Go IT! (GOIT)

Participant number	Participant organization name	Participant short name	Country
1 (coordinator)	Free Silicon Foundation (I)	FSI	Italy
2	Sorbonne University, LIP6	SU	France
3	CNRS	CNRS	France
4	Institute of Electronics and Computer Science	EDI	Latvia
5	Spanish National Research Council	CSIC	Spain
6	Association pour le developpement des recherches aupres des universites de l'academie de Grenoble	CMP	France
7	FibraServi	FS	Belgium

Short Summary. Europe's IT hardware development is constantly challenged by outrageously expensive development tools, legal constraints like NDAs or patents, lock-in threats, dependency from external vendors or supply chains and foreign political events. Europe's digital infrastructure (from consumer to critical appliances) is heavily relying on foreign closed-source chips which are literally black-boxes which may (and have been proven to) contain malicious features. This situation makes the hardware development expensive and inefficient, and undermines the very principles of sovereignty, resilience and re-usability. Open-source silicon chips, which are open in their entirety, i.e. down to the physical layout, carry the potential of catapulting Europe into a renaissance of digital technology. Several challenges are on the way, many of which will require the participation of the stakeholders (from the fertile ground made of "nerdy" hobbyists and makers who are the early protagonists of the scene, all the way up to large enterprises), as well as the participation of policymakers and regulatory bodies. The road ahead is steep, but rich of rewards. Therefore we loudly say: Go IT!

1 Excellence

1.1 Objectives

Introduction

Open-source hardware (OSH) is in its infancy and its evolution is influenced by the interests of the different players. In the 2015-2019 time period it was mainly developed by the makers/hacker scene and by a few small academic attempts. In the last few years, major companies like Google have exerted strong influence for example by gathering control on a silicon foundry (Skywater) and by opening for the first time part of a CMOS Process Design Kit (PDK). The interests of Europe are digital sovereignly, resilience and sustainability -interests which are not necessarily aligned with foreign major actors. For imagining the evolution of open-source hardware in the coming decade, we may look back at the evolution of open-source software and of GNU/Linux in particular which is by-the-way celebrating its 30st anniversary this year. On August 1991 Linus Torvalds announced the new operating system with the famous words: "*I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. […] Any suggestions are welcome, but I won't promise I'll implement them :-)*". In the late 90's open-source was no more just a "nerd" activity but it was perceived as a threat by big companies: in 2001, for example, the CEO of Microsoft Steve Ballmer said even that "Linux is a cancer". A few years later finally, the opposite became true. In the late 2010's, in fact, big companies embraced the open-source model. IBM for example

bought RedHat for $34 billion in 2018, Microsoft acquired GitHub for $7.5 billion in 2018 and the Mozilla Foundation revenues raised to $562 million in 2017.
A key-learning from the history of the development of open-source *software*, is that there is a very productive and essential underlying "humus" of *developers, hackers* (for a definition of the term see https://www.gnu.org/philosophy/rms-hack.html) and *enthusiasts* who see in the open-source movement (and often in the attached philosophical values represented by the Free Software Foundation) a means to realize their motivations and ideals. The belief of contributing to something useful to others or to a bigger cause, the chance of getting recognition from the community for having written good software, etc. are essential motivators for keeping this "humus" alive (Ke and Zhang 2010). Policy makers have the power of fostering this community (as exemplified later in this manuscript) or damaging it though unsuitable decisions. It is essential therefore that the community of developers, hackers and enthusiasts is properly represented.
The open-source domain is by now no longer an unknown territory. Ambitious players have understood its potential impact and have learned how to influence its development and take advantage from it. In the eyes of the original nerd/hacker community, one of the most worrying events over the last years is the war on licences perpetuated by large disinformation campaigns against the General Public Licence, once the most used licence in open-source projects and the licence of the Linux kernel, in favour of temporarily-open licences. For more details consult one of the several resources available online, such as the statement of the founder of the GNU project (Stallman, Richard 2019), the ban of Google against the Affero-GPL (APGL) (Google 2021) or the position of the founder of Owncloud and then of Nextcloud on licences (Karlitschek, Frank 2018).
By not representing any specific company but the economic and societal interests of the general public as a whole, and by carefully avoiding any potential conflict-of-interest, we will attempt to steer the evolution of open-hardware in a sustainable direction.
There are however several *obstacles* on the way and we will certainly not manage to steer the open-source hardware evolution alone. Instead, we foresee that it will be necessary to steer public funding in novel directions, funding which well exceeds the budget of the current proposal. It will be necessary, for example, to grow the cultural and educational ecosystem by letting European (re-)flourishing in the silicon engineering domain. This will require creating specific public calls for funding and coordinating the different institutes across different countries. It will require bringing together research and markets, universities and enterprises. It will require identifying and promoting the most suitable "rules of the game" for making open-source a sustainable reality, rather than an indirect public funding of corporate interests (like publicly-funded open-source projects being cloned by companies and then discontinued in the open-source domain).
For using a parallelism (which is partially inappropriate given the different political structure), we felt while writing this application like a Darpa manager without a portfolio: we do not have a giant budget to invest in a short time in a particular direction for implementing a particular roadmap, but we can draft a roadmap that some other funding entities will have to financially support.

Short summary of objectives

In a few words, this proposal will strive to reach all relevant key players and stakeholders, to identify all possible obstacles to open-source hardware development, formulate solutions, and feedback inputs to those with the power of influence (policy makers, managers, etc.) therefore supporting them to coordinate the evolution of open-source in Europe.
Further, we will coordinate and support the community of programmers and developers directly, by continuing to organize get-together events (like the Free Silicon Conference), by overcoming critical obstacles (like the availability and compatibility of PDKs and design tools), and by creating the prerequisites to grow in a sustainable manner (re-usability, licences, etc). In all these activities, dissemination and advertisement on different levels will play a crucial role.

More specifically, we have identified the objectives summarized below:
* **Study and support.** Having put together a consortium which owns deep technical understanding on all levels of hardware design (from high-level down to physical synthesis), and which is directly involved in leading open-source hardware projects (see section 3.2), we have the capability of best understanding the on-going efforts of the open-source hardware communities, their struggles, and their needs. We will do everything possible to communicate what is relevant in this context to the decision makers and to those with capacity of action.

* **Direct technical coordination.** We will continue and grow the coordination action that we have started over the previous years by organizing get-together events, like the past Free Silicon Conference (see https://wiki.f-si.org/index.php/FSiC2019). These events are of utmost importance because the open-source community is typically loose and the occasions for developers to meet each others in person are rare even if extremely useful.
* **University coordination.** We will actively reach out all relevant universities by offering talks, workshops and schooling events. We will contact the key local and regional decision makers (institute heads, local politicians, etc.) such as to promote and facilitate the creation of an international network of academics which understand the same language and which work towards the same goals.
* **Maturity, interoperability, availability of tools and components.** We will oversee technical developments (novel design automation tools, novel IP blocks, etc.) and facilitate the compatibility/interoperability between them and their availability to the community. This will require compiling and testing the tools, facilitating the creation of shared software interfaces (APIs, shared libraries, etc.), and facilitating the communication between the involved programmers. We will further package the available software and hardware libraries in the major software package repositories used by the open-source community, like on “aptitude” (“apt-get”) in Debian and advertise them on mainstream knowledge platforms like Wikipedia.
* **Open Process Design Kit (PDK).** We will work toward solving one particular and already well-known obstacle for open-source development: the release of an open-source Process Design Kit by a major CMOS foundry. This is an action which probably will require a significant amount of negotiations and a commensurate budget: we will do here everything possible to facilitate the process by providing technical advice and by connecting the relevant people.
Since the opening of a PDK will foreseeably not occur by the end of this project, we will facilitate the distribution of PDKs which are still protected by NDAs, but which are at least compatible with open-source design tools and non-proprietary standards.
* **IT security through open-hardware.** We will promote the concept of hardware-security by openness, and we will put in contact the relevant players to create a pilot demonstrator of the open-hardware security approach. This includes motivating the community of developers (of EDA and of hardware libraries) to work towards concrete demonstrators, as well as existing entities which may on the long run become auditing authorities such as the “TÜV Verband” in Germany (Fliehe, Marc 2021).
We will further discuss within our existing network (including SMEs, academic groups and independent developers), for elaborating a strategy and a series of recommendations to the policy makers to influence the growth of the “security by openness” approach. These may include recommending legal means, such as mandating the use of specific certifications, for example, for critical infrastructure.
* **Sustainability, re-usability, hardware licence.** We will work to disseminate the best available software tools, the best hardware projects, and the general philosophy and potential of the open-source world. We will listen to the concerns that enterprises may have when approaching the open-hardware domain, and provide and disseminate answers (e.g. by maintaining an online FAQ page) of legal nature with the help of external lawyers. We will participate to conferences (beyond those we organize ourselves) with stands and talks. We will reach out on social media and mailing-lists, and we will advertise on technical newspapers and newsletters.
We will further finalize and publish a licence which not only is suitable to protect silicon chips (which are unfortunately not covered by copyright law causing mainstream licences to be ineffective), but which will also guarantee the re-usability of published work.
* **Certifications and standards.**
Certifications and standards are not only ways to facilitate the interoperability of software tools or components, but they are also a means to exert political and legislative influence on the evolution of the hardware. In addition, we foresee that open-hardware will dramatically *simplify* the certification procedure at least in particular cases such as those related to security and safety (critical infrastructure, car manufacturing, etc.). It is worth noting the proliferation of open-source machine learning solutions to conduct reverse engineering and to help to impose the principle of security-by-default along the entire stack of computing systems, e.g. (Botero, Ulbert 2021)). Certification requires capabilities to assess functional models, technical specifications and end-product implementation. When open hardware promotes interoperability and portability, it could ease audit and certification procedures. However, replicability is not easy to be fulfilled during certification of OSH (EC 2021). The formal aspects of standardization and the requirements imposed

by certification bodies can help to overcome some of the limitations related to replicability. On this basis, we will contribute by providing technical inputs, consultation, or direct participation whenever possible, to the creation of certifications by the relevant offices and standards by the relevant key-players.

