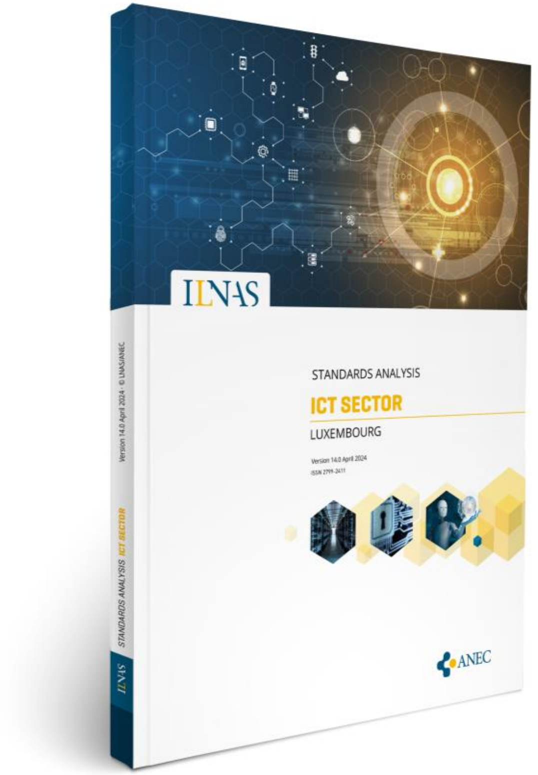
A main outcome of Project 1

"Drawing up a yearly national standards analysis for the Smart Secure ICT sector"

Twice a year, actually
Spring and Autumn

- Baseline resource
- Actionable, practical information
- Freely available online

What is this document?


ILNAS

STANDARDS ANALYSIS

ICT SECTOR

LUXEMBOURG

Version 14.0 April 2024

ISSN 2799-2411

ANEC

Version 14.0 April 2024 · © ILNAS/ANEC

STANDARDS ANALYSIS ICT SECTOR

ILNAS

Main information

A single-document resource of technical standardization committees covering the overall ICT sector

Purpose

To help you identify quickly and efficiently those SDOs and committees relevant to your business

What aims?

- Sources of technical standards that might impact you
- Identify committees connected to your business within which participating might by of interest

What is this document?

An overview of ICT standardization overall

Artificial Intelligence

Digital archiving

Internet of Things

Quantum Technologies

Programming languages

Digital Trust

Software engineering

Blockchain

Robotics

Smart cities

Cloud Computing

Financial technology

Green ICT

…and so much more…!

- *Budding technologies (and their security) → Recent committees in standardization… BUT ALSO*
- *Maintenance of standards, and contributions to standards projects, in more “classical” topics*

Content - Chapter 1: Technical Standardization and Standards

Generalities on standardization

- Quick overviews of ISO, IEC, ITU-T, CEN, CENELEC, and ETSI
- Definitions and purpose of standardization (World Trade Organization, European legislation)

A presentation of the main national actors

- ILNAS, your national standards body
- ANEC GIE, in support of ILNAS for the promotion and standardization…

…and the delivery of services!

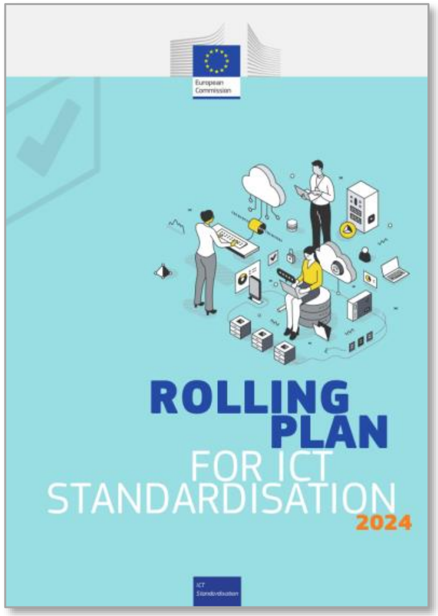
Your standardization partners in Luxembourg

Content - Chapter 2: ICT Subsectors definition

- Technical committees of interest broken down by sub-sectors

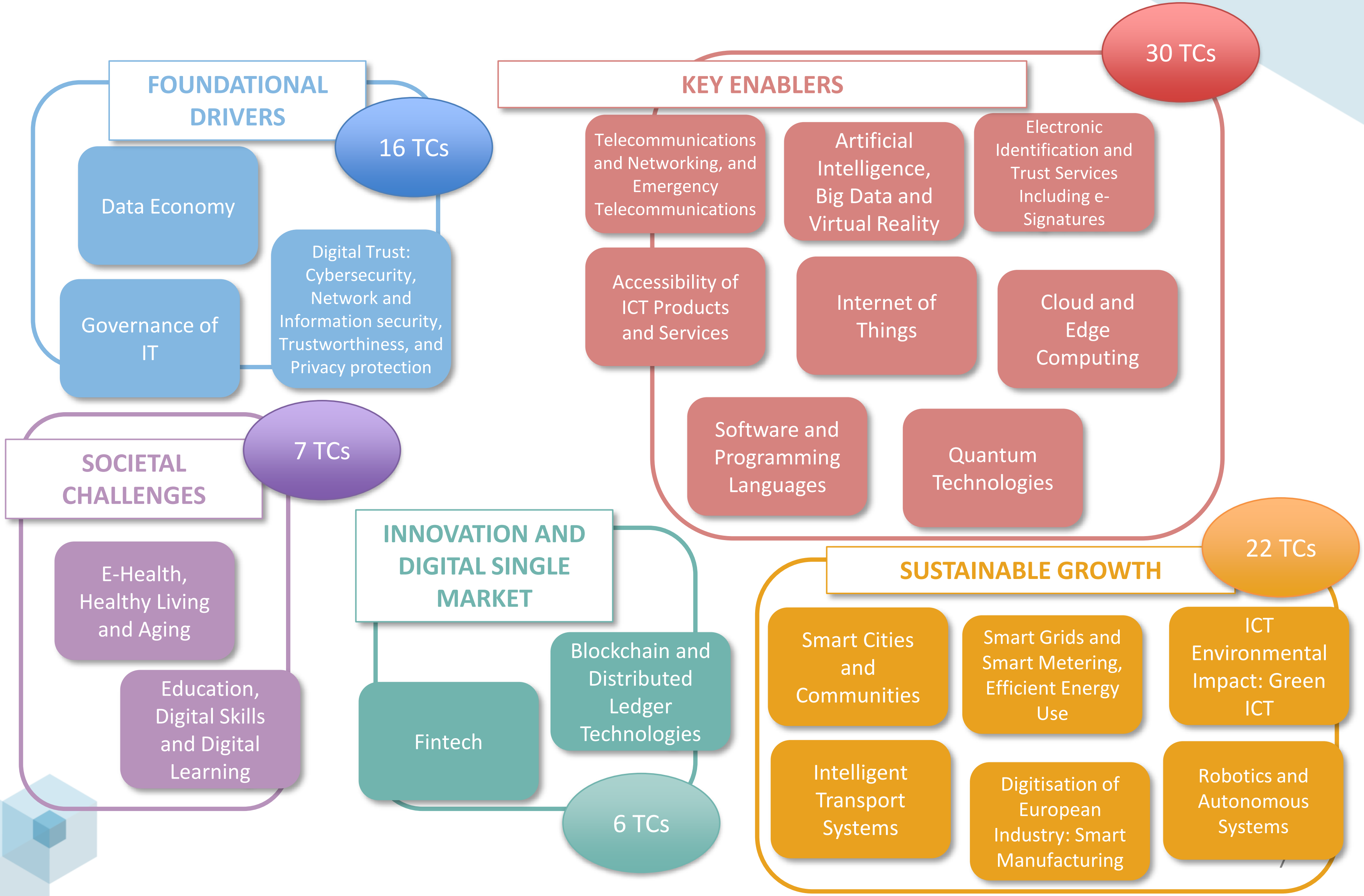
- Sub-sectors inspired by the European Commission’s Rolling Plan for ICT technical standardization, which defines the most important standardization initiatives and actions supporting EU policies

- The Rolling Plan 2024 identifies around 260 actions grouped into 39 technological or application domains under 5 thematic areas: foundational drivers, key enablers, societal challenges, innovation for the single market and sustainable growth



https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2024

Content Chapter 2: Subsectors



FOUNDATIONAL DRIVERS

16 TCs

Data Economy

Governance of IT

Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection

KEY ENABLERS

30 TCs

Telecommunications and Networking, and Emergency Telecommunications

Artificial Intelligence, Big Data and Virtual Reality

Electronic Identification and Trust Services Including e-Signatures

Accessibility of ICT Products and Services

Internet of Things

Cloud and Edge Computing

Software and Programming Languages

Quantum Technologies

SOCIETAL CHALLENGES

7 TCs

E-Health, Healthy Living and Aging

Education, Digital Skills and Digital Learning

INNOVATION AND DIGITAL SINGLE MARKET

Fintech

Blockchain and Distributed Ledger Technologies

6 TCs

SUSTAINABLE GROWTH

22 TCs

Smart Cities and Communities

Smart Grids and Smart Metering, Efficient Energy Use

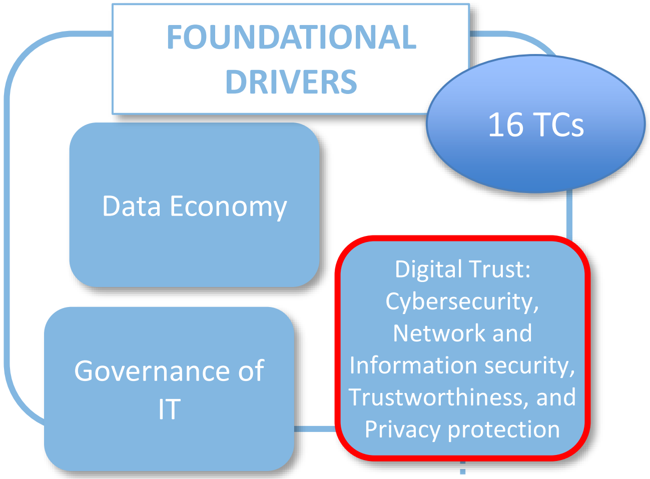
ICT Environmental Impact: Green ICT

Intelligent Transport Systems

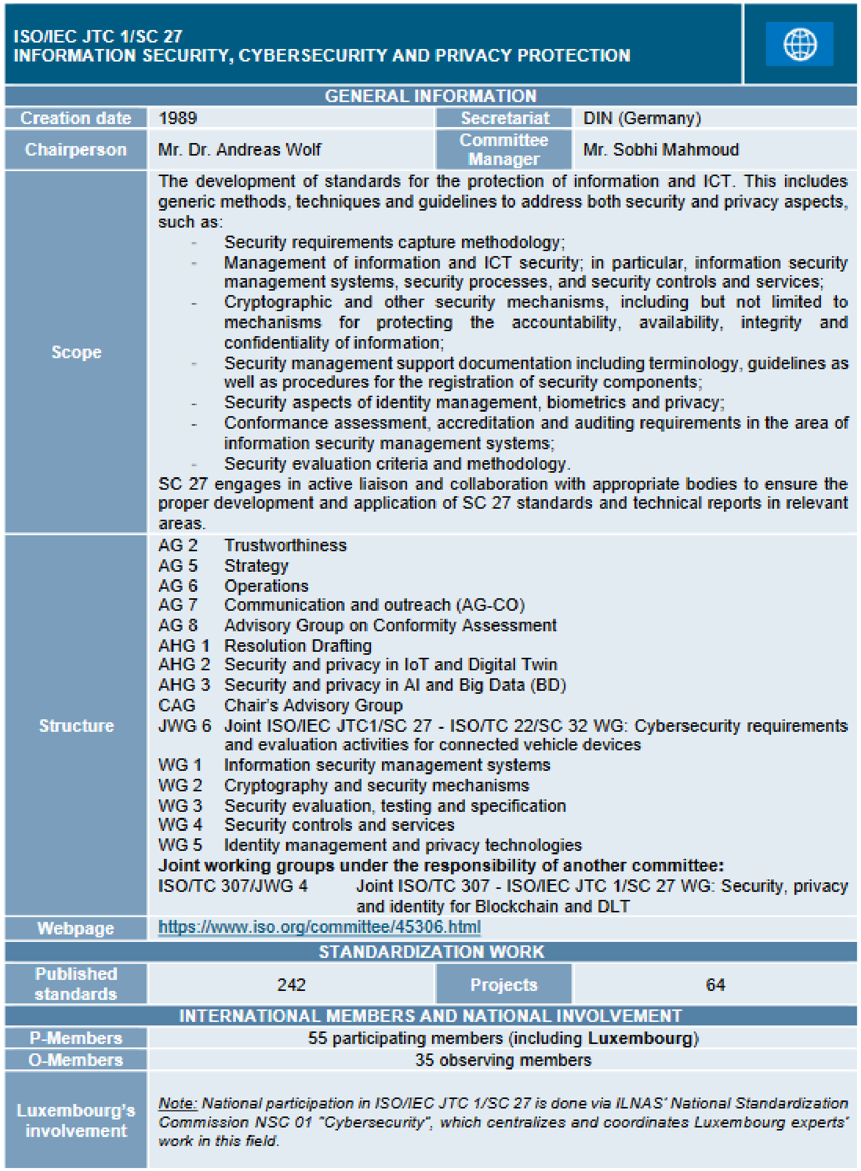
Digitisation of European Industry: Smart Manufacturing

Robotics and Autonomous Systems

Content - Chapter 3: ICT Sector Standards Watch – Technical Committee's ID-cards


FOUNDATIONAL DRIVERS
16 TCs
Data Economy
Governance of IT
Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection

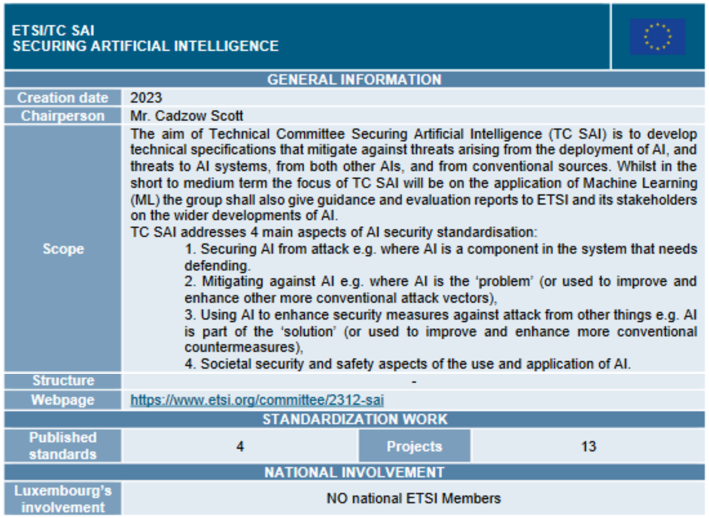
- ILNAS/NSC 01 – Cybersecurity
- ISO/IEC JTC 1/WG 13 – Trustworthiness
- ISO/IEC JTC 1/SC 27 – Information security, cybersecurity and privacy protection
- ISO/PC 317 – Consumer protection: privacy by design for consumer goods and services
- CEN/CLC JTC 13 – Cybersecurity and data protection
- ETSI/TC CYBER – Cybersecurity
- …



