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

D6.6 Dissemination, Communication and Community Building Final Report

Document Identification			
Status	Final	**Due Date**	31/10/2025
Version	1.0	**Submission Date**	27/11/2025

Related WP	WP6	**Document Reference**	D6.6
Related Deliverable(s)	D6.1, D6.2, D6.4	**Dissemination Level (*)**	PU
Lead Participant	UMINHO	**Lead Author**	Tiago Gomes
Contributors	UMINHO	**Reviewers**	UWU
			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.

(*) 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	01/09/2025	João Sousa (UMINHO)	Draft version / TOC
0.2	15/09/2025	João Sousa (UMINHO), Tiago Gomes (UMINHO)	Update Dissemination and Communication Content (Website/Publications/Events/Other)
0.3	22/09/2025	João Sousa (UMINHO), Tiago Gomes (UMINHO)	Update Dissemination and Communication Content (Community building/KPIs/Conclusions)
0.4	30/09/2025	João Sousa (UMINHO), Tiago Gomes (UMINHO)	Update Dissemination and Communication Content (Social Media Statistics/KPIs/Introduction)
0.5	18/10/2025	João Sousa (UMINHO), Tiago Gomes (UMINHO)	Document ready for internal review.
0.6	26/11/2025	Juan Alonso (ATOS)	Quality Assessment.
1.0	27/11/2025	Hristo Koshutanski (ATOS)	Final version submitted.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tiago Gomes (UMINHO)	31/10/2025
Quality manager	Juan Andres Alonso (ATOS)	26/11/2025
Project Coordinator	Hristo Koshutanski (ATOS)	27/11/2025

Table of Contents

List of Figures

List of Acronyms

Abbreviation / acronym	Description
CROSSCON	Cross-platform Open Security Stack for Connected Devices
D6.2	D6.2 Dissemination and Communication Plan
D6.4	D6.4 Dissemination, Communication and Community Building First Report
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 during the CROSSCON project by all partners, aligned with the dissemination and communication strategy and plan outlined in D6.2 [3], spanning from January (M3) to October 2025 (M36). 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.

Different dissemination and communication strategies were employed to target various audiences. General channels were used to engage a broad target audience and communicate the project's value, while specific content was disseminated to reach more focused audiences. As outlined in D6.2 [3], dissemination efforts included publishing scientific papers and participating in conferences. On the other hand, communication activities focused on managing digital and social media channels to share project updates and creating content in various formats for external audiences.

This approach has enabled CROSSCON to promote its work and results through several activities. The results achieved include:

- **Website:** 10K established sessions, 7.6K page views, 3.2K different users.
- **Social media:** 500+ followers, 17K impressions (12K on Twitter and 5K on LinkedIn), 743 interactions (367 on Twitter and 376 on LinkedIn).
- **Communication Material:** 7 YouTube Videos, 2 Brochures, 3 Press Release, 4 Newsletters, 1 General Presentation and 24 Blog Posts, at least 5 Media Hits.
- **Dissemination Material:** 8 journals, 39 conferences, 3 white paper, 42/11 events attended/organized, 3 winter/summer schools, 14 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.

1 Introduction

Dissemination and communication tasks are part of task T6.1 - *Dissemination and Communication* of WP6. This task aims to make the project's results publicly available through appropriate channels, ensuring they reach diverse stakeholder groups and can be applied in their respective domains. These tasks follow a defined plan and adopt targeted strategies to promote outcomes to both specialized and general audiences. Activities focus on enhancing visibility and fostering engagement by reaching out to society and demonstrating how EU funding contributes to addressing security challenges.

1.1 Purpose of the Document

Reporting on dissemination and communication activities supports the assessment of the project's impact by tracking how information is received and absorbed by different audiences [1]. As a public report, it also ensures transparency regarding the project's findings, results, and progress.

This document provides the final report on dissemination, communication, and community building, detailing all actions undertaken by CROSSCON during the project's lifetime, including those already covered in the first half of the project. It covers website statistics, the monitoring of communication tools and social media channels, stakeholder engagement, publications, conferences attended and organised, and training activities.

