European Semiconductor Industry Association

POSITION

EU / U.S. cooperation on semiconductor standardisation

Brussels, 14 October 2021

Introduction

The European Semiconductor Industry Association (ESIA) would like to explore possible avenues for **cooperation with the United States** on the **technical standardisation for semiconductors** with a view to supporting industry competitiveness. Standardisation is seen as a vehicle to secure supply chains in various countries and regions. Continuing geopolitical tensions has focused on semiconductors as a key strategic technology asset. The development of standards, on which the semiconductor industry is based, has recently been influenced by:

1. increased national standardisation efforts that lead to competing standards, including certification and legislation requirements;
2. growing tensions over nationalistic influence over formal international standards; and
3. competing industry standards with a strong regional bias already in development.

EU semiconductor manufacturers value international standards. The nature of the semiconductor business requires uniform markets to justify the large investments required for developing products. Regional or national standards impact the market both through soft measures (local market and local industry adoption, e.g., in end-equipment & assembly industry) as well as hard measures (mandatory national standards and legal certification requirements). The trend towards diverging standards should be countered where possible, and the effects of undue influence on and competition with international standards should be mitigated where needed. This effort will require more experts to join standard developing organisations (SDOs) and associations. Active engagement in international SDOs and leading the way in this area should be a key strategic objective.

Therefore, the European semiconductor industry calls upon the European Commission to establish a standards oversight committee alongside the U.S. government. The committee should take coordinated action in close collaboration with the EU and U.S. semiconductor industries to mitigate undue effects of the tensions:

Rue de la Duchesse 11/13
1150 Brussels
Belgium
Tel.: +32 2 290 36 60
Fax: +32 2 290 36 65
secretariat@eusemiconductors.eu
www.eusemiconductors.eu

ESIA is an industry association under the umbrella of
EECA: European Electronic Component Manufacturers' Association
EU Transparency Registry: 22092908193-23

- **Oversight & tracking**: Keep track of a regional standardisation force field for semiconductor relevant markets (including associated test and certification practices), formulating any coordinated EU / U.S. institutional-industry actions where needed for critical sectors of standardisation.
- **Ensuring open access**: Taking direct action to ensure open access to standards developing organisations (SDOs) and associated certification schemes and supporting EU / U.S. companies to have access to such organisations. Also, to remove unnecessary barriers for foreign companies to participate in EU / U.S. industry SDOs.
- **Safeguarding international standards**: Protect international & industry standards from undue influence where needed and support EU / U.S. representation in relevant SDOs.
- **Reducing regional market differences:** Help reducing regional EU / U.S. differences in the practiced semiconductor standards, so the EU / U.S. markets and standards stay relevant in a potentially fragmenting standards world.

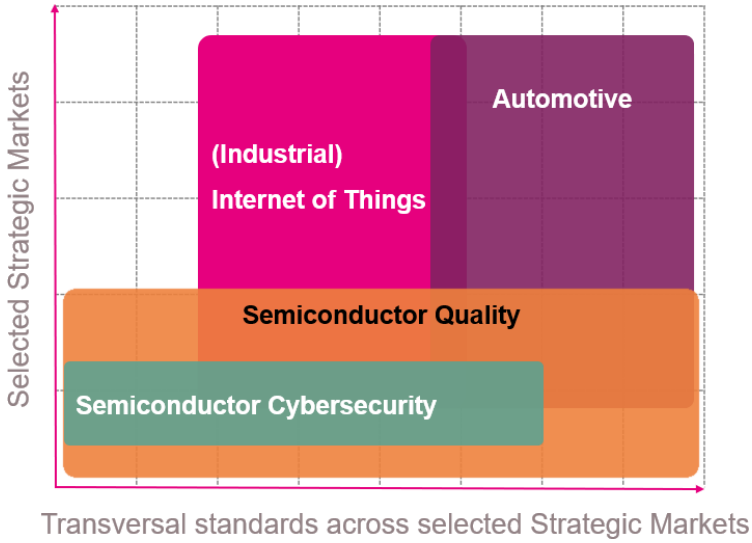
I. Scope of the initiative

EU-U.S. cooperation should be able to form a counterweight against nationalistic and regionalist forces in terms of market access and market size – international where possible, or well-aligned regional markets and complementary standards where international standards are out of reach. Furthermore, crucial international standards need to be carefully guarded so as to ensure these can keep supporting the above approach.

In terms of an EU-U.S. cooperation, the attention should not be focused on standards without any broader context; instead, specific standards linked to designated European industries should be addressed in order to be influential and protect its interests. Semiconductor companies will use their influence to sustain the competitiveness of the industry in a global context. EU-U.S. alignment needs to be explored, although the Asia-Pacific region (including but not limited to China, South Korea, Japan, and Taiwan) should not be ignored.

As a rule, the EU should avoid creating new standards, but rather attempt influencing existing ones to be aligned on industry expectations. Already, too many standards are competing, leading to detrimental fragmentation. A standards and alliances alignment effort should be part of a proper alignment strategy per strategic market.

In the first phase, the **cybersecurity** (incl. industrial Internet of Things) **and the semiconductor quality dimension** should be actively addressed in a transversal manner. Moreover, ESIA would propose to actively address the **automotive industry** application sector in more detail. Other domains of semiconductor-related standardisation should be designated for tracking and monitoring.



II. Oversight and Tracking

The regional standardisation force field is highly dynamic due to evolving regional trade & industry policies and associated regulatory activities, as well as the high pace of technology evolution. Semiconductor companies are involved in a large number of SDOs. To track trends towards regional standardisation, certification and regulation, the field of different standards committees should be clustered to a traceable number. For each cluster, there should be regular monitoring (twice a year) by those actively involved for signalling any trends toward detrimental regional developments. Based on this oversight and tracking activity, new active measures can be deployed: ensuring open access, safeguarding international standards, and reducing regional market differences. An initial list of standard domains is provided in Annex II.

III. IEC Technical Committee 47

The central international standards committee for semiconductor quality standards is International Electrotechnical Commission (IEC) Technical Committee 47 (TC 47). According to the IEC, the scope of the TC 47 on Semiconductor devices is:

> To prepare international standards for the design, manufacture, use and reuse of discrete semiconductor devices, integrated circuits, display devices, sensors, electronic component assemblies, interface requirements, and microelectromechanical devices, using environmentally sound practices.
>
> Activities include wafer level reliability, package outlines, terms and definitions, quality issues, physical environmental testing, device specific test methods, device specifications and minimum content, pinouts, interface requirements, and applications.
>
> Excluded from the scope are:
>
> - Passive integrated circuits or networking containing resistors and capacitators or their combination (TC 40).