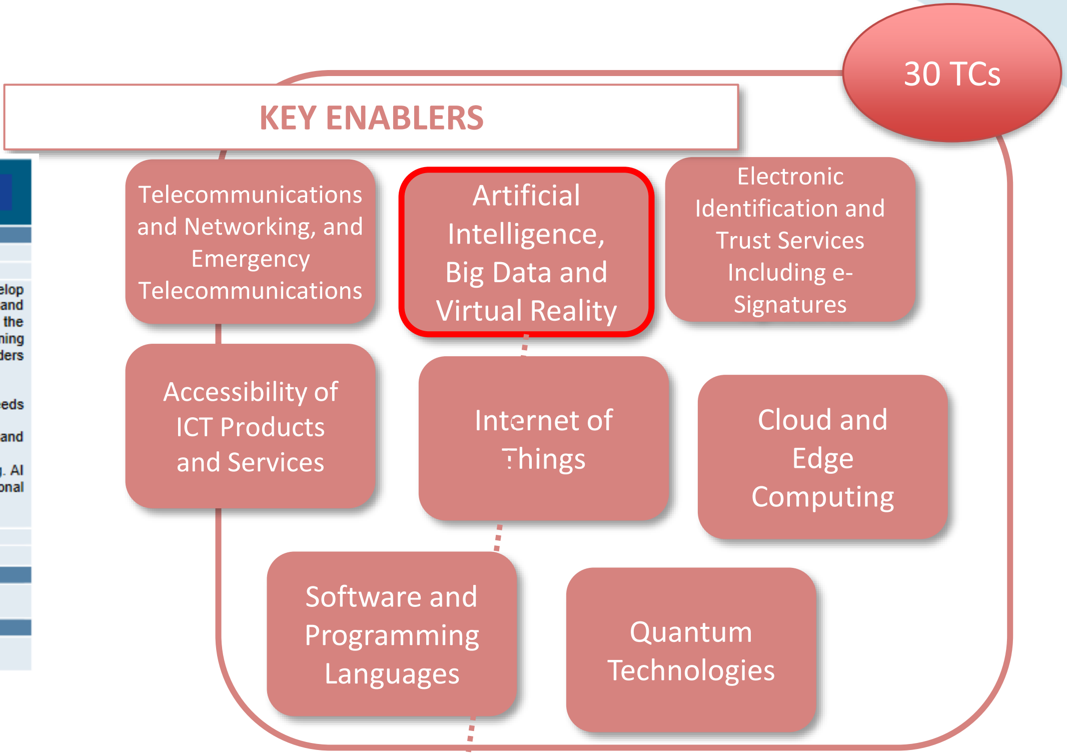
ISO/IEC JTC 1/SC 27
INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION

GENERAL INFORMATION			
Creation date	1989	Secretariat	DIN (Germany)
Chairperson	Mr. Dr. Andreas Wolf	Committee Manager	Mr. Sobhi Mahmoud
Scope	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: - Security requirements capture methodology; - Management of information and ICT security; in particular, information security management systems, security processes, and security controls and services; - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; - Security aspects of identity management, biometrics and privacy; - Conformance assessment, accreditation and auditing requirements in the area of information security management systems; - Security evaluation criteria and methodology. SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.		
Structure	AG 2 Trustworthiness AG 5 Strategy AG 6 Operations AG 7 Communication and outreach (AG-CO) AG 8 Advisory Group on Conformity Assessment AHG 1 Resolution Drafting AHG 2 Security and privacy in IoT and Digital Twin AHG 3 Security and privacy in AI and Big Data (BD) CAG Chair's Advisory Group JWG 6 Joint ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG: Cybersecurity requirements and evaluation activities for connected vehicle devices WG 1 Information security management systems WG 2 Cryptography and security mechanisms WG 3 Security evaluation, testing and specification WG 4 Security controls and services WG 5 Identity management and privacy technologies **Joint working groups under the responsibility of another committee:** ISO/TC 307/JWG 4 Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Security, privacy and identity for Blockchain and DLT		
Webpage	https://www.iso.org/committee/45306.html		
STANDARDIZATION WORK			
Published standards	242	Projects	64
INTERNATIONAL MEMBERS AND NATIONAL INVOLVEMENT			
P-Members	55 participating members (including **Luxembourg**)		
O-Members	35 observing members		
Luxembourg's involvement	*Note: National participation in ISO/IEC JTC 1/SC 27 is done via ILNAS' National Standardization Commission NSC 01 "Cybersecurity", which centralizes and coordinates Luxembourg experts' work in this field.*		

Content - Chapter 3: ICT Sector Standards Watch – Technical Committee’s ID-cards



ETSI/TC SAI SECURING ARTIFICIAL INTELLIGENCE			
GENERAL INFORMATION			
Creation date	2023		
Chairperson	Mr. Cadzow Scott		
Scope	The aim of Technical Committee Securing Artificial Intelligence (TC SAI) is to develop technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. Whilst in the short to medium term the focus of TC SAI will be on the application of Machine Learning (ML) the group shall also give guidance and evaluation reports to ETSI and its stakeholders on the wider developments of AI. TC SAI addresses 4 main aspects of AI security standardisation: 1. Securing AI from attack e.g. where AI is a component in the system that needs defending. 2. Mitigating against AI e.g. where AI is the ‘problem’ (or used to improve and enhance other more conventional attack vectors), 3. Using AI to enhance security measures against attack from other things e.g. AI is part of the ‘solution’ (or used to improve and enhance more conventional countermeasures), 4. Societal security and safety aspects of the use and application of AI.		
Structure	-		
Webpage	https://www.etsi.org/committee/2312-sai		
STANDARDIZATION WORK			
Published standards	4	Projects	13
NATIONAL INVOLVEMENT			
Luxembourg’s involvement	NO national ETSI Members		

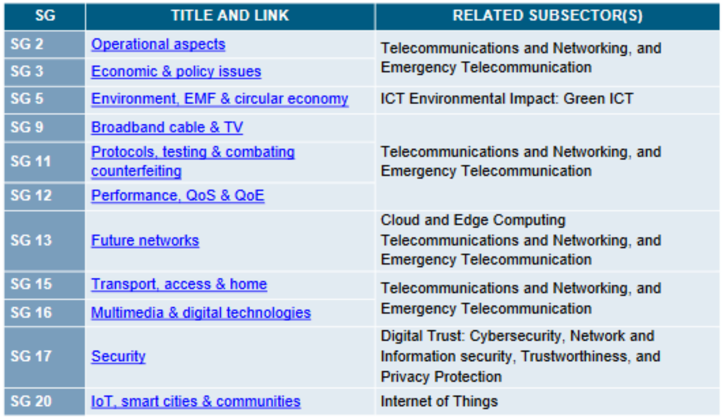

30 TCs
KEY ENABLERS
Telecommunications and Networking, and Emergency Telecommunications
Artificial Intelligence, Big Data and Virtual Reality
Electronic Identification and Trust Services Including e-Signatures
Accessibility of ICT Products and Services
Internet of Things
Cloud and Edge Computing
Software and Programming Languages
Quantum Technologies

- ISO/IEC JTC 1/SC 42 – Artificial Intelligence
- CEN/CLC JTC 21 – Artificial Intelligence
- ETSI/TC SAI – Securing Artificial Intelligence
- ISO/IEC JTC 1/SC 24 – Computer graphics, image processing and environmental data representation
- …

Content - Chapter 3: ICT Sector Standards Watch - Other information

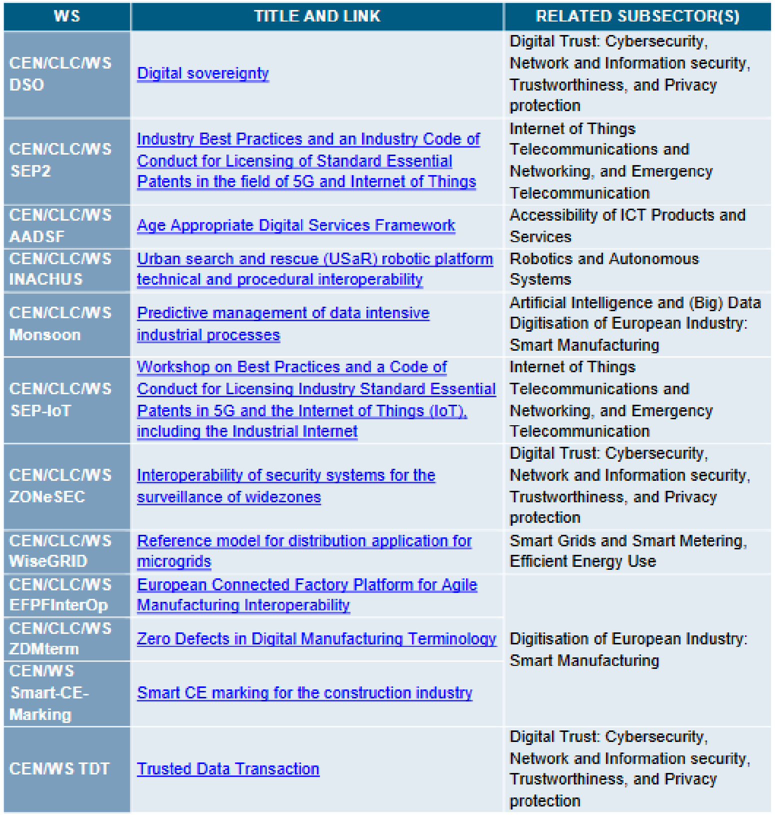
Also, some information on:

- ITU-T Study Groups
- ETSI Industry Specification Groups
- CEN/CENELEC Workshops



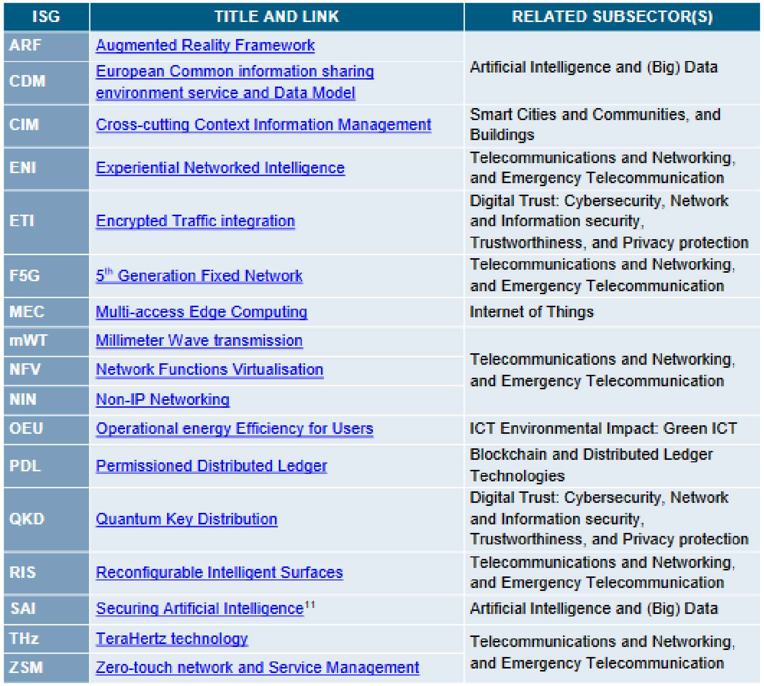
SG	TITLE AND LINK	RELATED SUBSECTOR(S)
SG 2	Operational aspects	Telecommunications and Networking, and Emergency Telecommunication
SG 3	Economic & policy issues	
SG 5	Environment, EMF & circular economy	ICT Environmental Impact: Green ICT
SG 9	Broadband cable & TV	Telecommunications and Networking, and Emergency Telecommunication
SG 11	Protocols, testing & combating counterfeiting	
SG 12	Performance, QoS & QoE	
SG 13	Future networks	Cloud and Edge Computing Telecommunications and Networking, and Emergency Telecommunication
SG 15	Transport, access & home	Telecommunications and Networking, and Emergency Telecommunication
SG 16	Multimedia & digital technologies	
SG 17	Security	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy Protection
SG 20	IoT, smart cities & communities	Internet of Things

Table 1: ITU study groups



WS	TITLE AND LINK	RELATED SUBSECTOR(S)
CEN/CLC/WS DSO	Digital sovereignty	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection
CEN/CLC/WS SEP2	Industry Best Practices and an Industry Code of Conduct for Licensing of Standard Essential Patents in the field of 5G and Internet of Things	Internet of Things Telecommunications and Networking, and Emergency Telecommunication
CEN/CLC/WS AADSF	Age Appropriate Digital Services Framework	Accessibility of ICT Products and Services
CEN/CLC/WS INACHUS	Urban search and rescue (USaR) robotic platform technical and procedural interoperability	Robotics and Autonomous Systems
CEN/CLC/WS Monsoon	Predictive management of data intensive industrial processes	Artificial Intelligence and (Big) Data Digitisation of European Industry: Smart Manufacturing
CEN/CLC/WS SEP-IoT	Workshop on Best Practices and a Code of Conduct for Licensing Industry Standard Essential Patents in 5G and the Internet of Things (IoT), including the Industrial Internet	Internet of Things Telecommunications and Networking, and Emergency Telecommunication
CEN/CLC/WS ZONeSEC	Interoperability of security systems for the surveillance of widezones	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection
CEN/CLC/WS WiseGRID	Reference model for distribution application for microgrids	Smart Grids and Smart Metering, Efficient Energy Use
CEN/CLC/WS EFPFInterOp	European Connected Factory Platform for Agile Manufacturing Interoperability	Digitisation of European Industry: Smart Manufacturing
CEN/CLC/WS ZDMterm	Zero Defects in Digital Manufacturing Terminology	
CEN/WS Smart-CE-Marking	Smart CE marking for the construction industry	
CEN/WS TDT	Trusted Data Transaction	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection

Table 3: CEN and CEN/CLC Workshops (WS)



ISG	TITLE AND LINK	RELATED SUBSECTOR(S)
ARF	Augmented Reality Framework	Artificial Intelligence and (Big) Data
CDM	European Common information sharing environment service and Data Model	
CIM	Cross-cutting Context Information Management	Smart Cities and Communities, and Buildings
ENI	Experiential Networked Intelligence	Telecommunications and Networking, and Emergency Telecommunication
ETI	Encrypted Traffic integration	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection
F5G	5th Generation Fixed Network	Telecommunications and Networking, and Emergency Telecommunication
MEC	Multi-access Edge Computing	Internet of Things
mWT	Millimeter Wave transmission	Telecommunications and Networking, and Emergency Telecommunication
NFV	Network Functions Virtualisation	
NIN	Non-IP Networking	
OEU	Operational energy Efficiency for Users	ICT Environmental Impact: Green ICT
PDL	Permissioned Distributed Ledger	Blockchain and Distributed Ledger Technologies
QKD	Quantum Key Distribution	Digital Trust: Cybersecurity, Network and Information security, Trustworthiness, and Privacy protection
RIS	Reconfigurable Intelligent Surfaces	Telecommunications and Networking, and Emergency Telecommunication
SAI	Securing Artificial Intelligence[11]	Artificial Intelligence and (Big) Data
THz	TeraHertz technology	Telecommunications and Networking, and Emergency Telecommunication
ZSM	Zero-touch network and Service Management	

Table 2: ETSI's Industry Specification Groups (ISG)

Content - Chapter 4: Opportunities for the National Market

Details on ILNAS and ANEC GIE products and services, related especially to ICT

- Information dissemination
  - Market meetings
  - News items in standardization
  - Technical sheets on ICT standardization topics
  - Videos
  - Standards watch service
- Consulting and purchasing standards
  - Reading stations
  - e-Shop
- Getting involved in standards development
  - Public enquiry commenting
  - Becoming a delegate in standardization
- Research and education
  - White papers and technical reports
  - General and technical training sessions

Additional information – How to consult or purchase standards?