1.2 Coordination and support measures and methodology

Preliminary considerations

Before entering into the details of the proposal, we would like to make a few considerations and define the term “open-source hardware”. This term, in fact, is used with very different meanings incompatible with each-others. In the general context, as defined for example by the “CERN Open Hardware Licence, OHLv2, the term “open-hardware’ may refer to “any device, component, work or physical object” and it may refer therefore also to mechanical part like a bicycle. This meaning clearly does not apply here. Still, even when limited to the context of *electrical engineering* the term “open-hardware” has been used heterogeneously. For example, the well-known Arduino platform is advertised as “open-hardware” or as “open-source electronics” despite the fact that the openness of the hardware design is *limited* to the printed circuit board, and does not affect at all the inner workings of its components like the microcontroller. As another example, even within the silicon chip or microprocessor community, the term “open-source hardware” is often used improperly: several academic groups, in fact, market their microprocessors as “open-source” even if *only the high-level language* (i.e. a minimal portion of the design) is published in the open-source domain. We will therefore propose a more complete definition:

Definition (open-source hardware). In the present proposal we will define the term “open-source hardware” in its widest possible meaning (within the present context): when referring to an electrical device, and in particular to a silicon chip like a microprocessor, we will mean a device which is open-source in its *entirety*, from the high-level description language, *down to the physical synthesis and the layout*. In other words, it must be possible (at least in principle) for an End User to understand the high-level design, compile the full design down to the layout which contains all transistors, and compare the result with its physical implementation (the chip). However, using the present definition, open-source hardware cannot exist without open-source electronic design automation (EDA) tools:

Open-source *hardware* requires open-source *software*; autonomy from EDA vendors. The Non Disclosure Agreements or the Licence Agreements of major EDA vendors do not allow the publication of any hardware design produced with their tools, therefore *preventing alone the existence of open-source hardware*.
In addition, the major EDA vendors often pursue a non-transparent pricing tactics where the full licence cost is too expensive for most SMEs which therefore must rely on various discounts negotiated with the vendor. This mechanism makes the growth of SMEs particularly vulnerable, and it is therefore desirable to offer to SMEs alternative EDA tools at an affordable price. Furthermore, the major EDA vendors are located outside of the EU and are vulnerable to sudden changes in international policies and exacerbation of export regulations. From within our network we have learned that at least one large European silicon design company has commissioned a risk assessment about the consequences of further restrictions which may affect for example EDA software licences. The tensions between US and China, which led for example to the “Huawei ban” over android, are an example of the risks that the domestic economy faces.
Open-source EDA tools are clearly an excellent candidate solution. Moreover, unless a radical change in the policy of the major EDA vendors occurs (*which we consider utmost unlikely*), the open-source EDA path will probably remain a *necessary* condition for the development of open-source hardware. This shows that *the world of “open-source hardware” and the world of “open-source software” are inevitably and intimately connected.*

Hardware security requires open-source. In the *software* domain there are two mainstream approaches to security: the first relies on proprietary software and the responsibility of the firm which produces the software to fix promptly all vulnerabilities and to distribute the corresponding patches, while the second consists of the open-source approach where the source code is equally (in principle) understandable by all users of the software.

The first approach is for example the one of Microsoft. Several entities, including public schools or public administration offices, adopt this approach because they can fully outsource the problem of security and blame an external company when something goes wrong. Thanks to leaked material, however, it is well known that the policy of release of software patches of foreign software companies endangers the domestic interests. Foreign nation states may not only receive a bug fix well in advance than Europe, but they will be handed a means to exploit the vulnerability wherever it has not been patched yet. This approach is clearly incompatible with with *Europe's sovereignty goals.*

Open-source in software and hardware are different but similar. In case a vulnerability is discovered, software and hardware behave in fundamentally different ways: While a software issue can be easily fixed by releasing a patch, a vulnerability found in hardware may require in the most pessimistic scenario an expensive replacement of the entire affected electronic chip/board. One may argue therefore that open-source hardware does not represent an economically viable way. On the other hand, reverse engineering of silicon chips is possible (despite tedious and expensive) (Tarnovsky 2010), therefore professional attackers will always remain in the position of discovering vulnerabilities which will remain hidden to the general public. Consider for example a bug in an electronic identification card which every citizen carries with him: we would argue that it is preferable that the discovery of a vulnerability was public, rather than in the hands of a few people with possible malicious intentions. In fact, the government would have the time to implement proper measures (like disabling all activities related with the affected chip), and work towards a solution rather than suffering unnoticeable and hard-to-prove glitches in the administrative system.

Unfortunately, due to the yet-negligible availability of open-source hardware, the mainstream approach so far in the hardware context (forced also by the lack of alternatives) has been to achieve "*security by obscurity*". This brought among others the birth of specialized silicon design companies whose task is to add extra obfuscating mechanisms in the physical design of a silicon chip (like adding extra transistors without a real function, or complicating a certain implementation of a function).

As highlighted also by multiple speakers at the Free Silicon Conference 2019 (FSiC 2019), it is necessary that the design of silicon chips is open in its entirety: Only in this way the end-user, or eventually an auditing company, will be able to understand the design of a given chip, reproduce its design entirely, and compare it with the physical implementation which can be imaged with either invasive or non-invasive technologies (PSI 2017).

Coordinating the open-source community for facilitating the proliferation of open-source chips is therefore equivalent to facilitate the proliferation of verifiable and therefore trustful hardware.

Description and explanation of coordination and support measures, and their overall methodology

We present this section in the same order as the list of objectives presented above.

*** Direct technical coordination.** The open-source domain is -roughly speaking- a space with *few rules and little coordination*. Open-source projects are started, forked, abandoned, merged or matured at an incredible speed. The rapid evolution of open-source is one of its strengths, and one of the reasons of its fast advancement. On the other hand, it is also one of its weaknesses: lack of coordination may lead for example to redundant work, lack of interoperability, under-development, insufficient visibility, incapability to find project partners, etc. Fortunately this weakness can be mitigated easily: With relatively small interventions (which are at the range of a project like this), significant improvements are possible. We were surprised to see, for example, how many new projects and cooperation activities started after brining together some of the main open-hardware developers at the (pre-COVID) Free Silicon Conference in Paris.

The coordination space of the open-source hardware community is largely still a *no man's land* open to be occupied, even if some big foreign tech giants have started their advancement.

Our role is to continue and strengthen such activity. The main coordination events will remain the future editions of the Free Silicon Conference, but across the different work packages we have planned several other activities which span from university lectures, to public talks, to webinars, to contests (see WP and milestone tables for more details).

*** Maturity, interoperability, availability of tools and components.** As mentioned in the previous paragraph, the open-source community has generally few rules, and this is reflected in the often scarce interoperability of open-source tools (at least in the early development stages). Our approach to this problem

is not to perform “Research and Innovation” on our own (even though many of us are active developers), but rather to discover existing tools and modify them *minimally* (possibly with the support of the original developers) such that they can *interoperate* with other tools, and that they can *compile* on standard platforms used by open-source developers (e..g the Debian GNU/Linux operating system).

*** University coordination.** Today the hardware design ecosystem is understandably largely centred around the classic paradigm set by mainstream commercial EDA vendors. In most electronic design courses around Europe, students are either taught to use mainstream proprietary EDA tools, or are left without training. Using mainstream EDA tools has the drawback that students are often reduced to “clicking machines” without a real understanding of the work done by the secret algorithms working in the background -a clear obstacle to innovation. *As a consequence, much of the knowledge about the inner workings of EDA software and of hardware synthesis has left the public domain.* Despite that, Europe has a long history of excellent electrical-engineering education as it can be seen by the number of companies which flourished on EU soil in the early days of computing (see Olivetti, Bull SAS, etc.) and the number of startups. Often these companies have witnessed failure after being acquired by foreign entities, or they have been incorporated -despite having received in some cases EU public funding- by the mainstream EDA vendors. Recently, for example, this has been the case of PhoeniX Software which has been acquired by Synopsys (PR-Newswire 2018).

European universities are further divided, or segregated, by the today’s impossibility of sharing any design produced with the help of mainstream EDA software (as mandated by the corresponding licence agreements). This has sometimes left academic research groups in nonsensical situations where, for example, every major European university is redeveloping from scratch the very same standard components, like a DDR3 memory controller (we know that from direct experience). This is clearly in contrast with the *findability, accessibility, interoperability, and reusability* (FAIR) European principles, and a clear loss of public resources.

If Europe shall have a chance to give a significant contribution to open-source hardware, universities shall re-gain the lost expertise. Moreover, academia can be a fertile ground for experimenting with the benefits of open-source: thanks to the open-paradigm, universities will be for the first time in decades be able to cooperate by *exchanging designs* with each other and construct coherently a *broad and complementary spectrum of expertises*. The goal is to coordinate this revival across all Member States which offer silicon design curricula. While the support from the policy makers will certainly play a major role here (see the roadmapping work package), we will start directly an active coordination on the field, by visiting the corresponding research groups, and talking with all the relevant people.