1.2 Relation to Other Project Work

The D6.6 belongs to the WP6, and it is related to following deliverables:

- **D6.1** ***Project Website [2]***. This deliverable reports on the project website, including its layout, structure, and content management. It connects to the present document by providing the infrastructure for monitoring the visibility of project results worldwide.
- **D6.2** ***Dissemination and Communication Plan [3].*** This deliverable defines the strategy and plan of actions for the dissemination and communication activities. These activities aimed to raise awareness about the CROSSCON project towards different target groups.
- **D6.4** ***Dissemination, Communication and Community Building - First Report [11]***. This deliverable presented the initial results of dissemination and communication activities, stakeholder engagement, advisory board interactions, and training activities during the first 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

At the project's start, a dissemination and communication strategy and plan were defined and documented in deliverable D6.2 [3]. Since then, WP6 activities have followed this plan, while also adapting to the project's key phases to enhance visibility and engagement. This chapter outlines the updates to the dissemination and communication strategy and plan over the project duration. Figure 1 presents the key project stages, events, blog posts, and other dissemination and communication actions. This diagram also serves as a reference for the remainder of the document, helping to position any T6.1 activity within the overall project timeline.

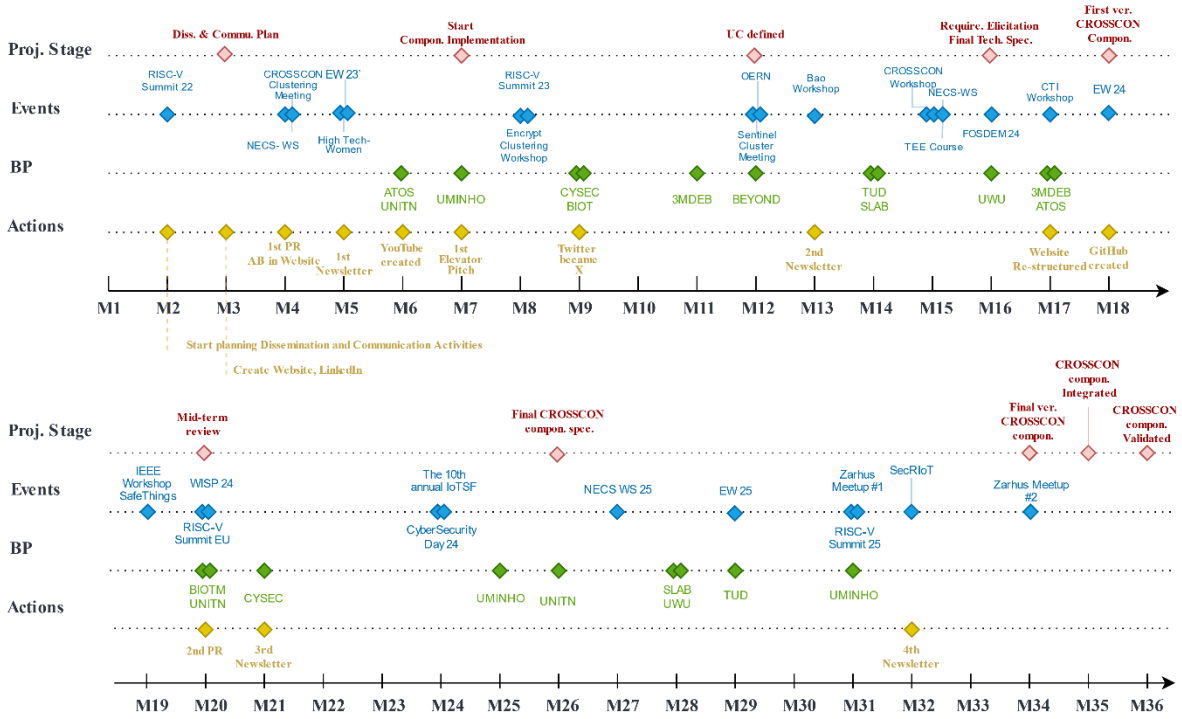


Figure 1: Timeline of key project stages, events, blog posts, and dissemination activities throughout the project.

