Cross-platform **O**pen **S**ecurity **S**tack for **Con**nected Devices

D6.2 Dissemination and Communication Plan

Document Identification			
Status	Final	**Due Date**	31/01/2023
Version	1.0	**Submission Date**	31/01/2023

Related WP	WP6	**Document Reference**	D6.2
Related Deliverable(s)	D6.1 Project Website	**Dissemination Level (*)**	PU
Lead Participant	UMINHO	**Lead Author**	Tiago Gomes, UMINHO
Contributors	UMINHO	**Reviewers**	Aljosa Pasic, ATOS
			Markus Miettinen, TUD

Keywords:
Dissemination, Communication, KPIs.

This document is issued within the frame and for the purpose of the CROSSCON project. This project has received funding from the European Union's Horizon Europe Programme under Grant Agreement No.101070537. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Tiago Gomes	UMINHO
Sandro Pinto	UMINHO

Document History			
Version	Date	Change editors	Changes
0.1	29/12/2022	Tiago Gomes (UMINHO)	Draft version / TOC
0.2	16/01/2023	Tiago Gomes (UMINHO)	Ready for first review
0.3	25/01/2023	Tiago Gomes (UMINHO)	Document update according to reviewers Final version for QA and submission.
0.4	31/01/2023	Juan Alonso (Atos)	Quality Assurance
1.0	31/01/2023	Hristo Koshutanski (ATOS)	Final version submitted

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tiago Gomes (UMINHO)	27/01/2023
Quality manager	Juan Andres Alonso (ATOS)	31/01/2023
Project Coordinator	Hristo Koshutanski (ATOS)	31/01/2023

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CA	Consortium Agreement
CD	Connected Device
CROSSCON	Cross-platform Open Security Stack for Connected Devices
D6.2	Deliverable number 2 belonging to WP6
DoA	Description of Action
EC	European Commission
EU	European Union
GA	Grant Agreement
HW	Hardware
IoT	Internet of Things
KPI	Key Performance Indicator
OA	Open Access
OEM	Original Equipment Manufacturer
PC	Project Coordinator
SME	Small and Medium-sized Enterprise
TEE	Trusted Execution Environment
WP	Work Package

Executive Summary

A detailed dissemination and communication plan is important but developing a strategy should always come first. Strategy drives the plan toward the execution of dissemination and communication actions and achievement of impact goals, as well as the alignment of impact goals with the overall project objectives and goals.

This document defines the dissemination and communication strategy and plan for the Cross-platform Open Security Stack for Connected Devices (CROSSCON) project. CROSSCON's strategy is closely aligned to its aims of designing a new open, modular, highly portable, and vendor-independent Internet of Things (IoT) security stack that can run on a wide range of devices that may use heterogeneous hardware architectures. CROSSCON's stack will be able to guarantee interoperable trusted services with high-level of assurance across an entire IoT system.

For a successful dissemination and communication of the project's goals, as well as of the scientific findings and practical results, this deliverable also gives detailed examples of the activities that are going to be conducted in order to reach target audiences, partners, and the different types of stakeholders. A set of top-tier journals and conferences is also presented, which are going to be used to disseminate the project's scientific results. To evaluate the success of such actions, different Key Performance Indicators (KPIs) and metrics will be used. The plan includes monitoring and assessment actions for such KPIs, each depending on the action that is going to be taken and its specific KPI.

This document also describes actions already done, such as the selection of the visual identity of the project, namely the logo and presentation templates, and the selection of social networks in which the project should be present. An important milestone briefly described in this document, and in more depth in deliverable D6.1 - *Project website*, is the public online presence of the project. Other channels envisaged in the initial strategy include brochures (both on paper and digital format) that will be distributed to the members of the consortium to facilitate the dissemination of the project in Face-to-Face events, workshops, conferences and symposiums.

The information present in this document, and the project's dissemination and communication approach in general, will be continuously reassessed and iterated throughout the project. An updated version of this plan will be provided during M18 through D6.4 - *Dissemination, Communication and Community Building - First Report.*

1 Introduction

1.1 Purpose of the document

This document presents the Dissemination and Communication Plan and describes the communication and dissemination actions to be adopted by the CROSSCON project, including the visual identity, website creation, communication tools and channels, conferences and publication goals, target audience groups, and stakeholder's strategy.

This plan is part of the Work Package 6 (WP6) - *Dissemination, Exploitation and Impact Creation*, which takes the duration of the entire project lifespan and intersects all project activities across all work packages. The main goals of the WP6 include:

- Creating synergies with relevant stakeholders and open-source communities:
  - Communities can be used as springboards to involve a large number of interested parties.
- Positioning CROSSCON at the intersection of technology communities and stakeholder groups:
  - Peer-reviewed paper publications;
  - Open-access (OA) publications;
  - Workshops (co-located to well positioned events);
  - Training activities including summer schools and online sessions;
  - Participation and talks in industry-related events;
  - Blogs and specialized articles.
- Using appropriate channels to reach a broad target audience, disseminate results, and communicate value proposition:
  - Online visibility;
  - Elevator pitches;
  - Online press-release presence;
  - Interaction with companies interested in adopting CROSSCON security stack.

