Ref. Ares(2024)3182168 - 30/04/2024

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

D6.4 Dissemination, Communication and Community Building First Report

Document Identification			
Status	Final	**Due Date**	30/04/2024
Version	1.0	**Submission Date**	30/04/2024

Related WP	WP6	**Document Reference**	D6.4
Related Deliverable(s)	D6.1, D6.2	**Dissemination Level (*)**	PU
Lead Participant	UMINHO	**Lead Author**	Tiago Gomes
Contributors	UMINHO	**Reviewers**	ATOS
			UNITN

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.
The dissemination of this document reflects only the author's view, and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.
This document and its content are the property of the CROSSCON Consortium. The content of all or parts of this document can be used and distributed provided that the CROSSCON project and the document are properly referenced.
Each CROSSCON Partner may use this document in conformity with the CROSSCON Consortium Grant Agreement provisions.

(*) Dissemination level: **(PU)** Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page). **(SEN)** Sensitive, limited under the conditions of the Grant Agreement. **(Classified EU-R)** EU RESTRICTED under the Commission Decision No2015/444. **(Classified EU-C)** EU CONFIDENTIAL under the Commission Decision No2015/444. **(Classified EU-S)** EU SECRET under the Commission Decision No2015/444.

Document Information

List of Contributors	
Name	Partner
Tiago Gomes	UMINHO
João Sousa	UMINHO
Luís Cunha	UMINHO

Document History			
Version	Date	Change editors	Changes
0.1	23/01/2024	João Sousa (UMINHO)	Draft version / TOC
0.2	20/04/2024	Tiago Gomes, João Sousa, Luís Cunha (UMINHO)	Ready for Internal Review
0.3	22/04/2024	Tiago Gomes, João Sousa, Luís Cunha (UMINHO)	Ready for Review
0.4	24/04/2024	Tiago Gomes, João Sousa, Luís Cunha (UMINHO)	First Draft after first Review
0.5	27/04/2024	Tiago Gomes, João Sousa, Luís Cunha (UMINHO)	Second Draft after second Review
0.6	29/04/2024	Tiago Gomes, João Sousa, Luís Cunha (UMINHO)	Final Version ready for QA
0.9	29/04/2024	Juan Alonso (ATOS)	Quality Assessment
1.0	30/04/2024	Hristo Koshutanski (ATOS)	Final version submitted

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tiago Gomes (UMINHO)	22/04/2024
Quality manager	Juan Andres Alonso (ATOS)	29/04/2024
Project Coordinator	Hristo Koshutanski (ATOS)	30/04/2024

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CROSSCON	Cross-platform Open Security Stack for Connected Devices
D6.2	Deliverable number 2 from Work Package 6
EC	European Commission
EU	European Union
IoT	Internet of Things
KPI	Key Performance Indicator
PC	Project Coordinator
TEE	Trusted Execution Environment
WP	Work Package

Executive Summary

This report includes the diverse dissemination and communication efforts conducted by the CROSSCON project and all partners, aligned with the dissemination and communication strategy and plan outlined in D6.2, spanning from January (M3) to April 2024 (M18). All the performed activities represent a step forward in disseminating and positioning CROSSCON as an innovative project that offers, among other results, a security stack that can run on a wide range of heterogeneous IoT devices.

We have been using appropriate general channels to reach the broad target audience and communicate value proposition, as well as specific means and messages for more focused target audiences. Following the strategy set in D6.2, dissemination efforts also include the publishing of scientific papers and participation in conferences. On the other hand, communication activities involve establishing and managing digital channels to convey progress to external audiences and creating relevant content in different formats.

The highlights in the period covered by the report include:

- **Website:** 4.3K established sessions, 7.6K page views, 3.2K different users.
- **Social media:** 500+ followers, 8K impressions (5K on Twitter and 3K on LinkedIn), 369 interactions (238 on Twitter and 131 on LinkedIn).
- **Communication Material:** 2 YouTube Videos, 2 Brochures, 1 Press Release, 2 Newsletters, 1 General Presentation and 11 Blog Posts, at least 2 Media Hits.
- **Dissemination Material:** 2 journals, 10 conferences, 1 white paper, 11/4 Workshops attended/organized, 4 winter/summer schools, 19 other training courses.

As a result of these initiatives, we've gathered comprehensive feedback from over 50 industrial and academic sources. This invaluable input has enabled us to finely tune our messaging, strategically position our outcomes, correct any technical misdirection, and ensure alignment with relevant policies. This iterative process of engagement has not only enhanced the clarity and impact of our work but also fostered stronger partnerships within the broader security IoT community.

The information in this document, and the project's dissemination and communication approach in general, will be continuously reassessed and iterated throughout the project's execution. A final version of this report will be provided during M36 through D6.6 - Dissemination, Communication and Community Building - Final Report.

1 Introduction

1.1 Purpose of the Document

Reporting all dissemination/communication activities helps in assessing the project's impact by tracking how the information is received and absorbed by different audiences [1]. Additionally, since this is a public report, it provides transparency about the findings, results, and progress of the project among all stakeholders.

This document presents the first report on the dissemination, communication, and community building, describing all actions adopted by CROSSCON during the first half of the project (M18). It includes the website statistics, the monitoring of the communication tools and social media channels, publications, attended and organised conferences, and training activities report. All these actions are part of task T6.1 - *Dissemination and Communication* of WP6.

1.2 Relation to Other Project Work

The deliverable D6.4 Dissemination, Communication and Community Plan has the main goal of reporting the dissemination and communication, stakeholders' engagement, advisory board, and training activities for the first half of the project. The D6.4 belongs to the WP6, and it is related to following deliverables:

- **D6.1 *Project Website* [2]**. Which presents a report on the project website, including the layout, structure, and content management.
- **D6.2 *Dissemination and Communication Plan* [3].** Which defines the strategy and plan of actions for the dissemination and communication activities. These activities aim to raise awareness about the CROSSCON project towards different target groups.
- **D6.6 *Dissemination, Communication and Community Building - Final Report*.** That 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** - Summarizes the dissemination and communication strategy and planning updates.
- **Chapter 3 -** Describes the dissemination and communication actions.
- **Chapter 4** - Describes the Community Building activities.
- **Chapter 5** - Discusses the Key Performance Indicators (KPIs) defined for the dissemination and communication actions.
- **Chapter 6** - Concludes this document.

2 Strategy and Planning Updates

This chapter provides updates regarding the dissemination and communication plan specified in the deliverable D6.2. It summarises all changes since January 2023 (M3) and April 2024 (M18). Overall, since M3, CROSSCON communication and dissemination changes encompasses: (i) the social media updates, i.e., Twitter (rebranded as X) and YouTube; (ii) other dissemination and communication resources; and (iii) the website layout updates.

2.1 Target Audiences and Objectives

We targeted various communities, including researchers, industry professionals, and policymakers. Communities and ecosystems (such as RISC-V) have served as springboards for engaging a wide range of interested parties. Additionally, an Advisory Board was utilized for disseminating information and communicating with different stakeholders.

The primary objectives of these dissemination and communication activities in the first half of the project were to raise awareness of the project's activities and its innovation potential. Examples of these generic and starting actions include press releases and establishing a web presence. During the first half of the project duration, it was important for the CROSSCON project to position itself at the intersection of cybersecurity, IoT, and open-source hardware communities. This was achieved by collaborating with related and relevant EU projects, including participation in clustering activities (e.g., Encrypt-Clustering Workshop, SENTINEL Cluster Meeting or CTI event). Additionally, training activities, including winter schools, have been utilized to attract a younger audience from the scientific community.

In the second part of the project, we believe that communication activities should shift from project-oriented to result-oriented, as the project results will be more mature. To this end, a series of blogs published on the website have already adopted this approach, focusing more on technology or solution-centric content. Moreover, we plan to hold more workshops and events targeting industry stakeholders. We intend to fine-tune messages and prepare elevator pitches through which the value proposition of CROSSCON can be communicated in a more direct and understandable manner.

2.2 Social Media Channels

Regarding changes in social media channels, CROSSCON created the YouTube account at month M6 where the first video was published at M7, achieving a total of 21 views and 2 likes. Figure 1 demonstrates the home page of CROSSCON YouTube account. Furthermore, Twitter is now rebranded as X. In the rest of the document, we refer to it as Twitter/X.

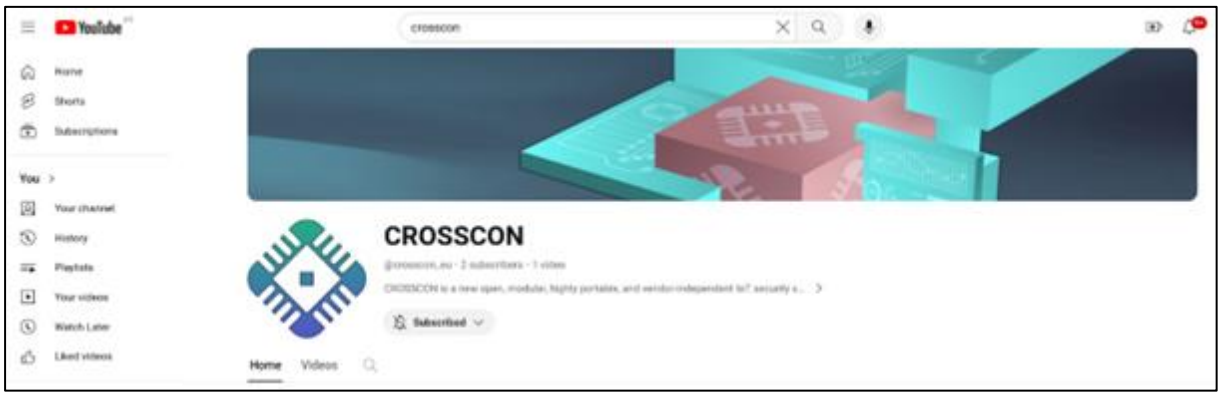


Figure 1: CROSSCON YouTube homepage.

In addition to addressing changes in social media channels, T6.1 uses other dissemination and communication materials, such as press releases, blog posts, media hits, newsletters, and presentations to both general and more specialized audiences. All this content were considered and reported as part of Section 3.6 of this document.

Overall, the production of this material was essential to achieve the results outlined in Section 3. While the majority of the materials were of high quality and achieved good results, some fell short of expectations. As a strategy for improvement, we believe that enhanced engagement can be achieved, for instance, by creating more posts featuring animated content or providing detailed descriptions of our achieved results on social media. This approach has the potential to significantly boost social media engagement, consequently enhancing the effectiveness of all used channels.

2.3 Website Updates

The project's website, as detailed in previous deliverables D6.1 and D6.2, serves as a key platform for reporting information about CROSSCON activities, both to stakeholders and the general audience. The goal is to provide a user-friendly design that allows the target audience to remain updated and actively engaged with CROSSCON's activities and results.

During the last months, the project's website structure has faced slight changes to facilitate its navigation and overall organization. Currently, the menu bar contains different sections, as detailed in Figure 2. It includes: an (i) **About** section, which specifies general information about the project, e.g., objectives, use cases, and partners' information; (ii) **News&Events**, which reports all activities that CROSSCON was involved with; (iii) **Resources** section, which includes submitted deliverables, some publications referring the project and all other necessary dissemination material; and (iv) **External Synergies**, which reports advisory board and other European projects that create synergies with CROSSCON.

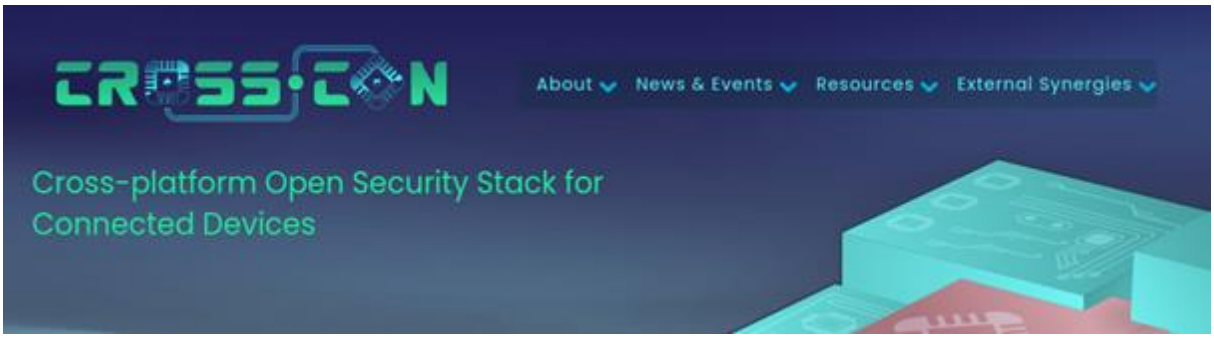


Figure 2: CROSSCON Website modified homepage.