2.1 Strategy from first to the second half of the project

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 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 (M4 and M15), have been utilized to attract a younger audience from the scientific community.

In the second part of the project (beginning in M18), communication and dissemination activities shifted from project-oriented to result-oriented, as the first version of CROSSCON components were launched (M18). 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, continue to attend and organize several workshops and events targeting industry stakeholders. As the project has progressed, CROSSCON components have matured, been integrated with one another, and validated as part of the use cases.

2.2 Communication Channels Progression

As part of its communication channels, Task 6.1 focuses on maintaining social media platforms, as they provide the most efficient means of interaction and real-time updates on the project. CROSSCON's social media presence includes LinkedIn, Twitter/X, YouTube, and GitHub. The LinkedIn and Twitter accounts were launched at M3 (with Twitter later rebranded as X at M9). A YouTube channel was created at M6, with the first video published at M7, which received 42 views and 3 likes. Figure 2 illustrates the homepage of the CROSSCON YouTube account. Throughout this document, Twitter will be referred to as Twitter/X.

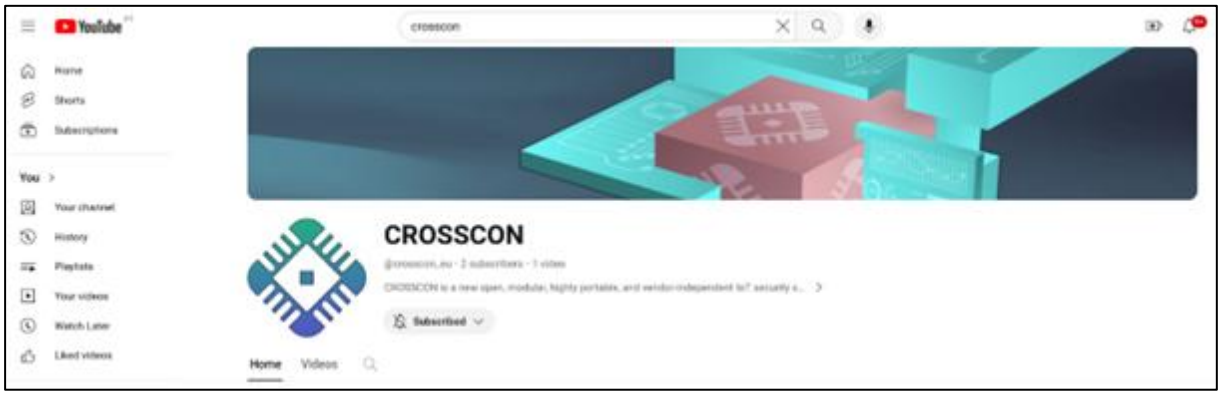


Figure 2: CROSSCON YouTube homepage.

In addition to addressing changes in social media channels, T6.1 uses other communication materials, such as press releases (M4, M20 and M36), blog posts (listed in Table 8), media hits, newsletters (M5, M13, M21 and M32) , 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.

2.3 Website Progression

The project's website, as detailed in previous deliverables D6.1 [2], D6.2 [3] and D6.4 [11], 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 first half of the project, the project's website structure faced slight changes to facilitate its navigation and overall organization. Currently, the menu bar contains different sections, as detailed in Figure 3. 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 blogs, newsletters, events and all other 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.