Reading stations

Free consultation of European (CEN,CENELEC & ETSI), international (ISO & IEC) and national (ILNAS) standards

- ILNAS
- Luxembourg Learning Centre
- LIST
- University of Luxembourg (Kirchberg)
- Luxembourg House of Cybersecurity
- Chambre des Métiers
- Lycée des Arts et Métiers
- Atert Lycée Rédange
- Commune d'Echternach

ILNAS e-shop

85 national standards

+81.000 European Standards (CEN, CENELEC and ETSI)

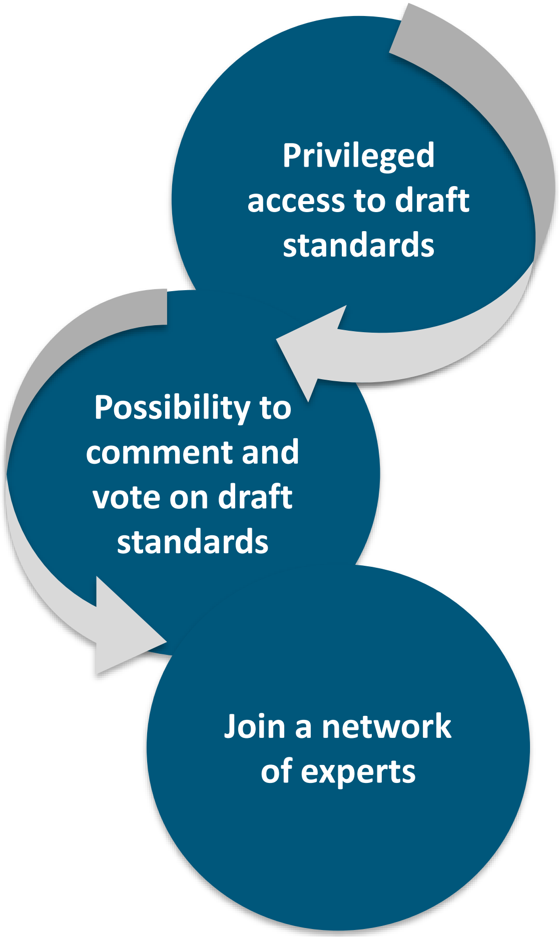
+74.000 International Standards (ISO and IEC)

+49.000 DIN standards

→ More than 200.000 normative documents at your disposal at competitive prices

Format: electronic
Language: English, French and German

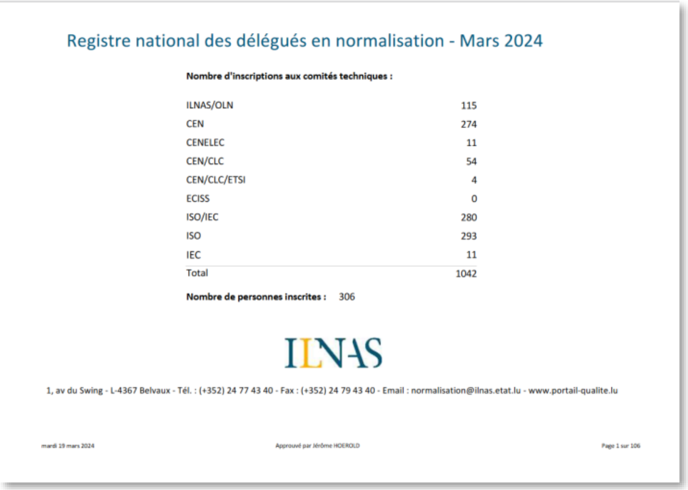
Additional information – How to participate in standardization?


Privileged access to draft standards

Possibility to comment and vote on draft standards

Join a network of experts

→ 306 national delegates
→ 1.042 registrations in technical committees


Registre national des délégués en normalisation - Mars 2024

Nombre d'inscriptions aux comités techniques :

ILNAS/OLN	115
CEN	274
CENELEC	11
CEN/CLC	54
CEN/CLC/ETSI	4
ECISS	0
ISO/IEC	280
ISO	293
IEC	11
Total	1042

Nombre de personnes inscrites : 306

ILNAS

1, av du Swing - L-4367 Belvaux - Tél. : (+352) 24 77 43 40 - Fax : (+352) 24 79 43 40 - Email : normalisation@ilnas.etat.lu - www.portail-qualite.lu

mardi 19 mars 2024   Approuvé par Jérôme HOEROLD   Page 1 sur 106

- Open to every socio-economic actor in Luxembourg with a certain expertise
- Free of charge
- Free training offered to the new delegates

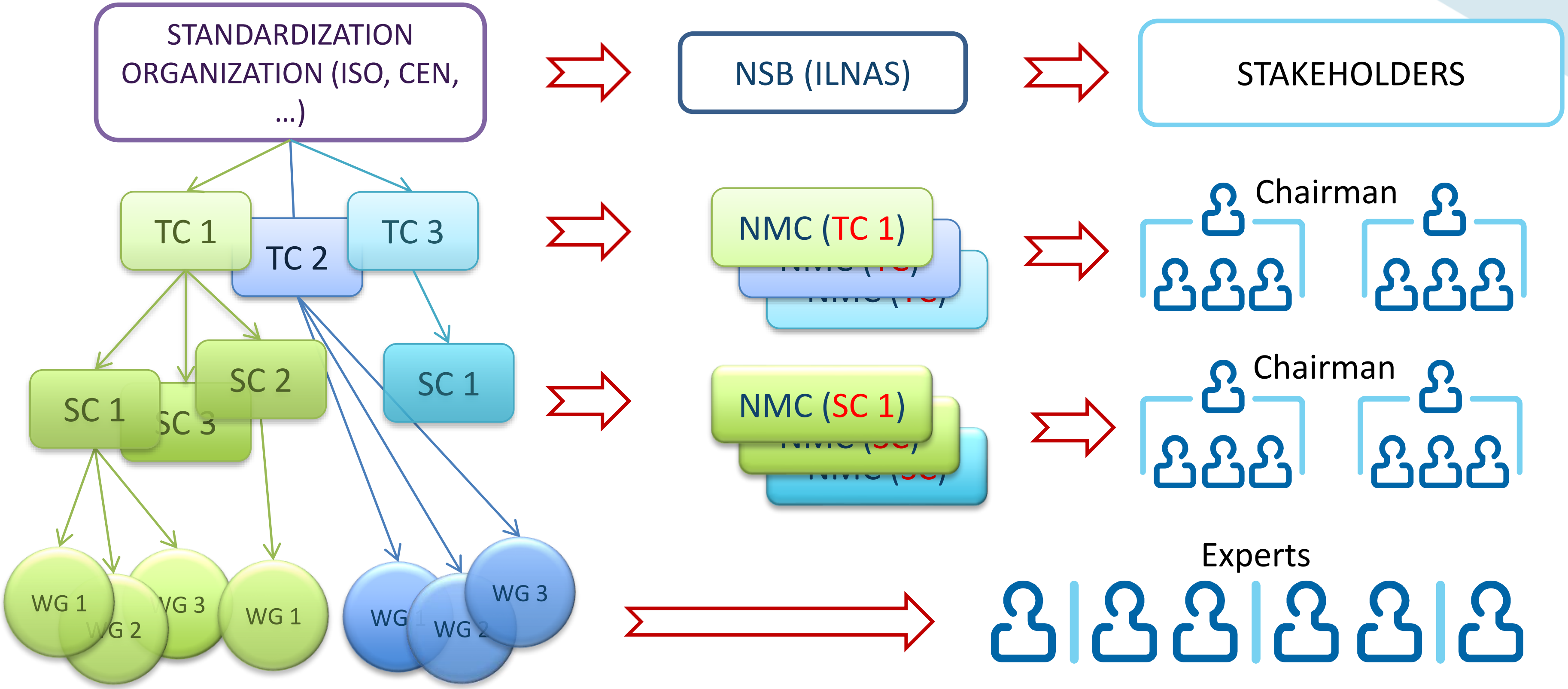
ILNAS

Additional information – How to participate in standardization?

	National level	European level		International level
General Standardization	ILNAS	cen	Vienna agreement	ISO
Electrotechnical Standardization	ILNAS	CENELEC	Frankfurt Agreement	IEC
Telecommunication Standardization	ILNAS	ETSI		ITU *

* ITU-T

Additional information – How to participate in standardization?



- **NSB**: National Standards Body
- **TC**: Technical Committee
- **SC**: Subcommittee - Entity established within a TC responsible for a large work program (focuses on an area of interest of the TC)
- **WG**: Working Group - Group established by a TC or SC that develops standards project(s) within the scope of activity of the TC/SC
- **NMC**: National Mirror Committee

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux
Tel. : (+352) 24 77 43 - 00 · Fax : (+352) 24 79 43 - 10
E-mail: info@ilnas.etat.lu

www.portail-qualite.lu

ETSI The Standards People

ETSI at a Glance

Claire d’Esclercs for ILNAS

25 April 2024

ETSI is a Community of Dynamic ICT Innovators

- Independent, non-profit organization
- 900 member organizations, drawn from 64 countries and on five continents
- 36-year track record of technical excellence in the ICT sector
- Strong community of experts and innovators
- Diverse members: SMEs, micro-enterprises, large corporations, research entities, academia, government and public bodies, societal stakeholders…

Networking par excellence:

- Attend any of our 70 conferences & interop events per year
- Exchange with industry leaders
- Meet and connect with customers and competitors in a neutral, professional environment

At the Heart of Digital

- At the forefront of emerging technologies
- ETSI benefits from close relationships with research bodies
- Our members gain a competitive advantage through early adoption of the latest standards in the R&D roadmap
- Collaboration within open-source projects
- Our members advance and promote new concepts within the community
- Our members bring innovation and industry insights to ETSI's working methods

ETSI Members shape:

- ✓ 5G / 6G
- ✓ Non-terrestrial Networks
- ✓ Internet of Things
- ✓ Cybersecurity
- ✓ Network Virtualization
- ✓ Artificial Intelligence
- ✓ Multi-access Edge Computing
- ✓ Quantum Safe Cryptography
- ✓ Radio

…and much more

We are Open & Inclusive

- Diverse members
  - 23 % of ETSI Members are SMEs and Micro-Enterprises
  - 15 % of ETSI members are Universities and Research Bodies
  - Over 100 technical groups hold more than 1 700 meetings per year
  - Members across diverse sectors of industry and society

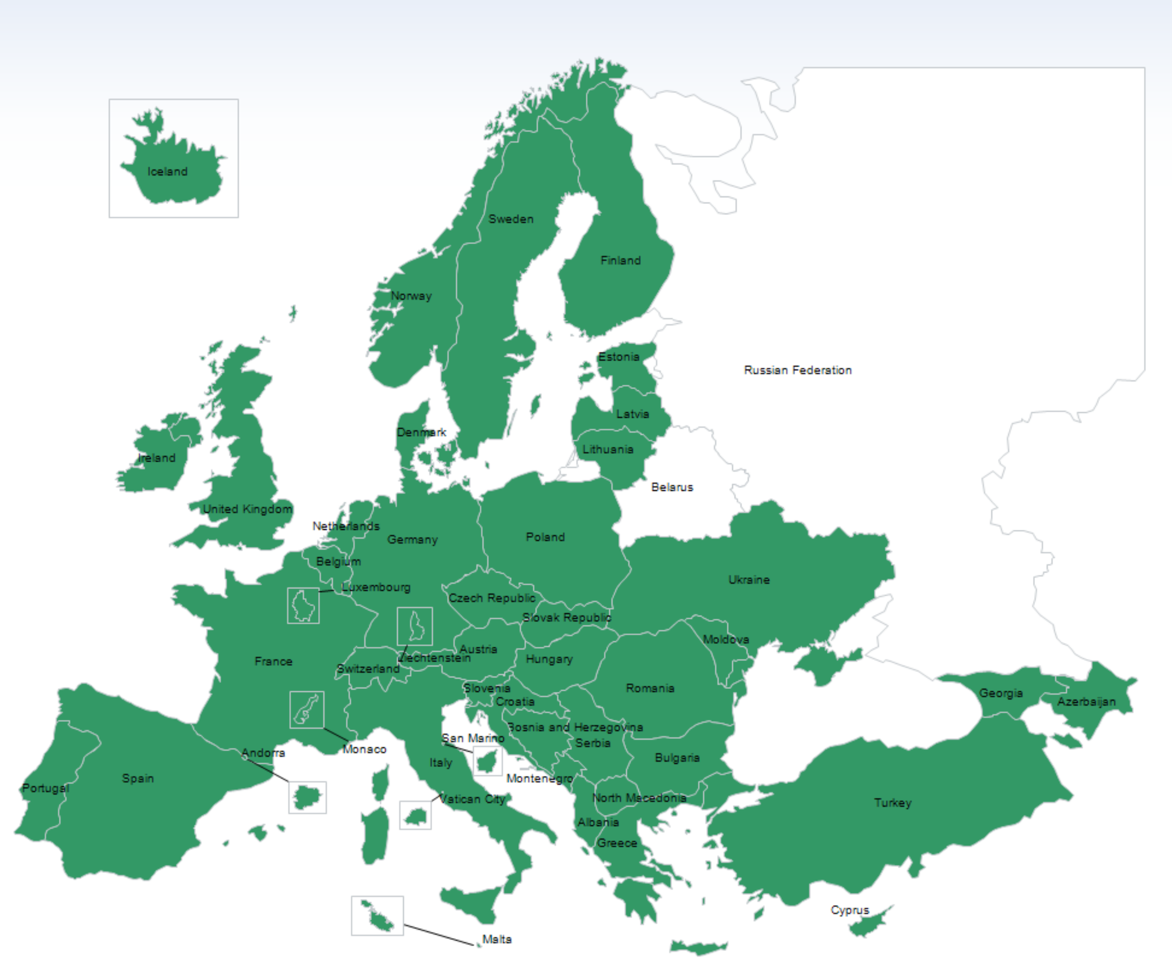
- *Members participate in all activities on equal terms*

- ETSI standards are free of charge for all: https://www.etsi.org/standards
  - 60 000 published standards
  - Over 1 800 standards published in 2023
  - 19,5 million downloads of standards in 2023

European roots, Global branches

- ETSI is a European Standards Organization (ESO)
- ETSI has been officially recognized as a European Standards Organization since 1994
- ETSI supports European regulation and policies
- ETSI develops Harmonised European Standards
- ETSI standards are key enablers for the Single European Market
- ETSI standards are widely used globally
- ETSI is a founding partner of 3GPP and oneM2M

Building a large unified European Market:



In the approval of European Standards (ENs), the NSOs have the exclusive responsibility for:

- ✓ carrying out the Public Enquiry (consultation with national industry)
- ✓ submission of the national position (the ‘vote’) on the standard
- ✓ ensuring the transposition of ENs into national standards
- ✓ ensuring the withdrawal of any conflicting national standard

Working in partnership with 41 National Standards Organisations

ETSI is Global

- ETSI encourages active involvement and contributions from diverse global members in an open, inclusive setting.
- Over 100 strategic partnerships are maintained to foster global standardization efforts.
- Collaborations span across various fora, consortia, as well as international and regional Standards Development Organizations (SDOs).
- The goal is to ensure ETSI standards gain worldwide acceptance.

3GPP boasts nearly 800 members hailing from 7 telecommunications SDOs worldwide.

It is developing specifications and standards for mobile networks, including 5G and beyond. The specifications aim to enhance network performance, capacity, and efficiency to support a wide range of services and applications, as well as interoperability and compatibility among different vendors' equipment and network components.

Similarly, oneM2M brings together over 200 stakeholders from 7 telecommunications SDOs globally. It plays a crucial role in driving interoperability, scalability, and security in the evolving landscape of IoT and M2M communications.
One of the main goals is to involve organizations from M2M-related business domains, such as telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.

ETSI Technical Groups

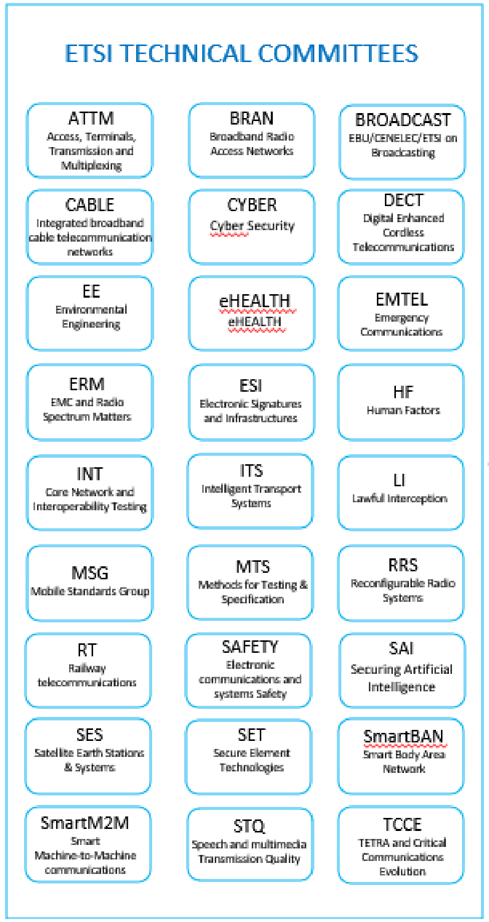
ETSI's standardization work is carried out in different technical groups:

- Technical Committee (TC)
- Industry Specification Group (ISG)
- Software Development group (SDG)
- ETSI Partnership Project (EPP)

The committees are coordinated by our **Operational Coordination Group (OCG)**, which includes the chairs of all the technical committees.