To successfully accomplish the aforementioned goals, it is crucial to create awareness and the early adoption of the CROSSCON stack and tools by all parties involved, including stakeholders, developer and manufacturer communities. This interaction will help in disseminating project results through the various scientific, communication, and community channels, creating a continuous interaction between all entities and resulting in an increased project's impact in all target sectors (scientific, technical, economic, social, etc.).

1.2 Relation to other project work

The deliverable D6.2 *Dissemination and Communication Plan* has the main goal of defining the clear strategy and plan of actions to promote the dissemination and communication activities to raise awareness about the CROSSCON project towards different target groups. D6.2 belongs to the WP6, and it is related to following deliverables:

- **D6.1** ***Project Website[3]***. Which presents a report on the project website, including the layout, structure, and content management.
- **D6.4** ***Dissemination, Communication and Community Building - First Report***. Reports the dissemination and communication, stakeholders' engagement, advisory board, and training activities for the first half of the project.
- **D6.6** ***Dissemination, Communication and Community Building - Final Report***. Which presents the dissemination and communication, stakeholders' engagement, advisory board, and training activities for the second half of the project.

1.3 Structure of the document

This document is structured into 5 major chapters, described as follows:

- **Chapter 1** - presents the introduction and description of this document;
- **Chapter 2** - shows the dissemination and communication plan, including the detailed activities, and target audience and partners;
- **Chapter 3** - describes the dissemination and communication channels for the scientific and social dissemination of the CROSSCON project;
- **Chapter 4** - describes the defined KPIs for the dissemination and communication actions;
- **Chapter 5** - concludes this document.

1.4 Glossary adopted in this document

- **CD/IoT.** Within this document the term IoT and CD are used indistinguishably to refer to connected devices in restricted environments.

2 Dissemination and Communication Plan

The dissemination and communication plan, to be reviewed during the project execution, details a set of actions aiming at the project dissemination and communication, according to the specific timeline each activity should be accommodated to. It starts by identifying the envisioned target audience groups where CROSSCON may notably have a big impact, followed by a set of actions focused on awareness and visibility. Partners must continually review their individual strategies, roles, and responsibilities (as firstly established during the project kick-off), and align these with the general consortium strategy and plan, including specific timelines and action frames, as well as formal establishment of Advisory Board (T6.3). A deep analysis will be enacted in order to delineate possible adjacent segments and exploitation chances in the market, by defining existing gaps in the European Union (EU) HW based CD/IoT value chain.

In the first 6 months, the project will rapidly build connections, thanks to the pre-existing contacts, with projects and communities related to open source HW, IoT, Cybersecurity, infrastructure (e.g., Cloud/Edge) and others, such as specific applications domains. Task T6.1 will set up web and social network presence and will elaborate, together with T6.3, a list of community events. The dissemination and communication strategy is structured around three main pillars:

- Create synergies with relevant stakeholders and open-source communities;
- Place CROSSCON at the intersection of technology communities and stakeholder groups;
- Use appropriate channels to reach target audiences, disseminate results, and communicate value propositions.

Raising awareness about secure application requirements in specific connected devices solutions will initially focus on low-cost devices. The narrative will first describe CD/IoT applications (e.g., smart home or industry 4.0 manufacturing plant with many different devices) as an example, and describe how they use secure services for connected devices today. Then it will describe the threat and impact to specific industry or IoT applications, needed for high assurance and how CROSSCON is helping to reduce the cost of secure and trusted services based on Root and Chain of Trust. Finally, it must also create awareness of other project result benefits, such as avoidance of vendor lock-in.

Besides scientific publications, it is also expected that actions are taken towards industrial stakeholders in form of blogs or specialized articles. Also, and within the context of the CROSSCON project, it is also important to foster participation in industry-related events, such as, RISC-V Summit, Embedded World, Black Hat, etc. In communication, the main target will be users of low-end IoT devices, and their feedback will be looked for, also as an input for the exploitation, where we plan to explore possibilities of patenting and licensing the technology, besides the drafting of legal documents (e.g., exploitation agreements) that would enable further innovation, as well as possible commercialisation.

2.1 Purpose of Dissemination Communication Activities

This initial dissemination and communication plan endorses the continuous terms established by the consortium members and approved by the EU Commission. As part of the recommendations and obligations with the purpose to promote CROSSCON, it is important to understand the Communication and Dissemination definition:

- **Communication [1]** means “taking strategic and targeted measures for promoting the action itself and its results to a multitude of audiences, including the media and the public, and possibly engaging in a two-way exchange. The aim is to reach out to society as a whole and in particular to some specific audiences while demonstrating how EU funding contributes to tackling societal challenges”.
- **Dissemination [1]** refers to “the public disclosure of the results by any appropriate means, including scientific publications in any medium”. Besides, dissemination “makes research results known to various stakeholder groups (like research peers, industry and other commercial actors, professional organizations, policymakers) in a targeted way, to enable them to use the results in their work”.

The Grant Agreement (GA) [2] - Grant Agreement-101070537-CROSSCON - between the EU Research Executive Agency and the CROSSCON partners highlights the importance of Dissemination and Communication activities, as has been mentioned by "ARTICLE 17 - COMMUNICATION, DISSEMINATION AND VISIBILITY" in the GA, which commits all partners to the obligation of promoting and disseminating results in a strategic, coherent and effective manner.