This report will be continuously updated until the end of the project (M36) and will use the following channel groups to analyse the sources of website's visitors:

- **Direct** - users that visit the CROSSCON website through the URL directly.
- **Organic Search** - users that visit the CROSSCON website using search engine results.
- **Referral** - users that visit the CROSSCON website from other websites.
- **Organic Social** - users that visit the CROSSCON website using social media referrals.
- **Unassigned** - users that visit the CROSSCON website through uncategorized sources.

3 Dissemination and Communication Activity Report

This chapter provides the CROSSCON dissemination and communication report of all activities performed during M1 to M18, reporting the (i) project's website and social media engagement; (ii) templates of material used to disseminate CROSSCON; (iii) the attended and organized conferences; (iv) the scientific publications; and all (v) other material used for the dissemination of the CROSSCON.

3.1 CROSSCON Website

The website analytics serve as valuable tool for assessing the overall user engagement. The present analytics report includes: (i) the number of views per menu bar section; (ii) the number of views per country; (iii) the sources of website visitors; and (iv) the traffic acquisition during the last months.

3.1.1 CROSSCON Website: Views per Section

Monitoring views of sections in the Website menu bar provides valuable insights into which sections are most popular among CROSSCON website visitors, helping us understand user preferences and interests. Based on collected data, CROSSCON can optimize the website's content strategy by focusing on the sections that receive the most views, or by improving less-visited sections to increase engagement. Table 1 summarises the user's interaction with each section in the menu bar.

The "homepage" is the most visited section, which is easy to explain since it is the first page users find when visiting the website. To improve the visibility of less visited sections, some future CROSSCON publications can be propagated through social media channels, including reference links that redirect people to these website sections.

Table 1: Views per section in menu bar of the CROSSCON website.

Page Tittle and screen class	Views	Users	Views per user
CROSSCON-Platforms Open Security Stack for Connected Devices	1587	1105	1.44%
Blog	317	149	2.13%
Publications	317	161	1.97%
News	281	107	2.63%
Related Projects	241	131	1.84%
Use Cases	240	107	2.24%
Events	236	108	2.19%
Dissemination Material	235	94	2.5%
Consortium	207	151	1.37%

3.1.2 CROSSCON Website: Views per Country

Figure 3 summarises the user's interaction by showing their country's location. Monitoring the website statistics provides valuable insights into the effectiveness of marketing initiatives in different regions. By looking at the world's heatmap we can conclude that news of the CROSSCON project has already spread to all continents. Given the data results, Portugal (with a total of 542) and Madrid (with a total of 317) are the country and city with more visits to the CROSSCON website, respectively.

COUNTRY	USERS	TOWN/CITY	USERS
Portugal	542	Madrid	317
Spain	411	Braga	226
Germany	355	Amsterdam	87
Italy	278	Helsinki	82
United States	275	Guimaraes	73
Poland	171	Athens	72
Switzerland	136	Gdansk	72

Figure 3: Website Traffic by country.

3.1.3 CROSSCON Website: Sources of Website Viewers

The default channel grouping classifies incoming website traffic into distinct categories, allowing us to analyse the sources of website visitors. As mentioned before, these predefined channel grouping include Direct, Organic Search, Referral, Organic Social, and Unassigned users.

Observing Figure 4, results show that **Direct** channel groups establish significantly more sessions than the other channels. More specifically, on the CROSSCON website, a total of 2.9K direct sessions were established, which could be justified by the user-friendly website domain. Since the URL for the website contains the name of the project and the ".eu" domain (usually used in other European projects), it is considered a predictable URL to search for. On the other hand, the **Unassigned** is the channel group with the least number of established sessions. These users accessed the website trough, for example, the QR code.

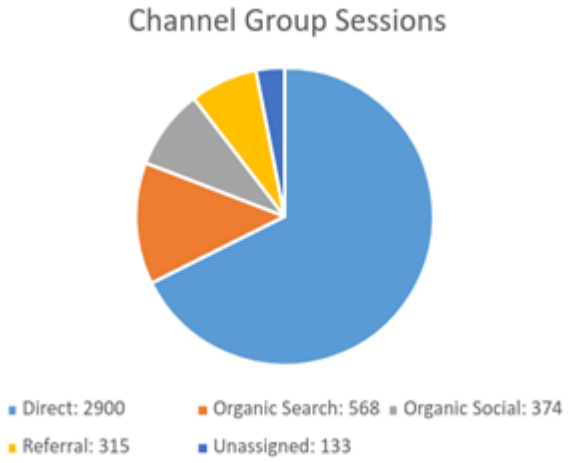


Figure 4: Channel Group Sessions of the CROSSCON Website.

3.1.4 CROSSCON Website: Traffic Interaction

Figure 5 depicts a graphic showing the percentage of visitors' interactions with the CROSSCON website since January 1st, related to a total of 3.4K users. Results show interaction in all months of the project, achieving maximum percentage, more than 60%, near the current date. This could be justified by the second newsletter released in M17. Another possible justification could be the presence of project members on several conferences in these last months of the project.

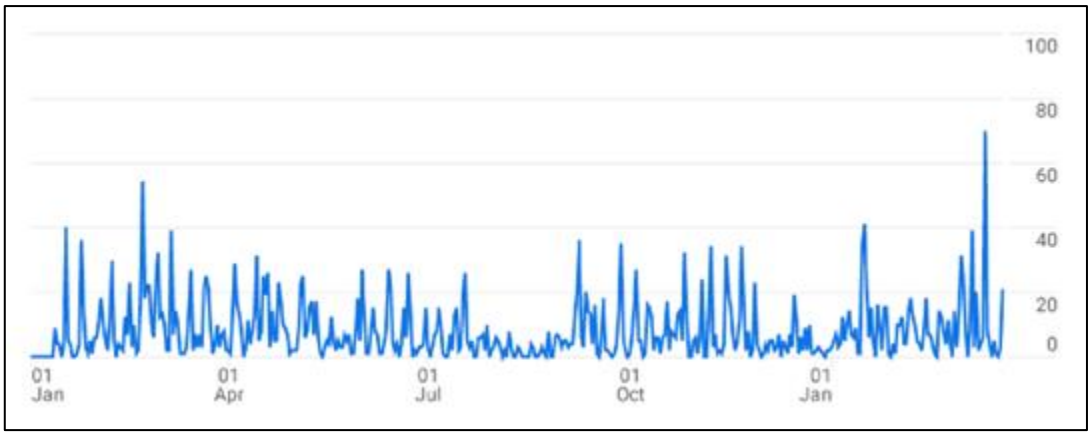


Figure 5: Traffic interaction of the CROSSCON website.

3.2 Social Media Channels

To reach the various target audiences and stakeholders, the social media channels represent a perfect tool to boost communication activities and share the work and progress of the project. In previous deliverables CROSSCON planned to use Twitter/X, LinkedIn, and YouTube. This section aims to report their impact on the project by summarizing user interactions, such as the number of followers, number of reposts in each month, etc.

To sustain audience interest and foster community growth among our intended targets, CROSSCON establishes appropriate practices for publishing content on social media. Some practices include the use of attractive banners, visuals, and emojis to increase engagement rate, actively encourage CROSSCON followers to participate in various events, interacting with stakeholders by mentioning them on posts, and using relevant hashtags to expand our scope within pertinent topics aligned with CROSSCON.

In addition to the project's official channel accounts for sharing information about the project and engaging with target audiences and potential end-users, CROSSCON has been referenced by content posted in other accounts. This 3rd-party account behaviour has a significant impact on the creation of synergies with other projects and specialised communities. As a result, there are more people engaging to project workshops or other events.

3.2.1 Twitter/X

Since the last deliverable, the project's Twitter/X account counts a total of 70 followers and 39 posts. Figure 6 illustrates the CROSSCON's Twitter/X profile, while Figure 7 illustrates the impressions generated over the last months in the Twitter social network Twitter/X. The months of May (776 views) and June (2084 views) of 2023 collected the highest number of impressions. These impressions are mainly justified with the presence of CROSSCON in the RISC-V Summit conference, which took place during the month of June. The CROSSCON project's participation in this innovative event significantly enhanced its impact, particularly through collaboration with the RISC-V community, which attracted increased attention and engagement. Notwithstanding, the months of August and December present a low number of impressions, justified by fewer social media publications.

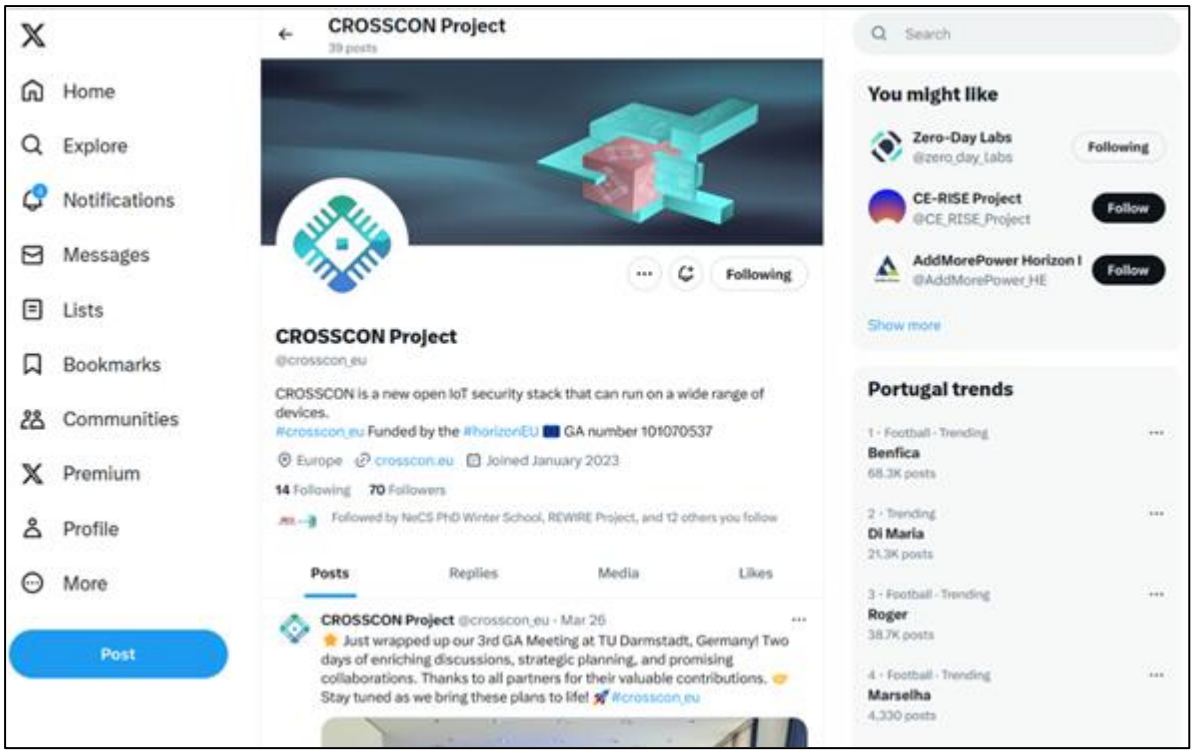


Figure 6: CROSSCON Twitter/X homepage.

As expected, the likes and retweets closely align with the results depicted in Figure 8. A cumulative total of 238 interactions were collected, comprising 87 retweets, which expanded our reach and amplified the impact of tweets. Additionally, the posts achieved 151 likes, indicating the perceived value of the shared content.

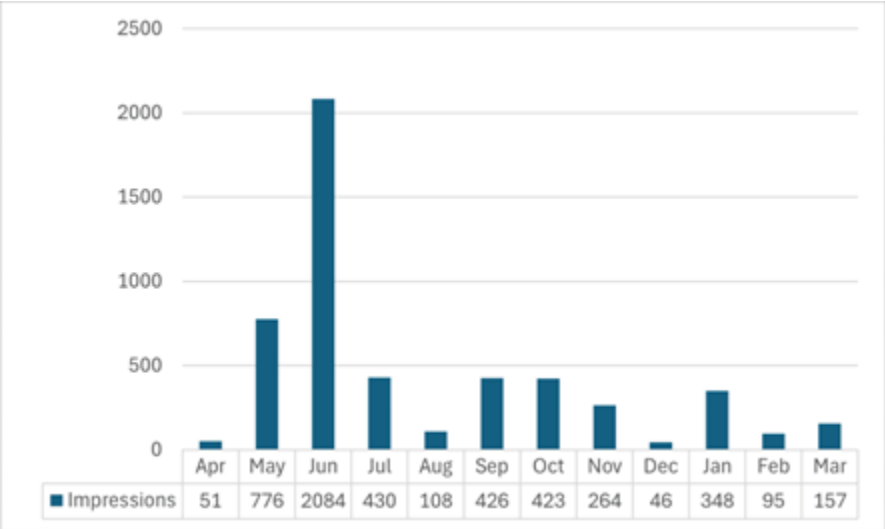


Figure 7: CROSSCON Twitter/X) impressions.