- Systems of photovoltaic conversion and all the elements in the entire photovoltaic energy system (TC 82).
- Devices covered by the scope of TC 22, TC 86 and JTC1.
- Discrete/integrated optoelectronic semiconductor devices for fiber optic telecommunications including hybrid modules (TC86).[1]

3.1 Operational challenges to TC 47

IEC TC 47 has experienced a continued increase in non-EU and non-U.S. standardisation efforts. The average time from start to finish for releasing an IEC standard amounts to almost three years, as counted form a new work item proposal until the publication of a harmonised standard. This includes seven stages[2] until the standard release, which includes three approval stages with different voting mechanisms. Initial approval of a new work item proposal (NP) is being brought to the attention of the relevant IEC technical committee (TC) or subcommittee (SC) by a National Committee (NC).

The approval process is a rather complex matter. For instance, to receive initial approval, the NP ought to receive a two-thirds majority of the active members (so-called 'P-members'[3]) within the TC / SC, as well as the commitment of said members to send a minimum required number of experts to begin the work. Committees with 16 P-members or less require min. four experts from different countries, whereas committees with 17 P-members or more stipulate min. five experts from different countries. Recently, NPs for the abovementioned scope were processed in SC 47 working groups, e.g. in working group 1[4] and 2[5] of SC 47E 'Discrete semiconductor devices', as well as in all four working groups of SC 47F 'Micro-electromechanical systems'.

The approach to standardisation is perfectly illustrated by the actions of non-EU and non-U.S. national research institutes to send large numbers of experts. They either submit new standardisation proposals for IEC standard SC / TC 47 that are going to be promoted in favour of their own domestic semiconductor solutions or they challenge the running standardisation draft documents with comments to jointly be agreed.

[1] IEC | International Electrotechnical Commission (18/06/2021). *TC 47 Dashboard*, Technical committees and subcommittees. URL: https://www.iec.ch/ords/f?p=103:7:614889508930016::::FSP_ORG_ID,FSP_LANG_ID:1251,25 (retrieved 23/06/2021)
[2] Standard development stages: Source https://www.iec.ch/standards-development/stages
[3] IEC member countries who send experts to participate actively in technical work are referred to as "P-members". IEC member countries who only have an observer status are referred to as "O-members".
[4] SC 47E WG 1: Semiconductor sensors
[5] SC 47E WG 2: Microwave devices

Recommendations:

safeguarding international standards, ensuring open access

ESIA strongly recommends that the EU and the U.S. align on an active monitoring role for the TC 47 (and possibly affiliated committees) and ensure no undue developments take place.

In order to overcome the challenge in TC 47 (as described above), more experts from the NCs of Europe and the U.S. are required to influence such international standards in our favour. These experts must be nominated by the European semiconductor industry or related research institutes as explained earlier.

In the medium or long term, a similar initiative might be relevant in relation to the *Joint Electron Device Engineering Council* (JEDEC). There are indications that JEDEC could soon face comparable challenges to TC 47.

EU and U.S. companies need to take active roles in developing national initiatives in this domain. It is important that there is government support to ensure equal access for EU and U.S. companies to such initiatives.

IV. EU-U.S. alignment on cybersecurity standards

The EU should collaborate closely with the U.S. to harmonise / standardise cybersecurity requirements, evaluation methodology and certification in these two economic regions. Harmonised cybersecurity standards across the Atlantic would be helpful to the global semiconductor value chain, as it will ensure cost-effective secure products for the two regions.

At present, the most widely used security evaluation standard that can be applied across multiple applications is Common Criteria (CC). Industry standards such as *Trusted Computing Group* (*TCG*), *Fast Identity Online* (*FIDO*) *Alliance*, *Wireless Power Consortium* (*WPC*), *Global System for Mobile communications Association* (*GSMA*), and others have adopted CC evaluation and certification methodology. Furthermore, *GlobalPlatform* has been developing Security Evaluation Standard for IoT Platforms (SESIP), which is also based on CC. Meanwhile, the European Union Agency for Cybersecurity (ENISA) has also been promoting CC within their various cybersecurity certification schemes, e.g. EUCC[6] or EUCS[7].

4.1 Initiatives in the EU and the U.S.

As for the EU, DG GROW is looking into standards for the Radio Equipment Directive (RED, or Directive 2014/53/EU)[8] Delegated Acts to activate cybersecurity requirements. The European Commission is likely to issue open standardisation requests for essential requirements

[6] European Common Criteria Scheme.
[7] European Union Cybersecurity Certification Scheme on Cloud Services.
[8] OJ L 153, 22.5.2014, p. 62-106. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN (retrieved 23/06/2021)

for a horizontal EU regulation on cybersecurity, with a more generic scope. These standards shall be developed by European standardisation organisations (ESOs).

In the U.S., California Senate Bill on "*Information privacy: connected devices*" mandates "*reasonable security features*" for connected devices.[9] Other states like Oregon, Illinois, Maryland, New York, and Virginia are expected to release cybersecurity regulations. The "*IoT Cybersecurity Improvement Act of 2020*" requires cybersecurity for connected devices, based on standards to be developed by the National Institute of Standards and Technology (NIST).[10] In May 2020, NIST published the standard NISTIR 8259A "*IoT Device Cybersecurity Capability Core Baseline*".[11]