2.2 Target audience and Partners

Following the lines of the CROSSCON proposal and considering the interrelation between the diverse activities to maximize the project's impact, one of the first actions was to identify early on the potential targeted audiences of CROSSCON along with their specific interest in the project. The consortium will focus on the following target stakeholders' groups in the dissemination activities, at appropriate times when valid and interesting results have been achieved:

- **Developers and providers of innovative IoT solutions**, including IoT innovators and leading small and medium-sized enterprises (SMEs), such as the CROSSCON partners (CYSEC, Barbara IOT, 3mDEB, and Beyond semiconductors), and larger system integrators. Many tangible results of the project, including the Trusted Execution Environment (TEE) manager, Hypervisor, toolchain, etc., can be used by different industry stakeholders.
- **Secure hardware and firmware security developers**, and other related consulting and training security service providers;
- **Academic and corporate researchers and scientists** in the fields of open hardware, firmware or embedded software, covering different related research domains such as security;
- **Networks and communities,** including universities, research centres, SMEs/Start-up associations and Digital Innovation Hubs;
- **Standardization bodies, pre-standardisation and open-source initiatives**. The validation methodology for "chain of trust" assurance levels will provide a balanced approach to certification of "security stacks" with layers that might have different levels of assurance and could be provided by different manufacturers or open-source communities. The main targets will receive ECCF, EUCC, EN 303 645, TUV IOT certification, E-IOT-SCS, and others. Among open-source initiatives, RISC-V, FIWARE, IOT security forum, and many others will be approached.
- **Policy makers**, especially those involved in security and privacy (e.g., ENISA, ECCC, units in the DG CNECT etc.). Contributions to policy initiatives (e.g., white papers) will focus on strategic impact areas such as EU digital sovereignty and policy objectives like those listed in 2030 Digital decade.
- **Security and privacy stakeholders**, organizations, working groups, researchers, technology providers, IoT infrastructure providers;
- **Enlarged community**, with IoT users across several domains, e.g., automotive, energy and utilities, health, agriculture, retail, industry, smart cities, etc.
- **Associations** such as ECSO, DAIRO, AIOTI, NGIOT, GAIA-X, IDS, IERC, FIWARE, FME, or RISC-V. The newly formed DAIRO or Data Spaces Business Alliance (DSBA) are particularly interesting targets because they involve many IoT and connected device stakeholders, but are not aware or at least not fully aware of challenges related to security in open hardware based IoT stacks, according to their research agenda.
- **Related Projects** such as IoT European Large-Scale Pilots initiative (IoT-LSP, https://european-iotpilots.eu/), IoT European Security and Privacy cluster of projects (IoTCrawler, CHARIOT, ENACTDevOps, SERIOT, BRAIN-IoTZ, SecureIoT, SOFIE), and others looking to deploy new approaches for security in connected devices.
- **Citizens and society in general**. General communication will use explanations and metaphors to reduce complexity and make technology understandable for general audience, and in this way increase trust and drive adoption of secure connected devices.

3 Dissemination and Communication Channels

This chapter provides further information on how CROSSCON uses different dissemination approaches to reach different groups of its target audience. By leveraging these channels, the project aims at effectively impact and engage a diverse group of stakeholders.

3.1 CROSSCON Website

The project website, detailed in Deliverable D6.1 - *Project Website* [3], serves as a key platform for disseminating information about CROSSCON both to stakeholders and the general public. Boasting an engaging, user-friendly design, the website acts as a portal, providing access to updates on the project's progress and achievements. As an important mean of communication, the project website also serves as an essential tool for keeping stakeholders informed and engaged with CROSSCON's activities and results.

The design and development of the website was under the responsibility of ATOS, while the edition and update of its content should be maintained by the project parter UMINHO. The procedures related to the operational aspects, e.g., content management and publishing are described in the deliverable D6.1 - *Project Website* [3]. Moreover, the monitoring and analysis of all website traffic will be collected every year, which can be used to make assessments and the re-structuring and edition of the website, if needed.

3.2 Social Media

In order to increase general awareness of CROSSCON, communication channels and innovation activities will focus on reaching a variety of audiences (e.g., citizens, media, stakeholders). The already selected social media channels (Twitter, LinkedIn, and YouTube) will engage and educate interaction with companies interested in adopting the CROSSCON platform. For instance, to promote cybersecurity awareness, an animated video featuring a simplified elevator pitch will be produced and shared on the website and social media platforms like YouTube. In addition, to make complex concepts like TEE and IoT security more suitable to a wider audience, we will use general vocabulary and common metaphors (e.g., bank vaults, bank services, etc.) in our explanations.

Partner UMINHO is responsible for the creation and management of social media accounts, and the edition of content to be published through the appropriate channels. The initial planning for the launch of CROSSCON social media profiles can be found in Table 1. Other relevant channels may be created in the appropriate time, if decided by the consortium.