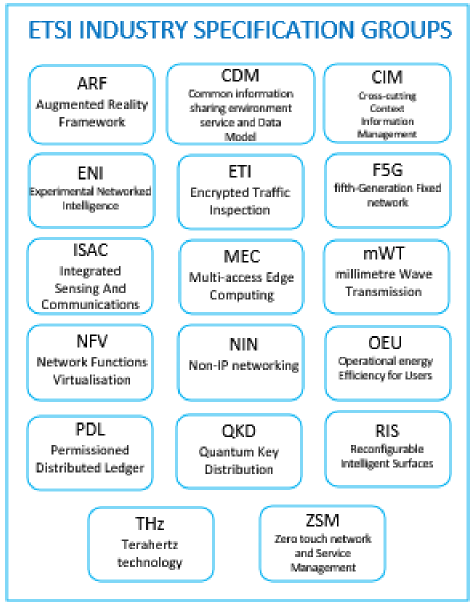
Each committee establishes and maintains a **work programme**, which consists of individual work items. Collectively, the work programmes of all our committees constitute the **ETSI Work Programme**.

See Work-Programme_2023-2024



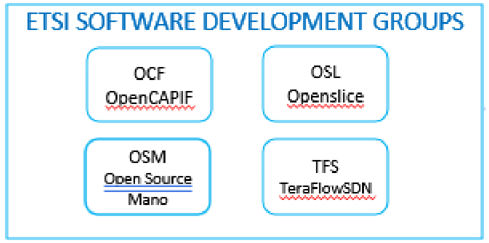
ETSI TECHNICAL COMMITTEES

ATTM Access, Terminals, Transmission and Multiplexing	BRAN Broadband Radio Access Networks	BROADCAST EBU/CENELEC/ETSI on Broadcasting
CABLE Integrated broadband cable telecommunication networks	CYBER Cyber Security	DECT Digital Enhanced Cordless Telecommunications
EE Environmental Engineering	eHEALTH eHEALTH	EMTEL Emergency Communications
ERM EMC and Radio Spectrum Matters	ESI Electronic Signatures and Infrastructures	HF Human Factors
INT Core Network and Interoperability Testing	ITS Intelligent Transport Systems	LI Lawful Interception
MSG Mobile Standards Group	MTS Methods for Testing & Specification	RRS Reconfigurable Radio Systems
RT Railway telecommunications	SAFETY Electronic communications and systems Safety	SAI Securing Artificial Intelligence
SES Satellite Earth Stations & Systems	SET Secure Element Technologies	SmartBAN Smart Body Area Network
SmartM2M Smart Machine-to-Machine communications	STQ Speech and multimedia Transmission Quality	TCCE TETRA and Critical Communications Evolution



ETSI INDUSTRY SPECIFICATION GROUPS

ARF Augmented Reality Framework	CDM Common information sharing environment service and Data Model	CIM Cross-cutting Context Information Management
ENI Experimental Networked Intelligence	ETI Encrypted Traffic Inspection	F5G fifth-Generation Fixed network
ISAC Integrated Sensing And Communications	MEC Multi-access Edge Computing	mWT millimetre Wave Transmission
NFV Network Functions Virtualisation	NIN Non-IP networking	OEU Operational energy Efficiency for Users
PDL Permissioned Distributed Ledger	QKD Quantum Key Distribution	RIS Reconfigurable Intelligent Surfaces
THz Terahertz technology	ZSM Zero touch network and Service Management	



ETSI SOFTWARE DEVELOPMENT GROUPS

OCF OpenCAPIF	OSL Openslice
OSM Open Source Mano	TFS TeraFlowSDN

https://www.etsi.org/committees

Interoperability

- ETSI's Centre for Testing and Interoperability conducts interoperability test events for a wide range of ICT implementations in a diverse multi-vendor, multi-network, multi-service environment

- Plugtests™, Hackathons and Hackfests support the efficient validation and implementation of standards and help the industry bring new products and services to market faster

- Technologies that our CTI department covers currently include 5G mobile, safety and mission-critical communications, intelligent transport, electronic signatures, network virtualization, and the Internet of Things.

ETSI Software Development Groups

- ETSI Standards Development Groups are the perfect tool for developing ‘early’ implementation work resulting from research and other sources of innovation. This tool has been designed for collaborative software development at ETSI based on the successful experience with Open Source MANO and TeraFlowSDN.

- SDGs allow for early experimentation, prototyping, validation and testing of concepts defined by ETSI Technical Groups and provide them with early and regular feedback.
  It’s an ideal mechanism for optimizing the quality of standards and reducing their time to market.

- Any group of at least four ETSI members can request the creation of a new SDG in ETSI from the ETSI Director-General, as long as the relevant criteria are met. Various licence types are allowed, including Open Source. ETSI SDGs are open to ETSI members, non-members and also individuals.

Open Source MANO by ETSI

TeraFlow SDN by ETSI

OpenSlice by ETSI

OpenCAPIF by ETSI

Current software related activities

Open Source MANO by ETSI

- **ETSI OSM – Open Source MANO** is developing an open-source NFV Management and Orchestration stack aligned with the ETSI NFV Information Model and APIs

TeraFlow SDN by ETSI

- **ETSI TFS—TeraFlowSDN** is developing an open source cloud-native SDN Controller that will enable smart connectivity services for future networks beyond 5G.

OpenSlice by ETSI

- **SDG OSL - OpenSlice** is developing an open source Operations Support System to deliver Network as a Service

OpenCAPIF by ETSI

- **SDG OCF – OpenCAPIF** is developing an open source Common API Framework as defined by 3GPP to enable API exposure and invoke in a secure and consistent manner.

Strategy

Designing tomorrow's world, ETSI is at the forefront of new Information and Communication Technology, leading the development of standards that enable a sustainable and securely connected society.

ETSI is driven by five strategy directions, namely being:

- At the Heart of Digital
- An Enabler of Standards
- Global
- Versatile
- Inclusive

We are ‘The Standards People’ of Tomorrow

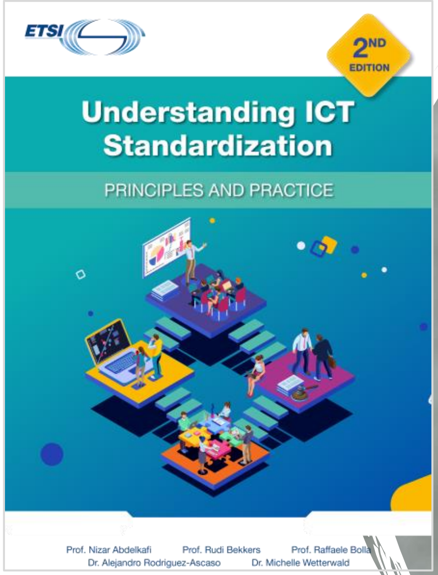
ETSI is establishing more and more relationships with academia

- 75+ links with universities and research centres; ETSI experts provide lectures
- Proactive support to lecturers and students

ETSI has developed high-quality educational materials on ICT standardization

- Textbook, ‘Understanding ICT Standardization: Principles and Practice’ (2^{nd} edition, 2022)
- Set of 350+ slides (currently being enhanced)
- Modular design to suit different educational levels and study programmes
- Downloadable for free:

www.etsi.org/education/education-about-standardization



ETSI

2ND EDITION

Understanding ICT Standardization

PRINCIPLES AND PRACTICE

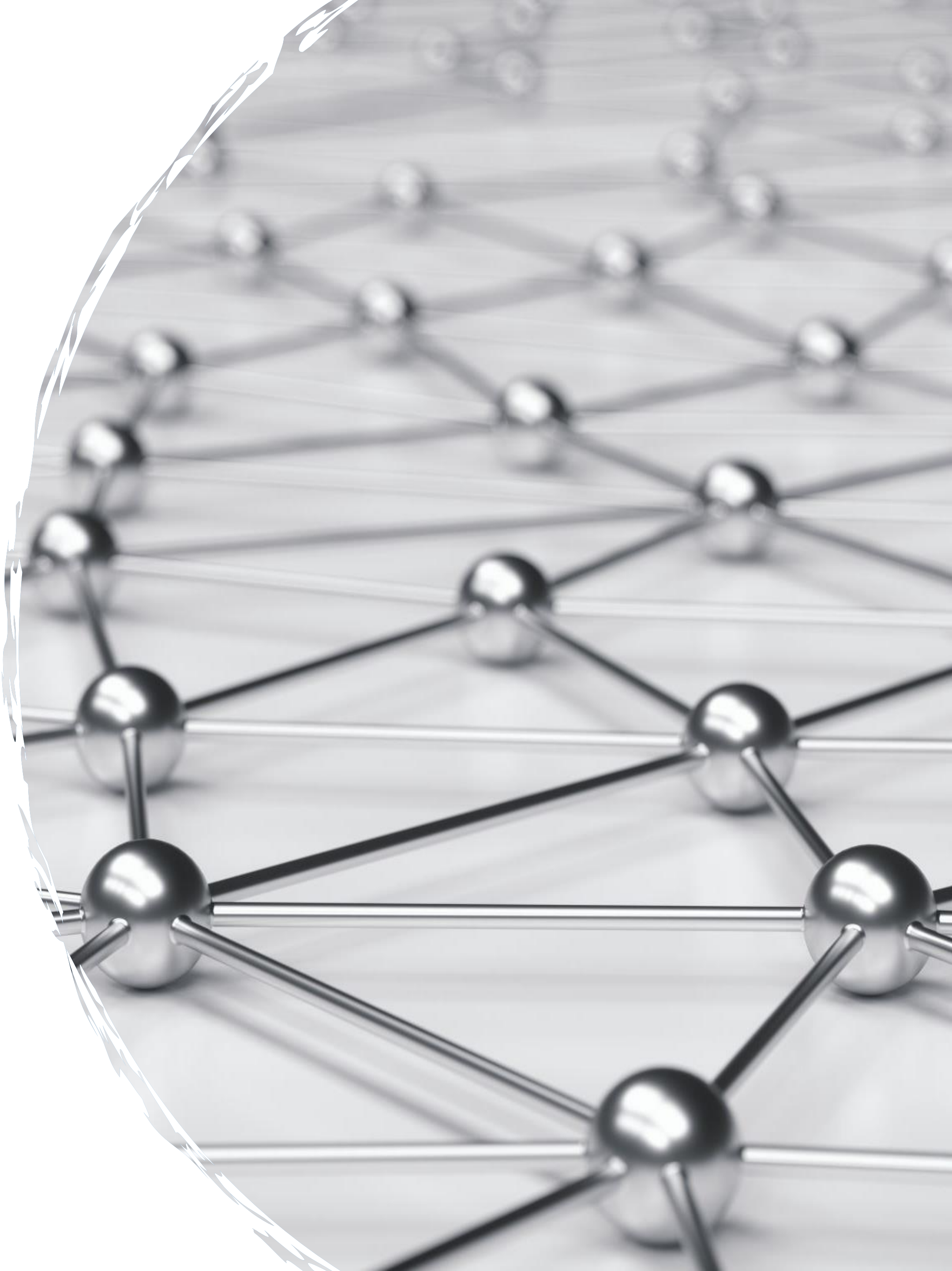
Prof. Nizar Abdelkafi Prof. Rudi Bekkers Prof. Raffaele Bolla
Dr. Alejandro Rodriguez-Ascaso Dr. Michelle Wetterwald

Design Tomorrow's World with the Standards People

Claire d'Esclercs
Director of Membership Development and Education
claire.desclercs@etsi.org

www.etsi.org

ETSI approach to Technology Research and Foresight and Initial thoughts on 6G Mobile Networks



Presented by: David Boswarthick. ETSI Director NET

For: <external use>

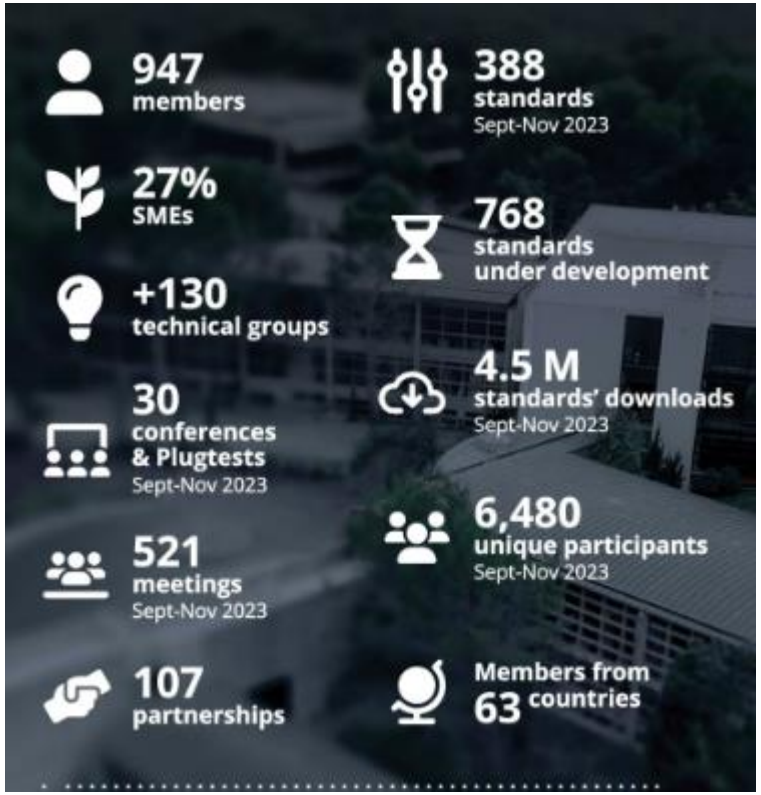
April 2024

CONTENT

ETSI Approach to R&I

ETSI, Bringing People Together

- Independent, non-profit standards organization
- Officially recognized by the European Union to support EU regulation
- **35+** year track record of technical excellence in the ICT sector
- Founding Partner of both **3GPP** and **oneM2M**
- Over **approx. 900** members from more than **60+** countries
- Diverse community: private companies, research and academia, governments, public bodies, societal stakeholders
- All deliverables are available for download for FREE from https://www.etsi.org/standards



947 members

27% SMEs

+130 technical groups

30 conferences & Plugtests Sept-Nov 2023

521 meetings Sept-Nov 2023

107 partnerships

388 standards Sept-Nov 2023

768 standards under development

4.5 M standards' downloads Sept-Nov 2023

6,480 unique participants Sept-Nov 2023

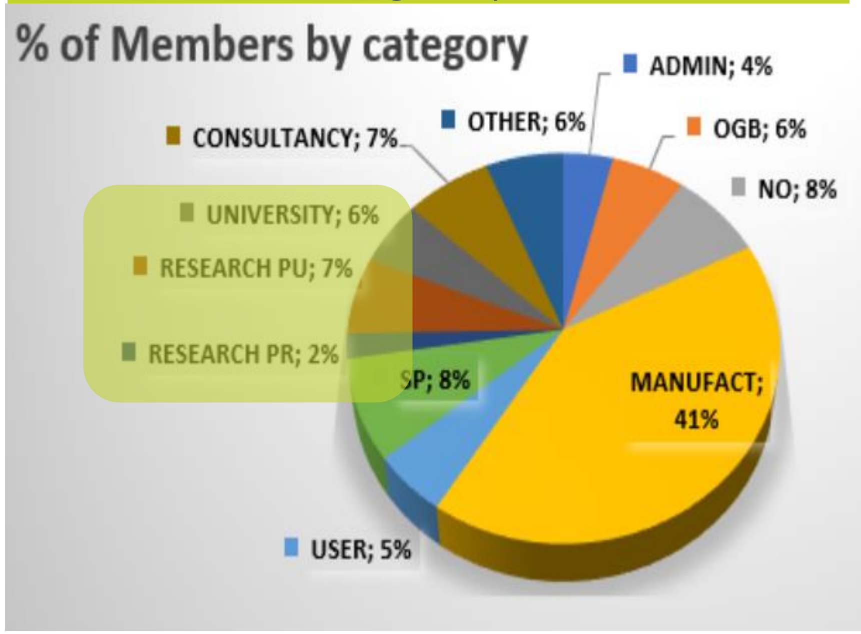
Members from 63 countries

Source: Jan 2024 edition of the ETSI Enjoy! magazine
https://www.etsi.org/newsroom/magazine

