EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION

CLC/TC 47X Business Plan

CLC/TC 47X: SEMICONDUCTOR DEVICES AND TRUSTED CHIPS
CLC/TC 47X : SEMICONDUCTEURS ET CONFIANCE DANS LE DEVELOPPEMENT DES PUCES ELECTRONIQUES

TC or SC title: Semiconductors and trusted chips

A Background

A.1 Date of establishment of the TC and a brief historical background

TC47X is continuation to the European Chip Act launch in 2022 and to integrate the European regulation published in September 2023. The European Innovation Council and Smes Executive Agency (EISMEA) granted the call for proposal " Standards for the certification of chips in terms of security, authenticity, reliability" – dated June 2022 – to DKE. This funded EU project, called "Trusted Chips", is the so-called pre-standardization activity. The main outcome of this phase is a gap analysis and potential roadmap which will set common European requirements and deliver guidelines across sectors. Moreover, it should support the European exchange and cooperation within the semiconductor field which fosters innovation across all sectors and ensures secure and reliable chips.
The TC47X should make reuse where applicable of the outcome from the European funded project "Trusted Chips" project.
This initiative is the implementation of possible European standards on "Semiconductor devices and trusted chips".

A.2 Current scope and working groups

The TC47X 'Semiconductor device and trusted chips' fostering the development and use of trustworthy semiconductor devices for microelectronics and embedded systems in the European Union. TC47X aims to establish a common framework in accordance with environmentally good practices for the design, manufacture, and use of semiconductor devices and trusted chips, with a focus on improving security, privacy, and resilience against cyber-attacks. The TC47X is part of a broader effort by the European Union to improve cybersecurity and protect critical infrastructure against cyber threats.

The TC47X will:

- Provide the necessary infrastructure to the European industry and experts to discuss the related future standardization activities.
- Adopt the relevant standards developed by IEC/TC47 and its subcommittees, as per the provisions of the Frankfurt Agreement.
- Address the standardization gaps identified by TC47X and liaisons partnersor a future European standardization roadmap.
- Develop European standards in response to the relevant standardization requests prepared by the European Commission (e.g. in support of the European Chips Act), particularly in terms of chips security, traceability and trustworthiness...
- Seeks to establish a compliance process to develop chips safely, enabling consumers and businesses to identify and choose products that meet scalable security standards.

B Business Environment

B.1 General

The semiconductor market is at the center of geopolitical and economic tensions and is made up of a multitude of product submarkets.
Standards can improve the link between the different market players and throughout the supply chain by offering a horizontal view because chips are present in all digital products.

Due to the worldwide chip shortage over the past years, it has become urgent for Europe to secure and strengthen its chip manufacturing value chain and European Commission proposes semiconductor legislative package to address shortages and strengthen Europe's technological lead.

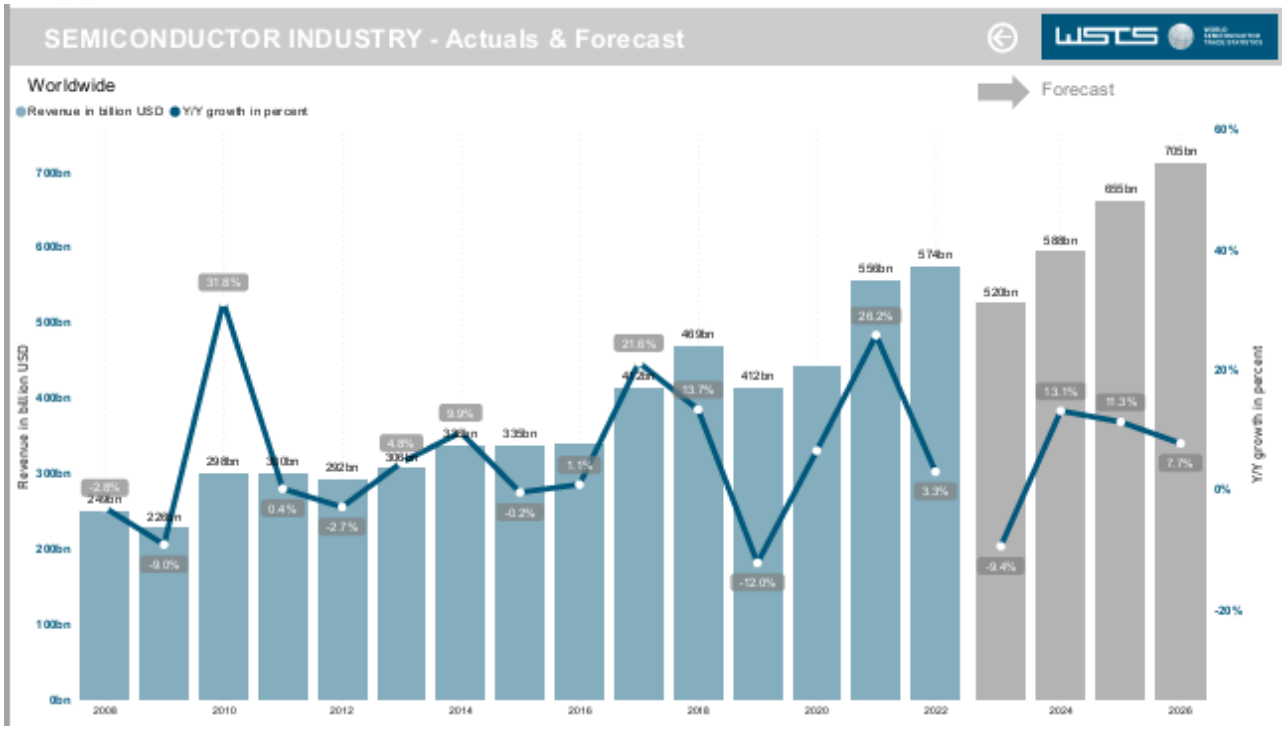
The European strategy and regulations (European Chips Act) concerning semiconductors have resulted in the prioritization of European standardization in this field in the annual work program of the European Union (AUWP).
This is reflected in the European Union's Annual Work Program 2022, which makes the topic of semiconductors a priority for European standardization. The objective is to provide standards to support the certification of chips to ensure that they are safe, and authentic..