Table 1: Social media channels

Channel	Link	Creation Date
Twitter	https://twitter.com/crosscon_eu	During M3
LinkedIn	https://www.linkedin.com/in/crosscon/	During M3
GitHub	https://github.com/crosscon	During M3
YouTube	(not yet created)	By M6
Other(s)	TBD	TBD

3.3 Publications

3.3.1 Scientific Publications

As part of the development of CROSSCON, the dissemination strategy includes the publication of research papers in high-impact journals, such as, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Computer Aided Design*, *Formal Methods in System Design*, *Transactions on Computer-Aided Design*, etc. Publications are committed to target Q1 and Q2 journals, according to the Scimago Journal Rank. Moreover, and because there are several top-tier venues aligned with the research topics covered by CROSSCON, conferences will also be considered, e.g., *IEEE Symposium on Security and Privacy*, *Usenix Security Symposium*, etc. Nonetheless, to cope with project's KPIs and deadlines, it is important to consider that conferences are organized yearly and they have submission deadlines. Table 2 and Table 3 summarizes the identified conferences and journals that fit in the project goals and selection criteria, among the best, organized by their main scientific field. All CROSSCON partners have access to these lists on the project's online repository and can update them if other conferences and journals are considered good targets for publication.

As a practice enforced by the project, most new scientific contributions will be published following the Open Access (OA) principle. Thus, the selected conferences and scientific journals appropriately comply with the OA policy. To increase the accessibility of results, preprints versions of publications will be set available on well-known archives (e.g., arXiv.org). The remainder of this section identifies scientific and academic conferences, journals, and workshops, where the findings and results from the CROSSCON project can be published. This also includes conference participation and talks, participation and organization of workshops, when possible co-located with top-tier venues and events. By publishing in highly respected and prestigious conferences and journals, CROSSCON will be able to widely disseminate its research and contribute to the advancement of the fields of computer science and device security.

Table 2: Scientific/Academic Conferences.

Journals and Conferences				
Main Field	**Title**	**Acronym**	**Rank**	**Link**
Security	IEEE Symposium on Security and Privacy	IEEE S&P	A* (CORE2021)	https://sp2023.ieee-security.org/
Security	USENIX Security Symposium	USENIX-Security	A* (CORE2021)	https://www.usenix.org/conference/usenixsecurity23
Security	ACM Conference on Computer and Communications Security	ACM CCS	A* (CORE2021)	https://www.sigsac.org/ccs/CCS2023/
Security	Network and Distributed System Security Symposium	NDSS	A* (CORE2021)	https://www.ndss-symposium.org/
Security	ACM Asia Conference on Computer and Communications Security	ASIA CCS	A (CORE2021)	https://asiaccs2023.org/
Security	International Symposium on Research in Attacks, Intrusions and Defenses	RAID	A (CORE2021)	https://raid2023.org/welcome.html
Security	International Conference on Virtual Execution Environments	VEE	B (CORE2021)	https://conf.researchr.org/home/vee-2022

Security	International Conference on Information Security and Cryptography	SECRYPT	B (CORE2021)	https://secrypt.scitevents.org/
Main Field	**Title**	**Acronym**	**Rank**	**Link**
Systems	USENIX Symposium on Operating Systems Design and Implementation	USENIX OSDI	A* (CORE2021)	https://www.usenix.org/conference/osdi23
Systems	Architectural Support for Programming Languages and Operating Systems	ASPLOS	A* (CORE2021)	https://asplos-conference.org/
Systems	ACM SIGOPS Symposium on Operating Systems Principles	SOSP	A* (CORE2021)	https://sosp2023.mpi-sws.org/
Systems	Eurosys Conference	Eurosys	A (CORE2021)	https://2023.eurosys.org/
Systems	USENIX Annual Technical Conference	USENIX ATC	A (CORE2021)	https://www.usenix.org/conference/atc23
Computer Arch/FPGA	International Symposium on Computer Architecture	ISCA	A* (CORE2021)	https://iscaconf.org/isca2023/
Computer Arch/FPGA	ACM/SIGDA International Symposium on Field-Programmable Gate Arrays	FPGA	N/A	https://www.isfpga.org/
Real-time	IEEE Real-Time Systems Symposium	RTSS	A* (CORE2021)	http://2023.rtss.org/
Real-time	IEEE Real-Time and Embedded Technology and Applications Symposium	RTAS	A (CORE2021)	http://2023.rtas.org/
Real-time	Euromicro Conference on Real-Time Systems	ECRTS	A (CORE2021)	https://www.ecrts.org/
Real-time	IEEE International Conference on Embedded and Real-Time Computing Systems and Applications	RTCSA	B (CORE2021)	https://rtcsa.org/
Formal Methods	Computer Aided Verification	CAV	A* (CORE2021)	http://www.i-cav.org/2023/
Formal Methods	International Symposium on Formal Methods	FM	A (CORE2021)	https://fm2023.isp.uni-luebeck.de/

Formal Methods	Formal Methods in Computer-Aided Design	FMCAD	B (CORE2021)	https://fmcad.org/FMCAD23/
Misc	Design, Automation and Test in Europe Conference	DATE	B (CORE2021)	https://www.date-conference.com/
TBD	TBD	TBD	TBD	TBD

Table 3: Scientific Journals.