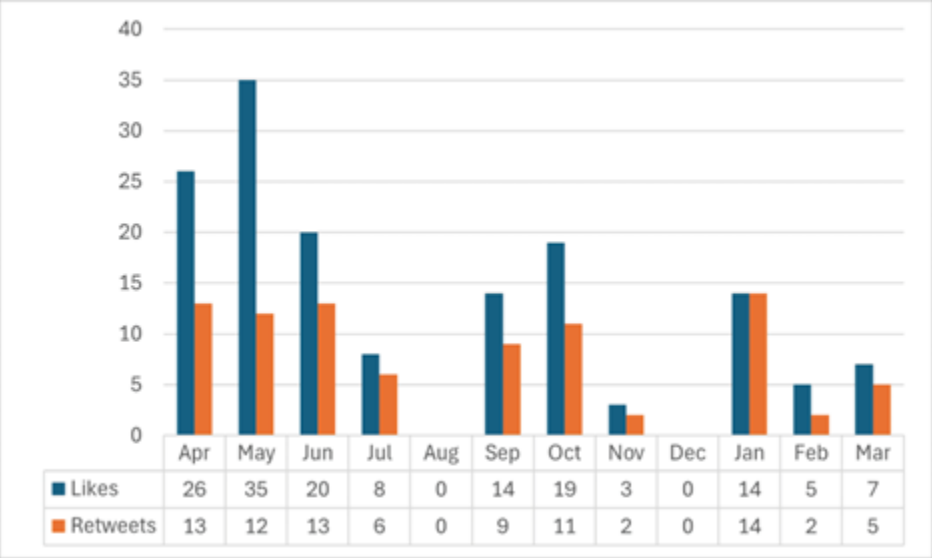


Figure 8: CROSSCON Twitter/X interactions.

Regardless of the number of original tweets or content retweeted on the CROSSCON account, the number of followers increased with a constant pace until reaching 72 followers by the end of September, as depicted in the following Figure 9. The target set by the end of the project is a total of 3000 followers (among all social media), and we have reached 72 in 1 year. This low number of followers can be related to the current phase of the project, where the implementation of core components (developed in Work Packages 3 and 4) are currently in progress and will only be available at the end of M18, April 2024.

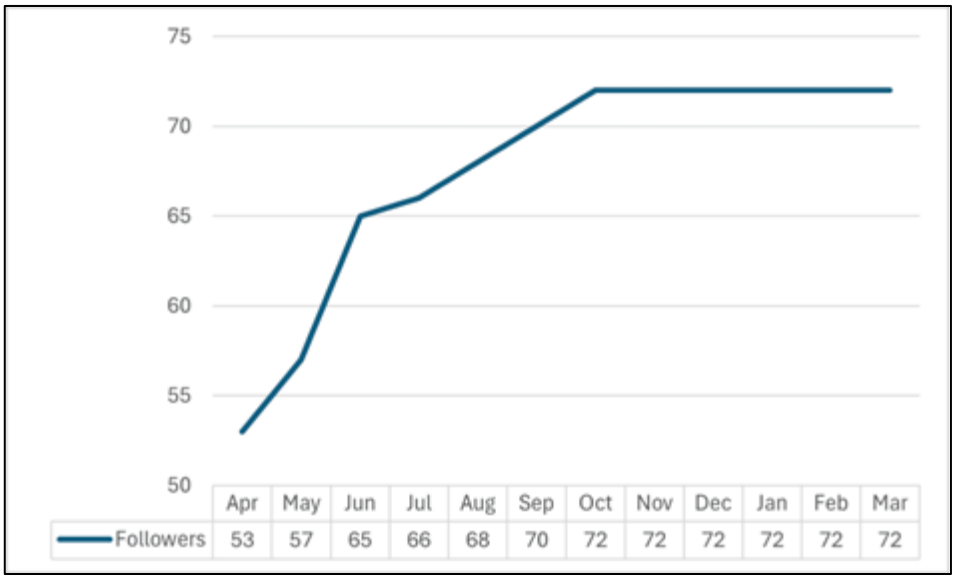


Figure 9: CROSSCON Twitter/X followers.

3.2.2 LinkedIn

While Twitter/X network caters to a broader range of interests and demographics, LinkedIn focuses on a professional and business-oriented audience, aiming to deliver content that is both informative and relevant to career development and industry insights. The following Figure 10 shows the main LinkedIn page, demonstrating a total of 173 connections.

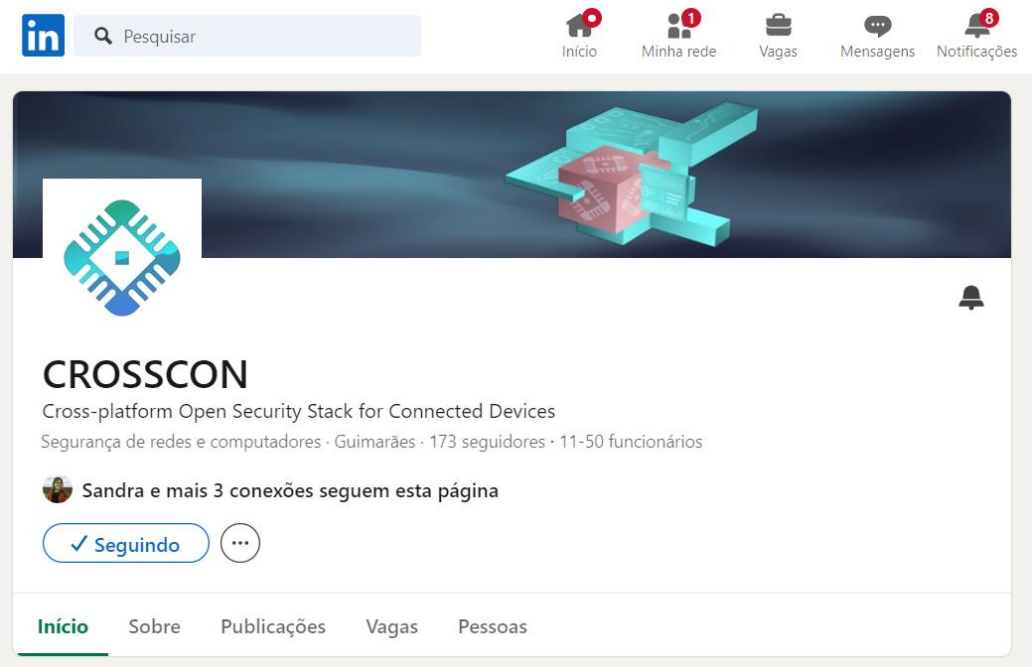


Figure 10: CROSSCON LinkedIn homepage.

Figure 11 illustrates the impressions generated over the last months in LinkedIn. October of 2023 (789 views) and March of 2024 (654 views) appear as the months with the highest number of impressions. These impressions are mainly justified with the CROSSCON GA meeting events, which took place during the months of October and March. At these in-person events, posts on social media related to significant milestones in the CROSSCON project were published. Because this type of content tends to be more engaging, the higher number of views is understandable. Notwithstanding, the month of December presents a low number of impressions, justified by the lack of social media publications. As expected, the likes closely align with the results depicted in Figure 12. A cumulative total of 131 likes were acquired, which expanded our reach and amplified the impact of our publications.

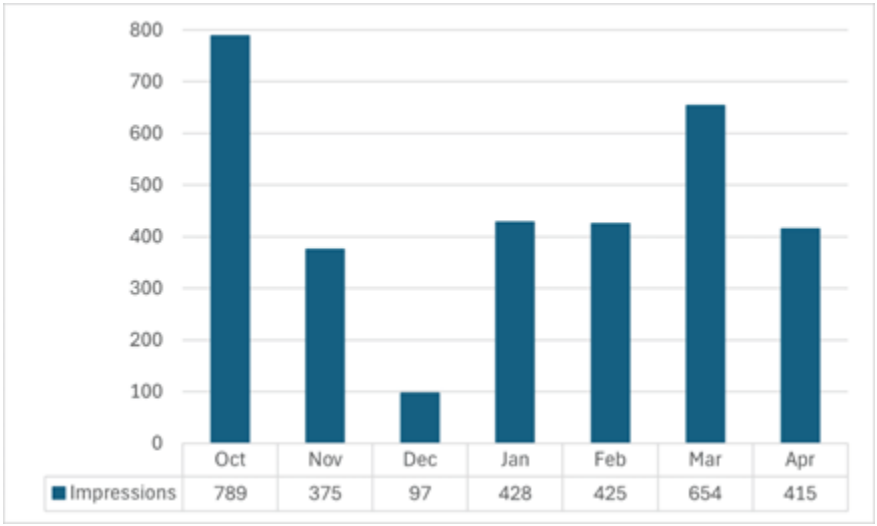


Figure 11: CROSSCON LinkedIn impressions.

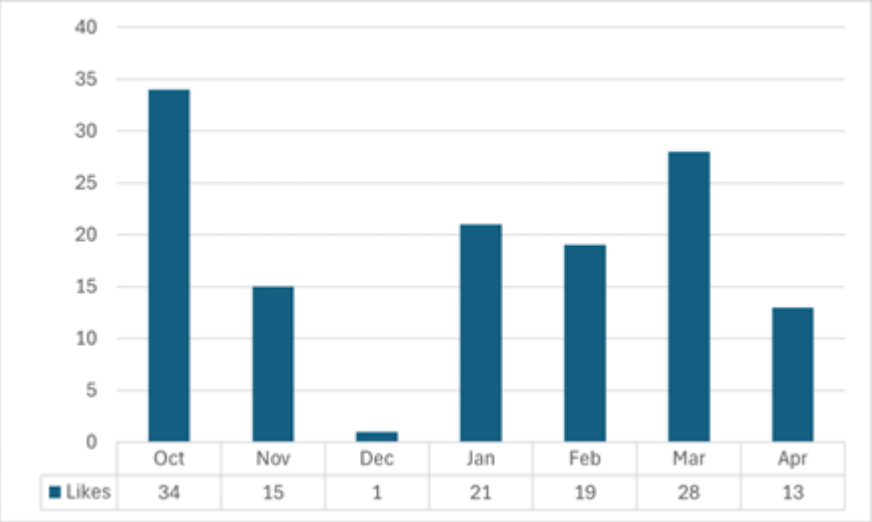


Figure 12: CROSSCON LinkedIn interactions.

Regardless of the number of original publications on the CROSSCON LinkedIn profile, the number of followers increased with a constant pace until reaching 172 followers in April, as depicted in the following Figure 13. The target set by the end of the project was 3000, and we have reached 172 in 1 year. For the same reasons as with Twitter, this low number of followers can be associated to the current phase of the project.

Additionally, to the "CROSSCON Project", the business page profile "CROSSCON" LinkedIn page reached a total number of 245 followers. These two profiles allow for a more dynamic way to reach more audiences. Nonetheless, the main account "CROSSCON" is the one that posts the updates, being the main page for interaction and the one we tracked the previous metrics.

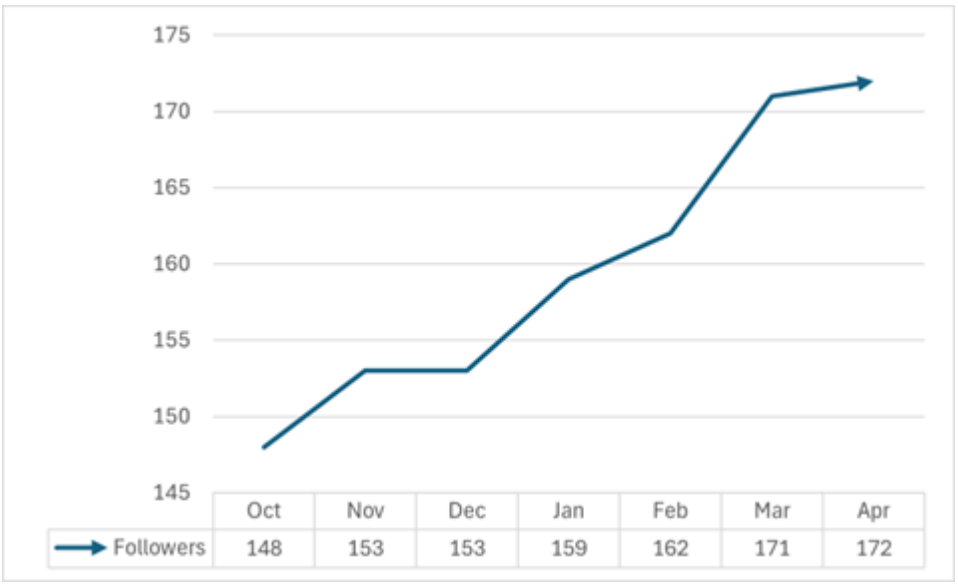


Figure 13: Number of followers of CROSSCON business LinkedIn account.