4.2 Composition in cybersecurity evaluation

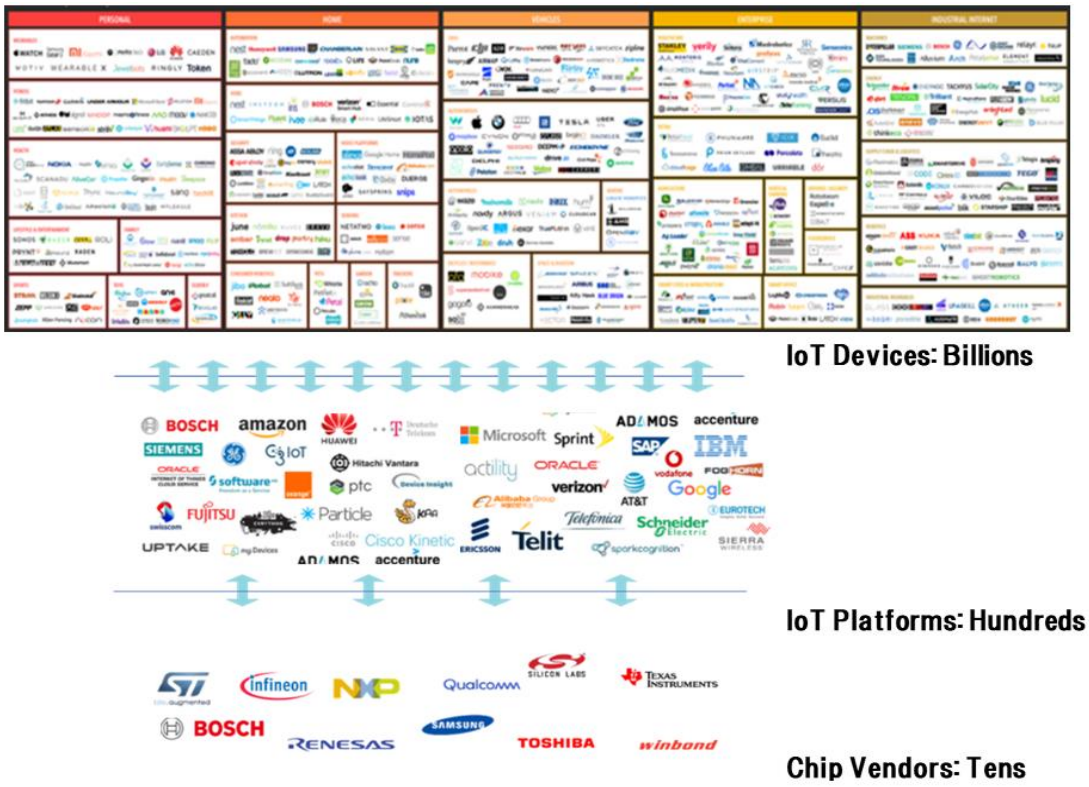
To understand how IoT device manufacturers shall comply with these new cybersecurity requirements, it is essential to understand the interdependencies among the different actors in the security domain.

The following diagram is demonstrating the impact of chip vendors in the complete ecosystem, as any security feature added in their chip will be propagated at platform level and ultimately within IoT devices. Therefore, any change in a chipset mastered by chip vendors will have a direct impact on the myriad of IoT devices.

To illustrate this ecosystem interaction on security, a good concrete example could be an IoT device software update. Billions of IoT products provide secure remote software updates relying on cryptography technology. Device manufacturers are not security experts and they rely on IoT platforms to provide a turnkey solution for a "*secure update*". As of today, several hundreds of IoT platforms are already available (see diagram on the next page).

But IoT platform developers are not cryptography experts either. They are relying on chip vendors to propose an embedded-on-silicon solution. As of today, a dozen of vendors are providing embedded cryptography to support safe software updates. Therefore, any cryptography solution along with their associated security evaluation will automatically benefit both IoT device manufacturers and IoT platform actors.

[9] S.B. 327, 2017 Biennium, 2018 Reg. Sess. (Cal. 2018). URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (retrieved 11/08/2021)
[10] Internet of Things Cybersecurity Improvement Act of 2020, H.R.1668, 116th Cong. (2020). URL: https://www.congress.gov/bill/116th-congress/house-bill/1668 (retrieved 11/08/2021)
[11] NIST Computer Security Resource Center | CSRC (29/05/2020). *NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline*, PUBLICATIONS. URL: https://csrc.nist.gov/publications/detail/nistir/8259a/final (retrieved 11/08/2021)



The effort required by device vendors for security compliance can be greatly simplified with composition as a single security evaluation done by the semiconductor vendor provide assurance on state-of-the-art cryptography for billions of products.

4.3 Examples of composite cybersecurity evaluation methodologies

In order to increase the competitiveness and trustworthiness of semiconductor-based devices, ESIA recommends that EU-U.S. standardisation initiative embraces the cybersecurity evaluation methods that allow composite security evaluations. Two such evaluation standards are Common Criteria (CC) and Security Evaluation Standard for IoT Platforms (SESIP).

CC evaluation methodology

The risk exposure to cybersecurity is high for application systems and infrastructures that are of high interests and / or financial value. In such systems, the devices and digital components require high security and the ISO standard 15408 – known as CC – is the *de facto* standard recognised worldwide. The EU is specialised in performing such CC evaluations and certifications. European CC certifications issued by the EU Senior Officials Group on the Security of Information Systems (SOG-IS) scheme are used and recognised worldwide. We expect that the EUCC scheme, successor of SOG-IS, will retain its recognition, especially in the high security level defined in the EU Cybersecurity Act (CSA, or Regulation (EU) 2019/881)[12].

[12] OJ L 151, 7.6.2019, p. 15-69. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (retrieved 19/08/2021)

The CC evaluation methodology is a rigorous process of evaluation which includes security audits of the product development processes and sites as well as penetration-testing[13] covering the most sophisticated logical and physical attacks.

CC provides a time-tested composition methodology, which has been particularly successful in govID and payment smart cards as well as devices in critical infrastructures, where the security evaluation of a device or system reuses the CC certification of the hardware on which it runs.

SESIP

SESIP is a flexible security evaluation methodology designed for IoT devices and developed by *GlobalPlatform*, a non-profit member-led organisation with vetted security expertise. SESIP facilitates end-device security evaluation, by composition of evaluated parts. It provides a standardised methodology supporting a broad range of regulatory and security frameworks, and is accessible to non-security experts.

SESIP reduces complexity, cost, and time-to-market for IoT stakeholders by offering a methodology based on composition that unifies compliance to standards, regulations and security requirements used in EU and U.S., such as ETSI EN 303 645 for Consumer-IoT (C-IoT), IEC 62443-4-2 for industrial IoT, and NISTIR 8259A for baseline security.

Recommendations:

reducing regional market differences

1. ESIA recommends that EU-U.S. standardisation initiative embraces the cybersecurity evaluation methods that allows composite security evaluations.
2. **For a high level of security, CC should continue being used**. The application areas should not be limited to the government area alone, it should also be used in sectors like industrial IoT and automotive systems when high-end security is required.
3. **For basic and substantial levels of security**, ESIA recommends **endorsing the SESIP approach for IoT platforms**, to support EU and U.S. cybersecurity standards and regulations of consumer end-devices with composition. ESIA also recommends SESIP recognition in EU security certification framework implementing the EU CSA (which is currently under construction).

Please see Annex I for examples of existing security standards from regional and global (public) and of existing security standards from industry (private) domain.