Scientific Journals			
Title	**Impact Factor**	**Quartiles * (from scimago)**	**Link**
IEEE Transactions on Dependable and Secure Computing	6.791	**Q1** - Computer Science (misc) **Q1** - Electrical and Electronic Engineering	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858
IEEE Security and Privacy	3.105	**Q1** - Computer Networks and Communications **Q1** - Electrical and Electronic Engineering	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
Computers and Security	5.105	**Q1** - Computer Science (misc)	https://www.sciencedirect.com/journal/computers-and-security
IEEE Transactions on Computers	3.183	**Q1** - Hardware and Architecture **Q1** - Software **Q1** - Theoretical Computer Science	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=12
IEEE Transactions on Information Forensics and Security	7.231	**Q1** - Computer Networks and Communications **Q1** - Safety, Risk, Reliability and Quality	https://signalprocessingsociety.org/publications-resources/ieee-transactions-information-forensics-and-security
Journal of Cybersecurity	N/A	**Q2** - Computer Networks and Communications **Q2** - Computer Science Applications **Q1** - Computer Science (miscellaneous) **Q2** - Hardware and Architecture **Q2** - Information Systems **Q2** - Software	https://academic.oup.com/cybersecurity
IEEE Transactions on Mobile Computing	6.075	**Q1** - Computer Networks and Communications **Q1** - Software **Q1** - Electrical and Electronic Engineering	https://www.computer.org/csdl/journal/tm

IEEE Transactions on Cybernetics	19.118	**Q1** - Computer Science Applications **Q1** - Human-Computer Interaction **Q1** - Information Systems **Q1** - Software **Q1** - Control and Systems Engineering **Q1** - Electrical and Electronic Engineering	https://www.ieeesmc.org/publications/transactions-on-cybernetics/
ACM Transactions on Embedded Computing Systems	N/A	**Q2** - Hardware and Architecture **Q2** - Software	https://dl.acm.org/journal/tecs
ACM Transactions on Cyber-Physical Systems	N/A	**Q1** - Computer Networks and Communications **Q2** - Hardware and Architecture **Q2** - Human-Computer Interaction	https://dl.acm.org/journal/tcps
IEEE Access	3.476	**Q1** - Computer Science (misc) **Q1** - Engineering (misc)	https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=6287639
Title	**Impact Factor**	**Quartiles * (from scimago)**	**Link**
Future Generation Computer Systems	N/A	**Q1** - Computer Networks and Communications **Q1** - Hardware and Architecture **Q1** - Software	https://www.sciencedirect.com/journal/future-generation-computer-systems
IEEE Embedded Systems Letters	1.524	**Q2** - Computer Science (misc)	https://ieee-ceda.org/publication/ieee-embedded-systems-letters-esl
IEEE Network	10.294	**Q1** - Computer Networks and Communications **Q1** - Hardware and Architecture **Q1** - Information Systems **Q1** - Software	https://www.comsoc.org/publications/magazines/ieee-network
Journal of Systems Architectures	N/A	**Q1** - Hardware and Architecture **Q1** - Software	https://www.sciencedirect.com/journal/journal-of-systems-architecture
IEEE Transactions on Cloud Computing	5.697	**Q1** - Computer Science Applications **Q1** - Hardware and Architecture **Q1** - Information Systems **Q1** - Software	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6245519
Formal Methods in System Design	N/A	**Q3** - Computer Science **Q3** - Hardware and Architecture **Q3** - Software	https://dl.acm.org/journal/fmsd

IEEE Internet of Things Journal	9.471	**Q1** - Computer Networks and Communications **Q1** -Computer Science Applications **Q1** -Hardware and Architecture **Q1** -Information Systems	https://ieee-iotj.org/
IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems	2.565	**Q1** - Computer Graphics and Computer-Aided Design **Q1** - Electrical and Electronic Engineering **Q1** - Software	https://ieee-ceda.org/publication/ieee-transactions-computer-aided-design-integrated-circuits-systems-tcad
TBD	TBD	TBD	TBD

3.3.2 Articles and White Papers

Project partners also participate in many different open-source communities, thus, they can serve as a springboard to potentially involve a large number of interested parties. Therefore, a set of recommendations and guidelines will be written in a form of white papers targeting not only scientific research agendas of such initiatives, but also policy makers.

To disseminate the project's proposal and goals, a first publication in a form of white paper will describe the key ideas of the project and how it will improve science towards building secure IoT devices. It will include the motivation, current state of the art and existing literature on the topic, the methods and techniques that will be used to perform research, the expected goals and outcomes, and the contribution to all stakeholders and users that will adopt CROSSCON. This white paper is the first step for the project dissemination, creating awareness of the CROSSCON benefits and interest from relevant target audiences. All artefacts are expected to be submitted for external peer-review and certification for venues that allow this high standard procedures.

3.3.3 Publication Procedures and guidelines

Throughout the development of the different tasks present in the Work Packages (WPs), it is expected that the project reaches a set of research findings with high levels of novelty and scientific impact, which will culminate in several publications around each task or sub-task deadlines. For a quick and efficient dissemination through publications, all partners must follow the guidelines defined by the European Commission (EC) regarding OA. Moreover, and concerning the CROSSCON project, when a partner intends to publish, all other consortium members must be notified about this intention, including the conference/journal, list of authors, title of the publication, subject areas, and an abstract for validation. This must be validated by UMINHO, who also checks if the appropriate KPIs are met. Every publication must include the project's acknowledgements, in conformity with EC guidelines [4].