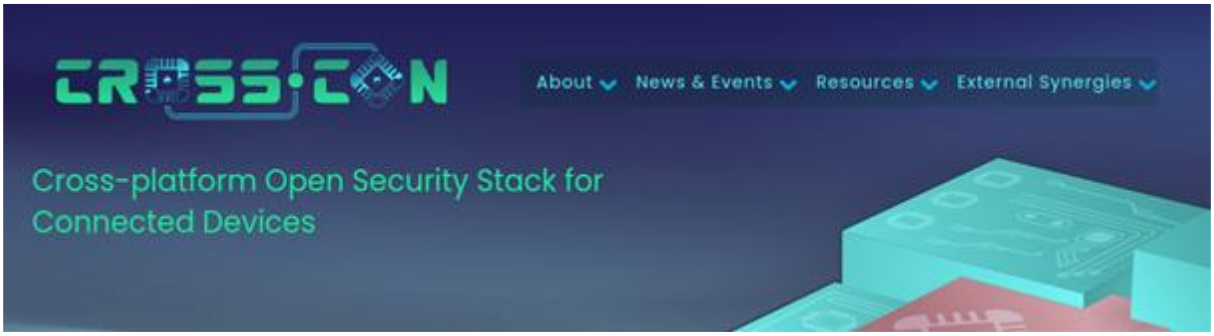


Figure 3: CROSSCON Website modified homepage.

The Advisory Board section of the project website was used as a key channel for disseminating information and facilitating communication with different stakeholders. Through this section, CROSSCON aimed to reach diverse communities, including researchers, industry professionals, and policymakers. In particular, established communities and ecosystems, such as RISC-V, served as entry points to engage a wide range of interested parties. The Advisory Board section of the website listed the following members:"

- **Calista Redmond**, CEO, RISC-V International (RISC-V.org), US
- **Paul Kearney**, IoT Security Foundation, UK
- **Detlef Houdeau**, Senior Director, Business Development, Infineon Technologies AG, DE
- **Nick Kossifidis**, ICS-FORTH / RISC-V TEE WG Chair, GR
- **Jürgen Schönwälder**, Jacobs University, DE
- **Argyro Chatzopoulou**, TÜV TRUST IT GmbH, AT

In the same website section, we also highlighted other European projects that created synergies with CROSSCON. These included **ENTRUST, ARCADIAN-IoT, SecOPERA, IoT-NGIN, REWIRE, ERATOSTHENES, ORSHIN, and CERTIFY.**

3 Dissemination and Communication Activity Report

This chapter provides the CROSSCON dissemination and communication report of all activities performed during M1 to M36, 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 during first half of the project, "Publications" section, some CROSSCON publications were propagated through social media channels, including reference links that redirect people to these website sections. Such dissemination activity made people to visit CROSSCON publications more often and allow us to pass from 317 views in first half of the project to 833.

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

Page Tittle and screen class	Views[M18]	Views[M36]
CROSSCON-Platforms Open Security Stack for Connected Devices	1587	5516
Blog	317	732
Publications	317	833
News	281	371
Library/Deliverables	241	366
Use Cases	240	368
Events	236	795
Dissemination Material	235	402
Consortium	207	361

3.1.2 CROSSCON Website: Views per Country

Figure 4 summarises the user's interaction by showing their country's location during first half of the project. 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 had already spread to all continents. Given the data results, Portugal (with a total

of 542) and Madrid (with a total of 317) were 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 4: Website Traffic by country.

During the second half of the project, the numbers changed slightly. Table 2 shows the number of views per country throughout the entire project. So far, the United States (1,608 views), Germany (943 views), and Portugal (908 views) are the countries where CROSSCON has achieved the highest reach.

Table 2: Website views per country.

Page Tittle and screen class	Views[M18]
United States	1608
Germany	943
Portugal	908
Spain	583
Italy	466
Netherlands	265
Poland	246
Greece	238
Switzerland	213

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. To analyse the sources of website's visitors we use the following channel groups:

- 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.

Observing Figure 5, during the first half of the project, results show that Direct channel groups established significantly more sessions than any other channel. Specifically, on the CROSSCON website, a total of 2.9K direct sessions were recorded, which can be attributed to the user-friendly and easily recognizable website domain. Since the website URL includes the project's name and the ".eu" domain

(commonly used for European projects), it is considered a predictable and intuitive address for users to search for. Conversely, the Unassigned channel group registered the lowest number of sessions. These users typically accessed the website through alternative methods, such as QR codes.

Throughout the entire project duration (until M36), although the number of sessions increased across all channel groups, the overall pattern of user behaviour remained consistent. An additional observation is that the number of Referral Group Sessions increased substantially, from 315 to 1,400, likely due to the inclusion of links in CROSSCON's social media publications that redirected users to the project website.