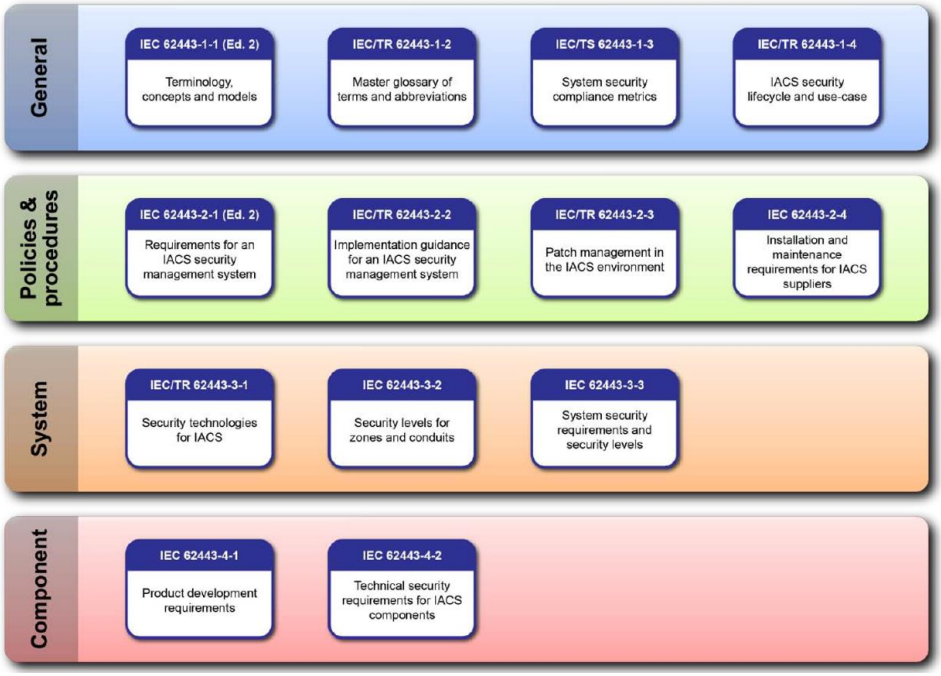
[13] A penetration test, or pen test, is an authorised simulated cyberattack against a computer system to identify weaknesses and check for exploitable vulnerabilities.

4.4 Security standards for industrial IoT semiconductors

The last years showed how industrial IoT increases productivity, allows maximum individualization of fabricated goods, and enables optimisation of processes combining IoT technology and artificial intelligence – and finally seamless collaboration between industrial facilities across globe. All these advances rely on the fact that the **involved devices, networks and services can be trusted**. Otherwise, industrial facilities will crash, products with lower quality are delivered to customers, and valuable IP is stolen. Thus, technologies enabling the implementation of cybersecurity mechanisms, such as cryptographic algorithms, secure hardware anchors, and secured communication protocols, must be globally interoperable across the industry.

With this increased automation and connected devices in manufacturing, there is an increased reliance on industrial IoT semiconductors. Industrial IoT semiconductors need to ensure that there is a reliable, secure, and sustainable supply-chain globally. Therefore, cybersecurity needs to be a one of the cornerstones of any connected device used in the manufacturing industry.

The International standards ISA / IEC 62443 series addresses the cybersecurity challenges of an industrial automation control system (IACS) in a systematic and holistic way. For example, a standard in this series, ISA-62443-4-2: 'Security for industrial automation and control systems, technical security requirements for IACS components', covers the cybersecurity technical requirements for components that make up an IACS, such as the embedded devices, network components, host components, and software applications. This standard, which is based on the IACS system security requirements of ISA / IEC 62443-3-3: 'System security requirements and security levels', specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures. The complete list of ISA / IEC 62443 series of standards is shown in the figure below:



Recommendations:

reducing regional market differences

ESIA recommends that IEC 62443 cybersecurity standards for industrial IoT should be endorsed and mandated by EU and U.S. for both domains: secure products and secure production.

ESIA recommends for **global interoperability** between companies in the EU and the U.S., it is important that all industrial IoT participants follow and use the same international standards and define the same security level for the exchange of confidential or strictly confidential information. It is expected that in the future, the boundaries between the **secure production** in a smart factory and the **secure products** will dissolve.

Please see Recommendations under 4.3 for cybersecurity certification relating to industrial IoT.

V. EU-U.S. alignment on automotive

The automotive industry is currently undergoing a revolution leading to the introduction of new services such as shared mobility, advanced driver assistance systems (ADAS) towards autonomous driving (AD), automotive connectivity, in-vehicle infotainment (IVI), not to forget electrification. Connectivity, including in-vehicle connectivity, and software architecture are key technologies enabling such services. The field is highly dynamic, triggering existential investments from car original equipment manufacturers (OEMs). Enabling standards are expected to evolve in a mix of industry and committee approaches. New clusters of standardisation activities may emerge as the field gains maturity. An initial list of automotive standard clusters is provided in Annex II (also see chapter II. Oversight and Tracking).

Recommendations:

oversight and tracking

ESIA recommends that special attention is devoted in the oversight and tracking activity towards the rapidly advancing field of semiconductor and information technology in automobiles, including the identification of new standardisation domains.

In one specific cluster, the current automotive semiconductor supply shortage is triggering regional developments that require immediate attention: automotive semiconductor quality.

5.1 Automotive semiconductor quality

Semiconductor quality and reliability takes a special role in the automotive domain. The demand for extremely high quality and reliability grades has led to the development of zero-defect strategies, emphasising not only product-based (testing) approaches, but adding production process and company process dimensions. Key standards are developed in industry

standards bodies, like the *Automotive Electronics Council* (AEC; AEC-Q100) and the *Automotive Industry Action Group* (AIAG; IATF 16949). These standards have been the basis on which electronics have been able to find their place in cars without compromising the overall reliability of cars. The standards have been created as a collaborative effort by the automotive engineering community.

Under pressure of the general trend towards greater supply chain autonomy, further amplified by the recent automotive semiconductor supply crisis, new entrants will shortly revisit these standards in specific markets and will likely drive for lower grade standards permitting easier market entrance. And though the inferiorly qualified products resulting from such standards will at first affect only indigenous products, the complexity of today's supply chains will create untenable pressure on the current EU and U.S. automotive supply chain, leading to gradual degradation of quality and reliability of electronics in the automotive industry, and which will unduly negatively influence the positions of the EU industry in this sector.

It is crucial that sufficient counterbalance can be provided to the understandable but opportunistic approach that will be a threat to the total automotive supply chain and the current position of the EU automotive semiconductor sector.