CROSSCON acknowledgements:

"This paper is supported by European Union's Horizon Europe research and innovation programme under grant agreement No 101070537, project CROSSCON (Cross-platform Open Security Stack for Connected Devices)."

3.4 Workshops and Industry-related events

CROSSCON members will be actively seeking out events that align with the research areas and impact goals. Since some workshops are co-located with relevant conferences, e.g., the 6th Computer Architecture Research with RISC-V (CARRV 2022) workshop was co-located with ISCA 2022, and SafeThings 2022 was included in the 43rd IEEE Symposium on Security and Privacy (S&P) 2022, the consortium must be actively monitoring and selecting conferences to participate in. Additionally, it is

important to mention that the consortium may organize their own workshops or other type of events when it is more suitable for the project needs. Since CROSSCON also targets partners in different industries related to the project, it is also important to participate in industry-related events. Table 4 summarizes top-level industry-related events that best suit the project interests and exploitation-driven goals.

Table 4: Industry-related Events.

Industry-related Events			
Title	**Description**	**Type**	**Link**
Embedded World	The embedded world Exhibition & Conference provides a global platform and a place to meet for the entire embedded community, including leading experts, key players and industry associations.	Exhibition Fair, Conference	https://www.embedded-world.de/en
HiPEAC	HiPEAC is a European research network for embedded systems and high-performance computing. It brings together researchers, industry and policymakers to collaborate on research and promote new technologies through workshops, training and conferences.	Workshops, Conference	https://www.hipeac.net/
RISC-V Summit	The RISC-V Summit is an annual event discussing the latest developments in the RISC-V instruction set architecture and its ecosystem, featuring technical presentations, panel discussions, workshops and companies showcasing their RISC-V related products and services.	Exhibition Fair, Conference	https://events.linuxfoundation.org/riscv-summit/
Black Hat	Black Hat is an internationally recognized cybersecurity event series providing the most technical and relevant information security research.	Summits, Webinars, Trainings	https://www.blackhat.com/upcoming.html
TBD	TBD	TBD	TBD

3.5 Event participation and organization

As a matter of fact, despite this initial dissemination and communication plan being written in month M3, consortium members have already participated in events related to CROSSCON. Table 5 summarizes some past and future events that are currently being planned by the consortium for participation, while Table 6 shows the events that are going to be organized by CROSSCON. Further updates and upcoming events must be update periodically in the shared list available on the private CROSSCON online repository. The report of these past and future events will be done in the future deliverables D6.4 and D6.6.

Table 5: Event Participation.

Type	Subject Area	Event	Location	Date	Speaker(s)
TALK	RISC-V Virtualization Tutorial	RISC-V Summit 20022	San Jose, CA, USA	12-15 December 2022	Sandro Pinto (UMINHO)
TALK	PhD School	NECS - PHD WINTER SCHOOL 2023	Vason, Trento, Italy	6-10 February 2023	Sandro Pinto (UMINHO) Ahmad-Reza Sadeghi (TUD) Alexandra Dmitrienko (WURZBURG)
TALK	Virtualization Today, Virtualization Tomorrow: Problems, Challenges, and Opportunities for Mixed-Criticality Systems	Embedded World 2023	Nuremberg, Germany	14-16 March 2023	Sandro Pinto (UMINHO)

CROSSCON partners plan to organise summer/winter schools that will contain courses covering the topics of the project. For each school, speakers will prepare lecture notes, which will be available online on the project website. The school will consist of frontal lectures of academics and domain experts, teamwork, tutoring, and a socializing event. The researchers of the CROSSCON, both from academia as well as from industry, will be encouraged to participate as lecturers in these schools. The schools will be also open to other young researchers to maximize the possible impact and dissemination of knowledge in the scientific community. Alongside with the school, CROSSCON will also organise clustering events with other related HE research projects with the aim of creating synergies and enhancing the dissemination impact of every single project. The expected KPI for the event organization is 1 school per year.

Table 6: Event organization.

Type	Subject(s)	Event	Location	Date	Organizer
PhD School	cyber-security	NECS - PHD WINTER SCHOOL 2023[1]	Vason, Trento, Italy	6-10 February 2023	UNITN
TBD	TBD	TBD	TBD	TBD	TBD

3.6 Other dissemination channels

To inform the public about the activities, services, product information, strategies, opportunities, or information about an industry or organization, CROSSCON will also disseminate project information though brochures and face-to-face activities, e.g., interviews. In addition to our efforts to increase awareness of CROSSCON through various communication channels and innovation activities, we will also work to increase visibility for women in cybersecurity. This will involve collaborations with the Women4Cyber Foundation and the inclusion of interviews with women working on the project. Atos and other consortium members have already established a strong partnership with the Women4Cyber Foundation.

To explain the results of the project also to non-experts, for each tool, implementation and paper made publicly available, a short video explaining the high-level goals and purpose of CROSSCON may be

[1] https://necs-winterschool.disi.unitn.it/

produced and published on YouTube and project website. These videos should be suited to the interested layman and will be made available through project's online channels.