B.2 Market demand

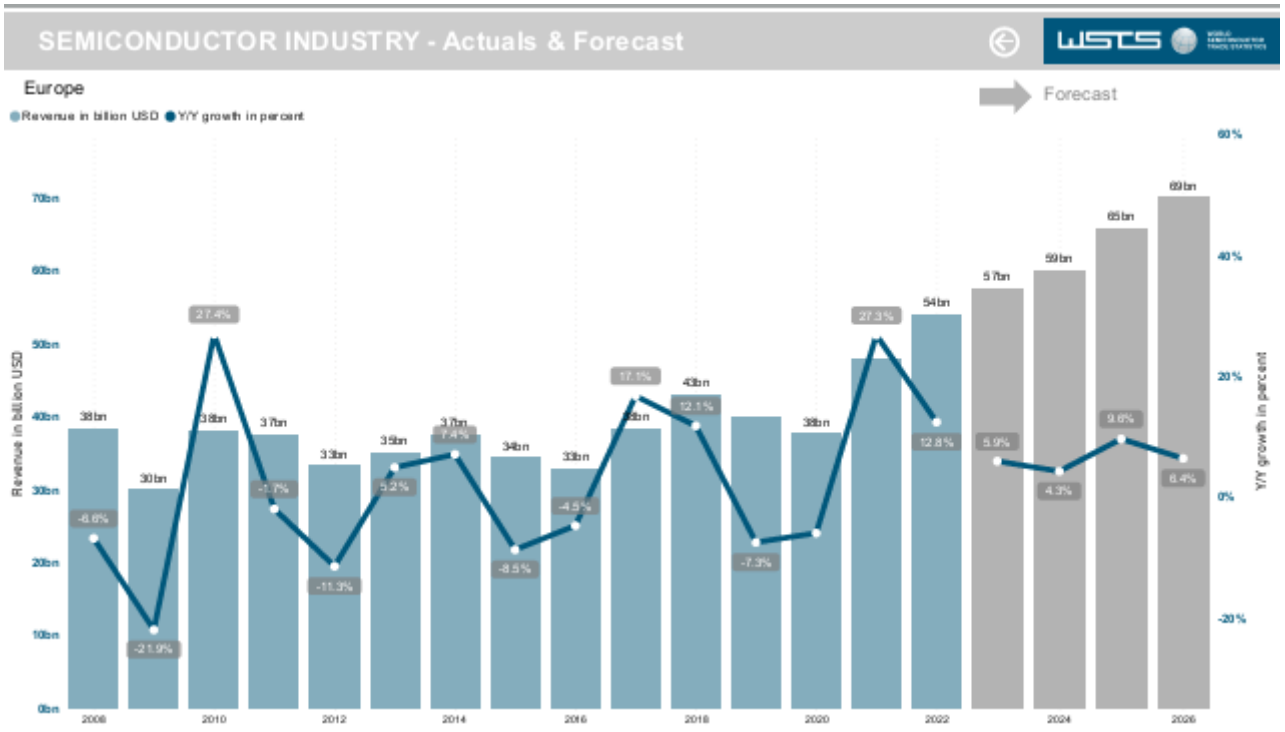
The (European) semiconductor industry needs:

- stable standards as the basis of the product portfolio
- standards to cover the fundament provided by chips to support cybersecurity of "connected objects", wired and wireless applications, security technology, smart and wired interfaces, computer applications and software.
- Widely accepted industry standards and uniform regulatory requirements to ensure that global markets do not fragment into “regional” versions.
- Security functions that are the kernel of concerns for the European semiconductor industry, particularly cybersecurity.
- Innovative standards covering new emerging subjects.
- Link between existing international industrial specifications and European standardization.