3.2.3 YouTube

An additional form to propagate content is through YouTube videos. The CROSSCON YouTube page intends to disseminate content like virtual sessions, interviews, demos, UC's tests videos. Currently, the project contains two related videos, one introducing CROSSCON (link) and other presenting the first training session organised and hosted by CROSSCON and the Bao Project's team, the "Hello Bao World - Virtual Workshop" (link).

In the YouTube video illustrated by Figure 14, CROSSCON announced to the community the project details, the UCs definition, and partners involved. Since the date of publication, this video has achieved

a total of 21 views and 2 likes. Since the YouTube community usually searches for tutorials, demos, or any other video activities, this type of publication has less views/interactions than the publications in other social media.

Figure 14: Video Introducing CROSSCON on YouTube.

In the YouTube video illustrated by Figure 15, CROSSCON propagates the first training session organised by CROSSCON. More specifically, the Bao Workshop, a hypervisor developed by one of the partners, the University of Minho (UMINHO). Since its publication date, this video has achieved a total of 440 views and 17 likes. For CROSSCON, these metrics are important since Bao serves as the core component for the CROSSCON Hypervisor.

Figure 15: YouTube Video of Bao virtual workshop.

3.3 CROSSCON Templates of Communication Material

This section reports on the CROSSCON communication material, usually defined in European projects as a set of resources like presentation, newsletter, and blog post templates. Later, this material can be used at several conferences, posts, etc.

3.3.1 CROSSCON Presentation Template

During the project's evolution, several internal and external meetings occurred to align the members on the progress of the project. Typically, these meetings require a presentation template to present the project to a general or specialized audience. This section aims at showing the CROSSCON presentation template. Figure 16 demonstrate the first and last slide of the presentations. Each presentation should mention the project name, the presentation date, the name of the presenter, the name of the presentation, and optionally the event name where it will be presented. The last page should contain the project logo, a mail to contact the presenter/s, EU acknowledgements, and each partner logo.

Figure 16: Template of the first and last slide to be presented in a general or specialized presentation.

3.3.2 CROSSCON Newsletter Templates

During project evolution it is important to document the most important activities by leveraging communication material like newsletters. Up to now, CROSSCON delivered two newsletters, both following the same template. For CROSSCON, besides the project updates, the newsletter should follow a specific structure, by providing to the reader a kind of magazine structure (see Figure 17). CROSSCON newsletters start with a front page, encompassing its table of contents, a short sentence by a specific partner author, the release date, some communication references and the CROSSCON logo.

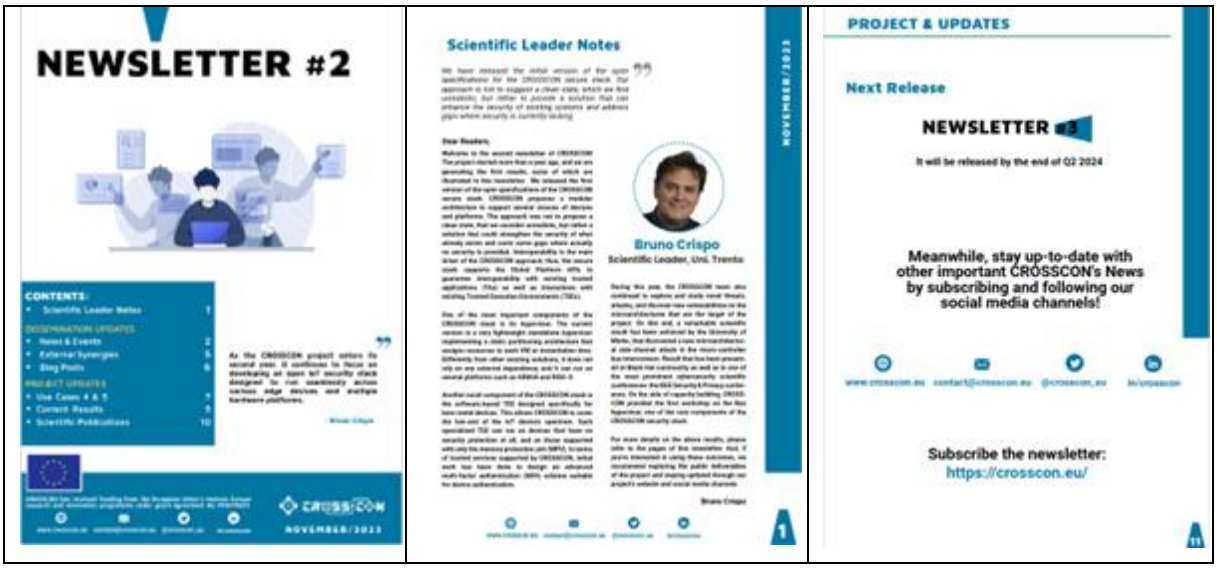


Figure 17: CROSSCON newsletter template.

The second page takes the form of an introduction and summary, where a specific author (the one mentioned in the front page) introduces the project and makes an overview of all project updates and activities that occurred since the last released newsletter. The main body of the newsletter may differ among different releases; however, it will always cover project update topics like: (i) a list of participated/organised events; (ii) scientific publications; and (iii) blog posts published by all CROSSCON partners. Finally, the last page should announce the date of the next newsletter release alongside an appeal to the community to follow CROSSCON on all social networks and to subscribe to the email newsletters on the website.

3.4 Publications

This section aims to report all released publications in the context of CROSSCON. To monitor all CROSSCON publication releases among all partners, T6.1 makes their announcement on the website and social media communication channels. This dissemination activity will be performed regularly until the end of the project.

3.4.1 Scientific Publications

The following Table 2 presents a comprehensive list of publications released by the CROSSCON project up to the publication date of this document. This report includes the title of each scientific publication, the venue where it was published, the type of KPI associated with it (whether it is a conference or a journal), the partners involved, and the corresponding link for accessibility. All described publications include the project's acknowledgements, in conformity with EC guidelines [4].

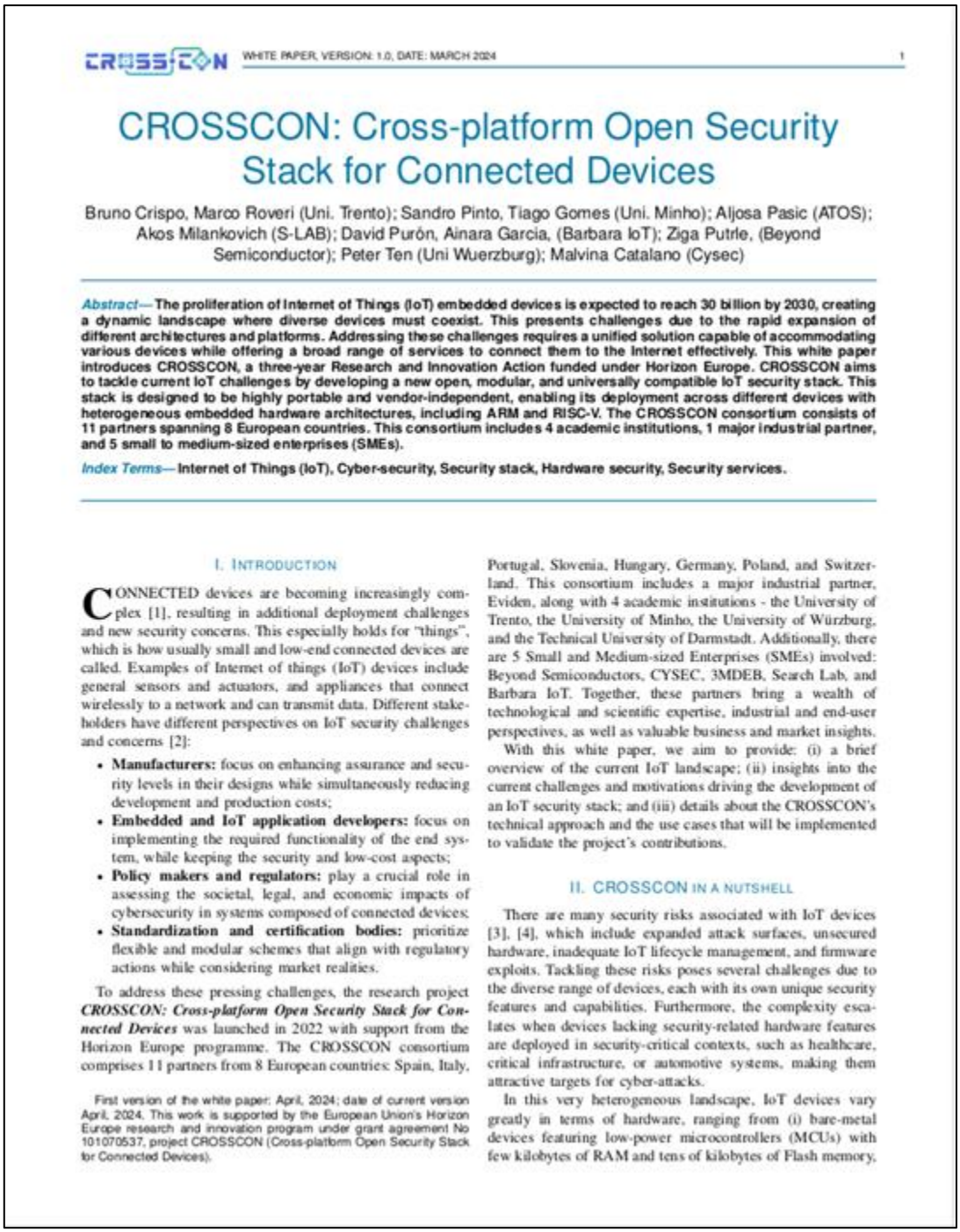
Table 2: List of scientific publications.

Title	Venue	Type	Partner	Link
Shedding Light on Static Partitioning Hypervisors for Arm-based Mixed-Criticality Systems	RTAS 2023	Conference	UMINHO	link
Efficient and Safe I/O Operations for Intermittent Systems	EuroSys '23	Conference	ALL	link
Interoperable IoT Security Stack: The RISC-V Opportunity	RISC-V Summit Europe 2023	Conference	UNITN	link
Device behavioural profiling for autonomous protection using deep neural networks	IEEE ISCC	Conference	UNITN	link
AppBox: A Black-Box Application Sandboxing Technique for Mobile App Management Solutions	IEEE ISCC	Conference	UNITN	link
µIPS: Software-Based Intrusion Prevention for Bare-metal Embedded Systems	ESORICS	Conference	UNITN	link
BUSted!!! Microarchitectural Side-Channel Attacks on the MCU Bus Interconnect	S&P 24	Conference	UMINHO	link
Marionette: Manipulate Your Touchscreen via A Charging Cable	IEEE TDSC	Journal	TUD	link

CryptojackingTrap: An Evasion Resilient Nature-Inspired Algorithm to Detect Cryptojacking Malware	IEEE TIFS	Journal	UNITN	link
FreqFed: A Frequency Analysis-Based Approach for Mitigating Poisoning Attacks in Federated Learning	NDSS	Conference	UWU	link
Beyond Random Inputs: A Novel ML-Based Hardware Fuzzing	DATE	Conference	TUD	link
CROSSCON: Interoperable IoT Security Stack for Embedded Connected Devices	Embedded World 2024	Conference	UMINHO	n/a
Lost and Found in Speculation: Hybrid Speculative Vulnerability Detection	IEEE DAC	Conference	TUD	n/a
WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors	USENIX 2024	Conference	TUD	n/a
One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices	S&P 2024	Conference	TUD	link

3.4.2 White Papers

To disseminate the project's proposal and goals, a first publication in the form of white paper is available on the CROSSCON website. The white paper describes the key ideas of the project and how it will improve the literature towards building secure IoT devices. This first white paper provides: (i) a brief overview of the current IoT landscape; (ii) insights into the current challenges and motivations driving the development of an IoT security stack; (iii) details about the CROSSCON's technical approach; and (iv) the use cases that will be implemented to validate the project's contributions. Figure 18 shows the first page of the white paper.