4 Key Performance Indicators (KPIs)

To measure the effectiveness of CROSSCON's dissemination and communication strategies, several Key Performance Indicators (KPIs) have been established in the proposal and will be revised throughout the project's lifespan. It should be noted that these measures do not directly assess the outcomes of the project, but rather reflect common and recognized practices for disseminating research results and achieving impact. All actions included in the dissemination plan shown in Table 7 are aimed at maximizing project results' impact and are linked to measuring KPIs in M18 and M36.

The main dissemination activities focus on peer-reviewed papers publication in highly relevant venues, summarized in Table 2 and Table 3, promoting OA publications, workshops organized by the project, as well several training activities including winter/summer schools. After the first KPI assessment in the month M18, appropriate actions and readjustment of the initial dissemination plan can take place, in case that gaps are detected.

Table 7: KPIs for the dissemination plan activities.

Dissemination activity - KPI description	KPI Target M18	KPI Target M36
Scientific publication	>= 6 journals and 10 papers	>= 16 journals and 32 papers
Open-access publication (journals)	>= 75%	
Impact factor journals	Q1 and Q2 in Scimago JCR	
Ranking of conferences	Scopus and Web of Science indexed	
Number of workshops attended/organized	>= 10/1	>= 30/3
Winter/Summer schools	1	3
Other training events (courses, webinars)	>=5	>=10
Liaison with projects	>=5	>=15
White papers	>=1	>=4
Demonstrators	0	>=4

In addition, the CROSSCON project also identified a well-defined set of communication actions aimed at maximizing the promotion of the project activities and results to multiple audiences (e.g., citizens, media, other stakeholders, etc.). Unlike the dissemination actions proposed in the dissemination plan, communication actions need to engage with a larger group of stakeholders, generate and fuel market demand, attract best experts and also show the success of EU collaboration. Consequently, Table 8 illustrates the set of communication actions along with the proper channel proposed to reach out to the specific target audience and the KPIs defined to measure a successful achievement and quantify the expected benefits. Unlike the previous monitoring of KPIs that is envisaged twice in the project, communication KPIs should be monitored regularly (monthly) in order to take appropriate correction actions as early as possible.

Table 8: KPIs for the communication actions.

Type of communication action	Format/channel	KPI	Target audience	Month
Create a community of twitter and LinkedIn users	Social media (Twitter, LinkedIn)	3000 followers	SC, I	M3
Foster online visibility of the consortium/project	Website	200 visits/month	GP	Monthly
	Blog	24 entries	GP	M36
Elevator pitch to brief the project to a wide audience (e.g., motion graphics animation and infographics)	Animation (e.g., YouTube)	1000 views	GP	M6
	Brochure (events, science fairs)	500 shares	GP	M6
Online press release	Website	3 PRs	GP, I, G	M24
Interact with companies interested in adopting the CROSSCON platform	Social media, newsletter	50 industrial feedbacks	I	Quarterly

5 Conclusions

This deliverable, *D6.2 Dissemination and Communication Plan* is part of task T6.1 – *Dissemination and Communication,* included in the WP6. A clear communication and dissemination strategy is one of the most important pre-requisites in order to make dissemination and communication plan, to start executing specific actions project impact goals. It helps not only in maximizing the impact and visibility of the CROSSCON project, but also drives its adoption. To ensure smooth and efficient execution of communication and dissemination actions, CROSSCON strategy includes the segmentation of specific target groups, that are identified and described in this deliverable, which aims at improving the match between the most suitable dissemination and communication channel and information to be presented to the specific target audience segment. For this purpose, the project uses different channels such as the project's website, social media, printed materials, meetings and events, etc.

The main dissemination actions include scientific publications in top-tier journals and venues, workshops and talks, and the participation in scientific and industrial events. The monitoring and evaluation of these actions are based on a set of KPIs that can help in evaluating the success and suitability of different actions and efforts spent. Similar holds for the community actions, with a well-defined set of KPIs and plans for its monitoring.

Therefore, the CROSSCON consortium will regularly analyse and update as needed the current dissemination and communication plan, taking actions when required. The detailed report of actions outlined in this plan and eventual update of this initial plan will be presented in the next report, *D6.4 - Dissemination, Communication and Community Building First Report,* scheduled to be released during the first half of the project (M18).