*** Open PDK.** The physical synthesis process of translating a Register-Transfer Level (RTL) design into a layout of physical components (transistors, memory cells, trenches, etc.) requires the knowledge of the physical properties of such components (like timing, capacitances, dimensions, etc.) and of additional rules (like the Design Rules) which are specific to every CMOS foundry. These rules are contained in the Process Design Kit, a set of files which is generally written in a format and in a language compatible *only* with the major EDA tools. Obtaining access to a PDK requires significant legal work. This is often not achievable by medium and small universities (if it wasn’t thanks to the work of Europractice), and it is challenging also for SMEs. Foundries so far have legitimately kept their PDKs as secret as possible because they contain significant details on the CMOS processes themselves which may be used by a competing foundry to copy the technology. Furthermore, PDKs are often developed with the help of engineers of the major EDA vendors, and it has been speculated whether the EDA vendors impose to the foundries the obligation of secrecy, which is something we consider very likely, especially since we know that EDA vendors impose secrecy on much less relevant EDA outputs. *Accessing a PDK is therefore one of the first obstacles that SMEs face when trying to develop a silicon product.* Secondarily, if the PDK is secret, it is also not possible to publish any step of the physical synthesis. Alone the output of the place-and-route tool, for example, is a function of the PDK and it cannot therefore be revealed. *Closed PDKs are therefore a clear obstacle to the development of open-source hardware.*

On the other hand, some older CMOS nodes have become so popular within the technical community, and have been described in such a large number of scientific papers, that they no longer contain significant secrets (unless they have been added with additional favours like BiCMOS, etc.) for most people skilled in the art. Keeping such a high level of secrecy on the related PDKs appears therefore as something no longer necessary.

Google understood the impact of an open PDK when it recently released the Skywater 130nm PDK to the public domain (https://github.com/google/skywater-pdk). As an early publisher, Google is attracting a

significant interest from the open-source hardware developers, therefore gaining important influence on the community.
It is very desirable therefore that also European foundries will release in the public domain at least one PDK. Even though most advanced CMOS nodes are located outside of the Continent, Europe contains precisely those foundries where we expect open-source to make the first appearance. In fact, open-source hardware will likely first gain terrain in older (and simpler) nodes (as it is happening now), and only later reach (as the tools and the community mature) the most advanced ones.
We are aware of several attempts from within our network to contact foundries and to convince them to open a PDK. The responses have been different, ranging from not seeing an economic advantage (a position which could flip once an ecosystem has been put in place), to legal constraints, to lack of internal resources. With this project we will identify the economic obstacles and legal obstacles with the help of external lawyers. We will therefore propose solutions and report to the European Commission. The ultimate goal is to obtain an open PDK within the duration of the project (unlikely) or in the following years (likely).
* **PDK compatible with open standards and open-source design flows.** Even if a European open-source PDK may not be available yet by the end of the project, there is another obstacle to open-hardware development related to PDKs: all current PDKs are written in a format which is compatible only with mainstream EDA tools, and use often *proprietary* languages (think for example at the SPICE language, or the DRC-deck language). Therefore, while awaiting that an open-source PDK will be officially released, a mitigation plan will be implemented: the release of European PDKs that are compatible with open-source design flows. This step will be conditioned by the authorization of the selected foundries. It is understood that in this scenario the signature of NDAs will still be required. Nonetheless, this work will enable the open-source community not to lose precious time. See work package on PDK for more details.
* **IT security.** The field of IT security is very broad and can be categorized based on the different adversaries, their power and their budget. These include *foreign governments* who pursue economic and strategic interest by exfiltrating data from high-level actors (see leaked material about the surveillance of Angela Merkel, Dilma Rousseff or UN Secretary General Kofi Annan), or by mass surveillance (through cloud, social media, all the way to wide-spread back-doors like the CVE-2017-5789 Intel Management Engine vulnerability -a sophisticated hardware-software vulnerability which we could test on our own), or by implanting software/hardware trojan in military equipment (like fighter jets). There are then *corporate interests* which have led to the birth of private surveillance businesses to eavesdrop on competition. At the other end, there are private individuals (less powerful, but much more numerous) who may pursue the most different interests, from monetary motives, to “cracking for fun”. All devices containing a silicon chip are today potentially vulnerable: From a smart card, to an IoT fridge, to a smartphone, to a heart pacemaker, to a car, to a banking server, to a government database, to a hospital device. Hardware vulnerabilities can be present in all ranges of chip dimensions: from a few kilo-gate electronic identity card (see the case of the Estonian cyber crisis https://en.wikipedia.org/wiki/ROCA_vulnerability), to a billion-transistors high-end microprocessor.
Hardware vulnerability can be inserted in all levels of the design process. They may be inserted already in the high-level design, or they can be inserted at the lowest end directly inside the foundry where extra transistors are added or are rewired. Pursuing the approach of a trusted supply chain is therefore very tedious. The open-source approach instead, by being fully verifiable and auditable, has a clear advantage. *Supporting open-source hardware therefore implies supporting IT security.*
However, the transition from having 100% black-boxes (as it is today the case) to complex chips (like a computer microprocessor) which are 100% open-source will likely not become reality by the end of this project. Instead, it will be necessary to proceed with steps, tackling for example, smaller yet critical projects. This is the case for example of Root of Trust (RoT) devices:
Root of Trust (RoT) hardware primitives help mitigating security threats at a software level, for example by sandboxing a certain memory address range and allowing modifications only through public/private key validation. Root of Trust (RoT) hardware primitives allow building provable secure systems under the assumption that the RoT itself is free from malicious features (e.g. by injection of extra transistors implementing a hardware backdoor). RoTs are therefore an ideal target for malicious attacks. Fortunately, RoT primitives are also relatively small in size (e.g. 100k gates) and are a *perfect candidate for initial implementations of the open-source hardware paradigm* (open down to the silicon level). RoTs are currently being researched by many security-oriented groups, and are therefore an ideal candidate for sensitizing the

community about the challenges of hardware security and to disseminate the solutions offered by open-source hardware.

*** Sustainability, re-usability, hardware licences.** A sustainable open-source ecosystem, is *not* an ecosystem which disappears shortly after its creation, nor a system which permits companies to subtract from the public domain publicly-funded code or code written by enthusiasts, etc.. Instead, it is an ecosystem where the very same "consumers" of open-source code are also "producers" of open-source code in an endless and self-sustaining circle where everybody can profit from the common advancements while still keeping their unique expertises. Today's big-data giants are excellent examples of code consumers, but they are certainly not a good model of contributors. With their "WARNING: code licensed under the GNU Affero General Public License (AGPL) MUST Not be used at Google", Google is a renowned example of this attitude (Google 2021) .

Through discussions from within our network (including managers of large European IT companies), we realized that it is not true that companies *do not want* to contribute back to the open-source community by releasing their own advancements, but there is primarily ignorance and fear about the legal implications of adopting a certain open-source licence, accompanied by the usual inertia in changing research and development models. This situation is partly caused by the lack of education (from engineering to management schools) on topics as important as open-source licences, and the lack of an entity which provides critical answers to frequently-asked questions (being developers ourselves, we heard already many). These questions should not be addressed by dubious entities with an NGO look which are financed, for example, by foreign big-data giants (which are unfortunately spreading inside and outside Europe). It is urgent therefore to support companies in finding their own ways to interface, co-exist and mutually profit from a healthy open-source ecosystem.

A central problem to availability of open-source tools and libraries, is the depletion of the ecosystem which occurs whenever an open-source project is transformed into a closed-source/proprietary one. This can occur whenever a project is released with a temporarily-open licence (known also as permissive licence, in the sense that closing the code is permitted), see (FSI 2020). In contrast to temporarily-open licences (or copyleft licence), forever-open licences guarantee the perpetual openness of a project and enforce its *reusability*. Forever-open licences have played a crucial role in the development and spread of open-source software. However, since hardware objects like silicon chips are legally considers *topographies* and are not protected by *copyright* law (which is the pillar of most software licences) there is yet no hardware licence which is both forever-open and which is compatible with other mainstream forever-open (copyleft) licences. The incompatibility affects also the recent OHLv2 licence, see: (CERN-FSI 2020). This problem, if left unsolved, will further continue to fragment the open-source community. The FSI has studied the problem in cooperation with some of the original authors of the mainstream open-source software licences. As part of this proposal, we will outsource to specialized lawyer some of the remaining legal issues, and foresee to deliver the expected licence by the end of the project.

*** Certifications and standards.** As it is established by the The European Observatory for ICT Standardisation, technological standards play an essential role in achieving interoperability of new technologies and can bring significant benefits to both industry and consumers. In addition, it is necessary to acknowledge the global power that the European Union is exercising through its legal institutions and the promotion of technological standards, see (Bradford, J.H. 2012). According to the Digital Single Market adopted in 2015, the identification of ICT standardization priorities is of major importance for the European ICT industry. Taking into account the European Processor Initiative and the recently created **European Alliance on Semiconductors** (Breton, Thierry 2021), there is a need for a high-level commitment to standardisation from a broad stakeholder base. As part of the industry and the research community, the collectives behind open source hardware should work in coordination with standard-setting organisations and certification bodies to fill the gap derived from the sale of European technological firms -see (FinancialTimes 2020)- and to contain the dependency on Chinese and other foreign suppliers. On this point, we have to take into account that openness paves the way to empower both technology developers and end users, which has positive outcomes in regards to technological independence and technology literacy. Moreover, all this effort must be conducted to meet security, safety and sustainability goals (Herrera, Alfredo 2020). The sustainability of the European cyber-physical space can be constructed by integrating open-source hardware as an asset to foster Fair, Accountable and Transparent technology, according to the

requirements given by the General Data Protection Regulation and the Regulation (EU) 2019/881 (Cybersecurity Act), (EU 2019) .