NOTE: new fields are emerging in supply chain traceability (including concepts like software bill of material, or SBOM[14]) and functional safety in ISO TC 22 / SC 32 (ISO 26262). These may have to be included in the active policy for this domain in due course.

Recommendations:

ensuring open access, safeguarding international standards

EU and U.S. authorities, in conjunction with automotive stakeholders, should take an active attitude to monitoring the automotive industry, specifically with respect to the proliferation of sub-quality grade semiconductor products and subassemblies in the EU and U.S. car industries.

Furthermore, they should help ensure that the current leading standards organisations in this domain are not unduly influenced to weaken the development if higher quality standards, e.g. AEC, JEDEC, the *Electronic System Design Alliance* (ESDA), and AIAG.

Lastly, to assist companies with a strong position in this sector, EU and U.S. authorities should play an active role in any alternate standards developments: by ensuring a level playing field to accessing and influencing these standards organisations, as well as by including such efforts as part of the financial support programme, even if this may entail the indirect sponsoring of non-EU personnel.

[14] A software bill of materials is a list of components in a piece of software that describes the constituent parts in a software product.

VI. Financial implications of industry participation in standardisation

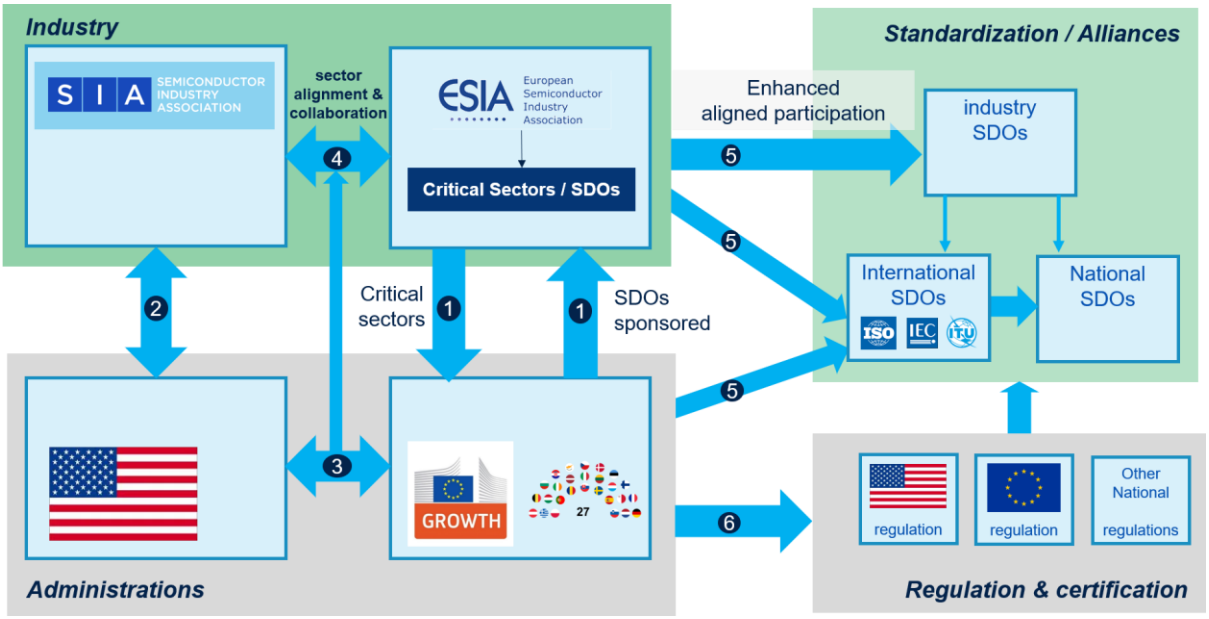
Standardisation is a key driver of innovation, and an essential tool to facilitate trade and interoperability. Since long, Europe has underestimated the importance of standardisation, and other regions' current position in SDOs is the result of long-term efforts. Building and strengthening EU companies' influence in standards and alliances will take time and the expected result will not be immediate. Nevertheless, such support is becoming increasingly eminent. Europe should build a real strategy with key semiconductors companies.

As part of the efforts to "*ensure open access*", "*safeguarding international standards*", and "*reducing regional differences*", industry will need to make significant scarce expert resources available to increase representation in SDOs. Also, the activities to co-drive "*oversight & tracking*" will require additional efforts.

There are complementary approaches suggested to support European standardisation efforts by semiconductor companies:

- Create collaboration between European research institutes and the semiconductor industry to drive standardisation in SDOs with goals set by industry.
- Direct compensation for standardisation-related investments of semiconductor companies could be considered.
- National standards organisations can improve their support for semiconductor related standardisation topics.

The overall resulting approach is illustrated in the diagram on the next page:



❶ European semiconductor companies and their associated SDOs need to be aligned on strategic sectors to be protected. Joined efforts coordinated by ESIA and DG GROW

should determine those sectors. Consideration could be given to fund industry activities in support of enhanced participation.

❷ U.S. process: SIA to be aligned with the U.S. administration on their objectives (not in our scope).

❸ EU-U.S. alignment on sectors, regulation and associated SDOs is expected.

❹ Alignment on sectors and SDOs among the EU and U.S. industries based on ❸

❺ Both SIA and ESIA members are acting on the targeted and sponsored *Industry Alliances* and SDOs, significant increasing board of directors, chair, co-chair positions, working group leaders and technology experts from industry. National representation in formal international standards should be strengthened by European national authorities.

❻ EU-U.S. Trade and Technology Council: Directive to national regulation.

For further information:

Hendrik Abma
Director-General
European Semiconductor Industry Association (ESIA)
Tel: + 32 2 290 36 60 • Web: https://www.eusemiconductors.eu/

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the semiconductor industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies, the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as the most R&D-intensive sector by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.