References

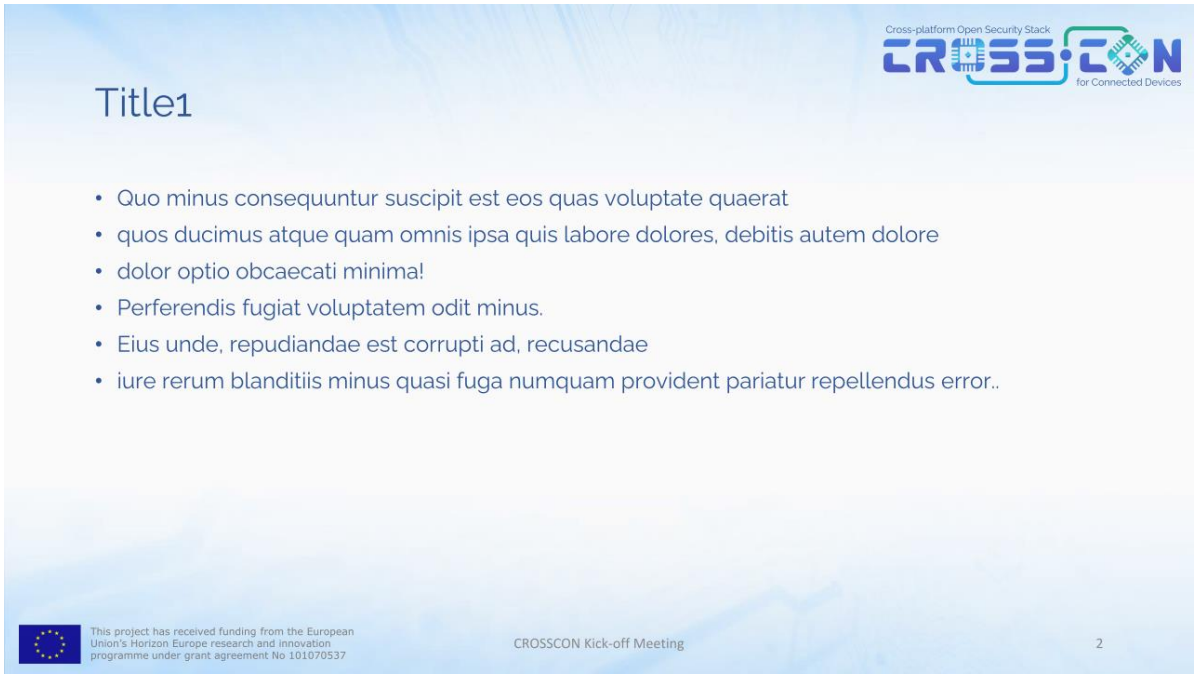
[1] European Commission (EC). "*Funding & Tender Opportunities - Support (FAQ)*". https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq/933, retrieved 2023-01-06)

[2] Grant Agreement, Number - 101070537, CROSSCON 2022

[3] A. Pasic (2023), D6.1 Project Website. Deliverable of the CROSSCON project.

[4] European Research Executive Agency (REA). "Communicating about your EU-funded project". https://rea.ec.europa.eu/communicating-about-your-eu-funded-project_en, retrieved 2023-01-27)

Annex I - PowerPoint Presentation Template



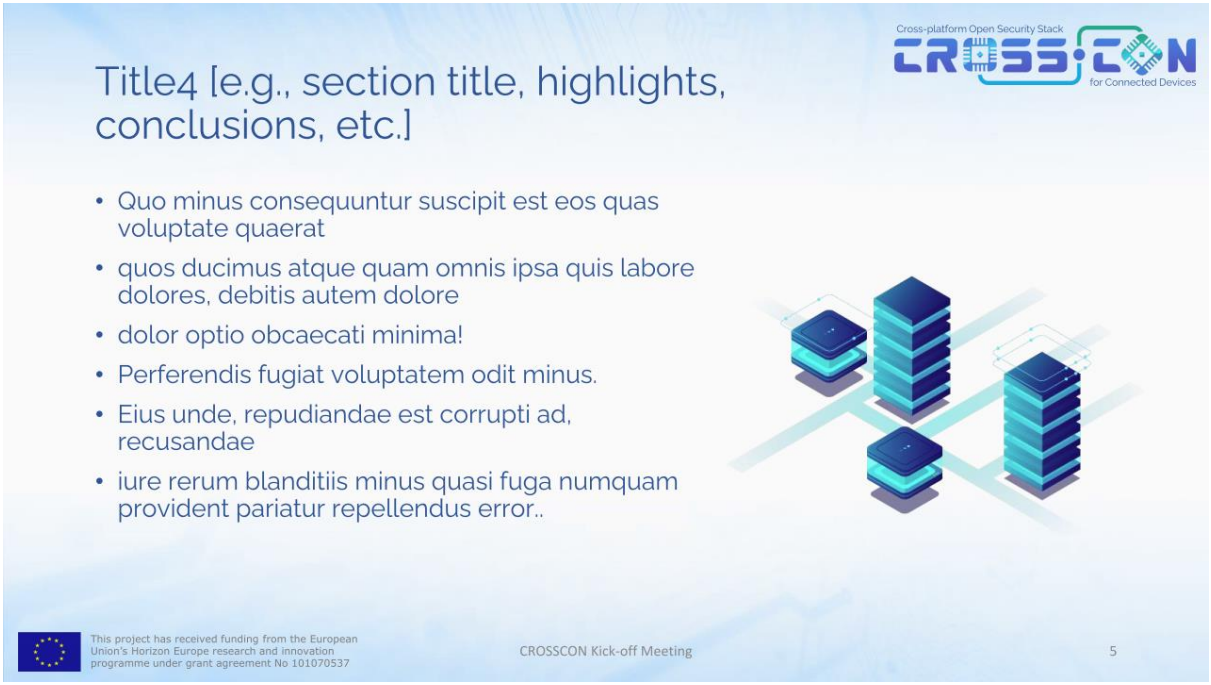


Figure 1: PowerPoint template for CROSSCON presentations.