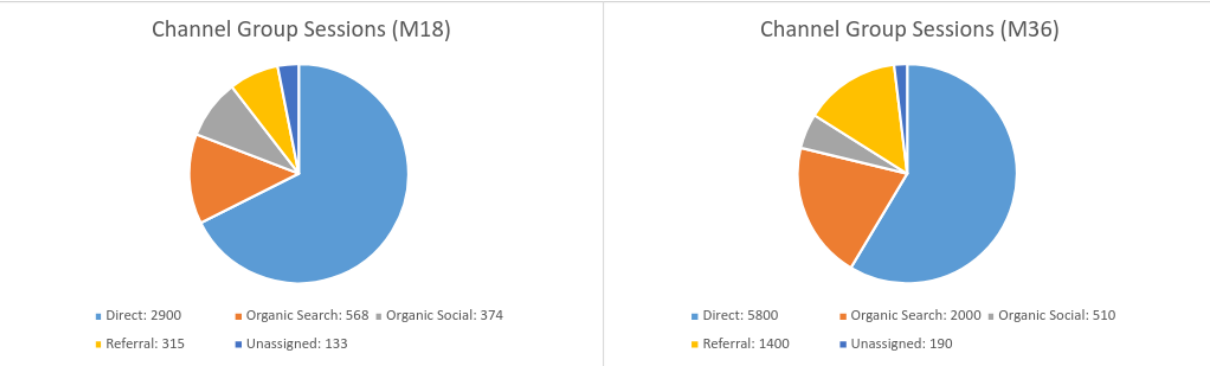


Figure 5: Channel Group Sessions of the CROSSCON Website (M18 and M36).

3.1.4 CROSSCON Website: Traffic Interaction

Figure 6 depicts a graphic showing the percentage of visitors' interactions with the CROSSCON website since January 1st (M3), related to a total of 7.6K users. Results show interaction in all months of the project, achieving a peak around 500 visitors near M20. This could be justified with the presence of project members on several conferences in these last months of the project (e.g., CROSSCON & (Secure)Friends in RISC-V Summit Europe).

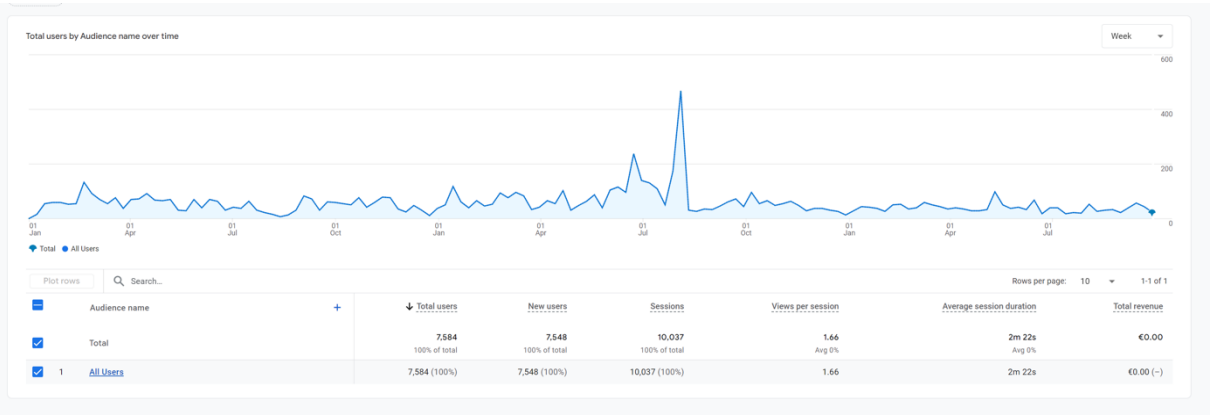


Figure 6: Traffic interaction of the CROSSCON website during the project lifetime.

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, GitHub 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 topics aligned with CROSSCON goals.