*** Instruction set architectures.** In the open-source domain there is already a de-facto standard instruction set architecture for *general-purpose processors*: RISC-V. The RISC-V project has started in 2010 in the USA (Berkeley) and it has been heavily subsidized by Darpa funding. It rapidly gained momentum by exploiting the first-mover advantage and today counts a large number of international "strategic members" and 14 "premier members" most of which are of giant proportions like Google, Huawei or Western Digital [https://riscv.org/members/]. However, none of the "premier members" are European entities.

The governance of RISC-V has often been criticized, see for example (libre-riscv 2019; reddit 2019), for being exclusive and not democratic, and the incorporation of the RISC-V foundation has recently moved from the US to Switzerland to avoid the restrictions imposed, for example, by the US International Traffic in Arms Regulations (ITAR). This opens again several questions about the autonomy and sovereignty of Europe. For example: 1. what would happen if the RISC-V foundation moves its incorporation from Switzerland back to the US? 2. what would happen if a major player (e.g. a big-data giant) purchases the foundation or hires its key members? 3. how does a broad adoption of RISC-V in Europe impact digital sovereignty?

In the RISC-V context, therefore, Europe has definitely lost the first-mover advantages. In Work Package 1 we will hence analyse the situation and propose measures to mitigate the risks and to strengthen Europe's position. These measures may include the use of certifications combined with legislation which make such certifications mandatory in specific contexts. They may also include the participation of standardization bodies like the International Organization for Standardization (ISO), or the European Telecommunications Standards Institute (ETSI).

In addition to the instruction sets for *general-purpose processors*, it is likely that specialized applications, like massively-parallel graphic-processing cores, or neuromorphic accelerators, *specialized open-source instruction* sets will perform better than the general-purpose ones.

Despite the mystification in certain academic groups about the alleged complexity of Instruction Sets, their definition, and their implementation has become a domain reachable by single-man efforts, as exemplified by C.Papon (see https://github.com/SpinalHDL/VexRiscv).

It is crucial therefore to encourage the activity in this direction by fostering educational programs, research, and translation to industry. This could lead to new unique competences where to profit of the first-mover's advantage. In Work Package 1 we will investigate the landscape and prepare reports with suggestions to the EC.

Implementation of open science practices

This project generally does not produce scientific research output, hence this section does not apply. Nonetheless, we are striving to maximize the openness of software and of hardware and we would like to use the same attitude also when it comes to publishing our reports which we will publish, unless inappropriate, online (see also table 3.1c).

Findable, Accessible, Interoperable, Reusable (FAIR) management of research output

Consistently with our open-source mindset, all ouputs generated by this project will be published to the maximum possible extent. For example our web pages (wikis, repositories,etc.) will be freely-accessible and released with a licence (e.g. Creative Commons, GPL, etc.) which will maximize re-usability. Wherever possible, moreover, we will edit directly Wikipedia (every third click on the internet is for Wikipedia), or add links in it for maximizing findability. Concerning interoperability, we have entire work packages dedicated to maximize it (hub for software, PDK compatible with open-source tools, standardization as tool for maximizing adoption, etc.).

2 Impact

2.1 Project's pathways towards impact

Impact on science and technology. We believe that there is a general consensus, also at the EC level, that open-source development in general allows for *faster scientific and technological innovation*. This is confirmed by several examples such as CERN which has been one of the protagonist in the last years of the open-hardware applied to mechanical objects, printed circuit boards, etc; and by NVIDIA which announced in 2017 that they would transition (as they finally did) away from proprietary standards towards RISC-V architecture motivating the decision with three key points: 1. *We want to keep control on architecture,* 2. *You don't have a real option to take an ARM core and turn it into something different and better,* 3. *Everybody will benefit if we work all together. (Sijstermans, Frans 2017)* . The motivations of RISC-V refer essentially to the avoidance of vendor lock-in and to the right to maintain the capacity of innovating in-house which is crucial for most, if not all, companies as well.

The above-mentioned arguments alone show that by fostering open-source hardware, our project will have direct impact on science and technology.

Still, open-hardware and open-source EDA tools will impact several more aspects:

*** Lowering the cost of software licences for small to large enterprises.** The few companies which can afford to pay at least one licence of mainstream EDA tools usually buy an abundantly lower number of licences than needed to minimize costs. This means that engineers have to share their "server time" among each other therefore reducing the work efficiency. We know of large European companies in the silicon design business who are intensively looking for open-source and cheaper alternatives, for example just only to perform design-rule checks (DRC). As an example, even if the available open-source DRC alternatives may not (yet) be at the level of today's de-facto "industry standards", engineers may gross out a large part of errors using gratis tools before making the finalization with the commercial tool.

Since open-source software is mostly gratis to use, or available at a reduced fee justified for example by providing support (see RedHat business model), the more and the better open-source EDA tools become, the more all ranges of enterprises, from small to large sizes, will manage to save significant money which can instead be invested e.g. into buying more compute power. We have no studies available for quantifying exactly such amounts (also because the economic deals with the EDA vendors are generally secret), but we have insider knowledge that the economic burden of licence costs is *very relevant* at every scale.

*** Lowering the risk of patent infringement.** Whenever open-source software or hardware is released with a licence which contains a patent provision (like the GPL, Apache, or OHL licence, but not the BSD or MIT licence), the user is guaranteed that the author of the software/hardware will not have the possibility to sue sooner or later the user who has made use of the published code. This risk is important for all commercial applications and it affects therefore all types of companies. The impact is both economic (less lawyers to verify patents in advance, less litigations, etc.) and technological since it accelerates the speed of adoption of better code or better designs.

* **Better research in academia and in research institutions.** Since 2017, all the listed supercomputers use an operating system based on the open-source Linux kernel [https://en.wikipedia.org/wiki/TOP500], and since a decade, the near totality of supercomputers do the same. Similarly, research at institutions like the particle accelerator CERN, or in most IT departments would be non imaginable without the use of open-source software. Similarly, it can safely be expected that the same will happen by adopting the open-hardware paradigm.

* **Autonomy.** As argued earlier, open-source hardware requires open-source design tools. As a consequence, the *dependence from foreign EDA companies* (and related export regulations, licence cost variations etc.) *is weakened, if not eliminated*. Furthermore, open-source hardware will facilitate the development of novel technologies (e.g. neuromorphic systems, etc.) without the constraints imposed by the (in-)capability and lack of flexibility of mainstream commercial EDA tools. This will enable domestic development and hence higher autonomy.

* **Agile response to urgent needs.** The lower costs of open-source hardware development and EDA tools will enable to adapt existing designs to different foundries (e..g older domestic nodes) in case of exceptional events (e.g. COVID) therefore responding more rapidly to deficiencies in the supply chain (e.g. lack of chips in the car industry).

By impacting the development of open-source hardware and open-source EDA tools, our project will impact indirectly all of the points mentioned above.

The project will further have *direct impact on society:*
* Fully-verifiable or fully-auditable open-source hardware will increase the *sense of trust and the comfort of the general public* facing novel technologies (Hoepman, Jaap-Heng 2021).
* The development of a forever-open licence suited for silicon chips and compatible with mainstream forever-open licences (like GPL) will enable the creation of a *sustainable community and ecosystem of hardware libraries*. Such a licence is essential because GPL was until no long ago the most frequently-used licence, and is still a broadly used licence. GPL-compatible hardware licences instead (like the “solderpad” licence) are temporarily-open licences and do not respond to the needs of a sustainable ecosystem.
* The upcoming editions of the conferences, workshops, schooling events and contests that we will organize as part of this project will help *aligning developers towards common goals and common standards* (e..g to make their software interoperable), and will consolidate and motivate the community.
* Coordinating and synchronizing the efforts of universities across Europe will strengthen the aggregate competences of the academic system as a whole.
* The creation of suitable certifications and standards will provide policy makers a tool to *adjust the development trajectory* and/or to protect specific domestic interests. Secondarily, if the standards are implemented in suitable forms (openly accessible, based on de-facto standards, rapidly updated, backwards compatible, etc.) they will provide *useful and highly desirable tools for the open-source community to increase interoperability and usage by third parties* (industrial uptake).
* By indexing, packaging and making available open-source EDA tools and hardware libraries we will increase the industrial uptake.

2.2 Measures to maximise impact – Dissemination, exploitation and communication (DEC)

Dissemination and communication is an integral part of this project. In some sense it is the core part: reach out to diverse (potential) actors in the open-source hardware ecosystems. Communicate with them to make them communicate amongst each other. This does not only include the technical groups who already contribute by publishing software and hardware designs in the open domain. We also target groups that have the potential to help sustaining and shaping the open-source hardware community in a human-centric way: On one side we want to reach the next generation of skilled people (by education) and make sure they find the necessary knowledge and tools to build open-source projects. On the other side we want to have active discussions with current stakeholders and especially policymakers to open more paths for the growth of open-source hardware. We already identified obstacles for the sustainable growth of open-source hardware, some can be solved with direct coordination, others need to be addressed by policy.
The pre-pandemic Free-Silicon Conference in 2019 showed us how big of an impact such an event can have on the collaboration between open-source groups: People met for the first time, exchanged ideas and visions and started working together in an uncomplicated and efficient way as it is typical for open-source projects.
In an ecosystem where funding is still scarce such platforms are a necessity. Hence we wish to continue and expand this efforts. Our work packages include communication efforts like giving talks at universities, organizing workshops, conferences, webinars and contests.
Beyond fostering interactions between groups and motivating people, such platforms help spreading technical knowledge. This is crucial because design of integrated circuits and required software needs specialized knowledge in the field which has disappeared from the public domain - partially because of the closed-source attitude of the big actors in the field of IC design.
There is already a range of open-source tools for IC design. Some of them get less attention than they deserve. Sometimes because of interoperability problems or because of difficult installation procedures. During this project we will help to advertise such projects, encourage and work on their interoperability and make them more accessible by providing software packages in a main-stream Linux distribution (Debian).
With a similar approach, we will also explore hardware library components (IP components): We will create a repository and an index of components which not only make them searchable and visible but also include measures for quality control such as systematic verification, simulation, DRC and LVS checks and continuous integration.