ETSI, Bringing People Together

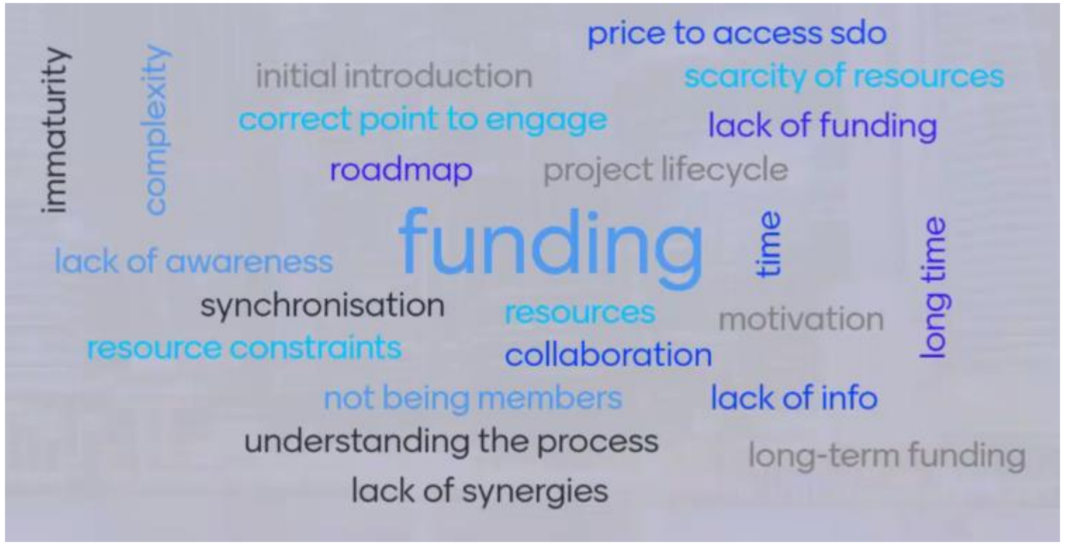
- Independent, non-profit standards organization
- Officially recognized by the European Union to support EU regulation
- **35+** year track record of technical excellence in the ICT sector
- Founding Partner of both **3GPP** and **oneM2M**
- Over **approx. 900** members from more than **60+** countries
- Diverse community: private companies, research and academia, governments, public bodies, societal stakeholders
- All deliverables are available for download for FREE from https://www.etsi.org/standards

Public / Private Research organizations and Universities make up for over **15%** of our ETSI membership and are present both in Europe and globally

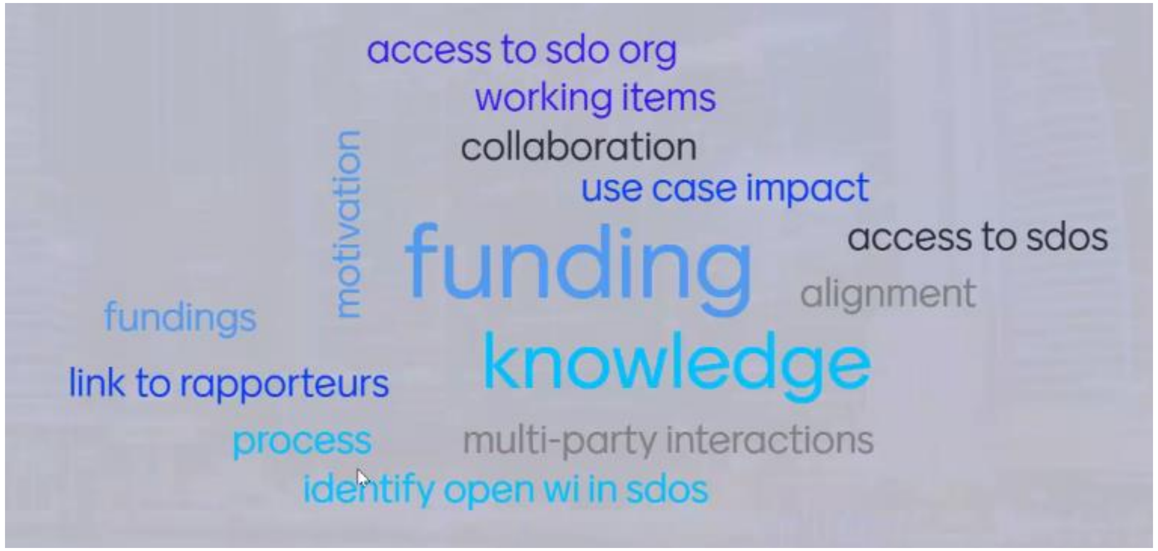


Source: Jan 2024 edition of the ETSI Enjoy! magazine
https://www.etsi.org/newsroom/magazine

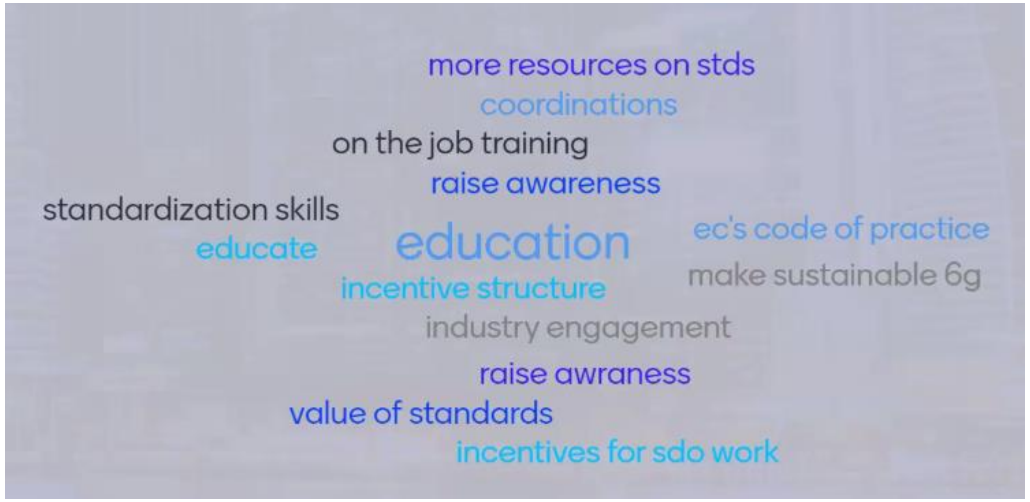
Barriers to Remove for Researchers



immaturity
complexity
price to access sdo
initial introduction
scarcity of resources
correct point to engage
lack of funding
roadmap
project lifecycle
funding
time
long time
lack of awareness
synchronisation
resources
motivation
resource constraints
collaboration
not being members
lack of info
understanding the process
long-term funding
lack of synergies



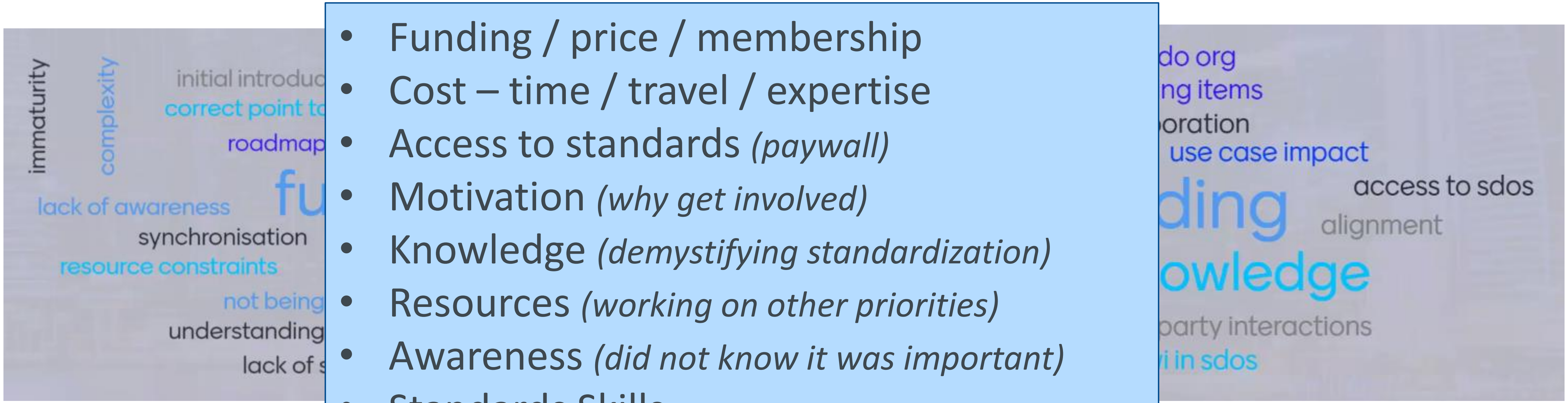
access to sdo org
working items
collaboration
use case impact
motivation
funding
access to sdos
alignment
fundings
knowledge
link to rapporteurs
process
multi-party interactions
identify open wi in sdos



more resources on stds
coordinations
on the job training
raise awareness
standardization skills
educate
education
ec's code of practice
incentive structure
make sustainable 6g
industry engagement
raise awraness
value of standards
incentives for sdo work

Audience survey from event

Barriers to Remove for Researchers

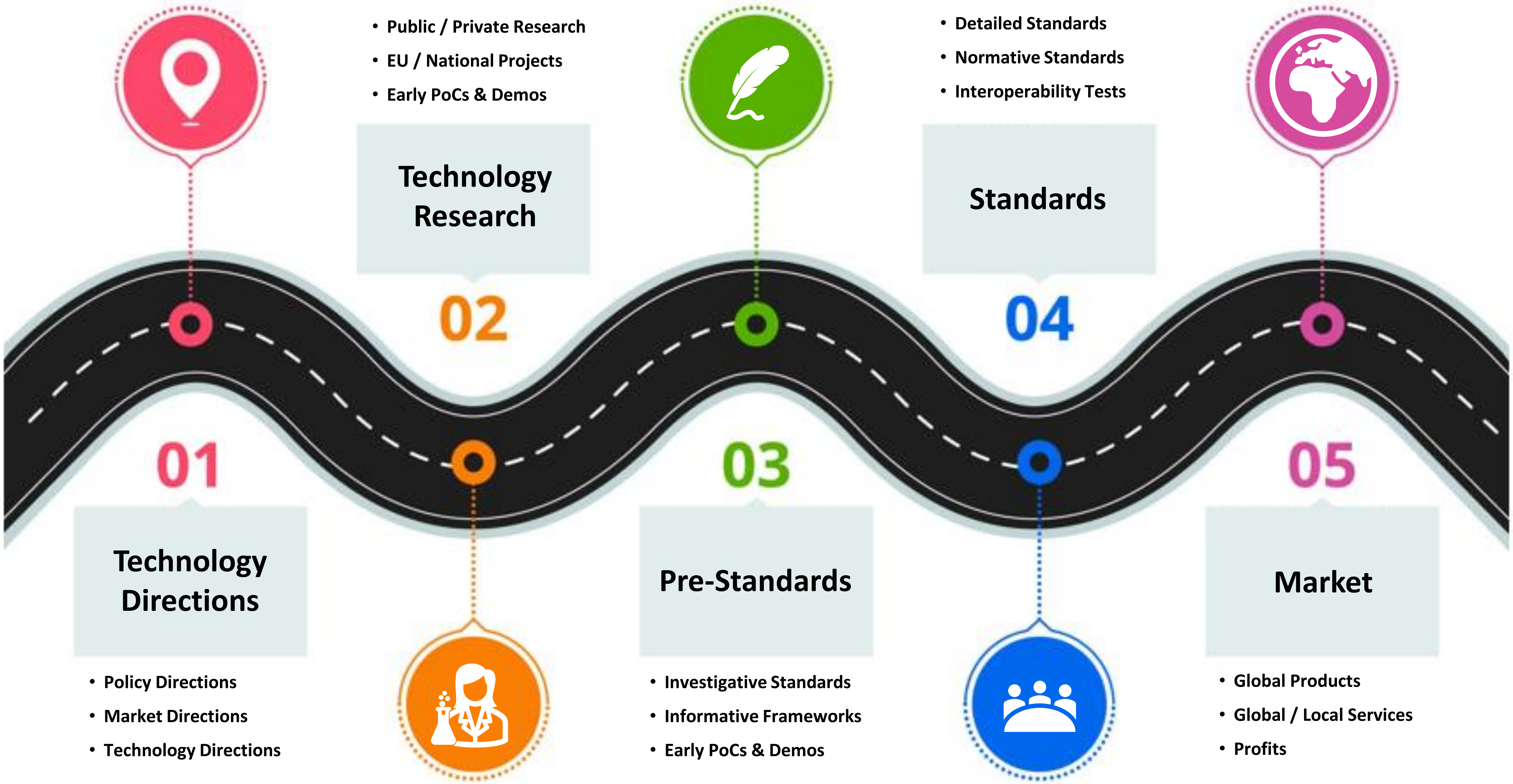


- Funding / price / membership
- Cost – time / travel / expertise
- Access to standards *(paywall)*
- Motivation *(why get involved)*
- Knowledge *(demystifying standardization)*
- Resources *(working on other priorities)*
- Awareness *(did not know it was important)*
- Standards Skills
- What is the VALUE of STANDARDIZATION?
- Incentives / where is the recognition?
- Education about Standards
- Lack of information - guidance
- Complex process – heavy investment
- Synch. research & standards cycles
- Contact point / where / who?

Audience survey from event

From Research to Market

From Research to Market



01

Technology Directions

- Policy Directions
- Market Directions
- Technology Directions

02

Technology Research

- Public / Private Research
- EU / National Projects
- Early PoCs & Demos

03

Pre-Standards

- Investigative Standards
- Informative Frameworks
- Early PoCs & Demos

04

Standards

- Detailed Standards
- Normative Standards
- Interoperability Tests

05

Market

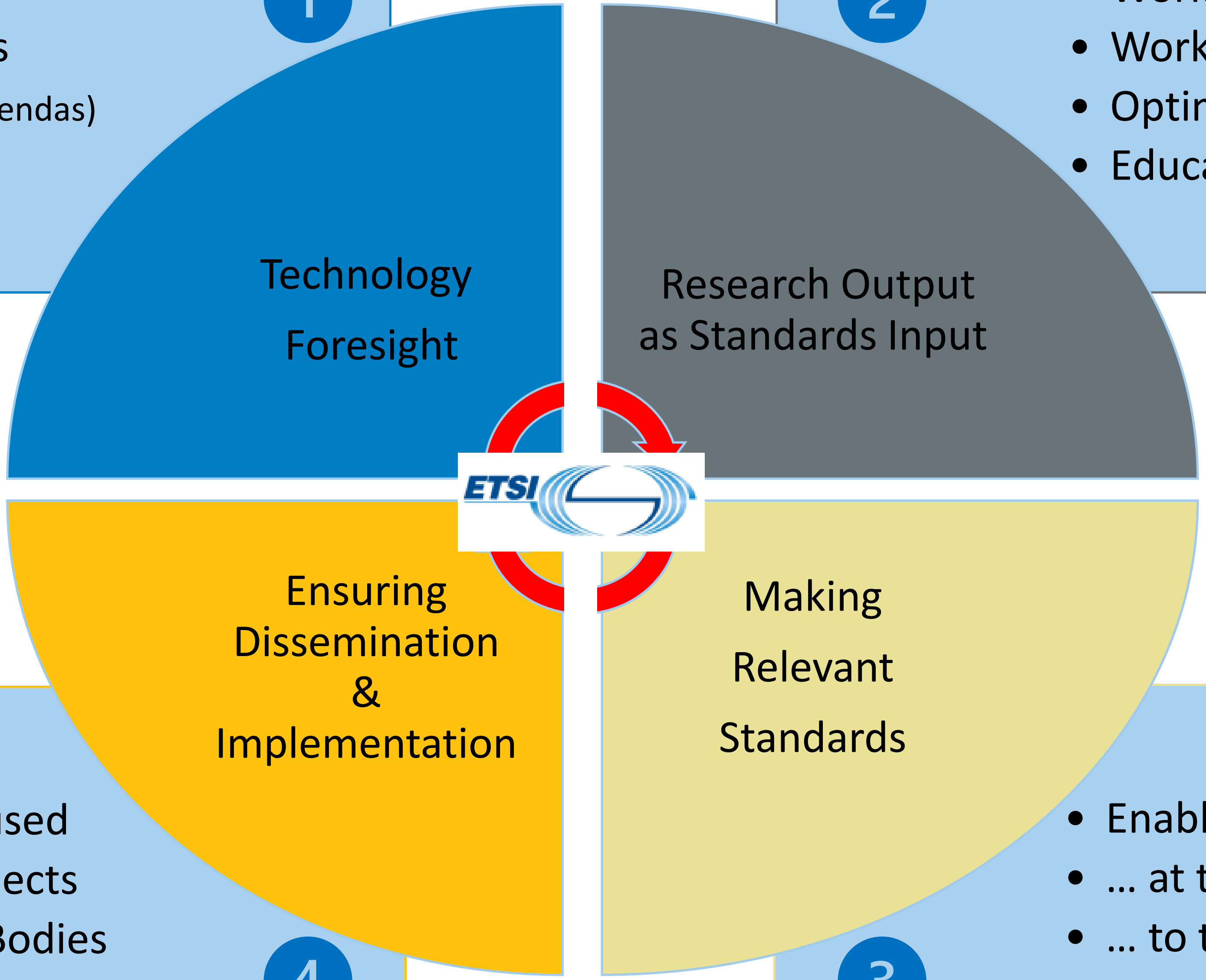
- Global Products
- Global / Local Services
- Profits

1

- Follow Tech. Roadmaps
- Follow Policy Directions
- Follow SRIAs (research agendas)
- Map Tech. Trends (ETR)

2

- Work with researchers
- Work with R&D projects
- Optimize Research in Stds
- Education / Inform / Advise



Technology Foresight

Research Output as Standards Input

Ensuring Dissemination & Implementation

Making Relevant Standards

3

- Enable the right standards
- … at the right time
- … to the right level of detail
- … Well written / relevant

4

- Ensure Standards are used
- … by researchers / projects
- … by other Standards Bodies
- … by Industry (implement in products)

ETSI Approach to Research and Innovation

ETSI encourages a constant flow of research & innovation into our standards work.