Annex I

Examples of existing security standards from regional and global (public) domains

Global

- Internet Corporation for Assigned Names and Numbers (ICANN)
  Source: https://www.icann.org/
- International Electrotechnical Commission (IEC)
  Source: https://www.iec.ch/homepage
- Institute of Electrical and Electronics Engineers (IEEE)
  Source: https://www.ieee.org/
- International Organization for Standardization (ISO)
  Souce: https://www.iso.org/home.html
- International Telecommunication Union (ITU)
  Souce: https://www.itu.int/en/Pages/default.aspx
- International Civil Aviation Organization (ICAO)
  Souce: https://www.icao.int/Pages/default.aspx
- Society of Automotive Engineers (SAE) International
  Source: https://www.sae.org/
- International Society of Automation (ISA)
  Source: https://www.isa.org/
- Joint Electron Device Engineering Council (JEDEC)
  Source: https://www.jedec.org/

USA

- American National Standards Institute (ANSI)
  Source: https://www.ansi.org/
- National Institute of Standards and Technology (NIST)
  Source: https://www.nist.gov/

Europe

- European Committee for Standardization (CEN)
  Source: https://www.cen.eu/Pages/default.aspx
- European Committee for Electrotechnical Standardization (CENELEC)
  Source: https://www.cenelec.eu/

- European Telecommunications Standards Institute (ETSI)
  Source: https://www.etsi.org/

Other

- China Communications Standards Association (CCSA)
  Source: http://www.ccsa.org.cn/
- China Automotive Technology and Research Center (CATARC)
  Source: https://www.catarc.ac.cn/
- National Integrated Circuit Standardization Technical Committee (NICSTC)
- Telecommunication Terminal Industry Association (TAF)
  Source: http://www.taf.org.cn/

Examples of existing security standards from industry (private) domain

- **3GPP: 3rd Generation Partnership Project**

"*The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations* [and] *covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.*"[15]

- **5GPP: 5th generation Partnership Project**

- **AEC: Automotive Electronics Council**

"*The AEC Component Technical Committee is the standardization body for establishing standards for reliable, high quality electronic components.*"[16]

- **AIAG: Automotive Industry Action Group**

"*AIAG is a unique not-for-profit organization where companies in the mobility industries have worked collaboratively to drive down cost and complexity in the supply chain.*"[17]

[15] 3GPP. *About 3GPP: About 3GPP Home*. URL: https://www.3gpp.org/about-3gpp/about-3gpp (retrieved 19/08/2021)
[16] AECMain. URL: http://www.aecouncil.com/ (retrieved 07/10/2021)
[17] AIAG | Automotive Industry Action Group. *About AIAG*. URL: https://www.aiag.org/about (retrieved 07/10/2021)

- **ASA: Automotive SerDes Alliance**

"*The Automotive SerDes Alliance is a non-profit industry alliance of automotive technology providers collaborating to encourage standardizing of asymmetric* [serialiser / deserialiser, or SerDes] *technology*".[18]

- **AUTOSAR: AUTomotive Open System ARchitecture**

AUTOSAR "*is a worldwide development cooperation of car manufacturers, suppliers and other companies from the electronics, semiconductor and software industry. Since 2003 they have been working on the development and introduction of an open, standardized software architecture for the automotive industry.*"[19]

- **Bluetooth SIG: Bluetooth Special Interest Group**

The Bluetooth SIG is "*fostering member collaboration to create new and improved specifications,* [driving] *global Bluetooth interoperability through a world class product qualification program, and* [growing] *the Bluetooth brand by increasing the awareness, understanding, and adoption of Bluetooth technology.*"[20]

- **CCC: Car Connectivity Consortium**

"*The Car Connectivity Consortium® (CCC) is a cross-industry organization advancing technologies for smartphone-to-car connectivity solutions.*"[21]

- **CAR 2 CAR Communication Consortium**

"*In the CAR 2 CAR Communication Consortium, leading European and international vehicles manufacturers, equipment suppliers, engineering companies, road operators and research institutions join forces for saving lives by research and development of C-ITS solutions facilitating to overcome road accidents*".[22]

- **CharIN**

[18] ASA | Automotive SerDes Alliance. *About ASA*. URL: https://auto-serdes.org/about-us/ (retrieved 07/10/2021)
[19] AUTOSAR. *FAQ: What is AUTOSAR?*. URL: https://www.autosar.org/faq/ (retrieved 07/10/2021)
[20] Bluetooth. *Vision and Mission*, About Us. URL: https://www.bluetooth.com/about-us/vision/ (retrieved 08/10/2021)
[21] Car Connectivity Consortium. *About Us*. URL: https://global-carconnectivity.org/about/ (retrieved 07/10/2021)
[22] CAR 2 CAR Communication Consortium. *About Us*. URL: https://www.car-2-car.org/about-us/ (retrieved 19/08/2021)

"*Under the CharIN umbrella, cross-industry stakeholders like automakers, charging station manufacturers, component suppliers, energy providers, grid operators, and many others continue moving towards interoperable charging, where vehicles, chargers, and software systems work together and to make the user experience reliable, easy and smooth.*"[23]

- **Connectivity Standards Alliance: "matter" (smart home) project**

The Connectivity Standards Alliance (CSA, formerly Zigbee Alliance) "*is the foundation and future of the IoT. Established in 2002, [its] global membership collaborates to create and evolve universal open standards for the products transforming the way we live, work, and play.*"[24]

- **COVESA: Connected VEhicle Systems Alliance**

Formerly known as the GENIVI Alliance, COVESA "*is a global, member-driven alliance focused on the development of open standards and technologies that accelerate innovation for connected vehicle systems, resulting in a more diverse, sustainable and integrated mobility ecosystem.*"[25]

- **ECPE: European Center for Power Electronics**

ECPE was founded "*on the initiative of leading power electronics industries as an industry-driven Research Network to promote education, innovation, science, research and technology transfer in the area of Power Electronics in Europe.*"[26]

- **EMVCo: Payment eco-system**

"*EMVCo manages and evolves EMV Specifications and supporting testing programmes that help enable card-based payment products to work together seamlessly and securely worldwide.*"[27]

- **ESDA: Electronic System Design Alliance**

ESDA "*is a forum to address technical, marketing, economic and legislative issues affecting the entire industry. It acts as the central voice to communicate and promote the value of the semiconductor design industry as a vital component of the global electronics industry.*"[28]

---

[23] CharIN – Empowering the next level of e-mobility. URL: https://www.charin.global/ (retrieved 07/10/2021)
[24] Connectivity Standards Alliance. *About: Who We Are*. URL: https://zigbeealliance.org/about/ (retrieved 19/08/2021)
[25] COVESA. *About COVESA*, About. URL: https://covesa.global/about-covesa (retrieved 07/10/2021)
[26] ECPE. *Objectives & Mission*, network. URL: https://www.ecpe.org/network/objectives-mission/objectives/ (retrieved 08/10/2021)
[27] EMVCo. *About EMVCo: Overview*. URL: https://www.emvco.com/about/overview/ (retrieved 19/08/2021)
[28] SEMI. *Electronic System Design Alliance*, COMMUNITIES. URL: https://www.semi.org/en/communities/esda (retrieved 08/10/2021)