CROSSCON WHITE PAPER, VERSION: 1.0, DATE: MARCH 2024 1

CROSSCON: Cross-platform Open Security Stack for Connected Devices

Bruno Crispo, Marco Roveri (Uni. Trento); Sandro Pinto, Tiago Gomes (Uni. Minho); Aljosa Pasic (ATOS); Akos Milankovich (S-LAB); David Purón, Ainara Garcia, (Barbara IoT); Ziga Putrle, (Beyond Semiconductor); Peter Ten (Uni Wuerzburg); Malvina Catalano (Cysec)

Abstract— **The proliferation of Internet of Things (IoT) embedded devices is expected to reach 30 billion by 2030, creating a dynamic landscape where diverse devices must coexist. This presents challenges due to the rapid expansion of different architectures and platforms. Addressing these challenges requires a unified solution capable of accommodating various devices while offering a broad range of services to connect them to the Internet effectively. This white paper introduces CROSSCON, a three-year Research and Innovation Action funded under Horizon Europe. CROSSCON aims to tackle current IoT challenges by developing a new open, modular, and universally compatible IoT security stack. This stack is designed to be highly portable and vendor-independent, enabling its deployment across different devices with heterogeneous embedded hardware architectures, including ARM and RISC-V. The CROSSCON consortium consists of 11 partners spanning 8 European countries. This consortium includes 4 academic institutions, 1 major industrial partner, and 5 small to medium-sized enterprises (SMEs).**

Index Terms— **Internet of Things (IoT), Cyber-security, Security stack, Hardware security, Security services.**

I. Introduction

CONNECTED devices are becoming increasingly complex [1], resulting in additional deployment challenges and new security concerns. This especially holds for "things", which is how usually small and low-end connected devices are called. Examples of Internet of things (IoT) devices include general sensors and actuators, and appliances that connect wirelessly to a network and can transmit data. Different stakeholders have different perspectives on IoT security challenges and concerns [2]:

- **Manufacturers:** focus on enhancing assurance and security levels in their designs while simultaneously reducing development and production costs;
- **Embedded and IoT application developers:** focus on implementing the required functionality of the end system, while keeping the security and low-cost aspects;
- **Policy makers and regulators:** play a crucial role in assessing the societal, legal, and economic impacts of cybersecurity in systems composed of connected devices;
- **Standardization and certification bodies:** prioritize flexible and modular schemes that align with regulatory actions while considering market realities.

To address these pressing challenges, the research project ***CROSSCON: Cross-platform Open Security Stack for Connected Devices*** was launched in 2022 with support from the Horizon Europe programme. The CROSSCON consortium comprises 11 partners from 8 European countries: Spain, Italy, Portugal, Slovenia, Hungary, Germany, Poland, and Switzerland. This consortium includes a major industrial partner, Eviden, along with 4 academic institutions - the University of Trento, the University of Minho, the University of Würzburg, and the Technical University of Darmstadt. Additionally, there are 5 Small and Medium-sized Enterprises (SMEs) involved: Beyond Semiconductors, CYSEC, 3MDEB, Search Lab, and Barbara IoT. Together, these partners bring a wealth of technological and scientific expertise, industrial and end-user perspectives, as well as valuable business and market insights.

With this white paper, we aim to provide: (i) a brief overview of the current IoT landscape; (ii) insights into the current challenges and motivations driving the development of an IoT security stack; and (iii) details about the CROSSCON's technical approach and the use cases that will be implemented to validate the project's contributions.

First version of the white paper: April, 2024; date of current version April, 2024. This work is supported by the European Union's Horizon Europe research and innovation program under grant agreement No 101070537, project CROSSCON (Cross-platform Open Security Stack for Connected Devices).

II. CROSSCON in a nutshell

There are many security risks associated with IoT devices [3], [4], which include expanded attack surfaces, unsecured hardware, inadequate IoT lifecycle management, and firmware exploits. Tackling these risks poses several challenges due to the diverse range of devices, each with its own unique security features and capabilities. Furthermore, the complexity escalates when devices lacking security-related hardware features are deployed in security-critical contexts, such as healthcare, critical infrastructure, or automotive systems, making them attractive targets for cyber-attacks.

In this very heterogeneous landscape, IoT devices vary greatly in terms of hardware, ranging from (i) bare-metal devices featuring low-power microcontrollers (MCUs) with few kilobytes of RAM and tens of kilobytes of Flash memory,

Figure 18 - First page of the white paper.

3.5 Conferences, Workshops and Industry-Related Events

During these past months of the project, the CROSSCON consortium has participated in various virtual and physical events throughout Europe, giving visibility and raising awareness of the expected outcomes. In the context of T6.2, events were uploaded to the website and promoted on social media. In some cases, we have also uploaded the recordings of virtual events to our YouTube channel or Video section on the project's website.

Considering the KPIs at play, the events are segmented into five distinct categories: workshops, summer schools, training events, other and demonstrations. Within the "workshops" category, we encompass cluster meetings and specialised workshops. "Summer schools" comprise educational programs, school events, and gatherings hosted by academic institutions. "Training events" encompass international webinars and gatherings tailored for educational purposes. The "demonstrators"

category encompasses the presentation of videos and live demos showcasing CROSSCON's capabilities. Lastly, the "other" category encompasses a spectrum of activities including general or scholarly talks and assistance provided at conferences.

To describe all CROSSCON events participation and organisation during the last months, Table 3 and Table 4 include a list of each of them, respectively. Each event in the list we include a KPI classification, the corresponding event name, location, date, and the CROSSCON partner attendance. To classify the KPI type we adopt the following description: “O” for other events; “TE” for Training Event; “W” for workshop; “SS” for summer school events; and “D” for demonstrator events.

Table 3: List of CROSSCON participated events.

KPI Type	Event Name	Location	Date	Partner/s
O	ENISA Cybersecurity Market Analysis Conference	Brussels, Belgium	23-24 Nov 2022	ATOS, CYSEC
TE	RISC-V Summit 2022	San Jose, CA, USA	12-15 Dec 2022	UMINHO
O	Barcelona Cybersecurity Congress	Barcelona, Spain	31 Jan - 2 Feb 2023	ATOS
SS	NECS - PHD WINTER SCHOOL 2023	Vason, Trento, Italy	6-10 Feb 2023	UMINHO
W | SS	CROSSCON Clustering Meeting	Trento, Italy	10 Feb 2023	TUD, BEYOND, UWU, UNITN
O	FOSDEM 2024	Brussels, Belgium	Q1'2024 (Feb)	3MDEB
TE	Embedded World 2023	Nuremberg, Germany	14-16 Mar 2023	UMINHO
W | SS	High-Tech Women	Darmstadt, Germany	30 Mar 2023	UWU
TE	CYSAT	Paris, France & Online	26-27 Apr 2023	CYSEC
TE	RISC-V Summit Europe	Munich, Germany	05-09 Jun 2023	UMINHO
TE	Global IoT Summit Europe	Berlin, Germany & Online	18-19 Oct 2023	ATOS
W	Encrypt - Clustering Workshop	Procida, Italy	6 Jun 2023	UNITN

KPI Type	Event Name	Location	Date	Partner/s
W	ERATOSTHENES - 2nd Workshop: Trust and Identity Management for IoT	Online	16 Jun 2023	UMINHO
O	OSFC 2023	USA	10-12 Oct 2023	3MDEB
O	ELCE 2023 (Embedded Linux Conference)	Online	Q4'2023 (Oct)	3MDEB
TE	OERN (Ordem Engenheiros Região Norte)	Online	9 Oct 2023	UMINHO
W	SENTINEL Cluster Meeting: Cyber Security and Data Protection Synergies	Caparica, Portugal	16-17 Oct 2023	UMINHO
W	SU-DS02 SecureCyber Project Cluster Communication Task Force Meeting	Online	18 Oct 2023	ATOS
W	Leading projects in cybersecurity	Online	19 Oct 2023	UNITN
O	Basque Open Industry	Bilbao, Spain	13-14 Nov 2023	BIOT
W | D	Bao Hypervisor Virtual Workshop	Online	15 Nov 2023	UMINHO
O	ENLIT EUROPE - Making the Intelligent Power Grid Happen	Paris, France	28-30 Nov 2023	BIOT
SS	NECS - PHD WINTER SCHOOL 2024	Cortina d'Ampezzo,Italy	8-12 Jan 2024	TUD, BEYOND, UWU
W	NECS – PhD Winter School 2024	Cortina d'Ampezzo, Italy	12 Jan 2024	TUD, BEYOND, UWU
TE	TEE Course (SLAB)	Online	17 Jan 2024	SLAB
W	The state of the semiconductor market in the EU	Online	29 Jan 2024	ATOS
TE	Identify and trust in IoT ecosystems	Online	14 Feb 2024	UMINHO

KPI Type	Event Name	Location	Date	Partner/s
W	CTI Workshop	Online	6 Mar 2024	UMINHO
TE	Embedded World 2024	Nuremberg, Germany	9-11 Apr 2024	UMINHO, BEYOND
TE	CYSAT	Paris	24-25 Apr 2024	CYSEC, CYSEC

Table 4: List of CROSSCON organized events.

KPI Type	Event Name	Location	Date	Partner/s
SS	NECS - PHD WINTER SCHOOL 2023	Vason, Trento, Italy	6-10 February 2023	UNITN
W | SS	CROSSCON Clustering Meeting	Trento / Italy	10 Feb 2023	UNITN
W | SS	High-Tech Women	Darmstadt, Germany	30 Mar 2023	TUD
W | D | TE	Bao Hypervisor Virtual Workshop	Online	15 Nov 2023.	CROSSCON + BAO Project
W	CROSSCON Workshop - Security Services for Connected Devices	Cortina d'Ampezzo (Italy)	12 Jan 2024.	UNITN, ATOS
SS	NECS - PHD WINTER SCHOOL 2024	Cortina d'Ampezzo (Italy)	8-12 Jan 2024.	UNITN
TE	TEE Course (SLAB)	Online	17 Jan 2024.	SLAB

Figure 19 provides diagrams depicting the involvement of individual partners in the events, as well as an overview of the countries where the events took place. Statistical analysis shows that online events were the most prevalent, with a total of 12 occurrences, followed by Italy, which hosted a total of five events and emerged as the most visited country by the CROSSCON consortium.

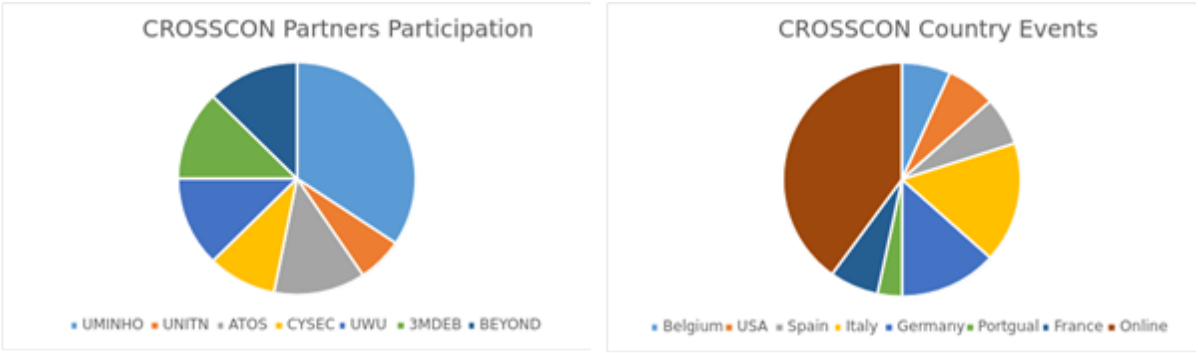


Figure 19: Analysis on event participation by CROSSCON.

3.6 Other Dissemination and Communication Channels

This section aims to outline all other dissemination and communication channels, encompassing a variety of materials that include a CROSSCON's brochure, press release, blog posts, general and specialised presentations, and newsletters. Each of these channels serves as a strategic tool for communicating different aspects of the CROSSCON project to various stakeholders.

- **Brochures:** These compressed documents provide an overview of CROSSCON's objectives, motivation and description. They are valuable for distribution at conferences and workshops, serving as tangible resources for potential collaborators or investors.
- **Press Releases:** Press releases are instrumental in generating media coverage and public interest in CROSSCON's milestones, partnerships, and advancements. They help increase visibility and credibility within the industry and among potential users and partners.
- **Blog Posts:** Blog posts offer a platform for in-depth discussions, case studies, and thought leadership pieces related to CROSSCON's technological innovations, use cases, and industry insights. They contribute to building thought leadership and engaging with a broader audience interested in the project's developments.
- **Media hits:** Media hits contribute to enhancing the project's visibility by disseminating CROSSCON news across various platforms such as magazines, blogs, and other forms of media.
- **Presentations:** General and specialised presentations provide opportunities to showcase CROSSCON's capabilities, achievements, and potential applications to diverse audiences, while helping to understand the project.
- **Newsletters:** Newsletters serve as regular updates on CROSSCON's progress, events, and news. They help to maintain engagement with stakeholders, keep them informed about recent developments, and encourage continued interest and support for the project.

3.6.1 CROSSCON Brochure

Figure 20 showcases the official Brochure designed for dissemination at conferences and similar events to effectively communicate the project's objectives. On the left side it takes the common format (one-page brochure), while on the right side it takes the tri-fold format. While tri-fold format is typically handed out to individuals, the one-page format is typically used to be displayed on a board or on a shelf for the public to see.