1

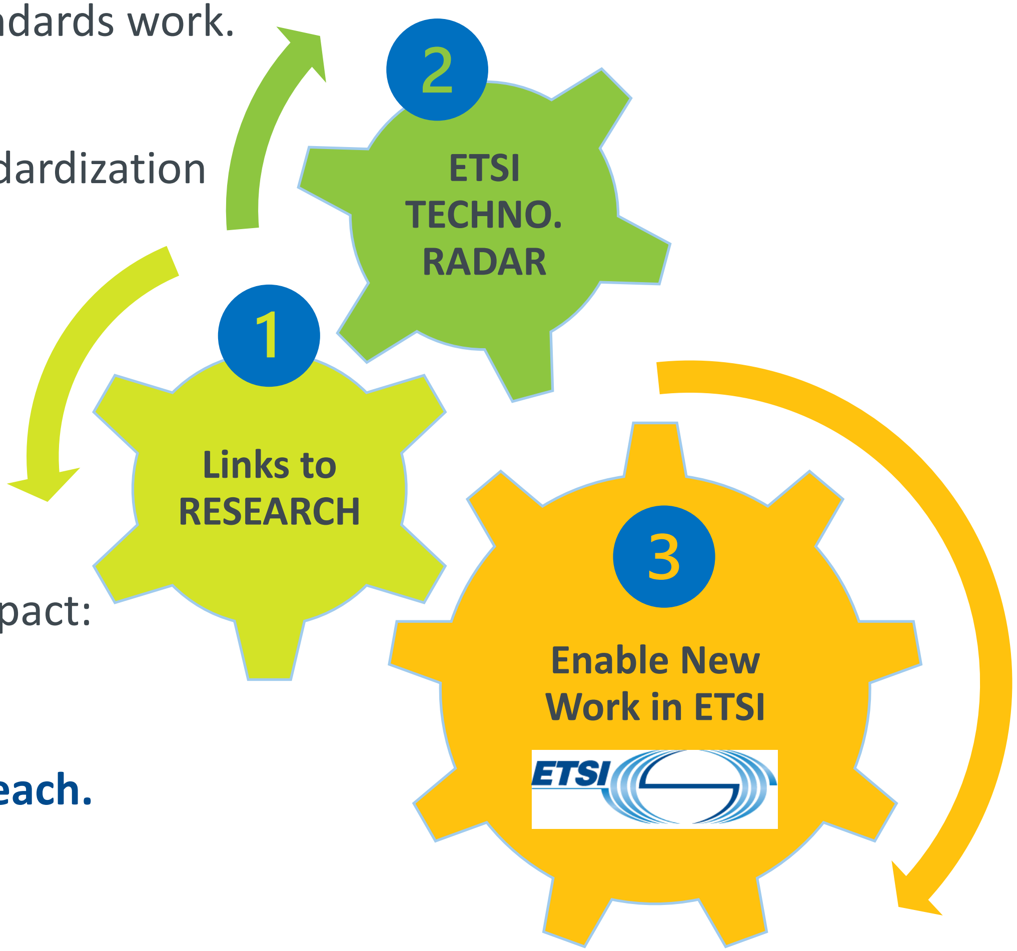
- **Enablers for Research and Innovation.**
  Build strong links between researchers, innovators, projects & standardization
  - Working with EU platforms
    (such as Horizon Europe, SNS JU, 6G-IA, NetworldEurope)
  - Working with national / EU / global research platforms & projects (e.g. HEXA-X / Next G Alliance / one6G / IOWN)

2

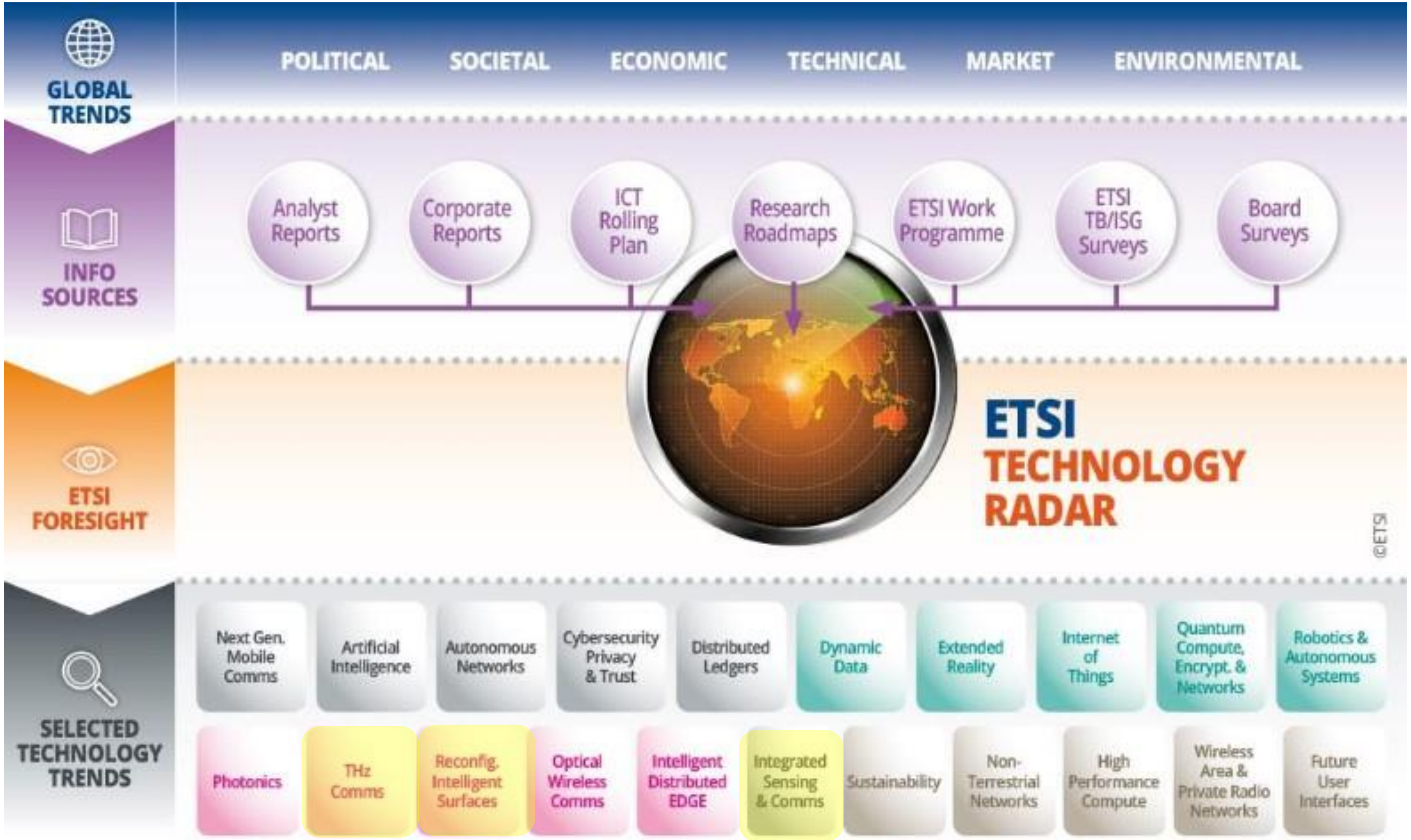
- **Technology Radar & Foresight.**
  Aware of the near-Future Technology Trends and their potential impact:
  - Produce & promote the ETSI Technology Radar (ETR)

3

- **Initiation of New Activities / Initiatives in ETSI & Education / Outreach.**
  - Outreach to universities and Education about Standardization
  - Research Helpdesk, general outreach, information
  - Enable the creation of new technical groups, areas of work in ETSI ... and more



ETSI Technology Radar -> Foresight



- ETSI Technology Radar (ETR) tracks the major technology trends that are *just over* the horizon .
- Latest ETR describes 21 technology trends & identifies opportunities for new ETSI work areas.
- Revised ETR WP published Dec. 2023.
- Your feedback on the ETR is welcome.

ETSI White Paper No. 45

ETSI Technology Radar

First edition – April 2021

ISBN No. 979-10-92620-39-1

[illegible]

ETSI Technology Radar: https://www.etsi.org/technologies/technology-radar

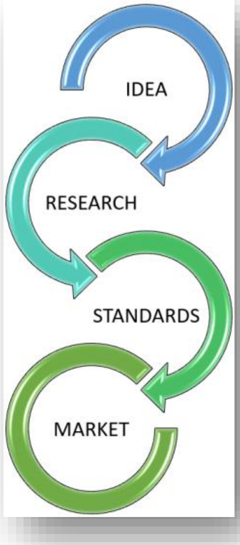
CONTENT

Research Enablers

How does ETSI provide value to researchers?

Simple Narrative:

- We want a competitive EU industry *(large, medium and small enterprises)* – ultimately generating wealth *(and wellbeing)* for EU citizens / institutes.
- Standardisation is a major competitive advantage.
- EU enterprises / EC funded projects / academia should be encouraged and helped to engage in standardization.



ETSI Resources for Researchers and Academics

Helpdesk for Researchers

www.etsi.org/research

https://www.linkedin.com/showcase/etsi-standardization-research-innovation-education

Helpdesk:
research@etsi.org

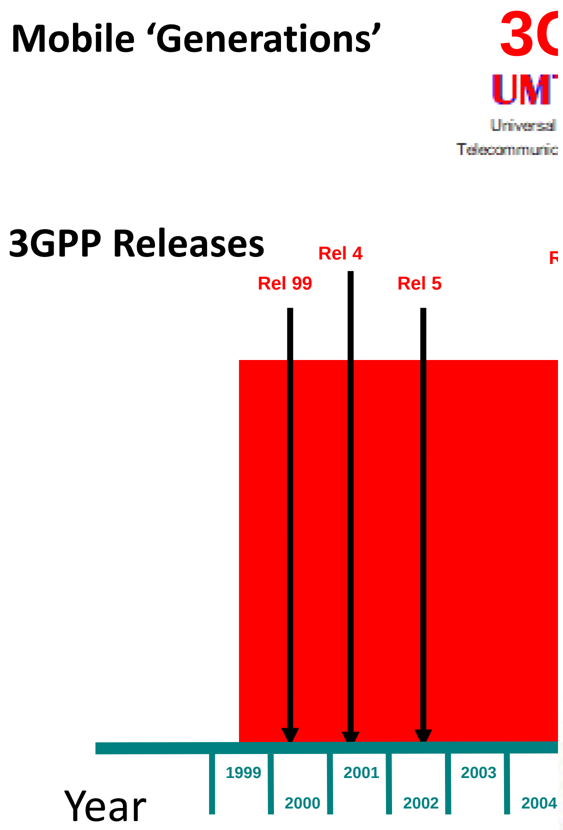
Director New Technologies:
David.Boswarthick@etsi.org

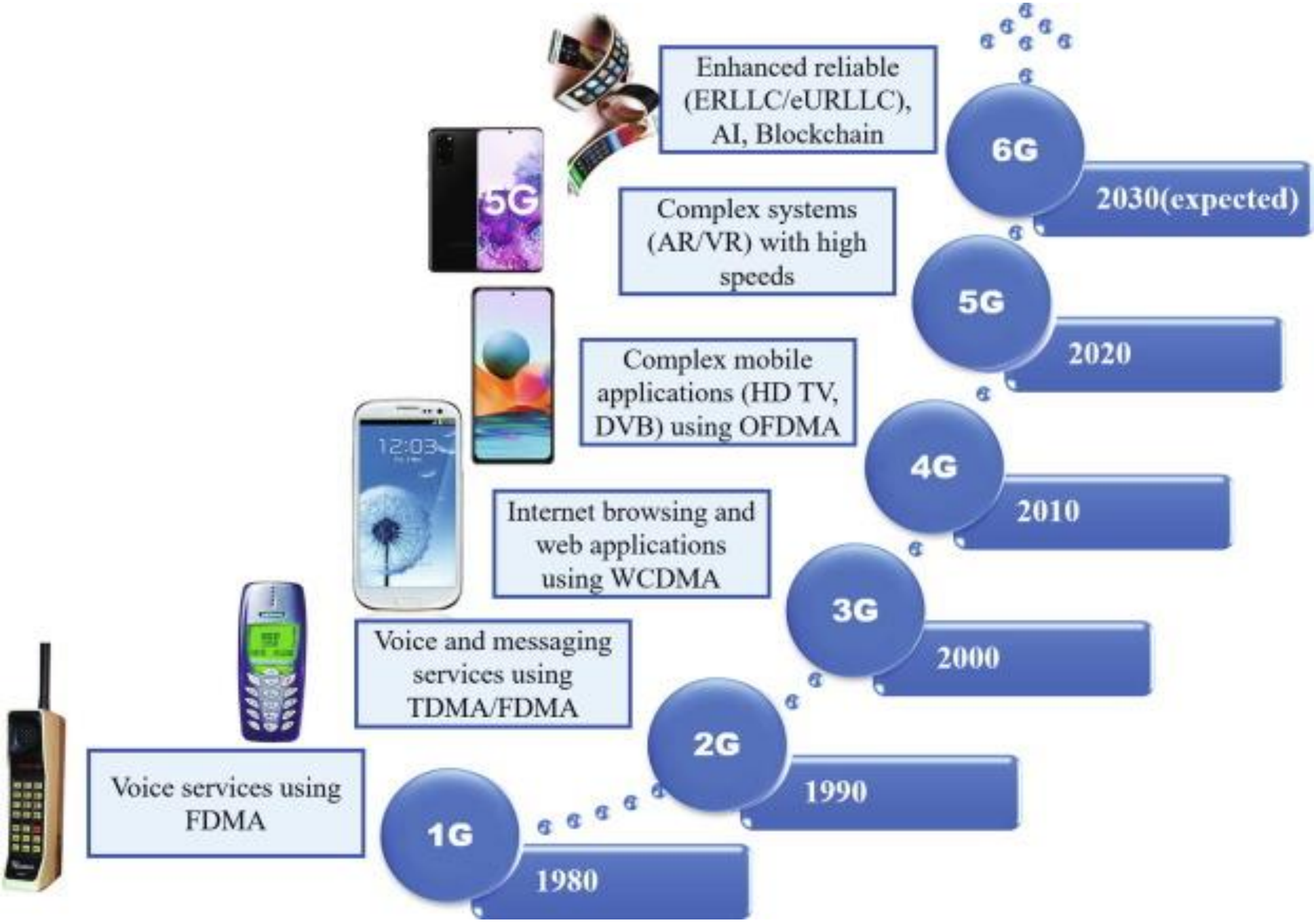
- Dedicated research Webpages
- Dedicated contact email
- Guides / Leaflets / Videos
- Support to EU Projects
- Advice on EU Research
- Setting up new Standards Groups
- Advice on Standards Activities
- … and more