- **EUROSMART**

EUROSMART is a "*trade association in the field of Digital Security. Since 1995, our organisation has been advocating for strong and comprehensive approach to strengthen its cyber resilience. Eurosmart is the funding father of the first European ethical hacking group on hardware devices.*"[29]

[29] Eurosmart. *What We Do*, ABOUT US. URL: https://www.eurosmart.com/activities/ (retrieved 08/10/2021)

- **FIDO Alliance: Fast Identity Online**

"*The FIDO Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance promotes the development of, use of, and compliance with standards for authentication and device attestation.*"[30]

- **FiRa: Fine Ranging Consortium**

"*The FiRa Consortium is the organization dedicated to growing the [ultra-wideband] ecosystem, so new use cases for fine ranging capabilities can thrive.*"[31]

- **GCF: Global Certification Forum**

GCF "*is a non-profit, global membership driven organisation offering mobile and IoT certification programmes based on conformity to agreed standards.*"[32]

- **GlobalPlatform**

GlobalPlatform has developed the Security Evaluation Standard for IoT Platforms (SESIP) to fit with security development of layered security, and provides scalable security assurance of security foundations (encryption, secure initialisation, secure update, secure communications, secure storage, etc.). The evaluation standard is based on re-using evaluation results from already evaluated parts (called composition), and allows to capitalise on security certifications done by the semiconductor industry to provide assurance on the implementation of security functions of the end-products. SESIP has defined a consistent set of security functional requirements (SFRs) suited for IoT devices. With a clear and simple definition, it allows all stakeholders to rely on certified security functions provided by third parties, such as chip vendors.

- **GSMA: Global System for Mobile Communication**

"*The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.*"[33]

[30] FIDO Alliance. *THE ALLIANCE: Alliance Overview*. URL: https://fidoalliance.org/overview/ (retrieved 19/08/2021)
[31] FiRa Consortium. *ABOUT FIRA*. URL: https://www.firaconsortium.org/about/consortium (retrieved 07/10/2021)
[32] GCF. *About*. URL: https://www.globalcertificationforum.org/about.html (retrieved 08/10/2021)
[33] GSMA. *ABOUT: About GSMA*. URL: https://www.gsma.com/aboutus/ (retrieved 19/08/2021)

- **ICCEA: International Conference on Computer Engineering and Application**

ICCEA "*provides an enabling platform for innovative academics, engineers and industrial experts in the field of Computer Engineering and Application to exchange new ideas and present research results.*"[34]

- **IETF: Internet Engineering Task Force**

"*The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.*"[35]

- **ioXt**

"*The mission of the ioXt Alliance is to build confidence in Internet of Things products through multi-stakeholder, international, harmonized, and standardized security and privacy requirements, product compliance programs, and public transparency of those requirements and programs.*"[36]

- **JasPar: Japan Automotive Software Platform Architecture**

"*JASPAR was established to enable standardization of electronic control systems and software of in-vehicle networks, thereby allowing industry-wide common implementation, more efficient development, and increased reliability.*"[37]

- **MIPI Alliance: Mobile Industry Processor Interface Alliance**

MIPI Alliance is a "*collaborative global organization serving industries that develop mobile and mobile-influenced devices. The focus of the organization is to design and promote hardware and software interfaces that simplify the integration of components built into a device, from the antenna and modem to peripherals and the application processor.*"[38]

- **NEVC: New Energy Vehicle Technology Innovation Centre**

[34] 2021 2nd International Conference on Computer Engineering and Application (ICCEA 2021). URL: http://www.iccea2021.com/ (retrieved 07/10/2021)
[35] IETF | Internet Engineering Task Force. *ABOUT: Who we are*. URL: https://www.ietf.org/about/who/ (retrieved 19/08/2021)
[36] ioXt. *About ioXt: About Us*. URL: https://www.ioxtalliance.org/about-ioxt (retrieved 19/08/2021)
[37] JASPAR. *About us*, Introduction of JASPAR. URL: https://www.jaspar.jp/en/about_us (retrieved 07/10/2021)
[38] MIPI Alliance. *About Us: MIPI Overview*. URL: https://www.mipi.org/about-us (retrieved 07/10/2021)

- **NFC Forum: Near-Field Communication Forum**

The NFC Forum members "*share development, application, and marketing expertise to develop the best possible solutions for advancing the use of Near Field Communication (NFC) technology which enables the lives of consumers worldwide and advances members' business objectives.*"[39]

- **OASIS: Organization for Advancement of Structured Information Standard**

"*OASIS Open offers projects—including open source projects—a path to standardization and de jure approval for reference in international policy and procurement.*"[40]

- **OLA: Open Link Association**

- **OMA: Open Mobile Alliance**

The Open Mobile Alliance (OMA) is a standards body which develops open standards for the mobile phone industry.

- **OPC Foundation: Open Platform Communication**

"*OPC is the interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries.* […] *The OPC Foundation is responsible for the development and maintenance of this standard.*"[41]

- **OPEN Alliance: One-Pair Ether-Net Alliance**

The OPEN Alliance "*is a non-profit, open industry alliance of mainly automotive industry and technology providers collaborating to encourage wide scale adoption of Ethernet-based networks as the standard in automotive networking applications.*"[42]

- **PCI-SIG: Peripheral Component Interconnect Special Interest Group**

The PCI-SIG "*is an association of 800+ industry companies committed to advancing its non-proprietary peripheral component interconnect (PCI) technology*".[43]

[39] NFC Forum. *About Us*. URL: https://nfc-forum.org/about-us/ (retrieved 07/10/2021)
[40] OASIS Open. *About: Organization*. URL: https://www.oasis-open.org/org/ (retrieved 19/08/2021)
[41] OPC Foundation. *About: What is OPC?* URL: https://opcfoundation.org/about/what-is-opc/ (retrieved 19/08/2021)
[42] Open Alliance. *About OPEN Alliance*. URL: https://www.opensig.org/about/about-open/ (retrieved 07/10/2021)
[43] PCI-SIG. *Membership*. URL: https://pcisig.com/membership (retrieved 08/10/2021)

- **RAIN Alliance: RAdio frequency Identification Alliance**

The RAIN Alliance "*is a global alliance promoting the universal adoption of* [ultra-high frequency radio frequency identification] *technology in a way similar to other wireless technology organizations*".[44]

- **TCG: Trusted Computing Group**

"*The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.*"[45]