A common obstacle for open-source silicon projects are PDKs (process design kits) which are with very few exceptions not available for open-source tools and require non-disclosure agreements with the foundry. Additionally, open-source silicon projects have at the moment a tendency for low-volume production. For this reasons we want to work towards low-volume fabrication possibilities (for example on multi-project wafers) that are compatible with open-source tools. Already now we have the channels to advertise such achievements to the community (such as websites of well-known open-source projects, conferences). Lowering the costs (licence costs) and barrier for fabrication will open new paths: SMEs get a real chance to enter the field of silicon design, open-source projects have the possibility to become more mature by getting manufactured and tested.
In some fields like computer security complete openness down to the silicon layout is absolutely necessary to build trustworthy systems. At the moment this is difficult. Therefore we identified the community in this field as possible early adopters of open-source hardware. We will use our existing network to promote open-source approaches in related research groups.
By direct experience we know that proprietary IC design tools are a major blockage for disruptive innovations: Those tools are suitable for technologies that are already widely adopted. But researchers cannot study and modify them to create new technologies (such as integrated photonics for highly efficient communication or low-power asynchronous digital circuits). This is possible with open-source tools and it is a potential that should be tapped.
During this project we will extend our network and strengthen it by organizing conferences and workshops. We will continue them beyond this project. In 2020 we received funding from SMEs for a conference which was unfortunately blocked by the pandemic. However, this fact makes us confident that we will be able to continue such activities because there is an interest from SMEs to contribute and provide funding.

In total (during the full duration of project and across the entire consortium), we will deliver a *minimum* of:

- three conference
- one contest
- one novel university lecture
- six technical webinars
- fifty public talks
- visit twenty university groups
- contact fifty enterprises
- three roadmaps
- six reports to the policy makers
- hundred posts on social media channels
- thirty EDA software packages
- two packages containing a complete EDA-flow
- five new Wikipedia pages, 1000 Wikipedia edits
- six paid advertisements
- six stands at external conferences

2.3 Summary of DEC measures

	Specific need	**Expected result**	**Dissemination, exploitation and communication methods**
1	More public funding for open-source hardware projects.	Convincing policy-makers on the necessity of investing more in specific directions	Delivery of reports to policy makers. Direct meetings with policy makers.
2	The general public (students, researchers, developers, policy makers, etc.) needs to better understand the different types of software/hardware licences and	Teaching programs at various schooling levels including lectures on copyright law and licences. Policy makers understand the importance of	Delivery of talks and workshops to schools and SMEs. Delivery of reports to policy makers.

	their impact on a sustainable growth.	this type of education.	
3	Existing open-source design tools for integrated circuits need to be better known, their interoperability must be established, their availability must be improved.	Software repositories with up-to-date software packages. Pre-compiled and packaged state-of-the-art software in mainstream package managers.	Disseminate through package managers and internet websites. Create more detailed Mediawiki documentation pages on the wiki.f-si.org website.
4	Grow the size of open-source hardware community.	Motivate academic groups to teach usage and development of open-source hardware design tools.	Give talks at universities. Organize and promote workshops, conferences & contests.
5	Increased autonomy in the IT hardware development.	Networks and platforms like conferences and workshops.	Use and maintain the network and communication platforms to keep the community actively connected.
6	A licencing framework for open-source hardware which is compatible with mainstream open-source software licences and which avoids hidden threats of patent infringement.	Release of an open-source hardware licencing framework, compatible with mainstream open-source software licences and containing a patent provision.	Advertise the new licensing framework. Publish documentation such as FAQ and examples.
7	Catalyse cooperation. Increase efficiency of open-source hardware community.	The community meets and exchanges ideas and visions for example at the Free-Silicon Conference (FSiC).	Create recurrent events. Advertise them on social media, mailing-lists, technical journals and webpages of open-source projects.
8	Trustworthy integrated circuits (open and verifiable)	Gained insight and connections to SMEs and research groups working on hardware security building blocks (Root-of-Trust, crypto accelerators)	Advertise the necessity of openness for the security of hardware systems.
9	Domestic manufacturing possibilities for open-hardware silicon especially on multi-project wafer runs (MPW).	Silicon PDK (process design kit) which is compatible with open-source tools. In the best case an open PDK.	Motivate the community (SMEs, academia) to take advantage of the possibility to fabricate designs made with open-source tools.
10	Mature open-source IC building blocks including analog blocks.	Better availability of necessary infrastructure: design software, PDKs.	Organize and advertise workshops about the usage of open-source design software and PDKs.
11	Increase energy efficiency of future computing architectures.	Create awareness that open-source facilitates the design of disruptive technologies like analog neural networks or photonics.	Give targeted talks to related groups.

	Target groups	**Outcomes**	**Impacts**
1	Members of the EU commission.	Creation of new funding opportunities.	Growth of the open-source hardware ecosystem.
2	Students, researchers, developers, policy makers, etc.	Software/hardware developers or their respective copyright holders will make better licence choices and create a more sustainable ecosystem.	More and better software/hardware available.
3	Open-source software/hardware developers	More efficient usage of existing open-source software. Higher engagement in open-source development.	Grow the user base, less installation obstacles. Larger number of SMEs being able to develop their own devices.
4	Academia, SMEs, enthusiasts.	More university courses on open-hardware development. Larger number of graduated engineers capable of using and improving open-source design tools.	More contributions to the open-source hardware ecosystem from academia.
5	Research teams, SMEs, students, developers, enthusiasts.	Stronger open-hardware community. Dissemination of ideas, visions and knowledge.	Less dependency on monopolies, more control on digital infrastructure.
6	Contributors and users of open hardware.	Less fragmentation issues caused by licence incompatibilities.	Consolidation of the open-source hardware ecosystem.
7	Open-source hardware and software developers.	Better inter-project cooperation. Awareness of other parallel efforts.	A more structured community. More and better software/hardware.
8	Related research groups, SMEs	More focus on open-hardware in the field of Root-of-Trust design.	Open-source security building blocks make it possible to build larger systems that are secure and trustworthy due to verifiability.
9	SMEs, academia	Target group starts using the mentioned fabrication possibilities.	Increase of business cases for open-source PDKs. Gaining experience and building trust in open-source tool-chains.
10	Developers of integrated systems or IC building blocks.	Actors from the target group start to create designs with the open-source tools and PDK.	Open-source tool-chains and hardware libraries get tested and mature when used in real designs. Openness allows publishing fabrication results and measurements which enhances trust into the reliability of open-source components.
11	Academia, SMEs	More research groups exploit the built-in flexibility of OS for designing disruptive technologies (like neural networks or photonics).	Potential of first-mover advantages. Increased innovation.

3 Quality and efficiency of the implementation

3.1 Work plan and resources

For the sake of compactness, the work plan is described directly through the tables below. The work package description include whenever appropriate or relevant the leading team and the time (in months from project begin) of completion of the corresponding deliverables.

Table 3.1a: List of work packages

WP number	WP title	Lead participant number	Lead participant short name	Person months	Start month	End month
1	Roadmapping and direct coordination		FSI	51	1	36
2	Sustainability and licences		FSI	28	1	36
3	Hub of open-source EDA software and hardware libraries, from high-level design to layout (physical synthesis)		EDI	70	1	36
4	Certification and standardization		CSIC	23	1	36
5	Open-source Process Design Kit (PDK), PDK compatibility with open-source EDA tools, open-source standard-cell libraries		CMP	51	1	36
6	Open source for hardware Root-of-Trust (RoT) components		CSIC	44	1	36
7	Project management		FSI	11	1	36
				Total: 278		

Table 3.1b: Work package description.

Work package number	1			**Lead beneficiary**		FSI	
Work package title	Roadmapping and direct coordination						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	36	4	2	2	2	3	2
Start month	1			**End month**		36	

Objectives:

1. Direct coordination of European academic activities. Create awareness about current challenges/threats and open-source solutions. Stimulate the creation of a European network of complementary and complete know-hows. Stimulate cooperation between research groups.
2. Direct coordination of the open-source hardware community to consolidate it and to align efforts towards bigger and common targets
3. Elaborate roadmaps which will help policy makers to coordinate and support open-source hardware development in Europe through calls, legislation and investments.

Description of work:

For objective 1.:

- deliver talks at all universities with chip design expertise across all Member States (lead: FSI)
- create contacts between relevant research groups (lead FSI)
- organize round tables between participants (lead FSI)
- incorporate key-learnings into the roadmapping activity (lead FSI)

For objective 2.:

- Organize yearly the future editions of the Free Silicon Conference aiming at being the biggest gathering of its kind (lead: FSI, host: SU)
- Participate with stands, speeches or workshops at other major gatherings, such as DATE, FOSDEM, ESSCIRC-ESSDERCETC, (lead: FSI)
- Disseminate major results over paying (e.g advertisement on technology journals) and non-paying (own social media, mailing lists) channels (lead: FSI)

For objective 3.:

- Open-hardware ecosystem: exploration, monitoring. (lead: SU)
- Identification of threats and mitigation strategies. Elaboration of concrete evolution trajectories including ideal, realistic and undesirable trajectories. (lead: FSI)
- Communication and negotiation with all relevant stakeholders. (lead:FSI)
- Reporting to policy-makers. (lead: FSI)

Deliverables:

D1.1 (T0 + 10): first roadmap version
D1.2 (T0 + 24): second roadmap version.
D1.3 (T0 + 36): final roadmap

Work package number	2			**Lead beneficiary**		FSI	
Work package title	Sustainability and licences						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	24	2	0	0	2	0	0
Start month	1			**End month**		36	

Objectives: Promotion of a sustainable and healthy cooperation environment for all involved parties: from the hobbyist to academia, to enterprises. Creation of suitable open-source hardware licence.