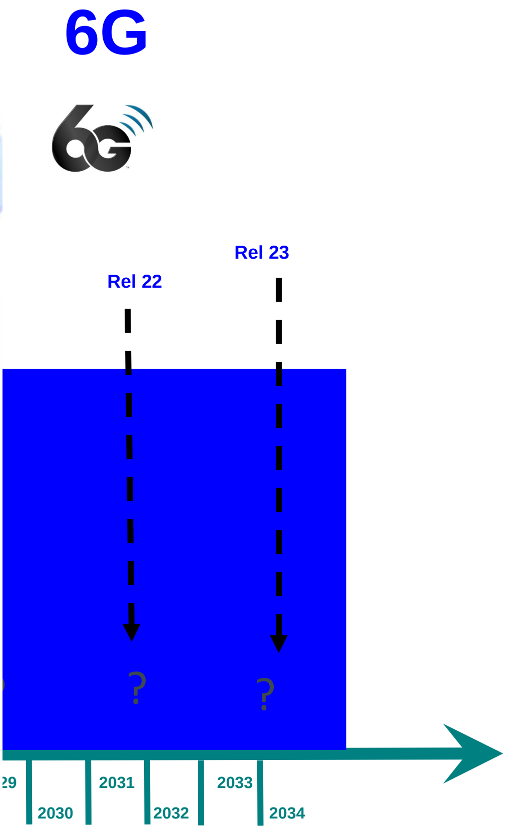
CONTENT

6G Future Directions

Mobile Generations, 3GPP Releases

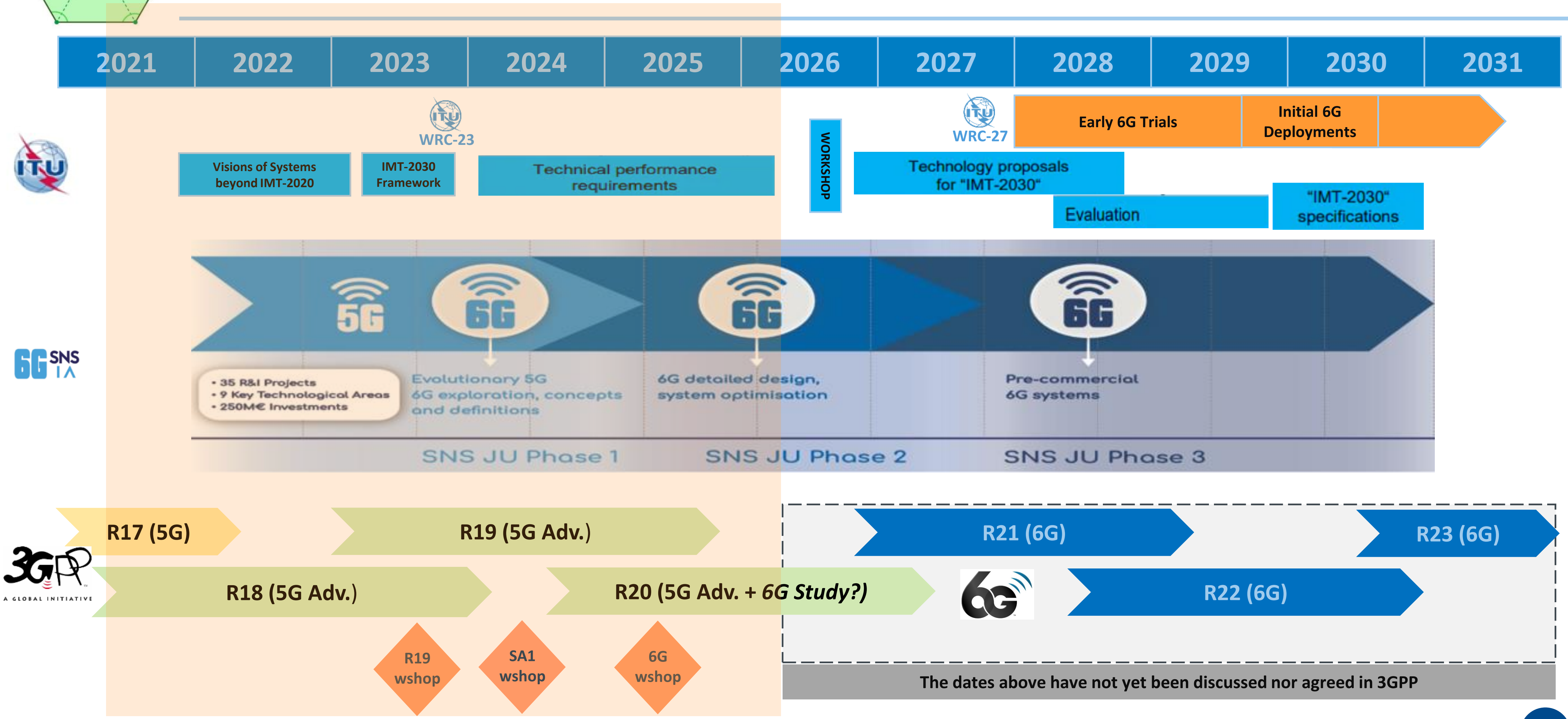



Enhanced reliable (ERLLC/eURLLC), AI, Blockchain
6G
2030(expected)
Complex systems (AR/VR) with high speeds
5G
2020
Complex mobile applications (HD TV, DVB) using OFDMA
4G
2010
Internet browsing and web applications using WCDMA
3G
2000
Voice and messaging services using TDMA/FDMA
2G
1990
Voice services using FDMA
1G
1980



Source: https://doi.org/10.1016/j.jksuci.2022.03.019

6G, Window of Opportunity (for pre-standards work)



2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2029 | 2030 | 2031

WRC-23

Visions of Systems beyond IMT-2020

IMT-2030 Framework

Technical performance requirements

WORKSHOP

WRC-27

Technology proposals for "IMT-2030"

Evaluation

"IMT-2030" specifications

Early 6G Trials

Initial 6G Deployments

- 35 R&I Projects
- 9 Key Technological Areas
- 250M€ Investments

Evolutionary 5G 6G exploration, concepts and definitions

6G detailed design, system optimisation

Pre-commercial 6G systems

SNS JU Phase 1

SNS JU Phase 2

SNS JU Phase 3

R17 (5G)

R19 (5G Adv.)

R18 (5G Adv.)

R20 (5G Adv. + *6G Study?)*

R21 (6G)

R22 (6G)

R23 (6G)

R19 wshop

SA1 wshop

6G wshop

The dates above have not yet been discussed nor agreed in 3GPP

6G, are we there yet?

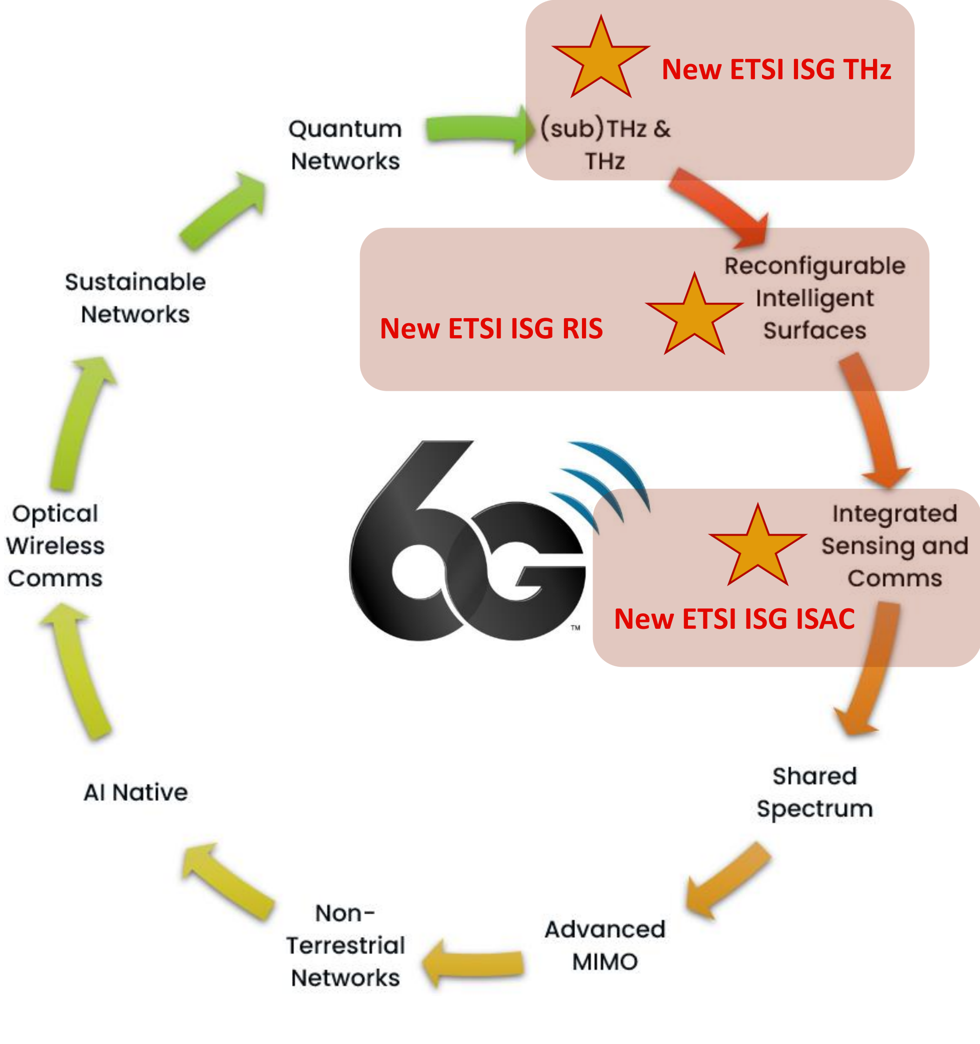
Current assumption is the first 6G services *may* be deployed in 2030, but of course expectations may change due to market pressures

6G is currently only at the Research & Vision phase, investigating potential technologies. More formal standards for 6G will follow later

We see many announcements of national, regional, corporate 6G programmes & visions with large investments in global 6G research

6G is expected to begin in 3GPP in Rel-20 (6G initial studies) and Rel-21 (6G service requirements), starting around 2024 -> 2025 ***

Recent consensus on "what is 6G" – a mixture of gradual technology **evolutions** from 5G with some **revolutionary** new concepts



Potential candidate B5G / 6G Technologies

***
NOTE: BEYOND R19, These are "indicative and estimated" dates only

Future Mobile Generations – It's just a question of perspective

Thank you for your attention

Contact:

David.Boswarthick@etsi.org
research@etsi.org

A view on recent trends in the standardization of cybersecurity

Where is cybersecurity developing towards?

Outline of content – an agenda of sorts

- A QUICK REVIEW OF WHERE WE ARE AND WHERE WE WANT TO GO
- EXISTENTIAL THREATS
- TECHNOLOGY OPPORTUNITIES
- REGULATORY OPPORTUNITIES
- FORECASTING THE FUTURE

A quick review …

Where we are

We've achieved recognition that security is good and essential and that it's difficult

Cryptography is now mainstream and expected

Where we are in a bit of a rut

We're still stuck with security being considered as a synonym of safety

We're still stuck with security being confused with privacy

Where we want to go

Effective deployment of security technology to manage risk to reasonable levels

Some review points

2G security through 3G, 4G and 5G

Strong and state of the art

Evolving with added functionality over time:

- Authentication of the phone, added authentication of the network, added longer keys for authentication (including a CMAC for the mutual element) and encryption, added in keying for higher layer functions, merging WiFi and cellular security models, moving from circuits to sessions

IoT and ICT towards an Internet of Everything

Rooted in IP but extending way beyond

Better understanding of ephemeral keying

Not just TLS1.3 but building out from session keys in 2G

A bit more review

We're pushing security at the heart of most standards work

In AI

In IoT

In smart cities

In Intelligent Transport

We are recognising privacy assurances aren't the same as security assurances

Assurance schemes are evolving to be suited for all device types and services

A last review point

We’ve achieved convergence (in the standards domain)

- Services are mostly platform agnostic
- Networks carry bits and those bits could be voice, data or video

Speed is available most of the time

- Domestic offerings of 1Gb/s are common
- Wireless (cellular) offerings of 100Mb/s and up are available (if not common)
- Blackspots of connectivity are shrinking

Digital citizens and digital society exist

Smart cars, smart cities, smart homes exist

Existential threats

- Quantum
- Pervasive encryption
- Bad guys
- Good guys with good intent but no knowledge
- Crypto
- Energy costs
- AI and its cousin ML

Quantum – an existential threat

Quantum computing will destroy the tenet of current asymmetric cryptography

- Most asymmetric cryptography is based on “hard” problems that can be resolved with quantum computers

Quantum safe algorithms are still in development and still not mature

- How much time do we need? Probably more than we have
  - X = the number of years the public-key cryptography needs to remain unbroken.
  - Y = the number of years it will take to replace the current system with one that is quantum-safe.
  - Z = the number of years it will take to break the current tools, using quantum computers or other means.
    - If X+Y>Z we’re in deep doodoo
  - T = the number of years it will take to develop trust in quantum safe algorithms
    - Adds a major complication and it now becomes if X+Y+T>Z we’re in deep doodoo

Quantum safe cryptography requires orders of magnitude increase in key size, signature size, computing resource

- Even devices that today are unconstrained will be in danger of becoming constrained (unable to offer equivalent functionality)

Countering the quantum threat

Quantum Safe Cryptography

Led by NIST and ETSI's CYBER-QSC groups

Identifying new algorithms and models for signature and encryption

Post quantum cellular

Work in 3GPP SA3 and ETSI SAGE

There is a way to overcome the threat – it will just take time

Pervasive encryption

Encryption is good, as is cryptography. The role of encryption of information being transported between two end-points has three widely recognized positive purposes depending on the context:

- confidentiality protection of the transferred content;
- enhanced trust in the identity of the parties associated with the information; and
- enhanced trust in the integrity of the information during transport.

End-to-end encryption = good, is a marketing mantra that isn’t all it seems, if it means everything is encrypted

- It removes pre-emptive filtering of malicious content
- It means networks are just pipes with no added value – can routing work if everything is encrypted with keys known only to the end points?
- Regulatory bypass (no oversight, operators are like rabbits caught in the headlights)

Countering threats of pervasive encryption

- Adoption of Zero Trust Architectures
  - Moves from Implicit to Explicit trust
- Require explicability and transparency of where encryption is used
  - Don’t assume – prove

- Work being addressed at ETSI ISG ETI

Bad guys, good guys

Bad guys will spend €s to make cents – it's a profit thing

The risk of penalty is built into their profit motive

Good guys don't have profits to justify their existence, they're always a cost item (an expense)

If you've not suffered from attack is it because your defence is good or you're not a target (yet)? How much should I spend on defence?

Good guys sometimes make bad decisions:

Encryption enables criminal activity to be hidden → let's ban encryption

Functionality comes first so let's get the code working and then secure it later

That webcam in the child's toy could be used to spy on me. Nobody would do that surely? It's just a toy

Crypto

- As in currency
  - ”I work in crypto” could give the impression to a layperson that you’re in banking or finance
- It’s not a security in the ICT sense but may be a financial security
- Crypto (currency) may divert expertise from everyday ICT security
- Crypto (currency) could be killed off by quantum threats
  - Where does my money go?
  - If there’s no central authority to endorse money does it exist?