- **Thread Group**

Thread Group "*is a low-power wireless mesh networking protocol based on the universally supported Internet Protocol (IP), and built using open and proven standards.*"[46]

- **USB-IF: Universal Serial Bus Implementers Forum**

The USB-IF "*is a non-profit corporation founded by the group of companies that developed the Universal Serial Bus specification.*"[47]

- **USI: Universal Scientific Industrial**

"*USI provides design, miniaturization, material sourcing, manufacturing, logistics, and after services of electronic devices/modules for brand owners.*"[48]

- **UWB Alliance: Ultra-Wideband Alliance**

The UWB Alliance works "*internationally to facilitate intelligent spectrum coexistence for next generation UWB-enabled multi-radio wearable and smartphone devices whilst minimizing unwanted interference.*"[49]

[44] RAIN RFID. *What is RAIN?*, RAIN TECHNOLOGY. URL: https://rainrfid.org/about-rain/what-is-rain/ (retrieved 08/10/2021)
[45] Trusted Computing Group. *About: About TCG*. URL: https://trustedcomputinggroup.org/about/ (retrieved 19/08/2021)
[46] Thread Group. *Thread Benefits*, WHAT IS THREAD. URL: https://www.threadgroup.org/What-is-Thread/Thread-Benefits (retrieved 08/10/2021)
[47] USB-IF. *About USB-IF*. URL: https://www.usb.org/about (retrieved 08/10/2021)
[48] USI. URL: https://www.usiglobal.com/en (retrieved 07/10/2021)
[49] UWB Alliance. URL: https://uwballiance.org/ (retrieved 07/10/2021)

- **VESA: Video Electronics Standards Association**

"*VESA supports and sets industry-wide interface standards for the PC, workstation, and consumer electronics industries* [providing] *a forum to develop, promote and support open standards for the display industry.*"[50]

- **W3C: World Wide Web Consortium**

"The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards."[51]

- **Wi-Fi Alliance**

"*Wi-Fi Alliance drives global Wi-Fi adoption and evolution through thought leadership, spectrum advocacy, and industry-wide collaboration* [including] *the development of innovative technologies, requirements, and test programs that help ensure Wi-Fi provides users the interoperability, security, and reliability they have come to expect.*"[52]

- **WLA: Wireless Lan Association**

"*The WLA is professional association for the WLAN community, and our mission is to define industry best practices and quality assurance in the delivery of Wi-Fi networks.*"[53]

- **WPC: Wireless Power Consortium**

The "*Wireless Power Consortium is an open, collaborative standards development group of more than 400 member companies from around the globe.*"[54]

[50] VESA. *About VESA*. URL: https://vesa.org/about-vesa/ (retrieved 08/10/2021)
[51] World Wide Web Consortium (W3C). *About W3C*. URL: https://www.w3.org/Consortium/ (retrieved 19/08/2021)
[52] Wi-Fi Alliance. *Who We Are*. URL: https://www.wi-fi.org/who-we-are (retrieved 08/10/2021)
[53] Wireless Lan Association. URL: https://wlanassociation.org/ (retrieved 08/10/2021)
[54] Wireless Power Consortium. *About WPC: About*. URL: https://www.wirelesspowerconsortium.com/about/about-wpc (retrieved 19/08/2021)

Annex II

List of standard domains

Market / transversal	Cluster	Description	SDOs
Automotive	Digital key, positioning	Ultra-wideband radio technology for car key applications and car positioning	CCC, ICCEA
Automotive	Automotive software architecture	Automotive software architectures for todays and future car applications	AUTOSAR, COVESA, JasPar
Automotive	In-vehicle networking	High-speed, longer distance in-vehicle communication & networking	IEEE 802.1, IEEE 802.3, IEEE 1722, ASA, OPEN Alliance, MIPI Alliance
Automotive	ADAS quality standards	Standards to determine the suitability and safety of ADAS functions	CATARC, IEC TC 22, UL 4600, IEEE 2851, SAE International
Automotive	Car electrification	Standards for electric vehicle charging, etc.	CharIN e.V., IEC TC 69, IEC TC 23 (IEC 62196)
Automotive, industrial (IoT)	Functional safety	Functional safety standard for automotive and industrial applications	ISO TC 22, IEC TC 65
Automotive, Quality	Automotive quality	Standards for various product quality metrics applicable to all semiconductor products in automotive application	AEC, AIAG, SAE International, NEVC
Consumer IoT	Ultra-wideband / fine ranging	Ultra-wideband radio technology to accurately and securely measure distances and determine locations	IEEE 802.15, FiRa Consortium, UWB Alliance

Consumer IoT	Low-power networking	Low power short range radio technologies for personal area networks (PAN) and meshed local area networks (LAN) networks	CSA, Thread Group, Bluetooth SIG, SPARKlink
Consumer IoT	Consumer IoT application	Interoperability for consumer IoT devices and accompanying cloud services	CSA, OLA
Consumer IoT	Wireless charging	Various standards for and applications of wireless charging of various types of devices, from < 1W to > 100W	WPC (Qi, Ki), NFC Forum, USI
Consumer IoT, industrial IoT	Wireless LAN	Wireless LAN	IEEE 802.11, Wi-Fi Alliance, WLA
General	High-speed serial bus technologies	High-speed interconnect standards for on-board and short wired applications	PCI-SIG, USB-IF, VESA
General	Low-speed serial interconnect	Lower speed interconnect standards for on-board and short wired applications	MIPI I3C, MIPI CSI-2, MIPI DSI-2
Industrial IoT	Industrial IoT security	System approach to security in industrial environments including components	IEC TC65, ISA, etc.
Quality	Product quality issues general	Standards for various product quality metrics applicable to all semiconductor products	IEC TC47, JEDEC, ESDA, NICSTC
Security	eSIM	Electronic authentication and security technology to replace mobile network operator subscriber identity modules (SIM) in cellular networks	GSMA, ETSI TC SCP, TAF, CCSA
Security	Near-field communication (NFC)	NFC technology + applications	NFC Forum, ISO/IEC JTC1/SC6, GCF, CCC

Security	Radio frequency identification (RF-ID)	Longer distance radio-based identification of tags	ISO TC 23/SC 19, ISO/IEC JTC1/SC31, ISO/IEC JTC1/SC17, RAIN Alliance
Security	Cybersecurity certification	Methods to evaluate the security qualities of a product implementation versus its security requirements	GlobalPlatform, ETSI TC Cyber, ISO/IEC JTC1/SC27, CEN/CLC/JTC13, EUROSMART