Description of work:

For promoting a sustainable and healthy cooperation environment:

- Contact potential large game-openers (e.g. Nokia) and stimulate/encourage setting high-standard

examples in cooperation and sharing of resources. Advertise accordingly the best results.
- Deliver talks at major universities (lead FSI)
- Give courses/lectures at university (lead: SU)
- Participate with stands at most relevant events (conferences, workshops, etc.) (lead FSI)
- Create a specific session about sustainability at the future editions of the Free Silicon Conference (lead: FSI)

For the hardware licence (lead FSI):
- With the help of external lawyers improve the current draft to guarantee legal enforceability in the largest possible number of countries.
- Once a legally-validated and credible licence is ready, contact the copyright-holder of mainstream licences (e.g. the FSF for the GPL) to negotiate cross-compatibility of licences

Deliverables:
D2.1 (T0+12): first report on performed activities and licence status.
D2.2 (T0+24): second report on performed activities and licence status.

Work package number	3			**Lead beneficiary**		EDI	
Work package title	Hub of open-source EDA software and hardware libraries, from high-level design to layout (physical synthesis)						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	0	28	2	33	2	1	4
Start month	1			**End month**		36	

Objectives:
1. Maturity, interoperability and availability of design tools.
2. Maturity, interoperability and availability of hardware libraries (IP components).

Note: The focus here is *not to develop software*, but to *adapt* software written by third-parties to make it interoperable and more accessible as well as creating a framework for sharing hardware library components.

Description of work: Improve accessibility of open-source chip design components - such as EDA software and hardware libraries - in order to increase their user base. On the side of EDA software this consists of creating a survey and maintaining a cartography of available EDA tools. The cartography gives an overview of interoperability between tools. Based on the gained insights a choice of promising tools gets packaged for a main-stream Linux distribution in order to simplify the installation procedure for users. Further, we create working tool-chain flows from the selected tools.
In parallel create a repository for hardware library components (IP components), including digital RTL libraries and layout blocks such as analog macros. Methods need to be found for ensuring the quality of the hardware components, for instance by continuous integration.

For objective 1.:
Task 3.1. Survey on available open-source EDA tools (lead: SU)
This includes aggregating following information:
- Metadata (e.g. name of the tool, address of the public repository, function in the design flow, date of creation, maintenance status)
- input and output formats

- license(s)
- supported platforms
- interoperability with other tools

Task 3.2. Highlight alternative design flows consisting of open-source EDA (lead: SU)

- Creation of a map of the open-source EDA structured by following the main steps of the design.
- Description of alternative design flows, combining several open-source EDA from different repositories.
- Packaging the interoperable tools in Debian Linux distribution.
- Advertise and document the work on mainstream knowledge platforms like Wikipedia.
- On its website https://mycmp.fr, CMP will give a strong visibility to open-source EDA tools and related open-source software solutions by creating a dedicated category for “open-source solutions” in its Add-On Services (AOS) webpage, a showcase meant to highlight specific services from and for companies and academics of the microelectronics community.

For objective 2.:

Task 3.3. Methodology investigation for shared and reusable hardware building blocks (lead: EDI, M1-M12)

- Find requirements for RTL code base, including documentation, verification and continuous integration.
- Find requirements for non-RTL hardware libraries such as layouts, e.g. DRC and LVS checks (also for continuous integration).
- Identify methods for sharing non-text based hardware library components such as layouts. Investigate possibilities for version control of layouts for visualizing layout differences between versions.
- Choice of suitable code flow, e.g. git-flow, Agile
- Investigate relationship with commercial FPGAs vendors (none of the vendors support open-source flows)

Task 3.4. Setup repository infrastructure and initial code base (lead: EDI, starting from M7)

- Find suitable structure of the repository.
- Setup simulation and verification infrastructure.
- Create and document mechanisms for sustaining quality, handling merge requests, testing code-coverage and generating documentation.

Task 3.5. Promote the repository and attract contributors (EDI, LIP6, FSI, lead: EDI, M19-M36)

- Address public in events like talks, webinars, workshops, conferences (Free-Silicon Conference)
- Foster awareness of implications for the scientific community, like repeatability of research results and ability to publish designs in their entirety.

Deliverables:

D3.1 (T0+12) Report on requirements, methodology and structure of the hardware repository.
D3.2 (T0+18) Report on the status of the hardware repository, its structure and tools.
D3.3 (T0+36) Report on hardware repository statistics, contributors and future prospects.

Work package number	4			**Lead beneficiary**		CSIC	
Work package title	Certifications and standards						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS

Person month for participant	3	0	0	0	20	0	0
Start month	1			**End month**		36	

Objectives:
- Identification of the most critical scientific and technical areas for promoting the culture of open-source in the deployment of secure hardware
- Survey of (semi-)automatic procedures to guide the analysis, design and audit of open-source hardware
- Study of the openness of the most relevant standardization bodies in security and safety
- Identification of the most relevant standardization committees for promoting a culture of open-source in dependable hardware and hardware in general

Description of work:
This work package is intended to improve standardization efforts in secure hardware by incorporating the main results form the open source community in terms of procedures and methodologies. Along the work package, the differences between the Open-Source Software (OSS) and the Open-Source Hardware (OSW) communities will be established, with a special focus on pinpointing the main characteristics in hardware development that impede to achieve the same level of openness as in software development. The divergences between open and closed standards will be taken into account, to foster cross-fertilization between standardization/certification and open design and manufacturing in the production of secure and reliable hardware.

Task 4.1. **Identification of the main initiatives in the development of open source hardware** (M1-M6, CSIC).
Although OSS has achieved a high level of maturity, OSH is still under development. In order to accelerate the adoption of open source in hardware design and implementation, it would be very useful to extract the main lessons of the evolution of openness inside the software development community. In this task we will consider initiatives as DIN SPEC 3105 and the Open Know-How Manifest Specification to identify the main challenges to achieve agility, portability and interoperability in these three main components in hardware life-cycle:
- Implementation of openness in processes and hardware
- Documentation formats and contents, along with discoverability
- Licensing

Task 4.2. **Improvement of open hardware methodologies and procedures by leveraging on the results of the main (cyber)security, safety and sustainability standardization committees** (M6-M35, CSIC).
This task is intended to establish a coordinated action between the outcomes of the rest of the work packages of the project and the roadmap given by the European Observatory for ICT Standardization in the context of the StandICT.eu (https://www.standict.eu/) initiative. Indeed, open hardware can contribute to overcome the shortcomings of privative standards by endorsing open standards, and to adequately implement fairness, accountability and transparency as it is required by the Directive 95/46/EC (General Data Protection Regulation). On the other hand, the outcomes of the different working groups in standards bodies can be used to improve interoperability and portability in open hardware. The coordinated action will comprise the participation in standards bodies in the fields of cybersecurity and artificial intelligence, and the organization of two workshops to gather experts from open hardware and standardization in those fields.

Task 4.3. **Exploring the inclusion of open-source hardware in the complex standards-laws-certifications in cybersecurity** (M6-M35, CSIC).
The main goal of this task is to describe in terms of conformity claims the set of requirements that open-source hardware projects should satisfy to be considered acceptable by certification bodies in cybersecurity and artificial intelligence, and to promote discussion about the pros and cons of the certification of open-source hardware. Among the different certifications, this project will consider IT security and how open-source hardware should be integrated into the future European cybersecurity certification framework. According to Regulation (EU) 526/2013 and Regulation (EU) 2019/881 (Cybersecurity Act), it is necessary

to ease the collaboration between the entities and actors involved in the creation of ICT standards, the definition of technical specifications for products and services, and the verification of compliance with standards and the reliability of end-products. By means of the participation in fora organized by European CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams), this task will foster the discussion of the advantages and shortcomings of prototyping and manufacturing open-source hardware from the perspective of certification bodies, testing laboratories and auditors and digital forensics investigators.

Task 4.4. Exploring the inclusion of open-source hardware design tools and libraries in standardization processes (M1-M36, FSI).
Identify most suited standardization entities which can lead the way to support the open-source hardware community to define standards and to disseminate them. Provide technical support to such entities to develop pilot examples of standardization tailored to open-source development, and corresponding dissemination. Foster the discussion among the technical open-source community (which is historically reluctant) about the advantages and need of standards and certifications.

Deliverables:
D4.1 (M12) Report on the main initiatives in open source hardware.
D4.2 (M20) Report describing goals, communication strategy and target audience in the organization of workshops to promote the adoption of open hardware in standardization and certification initiatives.
D4.3 (M36) Report on the conclusions from the workshops organized to foster the interaction between the open hardware, standards and certification communities.

Work package number	5			**Lead beneficiary**		CMP	
Work package title	Open-source Process Design Kit (PDK), PDK compatibility with open-source EDA tools, open-source standard-cell libraries.						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	3	8	2	0	0	30	8
Start month	1			**End month**		36	
Objectives: unpublished							
Description of work: unpublished							
Deliverables: unpublished							

Work package number	6	**Lead beneficiary**	CSIC
Work package title	Open source for hardware Root-of-Trust (RoT) components		

Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	0	2	0	0	42	0	0
Start month	1			**End month**		36	

Objectives:
- Review open initiatives for hardware implementations of secure building-blocks and primitives.
- Identify principal actors in hardware-assisted security exploring academic, research and industry sectors at European and international level.
- Boost open hardware initiatives to provide ad-hoc open-source RoTs for embedded microprocessors, microcontrollers and accelerators.
- Promote open culture for hardware security in academic sector.
- Establish synergies with other related excellence networks and working groups.