Energy costs

Cryptography consumes a lot of processing cycles

The longer the key, the more rounds, the more power that is needed

Same with memory

Needed to store keys, to process the crypto functions

Same with communications resource

Sending keys, overhead of signature

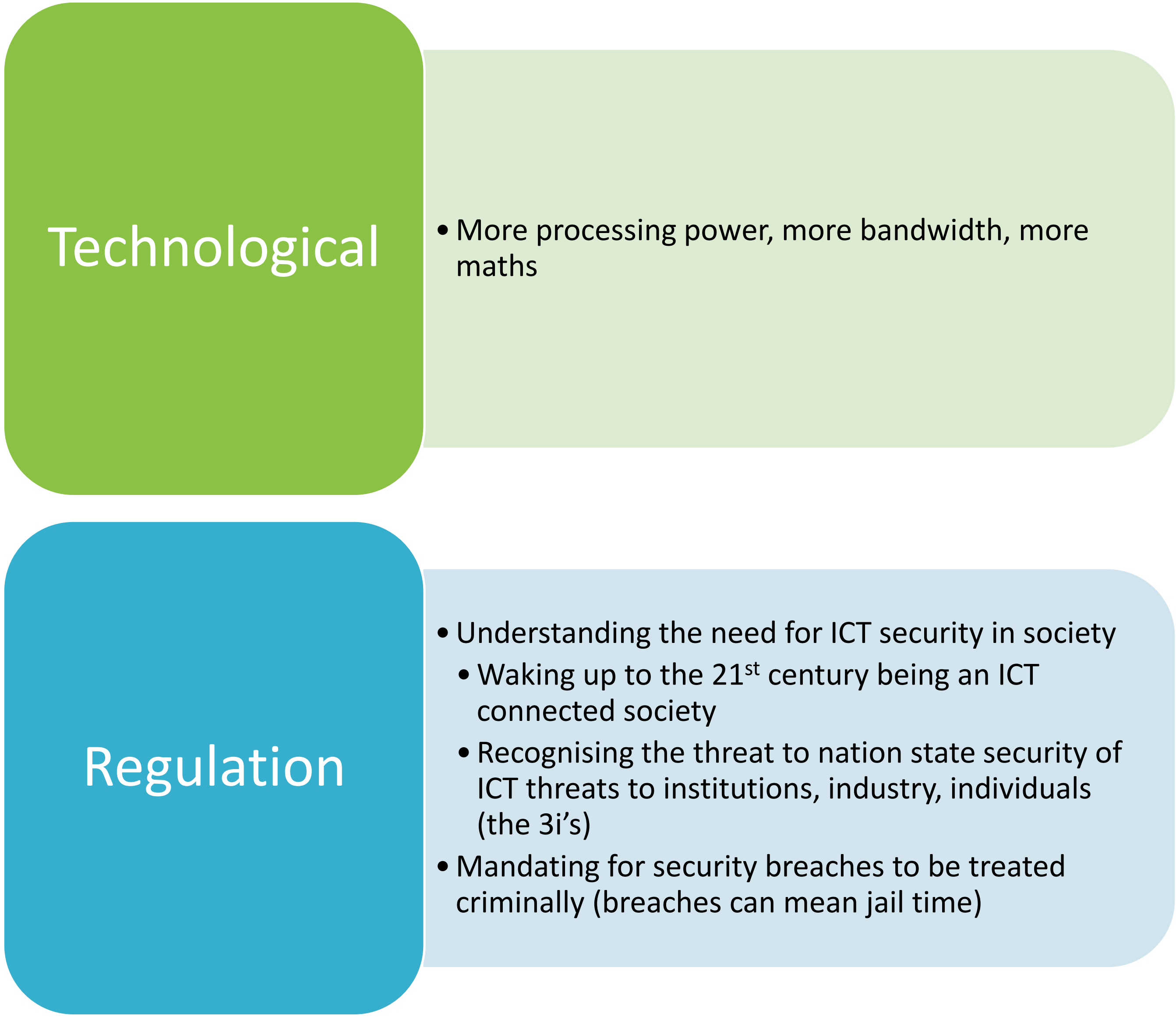
Today's crypto when used in new processes often becomes energy intense (in a bad way)

Bitcoin consensus protocols are notoriously energy inefficient

Artificial Intelligence

- In general terms more intelligence applied to a “hard” problem, and more intelligence power, cracks the problem or prevents the problem ever arising
- AI, and Machine Learning, offer a couple of things to worry base ICT security:
  - Lots of effort to uncover weaknesses in core crypto-systems compressed in time by algorithms finding weak correlations and multiplying them to be causations
  - Patterns unknown as weaknesses discovered by all out machine driven attack – botnets on steroids
- AI at the application level may be even worse – deep fakes destroy trust
  - Uncertainty breeds doubt and doubt destroys trust

Opportunities do exist



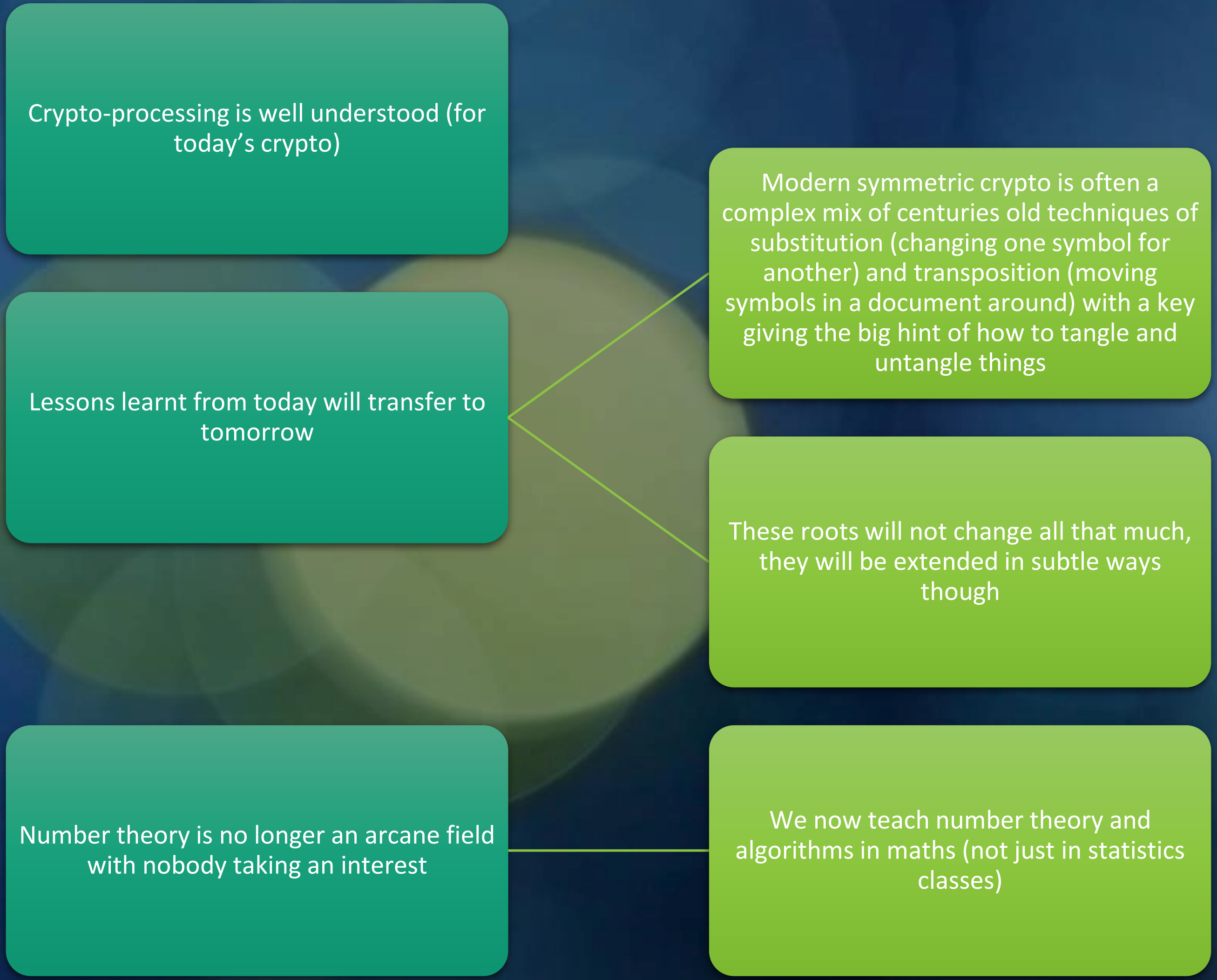
Technological

- More processing power, more bandwidth, more maths

Regulation

- Understanding the need for ICT security in society
  - Waking up to the 21st century being an ICT connected society
  - Recognising the threat to nation state security of ICT threats to institutions, industry, individuals (the 3i's)
- Mandating for security breaches to be treated criminally (breaches can mean jail time)

Technology is on our side



Crypto-processing is well understood (for today’s crypto)

Lessons learnt from today will transfer to tomorrow

Modern symmetric crypto is often a complex mix of centuries old techniques of substitution (changing one symbol for another) and transposition (moving symbols in a document around) with a key giving the big hint of how to tangle and untangle things

These roots will not change all that much, they will be extended in subtle ways though

Number theory is no longer an arcane field with nobody taking an interest

We now teach number theory and algorithms in maths (not just in statistics classes)

Technology, a good companion

- Good guys can use it to thwart the bad guys
  - Harness the power of AI/ML to identify attacks and attackers before they become an issue
  - Use Quantum to give an edge – alongside new processor designs use quantum mechanics to work on new algorithms, use QKD as an extension to more conventional key management schemes, explore the role of superposition and teleportation and entanglement in enabling security
  - Holographic processing (not holostate but multi-path processing in crystalline structures), multi-state processing, neural nets, all have a role to play

Risk management technologies?

- Risk is what we're trying to manage
- Risk assessment needs clear understanding of what we have (components) and how they fit together (interfaces)
- Modern systems are challenging for risk analysis as the components and their interfaces are auto-mutating, auto-evolving
  - We need to improve our ability to track risk in live systems
  - We can harness AI/ML to help us here

Regulation is going to help us

Security of users is at the core of many new regulatory initiatives:

The Cybersecurity Act in the EU

The Privacy directives and data protection directives

The Radio Equipment Directive

The proposed AI Act

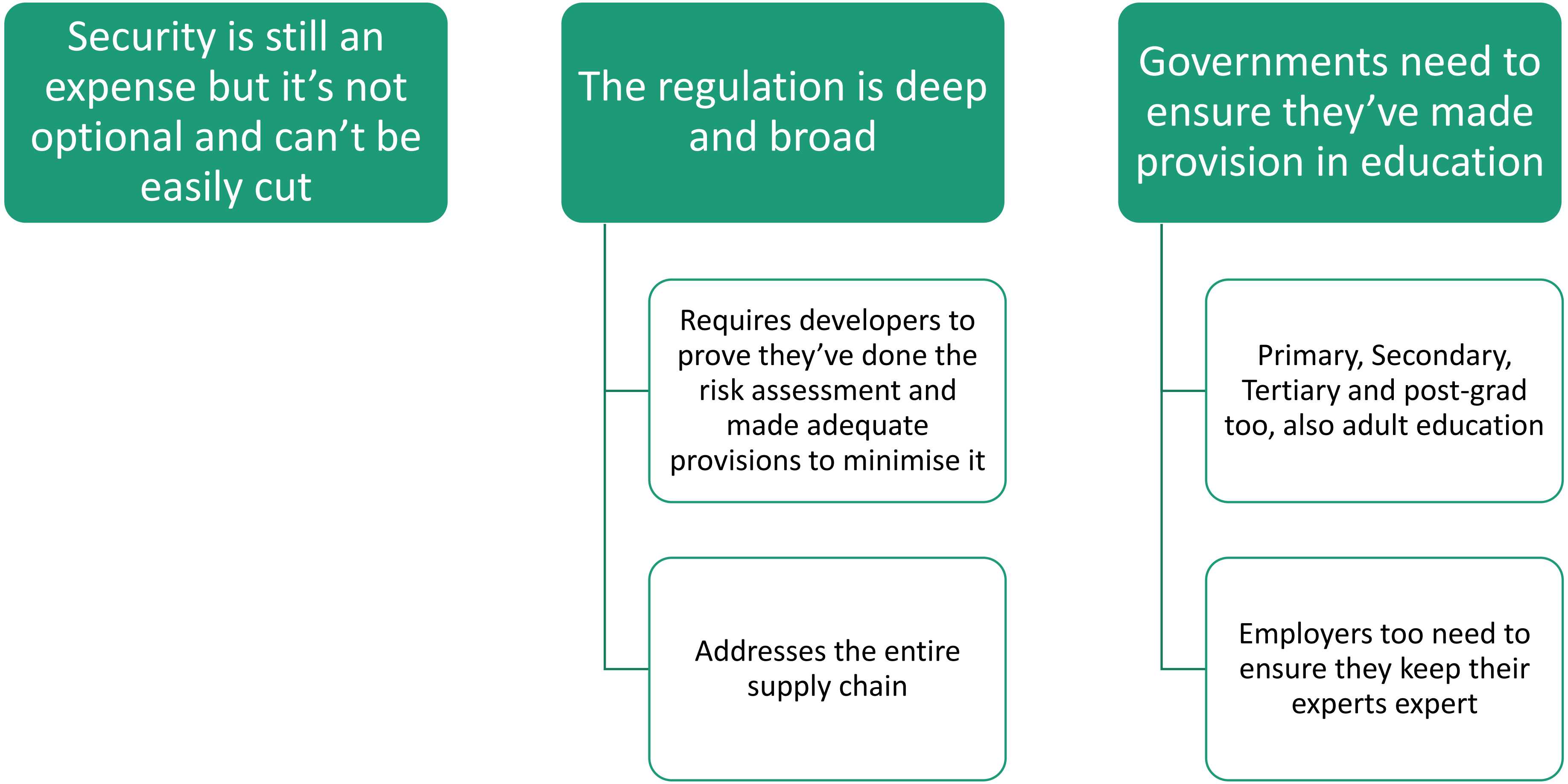
All of the above (and many others) make it clear that poor security which leads to harm is unacceptable

Security provisions, commensurate to the risk, are mandated by law

Penalties for failure are significant (The UK GDPR and DPA 2018 set a **maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater** – for infringements. Th EU GDPR sets a maximum fine of €20 million (about £18 million) or 4% of annual global turnover – whichever is greater – for infringements)

Similar levels of penalty are expected from the other acts

Regulation helps but how?



Security is still an expense but it’s not optional and can’t be easily cut

The regulation is deep and broad

Requires developers to prove they’ve done the risk assessment and made adequate provisions to minimise it

Addresses the entire supply chain

Governments need to ensure they’ve made provision in education

Primary, Secondary, Tertiary and post-grad too, also adult education

Employers too need to ensure they keep their experts expert

Regulation and technology work together

- Trust is not just personal but it’s still couched in society as if it were
    - Trusted institutions – government, school, church?
        - Why do we trust institutions? Are we simply educated to trust them?
    - Trusted roles – doctors, lawyers, accountants, engineers?
        - Do we trust them because of the steps they go through to become qualified?
    - Trusted technology – Operating systems, applications, hardware, comms
- New trust frameworks for ICT driven societies?
    - ICT led change has moved faster than many of our key institutions and roles
- We need to get to a point where trust is explicit, explicable and transparent in our ICT worlds

The crystal ball bit …

- Disclaimer: Forecasts are by nature unreliable, only hindsight is reliable (with the right analyst anyway)
- The easy bit:
  - Technology will continue to improve (Moore’s law downscaled to different levels of efficiency)
  - Software will become more testable
  - Users will expect secure systems by default
- The hard bit:
  - When things will happen is not an easy prediction

Commercial reality of forecasting

Processor architectures will change and the software they support will change

EXAMPLE: Apple have moved into SoCs for all platforms

… but only Apple know when actual changes will get to market

Software developments, and hardware developments, will be driven by sales pressure

EXAMPLE: a new OS demands new hardware and the market demands new every year

… but this suggests fashion and not novelty

Society will adopt and mould technology – not the developers

EXAMPLE: Facebook and Twitter are quite different as their use became mainstream

… but the destination is never certain when we start

Closing remarks #1

A system without security will not be viable to enter the market

Society will demand it, and vendors/developers/providers will have to provide it to survive

Regulators and nation states have to defend their citizens

If ICT is a source of threats then regulators and nation states have to ensure that ICT is secure in order to protect and defend their citizens

… and their sovereign wealth

… and their borders

Closing remarks #2

- Standards as drivers for interoperability will remain critical
  - The purpose of standards hasn't changed – they open markets to more players
  - One player can only serve a limited number of customers, a standard could allow 100s of players to serve the market, and that market could be 1000s of times bigger that a single player could serve.
  - One player can only evolve the market at their pace, 100s of players means there is a race for market share and market evolution

A take-away …

- *“Standardization does not mean that we all wear the same color and weave of cloth, eat standard sandwiches, or live in standard rooms with standard furnishings. Homes of infinite variety of design are built with a few types of bricks, and with lumber of standard sizes, and with water and heating pipes and fittings of standard dimensions",*
  W. Edwards Deming

Thanks for listening

Scott CADZOW, scott at cadzow dot com, somewhere in England