The CROSSCON brochure starts by offering a project overview, including the project's motivation, defining the CROSSCON stack, and providing background information related to trusted services within the security community. Additionally, it outlines all five use cases and articulates the primary goals of the project. At the bottom of the page, the brochure features all consortium members alongside a QR code, facilitating direct access to the CROSSCON website for further information.

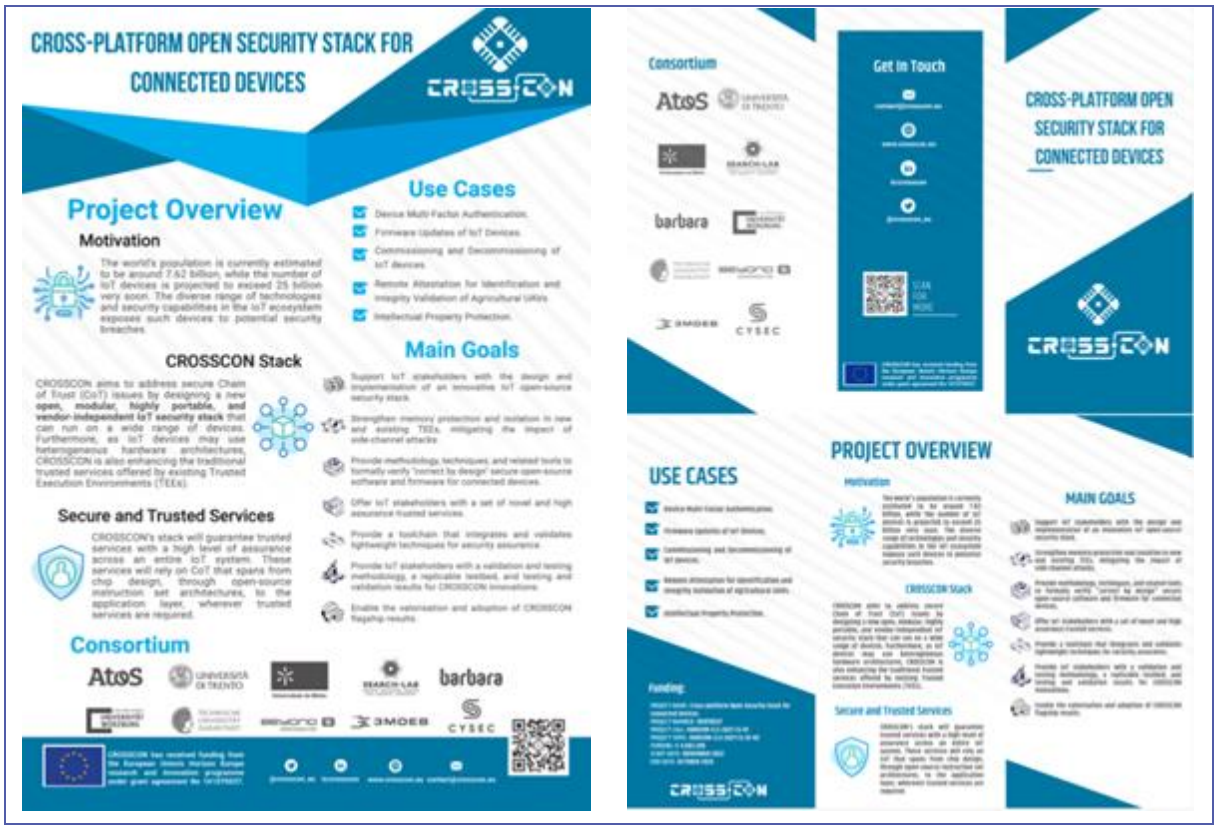
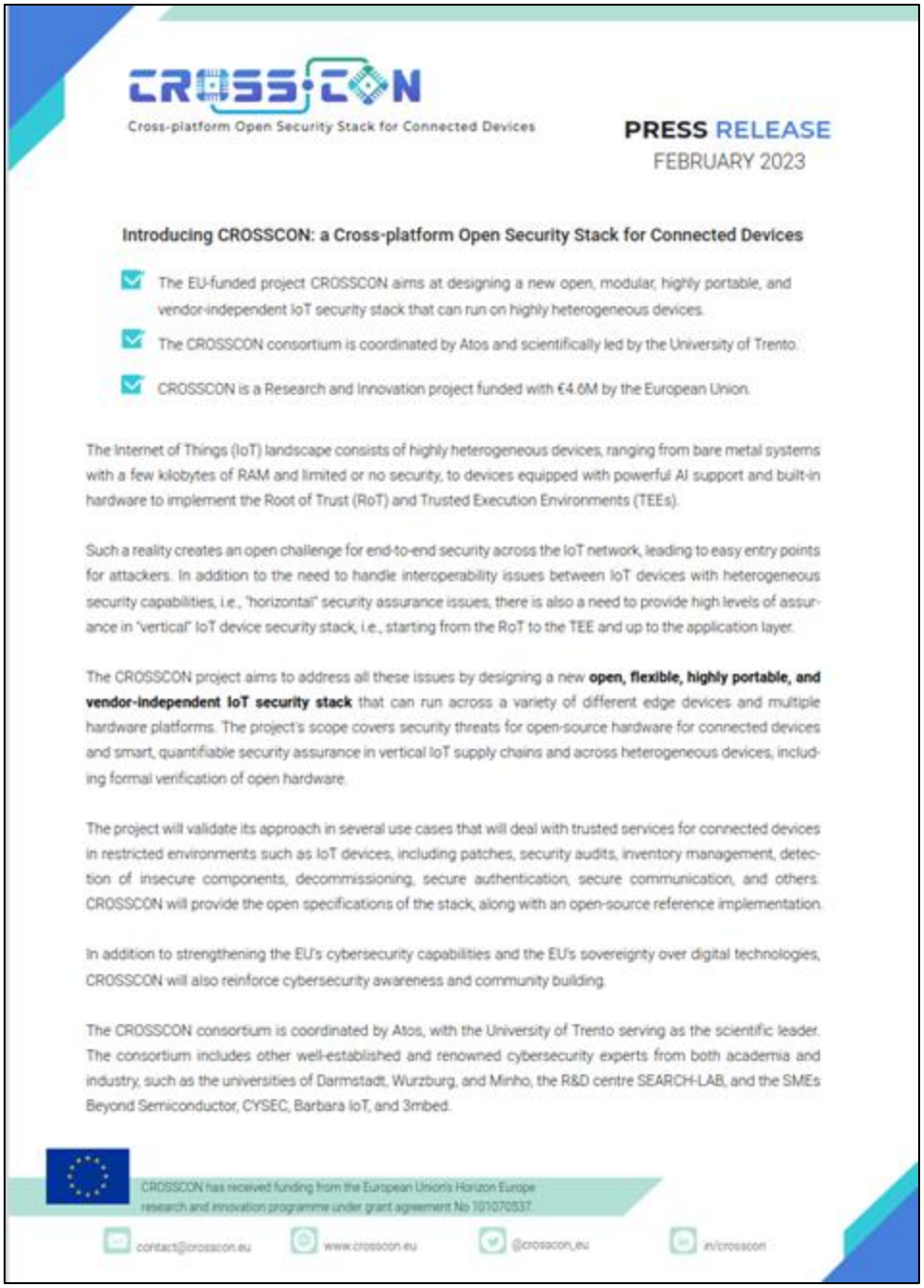


Figure 20: One-page and tri-fold brochures.

3.6.2 CROSSCON Press Release

Figure 21 depicts the first CROSSCON press release, whose aim is to effectively communicate the objectives, scope, and consortium partners of the CROSSCON project, providing key insights into its mission and impact within the cybersecurity landscape. This press release is currently available on the CROSSCON website (link for press release). New press release should follow the presented template and be submitted to some newspapers and organisation websites.



CROSSCON

Cross-platform Open Security Stack for Connected Devices

PRESS RELEASE
FEBRUARY 2023

Introducing CROSSCON: a Cross-platform Open Security Stack for Connected Devices

- The EU-funded project CROSSCON aims at designing a new open, modular, highly portable, and vendor-independent IoT security stack that can run on highly heterogeneous devices.
- The CROSSCON consortium is coordinated by Atos and scientifically led by the University of Trento.
- CROSSCON is a Research and Innovation project funded with €4.6M by the European Union.

The Internet of Things (IoT) landscape consists of highly heterogeneous devices, ranging from bare metal systems with a few kilobytes of RAM and limited or no security, to devices equipped with powerful AI support and built-in hardware to implement the Root of Trust (RoT) and Trusted Execution Environments (TEEs).

Such a reality creates an open challenge for end-to-end security across the IoT network, leading to easy entry points for attackers. In addition to the need to handle interoperability issues between IoT devices with heterogeneous security capabilities, i.e., "horizontal" security assurance issues, there is also a need to provide high levels of assurance in "vertical" IoT device security stack, i.e., starting from the RoT to the TEE and up to the application layer.

The CROSSCON project aims to address all these issues by designing a new **open, flexible, highly portable, and vendor-independent IoT security stack** that can run across a variety of different edge devices and multiple hardware platforms. The project's scope covers security threats for open-source hardware for connected devices and smart, quantifiable security assurance in vertical IoT supply chains and across heterogeneous devices, including formal verification of open hardware.

The project will validate its approach in several use cases that will deal with trusted services for connected devices in restricted environments such as IoT devices, including patches, security audits, inventory management, detection of insecure components, decommissioning, secure authentication, secure communication, and others. CROSSCON will provide the open specifications of the stack, along with an open-source reference implementation.

In addition to strengthening the EU's cybersecurity capabilities and the EU's sovereignty over digital technologies, CROSSCON will also reinforce cybersecurity awareness and community building.

The CROSSCON consortium is coordinated by Atos, with the University of Trento serving as the scientific leader. The consortium includes other well-established and renowned cybersecurity experts from both academia and industry, such as the universities of Darmstadt, Wurzburg, and Minho, the R&D centre SEARCH-LAB, and the SMEs Beyond Semiconductor, CYSEC, Barbara IoT, and 3mbed.

CROSSCON has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537.

contact@crosscon.eu www.crosscon.eu @crosscon_eu in/crosscon

Figure 21: First CROSSCON press release.

3.6.3 CROSSCON Blog Posts

Blog posts play an essential role in dissemination efforts, offering a dynamic platform to share project updates, insights, and achievements. By regularly publishing informative and engaging content, blogs effectively reach diverse audiences, including stakeholders, researchers, policymakers, and the public. These posts not only provide detailed information about project activities but also offer valuable perspectives and analysis, enriching the discourse surrounding the project's subject matter. Overall, blog posts serve as essential tools for maximizing project visibility, enhancing understanding, and fostering meaningful connections with stakeholders. Table 5 summarizes the blogposts available on the website, highlighting the title, partner, and date of publishing.

Table 5: List of CROSSCON blog posts.

Title	Partner	Date
We are open, but formal	ATOS+UNITN	Apr-23
TEEs are not Silver Bullets	UMINHO	May-23
Enhancing Security in Agricultural UAVs: The Power of Remote Attestation	CYSEC	Jun-23
Cybersecurity is a Community Effort	BIOT	Jul-23
Enhancing IoT Security through Device-to-Device Authentication	3MDEB	Aug-23
Information Flow Tracking: Enhancing Data Security and Privacy	BEYOND	Sep-23
FPGA-based Trusted Execution Environments and Their Use Cases	TUD	Oct-23
Ensuring the Integrity of IoT Devices: Best Practices for Secure Firmware Updates	SLAB	Dec-2023
Trust as a Foundation for Secure Internet of Things Services	UWU	Jan-2024
Embracing fTPM on embedded ARM Devices: Insights and Solutions	3MDEB	Feb-2024
Stack and Stick are in Stock	ATOS	Mar-2024

Figure 22 depicts a website screenshot that demonstrates an example of Blog Posts, including an attractive title, the CROSSCON logo, the CROSSCON social media handles, and a photo of the person who wrote the specific Blog Post.

Figure 22: Blogpost banner example.

3.6.4 CROSSCON Media Hits

Media hits are crucial for project success, serving as valuable opportunities to amplify visibility and reach diverse audiences. When a project receives coverage or is mentioned in media outlets, it increases awareness, fosters credibility, and promotes engagement. These hits not only showcase project achievements but also attract potential collaborators, funders, and stakeholders. Ultimately, media hits contribute significantly to the project's impact and sustainability by broadening its reach and influence.

During the last year, the project was mentioned on two occasions, both in online media. The first instance, highlighted by the headline "Universidade do Minho integrates European IoT cybersecurity project," received widespread coverage across various Portuguese news websites. This coverage emphasized the significant role played by the Portuguese project partner, Universidade do Minho, within a European project, featuring insights from WP3 leader Sandro Pinto and WP6 leader Tiago Gomes.

The second mention revolved around the participation of project members in a lecture sponsored by “Ordem dos Engenheiros do Norte”, a prominent engineering organization in Portugal. In this lecture, project members had the opportunity to present the project to a technical crowd, showcasing its objectives, progress, and significance within the realm of cybersecurity and IoT.