According to WSTS Forecast from November 2023 – the world semiconductor industry expects a growth in the forecasted period until 2026 – reaching >700bn US$ revenue.



According to WSTS Forecast from November 2023 – the European semiconductor industry expects a growth in the forecasted period until 2026 – reaching >70bn US$ revenue.



B.3 Trends in technology

The technology trend for chip security is focused on developing new and innovative approaches to enhance the security and trustworthiness of chips. Some of the key technology trends in chip security include:

1. Hardware-based security: Hardware-based security is becoming increasingly important.This approach involves incorporating security features directly into the hardware design of chips, making them more resistant to attacks and tampering.

2. Secure enclaves: Secure enclaves are isolated areas within a chip that are designed to protect sensitive data and code execution. This approach is becoming more popular in the development of chips.

3. Destructive or not destructive attacks such as: Side-channel attacks are a type of attack that exploits weaknesses in the physical properties of chips, such as but not limited to on timing, power consumption, and electromagnetic emissions. Mitigating these attacks is becoming increasingly important in chip security.

4. Formal verification: Formal verification is a rigorous approach to verifying the correctness of chip designs. This approach involves using mathematical methods providing an assurance level on the quality of the product. Open-source hardware: Open-source hardware is becoming more popular in chip security. This approach involves making the hardware design of chips open-source, allowing for greater transparency and collaboration in the development of secure and trustworthy chips.

Overall, the technology trend for chip security is focused on developing new and innovative approaches to enhance the security and trustworthiness of chips. These approaches are aimed at addressing the growing concern over the security of electronic devices and systems and are expected to have a significant impact on the development of secure and trustworthy chips in the future.

B.4 Market trends:

The market for Security, including but not limited to cybersecurity, safety and data confidentiality in Europe is expected to grow significantly in the coming years. The European Union (EU) has identified cybersecurity as a key priority area and has launched several initiatives to strengthen security in Europe such as the “Trusted Chips” project to which TC47X links to master the end-to-end development and use. The EU Security Strategy, for example, aims to enhance the EU’s resilience to security threats and promote a secure and trustworthy digital environment.

The EU Cyber Resilience Act (CRA) will ensure that digital products, such as wireless and wired products and software, are more secure for consumers across the EU: in addition to increasing the responsibility of manufacturers by obliging them to provide security support, software update and market surveillance to address identified vulnerabilities it will enable consumers to have sufficient information about the cybersecurity of the products they buy and use.

The Security market in Europe is highly competitive, with many players offering a wide range of products and services to meet the diverse needs of various industries.

The EU’s cybersecurity initiatives and regulations are expected to continue to drive growth and innovation in the European cybersecurity market.

The focus markets in Europe relevant for the “semiconductors devices and trusted chips” standardization work needs to be identified by TC47X and the EU funded project “Trusted Chips”.

B.5 Ecological environment

CLC/ TC 47X is mirroring the IEC TC 47 therefore the following principle of IEC TC 47 will be applied.

Note: The next part refers to the IEC TC 47 document

"TC47 develops international standards, guidelines and technical reports that can help to guide the manufacturing process and evaluate the performance and reliability of energy harvesting devices. These energy harvesting devices play an important role in the industry and these actions can contribute to affordable and clean energy, decent work & economic growth, and industry, innovation & infrastructure.

The development of efficient semiconductor devices and reliable quality and reliability assessment for them support "responsible consumption & production" of semiconductor industry. These kinds of technical actions help a lot in supporting a sustainable cities and communities. TC47 includes standards for new wide bandgap semiconductors - whose use creates more efficient power supplies and are fundamental for enabling Electrification, Renewable Energy sources, and the next generation Grid.

In the process of discussing and developing standards in accordance with the principles of IEC's standard development, participating all national committees cooperate and strive with each other to achieve Sustainable Development Goals."

We are working on TC 47X according to the European regulation 2023/1781 which is requested in the Chips Act.

TC is expected to receive EC mandates to influence work and to develop potential harmonized standards.

B.6 Involvement of societal stakeholders

The TC47X is open to all interested parties. Due to the nature of the planned work of the committee for standardisation on business-to-business interface, it will be difficult to get societal stakeholders involved. However, we intend to involve Annex III organisation if they have an interest. Any proposal to involve societal stakeholders is welcome.