Description of work: Embedded processors can be protected by deriving trust using a RoT. A hardware RoT uses, as a device secret, a digital identifier derived from hardware. This could be implemented using a Physical Unclonable Function (PUF) that exploits tiny variations in the silicon manufacturing processes of semiconductor circuitry. Neither PUF designer nor chip manufacturer knows these secret keys. Other building blocks of the RoT are a source of entropy and crypto functions to implement encryption/decryption algorithms and digital signatures. The combination of these components can provide a full suite of security services for an embedded system: device authentication, on-line generation of reliable cryptographic keys, hardware-enabled secure booting and Trusted Execution Environment (TEE) deployment.

Task 6.1. **Prospecting open initiatives in hardware security** (M1-M12, CSIC).
Algorithms for encryption/decryption and digital signatures come from competitive open calls. For evaluation purposes, groups that propose them distribute software implementation for embedded systems. However, hardware implementations are not always available and there is a lack of common criteria to provide them.
This task will address the following actions:
- Review of open available RTL descriptions of cryptographic algorithms in current open competition for Post-Quantum Competition and Lightweight Cryptography.
- Review of available repositories for hardware benchmarking.

Task 6.2. **Fostering open hardware to build ad-hoc RoT** (M6-M35, CSIC).
Many electronics vendors offer among their portfolio the possibility to build hardware RoT on embedded systems. However, these are closed solutions built around proprietary hardware “Intellectual Properties” (IPs) modules. *This task will drive a drastic change in philosophy*. The goal is to foster open ad-hoc RoTs that can be configured according to the security requirements and other limited restrictions (scalability, portability, monetary cost).
This task will address the following actions:
- Raise awareness of the scientific community therefore promoting the creation of an ecosystem to build ad-hoc open RoTs.
- Standardize design requirements to facilitate open hardware of ad-hoc RoT.
- Foster the integration of open hardware RoT on RISC-V processors.
- Monitor security enhancements in the RISC-V-based processors.

Task 6.3. **Promoting open source in hardware security for future next generations** (M6-M35, CSIC).
Awareness of the importance of open source to boost advances in hardware security, starting from the educational levels will be addressed in this task. The following actions will be planned:
- Provide open educational resources to asset basic concepts in hardware security.
- Participation in specialized teaching conferences to promote open source in hardware security.

- Motivation of undergraduate and Master students through the organization of international design contests.
Deliverables: D6.1 (M36) Report on future prospects to boost open hardware for securing embedded systems.

Work package number	7			**Lead beneficiary**		FSI	
Work package title	Project management						
Participant number	1	2	3	4	5	6	7
Short name of participant	FSI	SU	CNRS	EDI	CSIC	CMP	FS
Person month for participant	6	1	0	1	1	1	1
Start month	1			**End month**		36	
Objectives: Coordination of the whole project, including interfacing with the EU officers, monitoring the quality of the activities, and ensuring that they are aligned with the overall goals.							
Description of work: This WP consists of regular management of the project activities to guarantee the proper and timely progress of the project by coordinating the activities of each partner. The management activities include the administrative efforts. The work includes regular teleconferences with all participants.							
Deliverables: D7.1: Project management plan (including initial Data management Plan) D7.2: Year one report D7.3: Year two report D7.4: Year three report							

Table 3.1c: List of Deliverables.

Deliverable number	Deliverable name	WP	Lead participant	Type	Dissemination level	Delivery date in months
D1.1	First roadmap	1	FSI	R	PU	10
D1.2	Second roadmap	1	FSI	R	PU	24
D1.3	Third roadmap	1	FSI	R	PU	36
D2.1	Report on activities and licence development	2	FSI	R	PU	12
D2.2	Report on activities and licence development	2	FSI	R	PU	24
D3.1	Report on requirements, methodology and structure of the hardware repository	3	SU	R	PU	12
D3.2	Report on the status of the hardware	3	SU	R	PU	18

	repository, its structure and tools					
D3.3	Report on hardware repository statistics, contributors and future prospects	3	EDI	R	PU	36
D4.1	Report on the main initiatives in open source hardware	4	CSIC	R	PU	12
D4.2	Report describing goals, communication strategy and target audience in the organization of workshops to promote the adoption of open hardware in standardization and certification initiatives.		CSIC	R	PU	20
D4.3	Report on the conclusions from the workshops organized to foster the interaction between the open hardware, standards and certification communities.		CSIC	R	PU	36
D5.1	unpublished		CMP		SEN	
D5.2	unpublished		CMP		SEN	
D5.3	unpublished		CMP		SEN	
D5.4	unpublished		CMP		SEN	
D6.1	Report on future prospects to boost open hardware for securing embedded systems	6	CSIC	R	PU	36
D7.1	Project management plan (including initial Data management Plan)	7	FSI	R, DMP	PU	3
D7.2	Year one report	7	FSI	R	PU	12
D7.3	Year two report	7	FSI	R	PU	24
D7.4	Year three report	7	FSI	R	PU	36

Table 3.1d: List of milestones

Milestone number	Milestone name	WP	Due date	Means of verification
M1.1	Map of core hardware expertises in academia across Europe (public web page on wiki.f-si.org and on Wikipedia. The pages will be updated thereafter when appropriate)	1	12	Online check
M1.2	Free Silicon Conference 2022	1	11	Participation
M1.3	Free Silicon Conference 2023	1	23	Participation
M1.4	Free Silicon Conference 2024	1	35	Participation
M2.1	Finalization and announcement of the novel licence	2	36	Online check
M3.1	Survey of open-source EDA tools, published on the hub web page	3	12	Online check
M3.2	Update the open-source EDA hub and report compilation and testing results (web page)	3	24	Online check

M3.3	Publicly available hardware repository	3	30	Online check
M3.4	Update the open-source EDA hub (web page)	3	30	Online check
M3.5	Software packages of selected interoperable open-source EDA tools	3	36	Online check
M4.1	Organization of a workshop on open source hardware and cybersecurity	4	20	Participation
M4.2	Organization of a workshop on open source hardware and artificial intelligence	4	28	Participation
M4.3	Organization of a workshop on open source hardware, digital forensics, audit and certification	4	32	Participation
M5.1	unpublished			
M5.2	unpublished			
M5.3	unpublished			
M5.4	unpublished			
M5.5	unpublished			
M5.6	unpublished			
M6.1	Newsletter to disseminate available repositories among subscribers	6	12	Online check
M6.2	Organization of an open discussion panel to fix strategies around open ad-hoc RoTs	6	15	Participation
M6.3	Organization of an international student contest to promote open hardware for security purposes	6	30	Participation

Table 3.1e: Critical risks for implementation

Description of risk (likelihood/severity)	Work package involved	Proposed risk-mitigation measures
No EU foundry will release an open-source PDK by the project end (high)	5	Release of NDA-protected PDKs which are compatible with open-source EDA tools (see objective 2 of WP5)

Table 3.1f: Summary of staff effort

Participant short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	Total person-months per participant
FSI	36	24	0	3	3	0	6	72
SU	4	2	28	0	8	2	1	45
CNRS	2	0	2	0	2	0	0	6
EDI	2	0	33	0	0	0	1	36
CSIC	2	2	2	20	0	42	1	69
CMP	3	0	1	0	30	0	1	35
FS	2	0	4	0	8	0	1	15
Total	51	28	70	23	51	44	11	278

Table 3.1g: ‘Subcontracting costs’ items

Participant short name: FSI		
	Cost (EUR)	Description of task and justification
Subcontracting	100’000	Lawyer for licence development.

Participant short name: CMP		
	Cost (EUR)	Description of task and justification
Subcontracting	unpublished	unpublished

Table 3.1h: ‘Purchase costs’ items

Participant short name: FSI		
	Cost (EUR)	Justification
Travel and subsistence	27’000	Delivering talks to universities, SMEs, participating to conferences, meeting policy makers, etc. About 18+36 trips for two members, at an average of 500Eur/trip
Other goods, works and services	24’000	Paid advertisement in technical journals (6k), paid advertisement in other platforms (18k)
Remaining purchase costs (<15% of pers. costs)	20’000	Server costs, hardware, minor expenses.
Total	71’000	

Participant short name: SU		
	Cost (EUR)	Justification
Travel and subsistence	45’000	Travelling of the personnel (15’000) and sponsoring travelling of external participants at own conferences (30’000).
Other goods, works and services	21’000	Organizing events (catering, room rental, etc.)
Remaining purchase costs (<15% of pers. costs)	0	
Total	66’000	

Participant short name: CSIC		
	Cost (EUR)	Justification
Travel and subsistence	24’000	Delivering talks to workshops/universities, participating at conferences, panels, etc.
Other goods, works and services	30’000	Paid advertisement in technical and open journals, material for advertisement and dissemination (leaflets, porters, brochures) of planned activities, conference registrations, awards for student contest.

Remaining purchase costs (<15% of pers. costs)	0	
Total	54’000	

Participant short name: CMP		
	Cost (EUR)	Justification
Travel and subsistence	unpublished	
Other goods, works and services	unpublished	
Remaining purchase costs (<15% of pers. costs)	unpublished	
Total	unpublished	

Participant short name: EDI		
	Cost (EUR)	Justification
Travel and subsistence	6’000	Travelling of personnel
Other goods, works and services	0	
Remaining purchase costs (<15% of pers. costs)	0	
Total	6’000	

Participant short name: FS		
	Cost (EUR)	Justification
Travel and subsistence	5’000	Delivering talks to universities and SMEs; participating at conferences; technical discussion with foundries; etc. About 10 trips at an average of 500Eur/trip
Other goods, works and services	0	
Remaining purchase costs (<15% of pers. costs)	10’000	Server costs, hardware, minor expenses.
Total	15’000	

Table 3.1i: ‘Other costs categories’ items (e.g. internally invoiced goods and services)
None.