Figure 23: Media hits publications promoting CROSSCON.

3.6.5 General Audience Presentation

Considering the importance of the project's presence at events catering to both specialized and general audiences, we have prepared a General Audience Presentation for any CROSSCON partner to utilize when showcasing the project. This presentation, attached to this document as Annex A, includes several key elements: (i) general project details and terminology, ensuring clarity and consistency in communication during the presentation; (ii) project motivations and objectives to provide context and purpose; (iii) use-case explanations using simple vocabulary, comparisons with common technological processes, and interactive visuals for enhanced understanding; (iv) overview of the CROSSCON stack, describing each component of the system stack; (v) presentation of the CROSSCON approach, outlining the various WPs and their respective responsibilities; (vi) the project roadmap, illustrating different project milestones; (vii) the project status, including reported deliverables and progress updates related to CROSSCON components; and (viii) contact information for easy communication with the CROSSCON project team. This comprehensive presentation serves as a valuable tool for effectively communicating the essence and progress of the CROSSCON project.

3.6.6 CROSSCON Newsletters

Newsletters serve as an invaluable communication tool for European projects, facilitating the dissemination of information, updates, and achievements to stakeholders and the wider community. Within the context of our project, the publication of newsletters in March 2023 and November 2023, has played an important role in fostering engagement, enhancing transparency, and amplifying the impact of our endeavours. The first newsletter, released in March, featured a special note from the Project Coordinator, Hristo Koshutanski, offering insights into the project's core objectives. This edition also provided a concise overview of the project's outline and included highlights of the blog posts, related news, and upcoming events.

Figure 24: First and second CROSSCON newsletters.

The subsequent newsletter, published in November, continued our commitment to transparent communication. With a special note from the scientific leader, Bruno Crispo, readers gained valuable insights into project updates related to the use cases and scientific publications. Additionally, it provided an overview of the blog posts, news updates, and events that happened between the

publication of both newsletters. In summary, both newsletters contributed as very important dissemination tools for the broader community. Both newsletters are already available on the website.

To sign up for future newsletters, users can use the dedicated field on the CROSSCON website (www.crosscon.eu). This designated area is located at the bottom of the CROSSCON website page and by simply submitting their mail to the mailing list, they are subscribed to upcoming newsletters. Currently, there are 15 subscribers to this mailing list.

4 Community Building

This section focuses on community building, reporting on practical community interactions that enhance collaboration and knowledge sharing. By fostering connections and empowering stakeholders, CROSSCON seeks to amplify the impact of our project and foster lasting relationships among participants. In this section, we cover the organized training activities and the external synergies that CROSSCON established since the project started.

4.1 Training Activities

A training activity is associated with an event in which the main goal is to demonstrate some knowledge about a specific area or component to a general or specialised audience. In CROSSCON, some training activities were organised, the "Bao Hypervisor Virtual Workshop" and the "Trusted Execution Environment (TEE) course".

4.1.1 Bao Hypervisor Virtual Workshop

The **Bao Hypervisor Virtual Workshop** aimed to disseminate the core component of the CROSSCON Hypervisor, the Bao hypervisor. In this CROSSCON event, UMINHO partners introduce the Bao hypervisor by including topics like Bao's internals and configuration. It provided a hands-on setup guide for various configurations with FreeRTOS and Linux on Arm and RISC-V architectures. Additionally, this session includes topics like the resource assignment using static partitioning design, inter-VM communication and interference mitigation techniques (e.g., cache coloring). At the end, the presentation included multiple Q&A sessions, which garnered positive feedback and demonstrated significant interest in this CROSSCON Hypervisor component. The workshop attracted nearly 100 participants. This workshop is currently available on YouTube on this link.

Figure 25: Banner used for Bao Hypervisor virtual workshop.

4.1.2 TEE Course

The **TEE Course** involved the core principles of secure computing, with a spotlight on TEEs. Presented by the Search-Lab partner, a leading authority in security testing and evaluation of ICT products, this online course offered an accessible learning opportunity for the security community. During the course, participants explored the fundamental concepts of TEE technology, gaining invaluable insights of its security capabilities. Search-Lab's expertise provided a comprehensive overview of TEE architecture, security protocols, and evaluation methodologies. The course fostered engaging discussions and Q&A sessions, promoting knowledge exchange and collaboration among participants. The workshop attracted over 30 participants. Video recording will be disclosed soon.

Figure 26: Banner used for CROSSCON TEE course.

4.2 External Synergies

As a result of participating and organizing events, CROSSCON was actively interacting with other security projects, creating external synergies. Due to similar goals, several European projects can establish connections while attending the same events. Typically, this event allows them to share knowledge, exchange IoT technological components, or even the publication of technological content. During the last months, CROSSCON has interacted with several European Projects like Entrust, Arcadian-IoT, SecOpera, IoT-NGIN, REWIRE, ERATOSTHENES, ORSHIN, IRIS, SPATIAL, SECANT, IDUNN, KRAKEN, ELECTRON, TRUSTaWARE, SENTINEL and CERTIFY. Alongside numerous projects mentioned previously, CROSSCON actively participates in the Secure Cyber Cluster. This collaboration emerged as a pioneering initiative during the SENTINEL cluster meeting in Lisbon, aimed at establishing a unified brand capable of disseminating individual content, updates, and collaborations effectively. By centralizing project information and synchronizing efforts, this initiative enhances project visibility and attracts a broader audience to engage in project activities.

5 Key Performance Indicators

To measure the effectiveness of CROSSCON's dissemination and communication strategies, several KPI have been established in the proposal and will be compared with achieved results of this report. Table 7 correlates the projected KPIs set for M18 with the achieved KPI of the corresponding dissemination actions.

Over the past 18 months, CROSSCON partners have been actively contributing to academic research by publishing in 2 journals and 10 conferences (as detailed in Table 2, Section 3.4). In terms of workshops ("W"), CROSSCON has organized 4 and participated in 11 (as outlined in Table 3 and Table 4, on Section 3.5). Moreover, the project has been showcased in 4 winter/summer schools ("SS") and attended 19 other ("O") and training events ("TE"). These additional training events encompass various activities such as webinars, conference assistance, and other gatherings not categorized as workshops or summer schools. Finally, one white paper is currently available at the website page, and as part of demonstrators ("D"), CROSSCON participated/organized one event (i.e., the Bao hypervisor virtual workshop event).

Table 6: KPIs report for the dissemination activities.

Dissemination activity - KPI description	Projected KPI Target M18	Achieved KPI Target M18
Scientific publication	>= 6 journals and 10 papers	2 journals and 10 conference 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	Workshops attended: 11 Workshops organized:4
Winter/Summer schools	1	4
Other training events (courses, webinars)	>=5	19
Liaison with projects	>=5	8
White papers	>=1	1
Demonstrators	0	1

We acknowledge that some of the KPIs are quite ambitious. For instance, the scientific publications are a little behind the desired target. However this is normal since the CROSSCON core component's implementations will start to be available at the end of April, which will allow for the documentation and assessment of literature relevant content.

Additionally, the CROSSCON project has outlined a clear plan of communication strategies aimed at maximizing the visibility of its activities and outcomes across diverse audiences. Correspondingly, similar to Table 6, Table 7 delineates the achieved KPIs in comparison to the projected KPIs set for M18 of the respective communication actions.

During the past 18 months, the engagement of the LinkedIn and X communities fell short of expectations, evidenced by a lower-than-anticipated number of followers (500+ social media followers). Nonetheless, there have been notable successes, including a substantial level of website traffic (approximately 7.6K page views) and a total of 11 blog posts submitted. Regarding multimedia content, CROSSCON has accumulated considerable interactions, with 461 views on YouTube videos and at least 500 shared brochures across 31 events. Furthermore, the project has issued one press release and submitted 2 newsletters, all accessible on the website. Throughout these events,

CROSSCON has engaged with various industries, sharing a mutual interest in utilizing CROSSCON for their needs. The feedback received from these interactions has been positive, with more than 50 different communities actively engaging with CROSSCON.

Table 7: KPIs report for the communications activities.

Type of communication action	Format/channel	Projected KPI	Achieved KPI
Create a community of twitter and LinkedIn users	Social media (Twitter, LinkedIn)	3000 followers	500+ (combined)
Foster online visibility of the consortium/project	Website	200 visits/month	7.6K page views
	Blog	12	11
Elevator pitch to brief the project to a wide audience (e.g., motion graphics animation and infographics)	Animation (e.g., YouTube)	1000 views	461
	Brochure (events, science fairs)	500 shares	500+
Online press release	Website	3 PRs	1
Interact with companies interested in adopting the CROSSCON platform	Social media, newsletter	50 industrial feedbacks	50+

6 Conclusions

This deliverable, D6.4 - Dissemination, Communication and Community Building - First Report is part of task T6.1 – Dissemination and Communication, included in the WP6. Reporting all project activities is important to expose the impact of the project to the community. Overall, the results exposed in this deliverable showed that most dissemination and communication activities done by CROSSCON and its consortium partners have been successful and executed in line with the plans presented on the previous deliverable D6.2. The reason behind some KPIs not being completely achieved, e.g., the expected number of followers on social media channels, or even the low number of publications in journals, can be justified by the fact that some CROSSCON's core components are still under development and currently not publicly available (first release by M18), which will allow for the documentation and assessment of literature-relevant content. Notwithstanding, some activities are already in progress to meet the expected KPIs soon, which is the case of the number of blog posts, and some under review journal publications.

A potential strategy to boost social media engagement could involve creating more posts featuring animated content or detailed descriptions of our work. As we move into the latter stages of the project, significant changes are anticipated as CROSSCON becomes more actively involved with the community. However, it is crucial to maintain regular monitoring of communication KPIs (monthly) to promptly address any issues that may arise. As a result, the CROSSCON consortium will consistently assess and update the current dissemination and communication plan as necessary, taking action when required. The comprehensive report detailing these actions and any updates to the initial plan will be presented in the upcoming report, D6.6 - Dissemination, Communication and Community Building Final Report, scheduled for release in the project's second half (M36).

In conclusion and looking ahead, CROSSCON plans to continue undertaking the following activities: organizing its own events, participating in international conferences, and publication of scientific papers to conferences and journals to showcase the project's work and progress. Additionally, identifying relevant exhibitions aimed at engaging key stakeholders to showcase CROSSCON's work, leveraging synergies with other projects and initiatives to expand stakeholder outreach, and continuing to produce materials such as blog posts, specialized PowerPoint presentations, videos, press releases, and newsletters. The outcomes of these activities, carried out between months 18 and 32, will be detailed in D6.6, the project's final report.

References

[1] E. C. (EC), "Funding & Tender Opportunities - Support (FAQ)," [Online]. Available: https://rea.ec.europa.eu/communicating-about-your-eu-funded-project_en. [Accessed 06 01 2023].

[2] CROSSCON, **D6.1 Project Website**., A. Pasic, 2023.

[3] CROSSCON, **D6.2 Dissemination and Communication Plan**, T. Gomes, 2023.

[4] Grant Agreement, Number - 101070537, CROSSCON, 2022.