B.7 Involvement of SMEs

The TC47X will involve SMEs to cover a very important area of the semiconductor supply chain and users. A major part of the IoT market, especially markets like medical, industrial and consumer applications, are SMEs. These SMEs could be directly involved into semiconductors business, but the majority is served via distribution channels. An example from Germany for the medical market shows the significant involvement of SMEs. About 90% of the companies are SMEs (defined by number of employees <250). Therefore, the SME involvement is very important. However, it needs to be clarified if this can be done via European SME organization and/or via European distribution companies.

C System approach aspects

TC47X will differentiate between subcomponents and end products. TC47x will avoid risk of adding unnecessary complexity by using a "one-size-fits-all" approach for trust including security concerns derived from the nature of different technologies:

- Hardware at the subcomponent level,
- Product platforms made of hardware and firmware subcomponents.
- Across those product categories, products will have different risk levels, and security conformance concerns ranging from the method to demonstrate conformance with the essential cybersecurity requirements, vulnerability management, product maintenance, etc.

The following points will not be addressed at first but may be considered in the future.

- Software-only products as subcomponents
- Combined hardware – software such as full system
- Software-only products as applications or as-a-service

D Objectives and strategies (3 to 5 years)

The stakes are:

- Identify the focus markets in Europe relevant for the “semiconductors devices and trusted chips” standardisation work.
- Identify the existing standards and alliances covering our objectives; Evaluate and fill the gaps (if necessary) for “semiconductors devices and trusted chips” standardization work. Make use of the outcome form the EU funded “Trusted Chips” project.
- Identify with the stakeholders, especially SMEs / Distribution channels the gaps of “trusted electronics.”
- List all the existing Standards and Industrial Alliances and European programs such “Cybersecurity Resilient Act”, addressing this trust chain and establish liaison when required to make use of existing standards and identify gaps where applicable.
- Securing and strengthening the chip manufacturing value chain. Not only cybersecurity, but also other attacks such as but not limited to counterfeit chips, safety, data confidentiality and data corruption.
- Aligned with “Trusted Chips” EU funded project (lead by DKE), define a trust chain from the manufacturing up to the chip integration into board or module level into a final device
    - including firmware implementation,
    - (cyber) security and device integration into the board or module level to end product done by third-party, relevant validation processes.
- Support Europe's competitiveness and resilience
- Contribute to the digital and ecological transitions.
- Ensuring Interoperability (e.g. by use of standards which is very important for SME)
- Permit trust in chips to be carried through more complex ownership change.
- Identify stakeholders and address the need to transfer security and trust responsibilities. As an example, the “security key” transmitted by Silicon provider to the end user via operating system vendors.

E Action plan

A listing of relevant existing documents at the international, regional and national levels.
Any known relevant documents (such as standards and regulations) shall be listed, regardless of their source, and should be accompanied by an indication of their significance.

- ISO/IEC 27000 series for chips cybersecurity aspects: Information security management systems
- ISO 15408 Evaluation criteria for IT Security
- ETSI 303 645 (security requirements for consumer Iot)
- Common Criteria (incl. CSA EUCC security certification)
- SESIP (security evaluation of IoT platforms e.g. MCU for basic, substantial level) (EN17927)
- JC13 Working Group 9
- Etc.

High level implementation program:

- Define the scope of the TC47X aligned with the “Trusted Chips” EU funded project.
- Take regular inputs, including the roadmap, and be influenced by “Trusted Chips” EU funded project.

- Identify relevant EU regulation frameworks to be included in the TC47X process, for example: CRA (Cyber Resilience Act)
- Identify the gap between selected regulations and cutting-edge technology.
- Initiate research on open topics
- Identify relevant international standards, SSOs and Industry Alliances to be included in the TC47X process, for example: other ISO, IEC, ETSI, SESIP …etc…
- Identify the gap between selected international standards, SSOs & Industry Alliances, and state-of-the-art technology.
- Identify and manage potential liaisons with these organizations.
- Initiate new working groups to fill gaps if necessary.
- Define the overall TC47X implementation strategy considering upper points to achieve the defined and agreed objectives.
- Application to global strategy in relevant markets to define the markets we need to focus on such as IoT, Transportation/Automotive, Health Care/Medical
- Consolidate all different inputs from all relevant markets for final deliveries.

F Useful links to CENELEC web site

TC 47X dashboard giving access to Membership, TC/SC Officers, Scope, Liaisons, WG/MT/PT structure,
Publications issued and Work and Maintenance Programmes.

TC47X website:
CENELEC Technical Bodies - CLC/TC 47X (cencenelec.eu)