Table 3.1j: ‘In-kind contributions’ provided by third parties
None.

3.2 Capacity of participants and consortium as a whole

Below is a description of the individual members of the consortium. As highlighted in the following, all of the participants have experiences closely related to the present project. Some of them are in addition deeply rooted in open-source hardware and have been pioneering the field.
Specifically:

- FSI has been coordinating and supporting the open-source hardware community since its existence through direct interaction with the developers and -most importantly- by organizing the Free Silicon Conference (see e.g. https://wiki.f-si.org/index.php/FSiC2019). Two of the founding members of the FSI (L.Alloatti and T. Kramer) are currently working on open-source EDA development in two projects founded by Nlnet (https://nlnet.nl). A third founding member (M.Koefferlein) is the creator of the open-source layout editing tool KLayout (see https://klayout.org). The latter is a tool which is used by uncountable academic groups and companies all over the world. KLayout is one of the most mature open-source EDA-components and it sets therefore an example for other open-source EDA tools.
  In addition, L.Alloatti has co-developed the first microprocessor with optical input/output (Sun et al. 2015) together with the group of Krste Asanović who started the RISC-V project. The chip contained a dual-core RISC-V microprocessor.
- Sorbonne Université (SU) is a multidisciplinary, research-intensive and world-class academic institution. It was created on January 1st 2018 as the merge of two first-class research intensive universities, UPMC (University Pierre and Marie Curie) and Paris-Sorbonne. Sorbonne University is now organized with three faculties: humanities, medicine and science each with the wide-ranging autonomy necessary to conduct its ambitious programs in both research and education. SU counts 53,500 students, 3,400 professor-researchers and 3,600 administrative and technical staff members. SU is intensively engaged in European research projects (163 FP7 projects and 195 H2020 projects). Its computer science laboratory, LIP6, is internationally recognized as a leading research institute. LIP6 is a Joint Research Unit of both SU (Sorbonne Université) and CNRS. Both entities invests resources within LIP6 so CNRS is then an Affiliated Entity linked to SU. SU, and in particular the LIP6 group, is one of the pioneering academic groups in open-source EDA tools. It inherited the EDA tools left by the French computer company Bull (now part of Atos) under a GPL licence and it maintains the corresponding code base (distributed under the name of Alliance and Coriolis) since then. The team at SU is also currently working on an open-source hardware projected funded by Nlnet.
- The Institute of Electronics and Computer Science (EDI) in Riga, Latvia is a non-profit public research institute founded in 1960. The team involved in the GOIT project has expertise in digital circuit design ranging from design of Neural Network (H2020 ECSEL 3Ccar, G.A.: 662192) and IR image preprocessing circuits (H2020 ECSEL APPLAUSE, G.A.: 826588) to acceleration of localisation for autonomous drones (H2020 ECSEL COMP4DRONES, G.A: 826610) and real-time control (H2020 ECSEL I-MECH, G.A.: 737453).
- The Spanish National Research Council (CSIC) is Spain’s largest public research institution and ranks third among Europe’s largest research organizations. Two research groups of CSIC are involved in the GOIT proposal, namely the research group in Digital and Mixed Integrated Circuits Design (UDDM) that leads WP6, and the research group in Cryptology and Information Security (GiCSI)that leads WP4. UDDM belongs to the Institute of Microelectronics in Seville, and GiCSI belongs to the Institute of Physical and Information Technologies. Some of the CSIC members who are part of the GOIT proposal are participating in an on-going H2020 RIA project called SPIRS (GA ID: 952622). SPIRS will encompass the complete design of a hardware dedicated Root of Trust (RoT) that will be used to secure a RISC-V processor core. The results obtained in SPIRS can be disseminated through the actions planned in WP6 of GOIT, with the aim of completing the expected outcomes.
- Created in 1981, CMP is a non-profit institution organising the affordable access to Multi-Project Wafer (MPW) shuttle runs for different technologies for Universities, Research Laboratories and Industrial companies. Thanks to its long-term collaborations with foundries, CMP enables prototypes fabrication and low volume production on industrial processes, as well as related packaging services. Advanced industrial technologies are made available in CMOS, SiGe BiCMOS, HV-CMOS, SOI, MEMS, 3D-IC, Photonics technologies etc. CMP distributes the design rules for each technology

and the standard cell libraries for each specific software tool (design kits) free of charge and supports several CAD software tools for both industrial companies and Universities. CMP is pioneering open-source CAD tools development and dissemination. CMP launched in 1979 the CAD tool for layout edition "LUCIE", at the same time as the US MOSIS was distributing their layout editor "MAGIC". These two open-source layout editors were the first-ever tools for circuits design for the community.

- FS is one of the pioneering startups in the open-source hardware domain. It is owned by Staf Verhaegen, who has worked for almost 25 years at IMEC, designing radiation hardened standard-cell libraries and memories amongst others and building up his expertise on PDKs this way. The purpose of the startup is to drive innovation in the micro-electronics space by making it accessible to more people and companies. Several solutions are developed to reach this goal. One is to shield open-source developers from proprietary PDKs; another one is providing the necessary open source building blocks like standard cell, memory, analog and mixed-signal blocks necessary to develop open source hardware. All this work is partially funded by the European NGI Zero project managed by the NLnet foundation.

Concluding remarks

This project was written during a considerable amount of paid and unpaid hours. The process of writing it was for all members of the consortium a sufficient reason to participate to countless brainstorming sessions, during which several ideas have been rapidly generated, discarded or improved. We feel that sufficiently new ideas have been generated for justifying the publication of this manuscript. The publication will further increase the transparency of the selection process, and will offer to the broad public the possibility of criticising and commenting the proposal.

4 References

Botero, Ulbert. 2021. “Hardware Trust and Assurance through ReverseEngineering.” https://arxiv.org/pdf/2002.04210.pdf.

Bradford, J.H. 2012. “Gpr Prestack Amplitude Recovery for Radiation Patterns Using a Full Wave-Equation, Reverse-Time Migration Algorithm.” *SEG Technical Program Expanded Abstracts*, 1–5. https://doi.org/10.1190/segam2012-1444.1.

Breton, Thierry. 2021. “How a European Chips Act Will Put Europe Back in the Tech Race.” *EC*. https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-chips-act-will-put-europe-back-tech-race_en.

CERN-FSI. 2020. “Concerns on the Impact of OHL on GPL Community.” https://forums.ohwr.org/t/concerns-on-the-impact-of-ohl-on-gpl-community/848400.

EC. 2021. “Study about the Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy.” https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and.

EU. 2019. “EU Regulation 2019/881.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG.

FinancialTimes. 2020. “Libre-RISC-V (GPU Effort) Looking at POWER.” https://www.ft.com/content/4970848d-7821-45dc-b8cb-211036be5d30.

Fliehe, Marc. 2021. “Digitalisation.” https://www.tuev-verband.de/en/digitalisation.

FSI. 2020. “White Paper for the European Commission.” https://wiki.f-si.org/index.php?title=White_paper_for_the_EC,_January_2020.

FSiC. 2019. “Free Silicon Conference.” https://wiki.f-si.org/index.php/FSiC2019.

Google. 2021. “AGPL Policy at Google.” https://opensource.google/docs/using/agpl-policy/.

Herrera, Alfredo. 2020. “The Promises and Challenges of Open Source Hardware.” *Computer IEEE* 53: 101–4. https://doi.ieeecomputersociety.org/10.1109/MC.2020.3011080.

Hoepman, Jaap-Heng. 2021. “Increased Security through Open Source.” https://arxiv.org/pdf/0801.3924.pdf.

Karlitschek, Frank. 2018. “Why I Forked My Own Project and My Own Company OwnCloud to Nextcloud.” https://conf.tube/videos/watch/05857289-4f99-4109-bd71-f5e0a779a544.

Ke, Weiling, and Ping Zhang. 2010. “The Effects of Extrinsic Motivations and Satisfaction in Open Source Software Development.” *J. AIS* 11 (December). https://doi.org/10.17705/1jais.00251.

libre-riscv. 2019. “Power Pc.” http://lists.libre-riscv.org/pipermail/libre-riscv-dev/2019-October/003035.html.

PR-Newswire. 2018. “Synopsys Expands Photonic Design Solution with the Acquisition of PhoeniX Software.” https://www.prnewswire.com/news-releases/synopsys-expands-photonic-design-solution-with-the-acquisition-of-phoenix-software-300596120.html.

PSI. 2017. “3-D X-Ray Imaging Makes the Finest Details of a Computer Chip Visible.” https://www.psi.ch/en/media/our-research/3-d-x-ray-imaging-makes-the-finest-details-of-a-computer-chip-visible.

reddit. 2019. “Libre-RISC-V (GPU Effort) Looking at POWER.” *Reddit*.

Sijstermans, Frans. 2017. “RISC-V in NVIDIA.” https://www.youtube.com/watch?v=g6Z_5l69keI.

Stallman, Richard. 2019. “GitHub’s Encouragement of Sloppy Licensing.” https://lists.gnu.org/archive/html/gnu-system-discuss/2019-11/msg00277.html.

Sun, Chen, Mark T. Wade, Yunsup Lee, Jason S. Orcutt, Luca Alloatti, Michael S. Georgas, Andrew S. Waterman, et al. 2015. “Single-Chip Microprocessor That Communicates Directly Using Light.” *Nature* 528 (7583): 534–38. https://doi.org/10.1038/nature16454.

Tarnovsky, Christopher. 2010. “Deconstructing a ‘Secure’ Processor. Flylogic, Inc. Black Hat DC 2010, Washington D.C.”