Annex A - PowerPoint Presentation Template


Project Details
Project Name: Cross-platform Open Security Stack for Connected Devices
Project Call: HORIZON-CL3-2021-CS-01
GA Number: 101070537
Budget: 4.6M €
Duration: 36 Months (Nov-2022 to Oct-2025)
Consortium: 10 Members (8 countries)
Project Coordinator: Hristo Koshutanski (ATOS)
Scientific Coordinator: Bruno Crispo (UNITN)
Exploitation Coordinator: Aljosa Pasic (ATOS)
Atos
barbara
SEARCH-LAB
3MDEB
CYSEC
Project Overview


Project Terminology
Open-Source Hardware (OSH) - Hardware designs and specifications that are made freely available to the public under an open-source license;
Heterogeneous devices - Collection of devices or components within a system that differ from one another in terms of their hardware architecture, capabilities, or characteristics.
Trust - Level of reliability and assurance that a device possesses to ensure different security primitives;
Root-of-Trust (RoT) - The foundational and most trusted element in a computing system, serving as the starting point of the Chain-of-Trust;
Chain-of-Trust (CoT) - A sequence of trusted relationships established between different components within a device;
Trusted Services - A set of secure and reliable mechanisms designed to enhance the security, privacy, and trustworthiness of devices and applications, e.g., device authentication, secure firmware updates, remote attestation, etc;
Project Overview


Project Terminology
Security Stack - A set of software/hardware technologies designed and deployed to protect a device against cybersecurity threats;
Interoperability - The ability of different systems, devices, or software to work together and exchange information seamlessly;
Formal Verification - A method that uses mathematical approaches to prove the correctness of hardware or software systems;
Toolchain - A set of software development tools that are used to perform a specific task or to build a particular type of software for a target device;
Trusted Execution Environment (TEE) - A secure and isolated environment within a device where critical operations can be executed with a high-level of confidentiality and integrity;
Hypervisor - A software layer that creates and manages multiple isolated execution environments (virtual machines) on a device;
Project Overview


Project Motivations
Lack of Open-Source Hardware Solutions
Most IoT solutions rely on proprietary hardware with closed-source licence, limiting innovation and collaboration;
Open-source promotes transparency, fosters creativity, and drives advancements;
Lack of Root- and Chain-of-trust
Current IoT devices lack robust and complete Root-of-Trust and Chain-of-Trust, posing significant security risks;
Establish a robust security foundation for IoT ecosystems fosters trustworthiness among users and stakeholders;
Lack of Interoperability Between IoT Devices
Due to the wide spectrum of heterogeneous devices, current IoT devices often struggle to communicate effectively with each other;
Device interoperability ensures seamless connectivity across the network;
Project Overview


Project Motivations
High Costs of Developing Trusted Services
Developing a secure IoT service might require significant investments (e.g., in specialized hardware), advanced security expertise, and extensive testing processes. High costs can become prohibitively expensive for small startups or organizations with limited resources, hindering their ability to enter the market.
Through open, modular, and cost-effective IoT security solutions, trusted service development becomes accessible to a broader audience, fostering innovation across various applications.
Vulnerabilities in Core Trust Components
Security flaws in crucial trusted components could undermine the reliability of IoT systems;
By strengthening the key trusted components, we are creating the path to a more secure and reliable IoT landscape;
Project Overview


Project Objectives
1. CROSSCON envisions a secure ecosystem where security starts at RoT and extends to all CoT components;
2. CROSSCON strengthen memory protection and isolation in both new and existing TEEs, mitigating the impact of cybersecurity threats;
3. CROSSCON enhances trusted services offered by TEEs;
4. CROSSCON deliver a toolchain with lightweight techniques for security assurance;
5. CROSSCON establish a security approach by tackling CoT issues and designing a new open, modular, highly portable, and vendor independent IoT security stack that can run on a wide range of devices;
Project Overview

Use-Cases

UC1: Device Multi-Factor Authentication

Single-Factor Authentication (SFA) only uses one credential/method for the authentication process, e.g., username/password, pin code, etc.

Passwords alone can pose significant security risks, as they can be easily compromised through phishing or man-in-the-middle attacks (MITM). This underscores the importance of enhancing security, and introducing Multi-Factor Authentication (MFA) schemes.

Multi-Factor Authentication (MFA) traditionally authenticate access with two or more factors which could include:

- Something you have (e.g., Smart card, tokens);
- Something you are (e.g., Biometrics);
- Something you know (e.g., Passwords).

CROSSCON aims at introducing new authentication methods based on context and behavioral authentication.

Use-Cases

UC2: Firmware Updates of IoT Devices.

Keeping IoT devices secure is closely tied to the vital process of **updating their firmware,** which is usually performed via the Internet. Typically, these updates come in two main flavors:

- **Full Updates:** Which completely replace the device's firmware;
- **Partial Updates:** Which modify specific sections of the firmware instead of applying changes to the entire firmware version;

Such updates must be performed securely, otherwise malicious or patched software can intentionally create or open several vulnerabilities and risks.

CROSSCON aim to cover secure firmware updates Over-The-Air (OTA).

Use-Cases

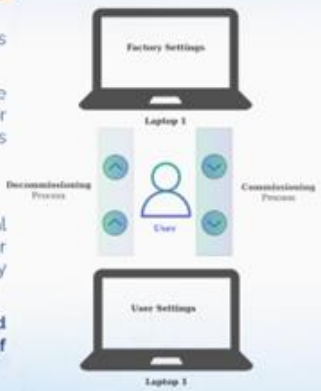
UC3: Commissioning and Decommissioning of IoT devices.

When setting up an IoT device, it's important to go through a commissioning process to ensure proper operation:

- **IoT Device Commissioning** is the process by which connected devices acquire the necessary information and configuration parameters for their intended use or application. Commissioning is a critical step in the IoT device lifecycle and needs to happen before the device starts.

By its turn, the decommissioning process restores the device to its original state:

- **IoT Device Decommissioning** is the process of returning the device to its original state when it is no longer in use or is repurposed for a different customer or purpose; Decommissioning is particularly crucial for industrial devices that may contain sensitive information.



CROSSCON is committed to implementing robust commissioning and decommissioning procedures for applications, ensuring the highest levels of security and reliability in IoT device operations.

Use-Cases

UC4: Remote Attestation for Identification and Integrity Validation of Agricultural Unmanned Aerial Vehicles (UAVs)

Agricultural UAVs are essential for helping farmers in several tasks, e.g., seeding, fertilizing, irrigating, and pest controlling. Nevertheless, they also bring several privacy- and safety-related challenges and concerns within the realm of agricultural UAVs.

Remote attestation: is a method by which a client authenticates it's hardware and software configuration to a remote host.

Using remote attestation, a user can ensure that a UAV is running a trusted software and hardware stack that meets the necessary **privacy**, **safety**, and **legal** requirements.

CROSSCON will provide secure remote attestation on agricultural UAVs.

Use-Cases

UC5: Intellectual Property Protection for Secure Multi-Tenancy on FPGA

Reconfigurable technology supports compute-intensive tasks. To optimize resource usage, multiple clients (i.e., tenants) can share the **reconfigurable platform**.

Thus, these resources must be temporal and/or spatial isolated:

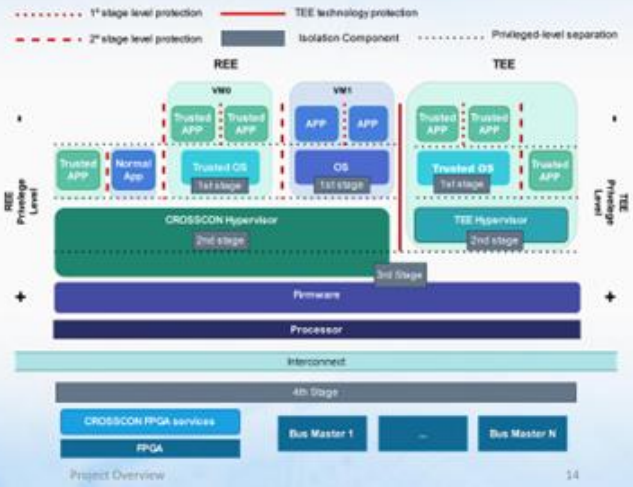
- **Temporal**: Only one tenant has access resources at a time;
- **Spatial**: Tenants have access to resources simultaneously;

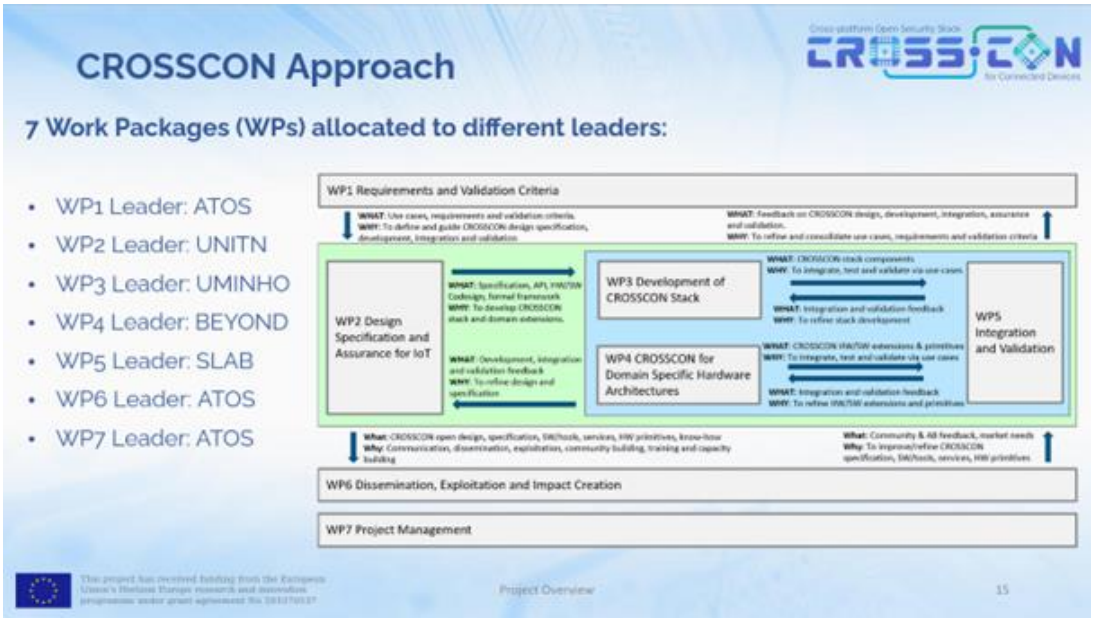
CROSSCON will provide secure multi-tenancy, assuring that the workload of one tenant cannot interact with others (or affect the hardware resources), also ensuring that no data can be leaked by any means.

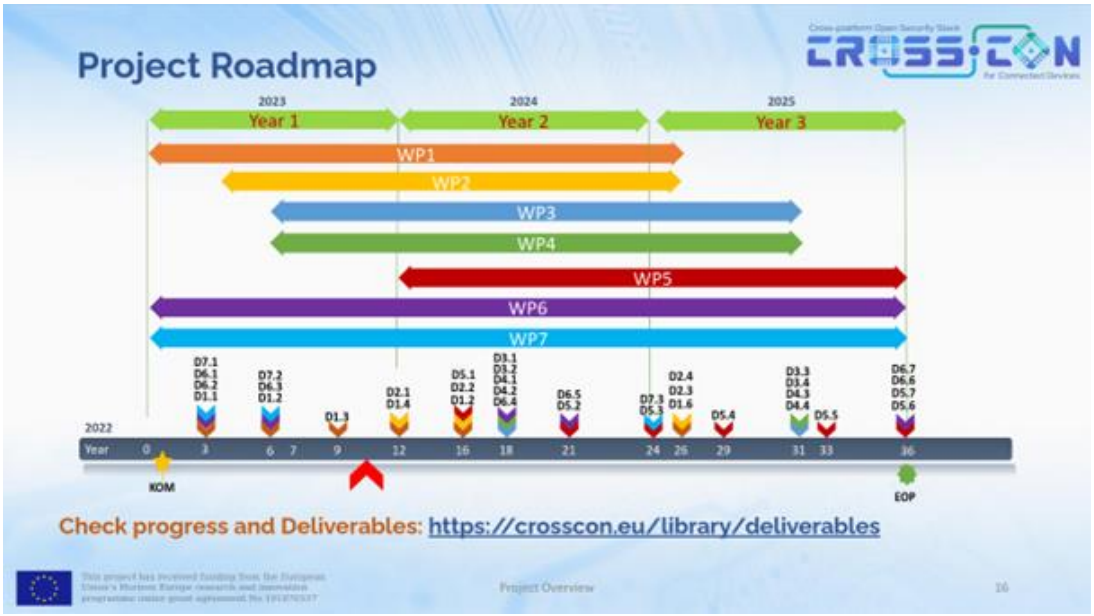
CROSSCON Stack

CROSSCON Stack Overview:

- Extends **interoperability** across heterogeneous devices;
- Offers a unified level of **abstraction** across **multiple hardware platforms**;
- Enriches existing **security** features by adding **new trusted services**;




CROSSCON Approach
7 Work Packages (WPs) allocated to different leaders:
WP1 Leader: ATOS
WP2 Leader: UNITN
WP3 Leader: UMINHO
WP4 Leader: BEYOND
WP5 Leader: SLAB
WP6 Leader: ATOS
WP7 Leader: ATOS
WP1 Requirements and Validation Criteria
WP2 Design Specification and Assurance for IoT
WP3 Development of CROSSCON Stack
WP4 CROSSCON for Domain Specific Hardware Architectures
WP5 Integration and Validation
WP6 Dissemination, Exploitation and Impact Creation
WP7 Project Management
Project Overview
15


Project Roadmap
2023
2024
2025
Year 1
Year 2
Year 3
WP1
WP2
WP3
WP4
WP5
WP6
WP7
2022
Year
KOM
EOP
Check progress and Deliverables: https://crosscon.eu/library/deliverables
Project Overview
16


Get in touch:
contact@crosscon.eu
in/crosscon
www.crosscon.eu
@crosscon_eu
SCAN FOR MORE!
Project Overview
18


Thank You!
Cross-platform Open Security Stack
CROSS-CON
for Connected Devices
Atos
UNIVERSITÀ DI TRENTO
SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY
barbara
UNIVERSITÄT WÜRZBURG
TECHNISCHE UNIVERSITÄT DARMSTADT
BEYOND SEMICONDUCTOR
3MDEB
CYSEC
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537
Project Overview
19