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 third-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. A notable example is the SecureCyber Cluster LinkedIn page, which has published posts mentioning CROSSCON and contributing to broader visibility and engagement [5]. The Cyber Threat Intelligence (CTI) cluster, was organized by several EU-funded projects with the goal of gathering, producing, and sharing critical cyber threat information, specifically for IoT environments. Such collaboration was possible thanks to the SENTINEL Cluster Meeting Event.

3.2.1 Twitter/X

Since the last deliverable, the project's Twitter/X account counts a total of 82 followers and 77 posts. Figure 7 illustrates the CROSSCON's Twitter/X profile, while Figure 8 illustrates the impressions, likes and retweets generated over the last months in the Twitter social network Twitter/X. Overall of June 2023 (1800 views) and June 2024 (views 1505) 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.

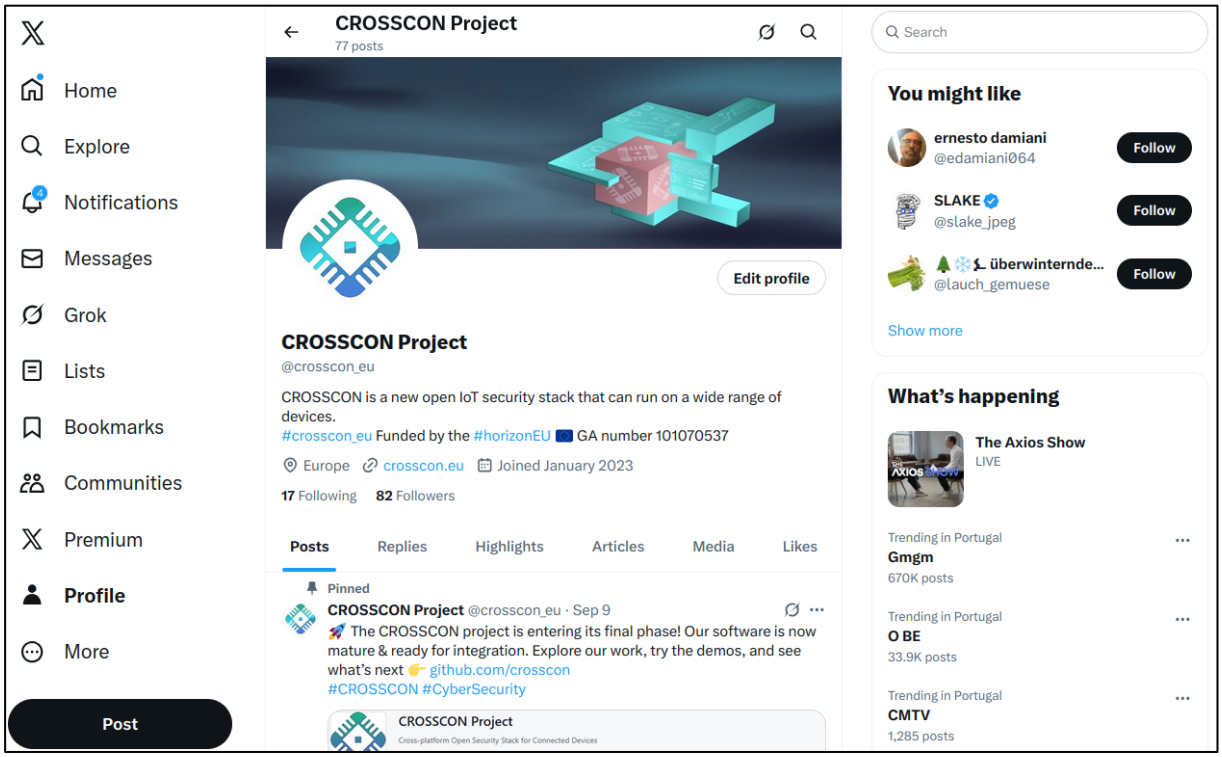


Figure 7: CROSSCON Twitter/X homepage.

As expected, the likes and retweets closely align with the impressions. A cumulative total of 238 interactions were collected, comprising 218 retweets, which expanded our reach and amplified the impact of tweets. Additionally, the posts achieved 367 likes, indicating the perceived value of the shared content.

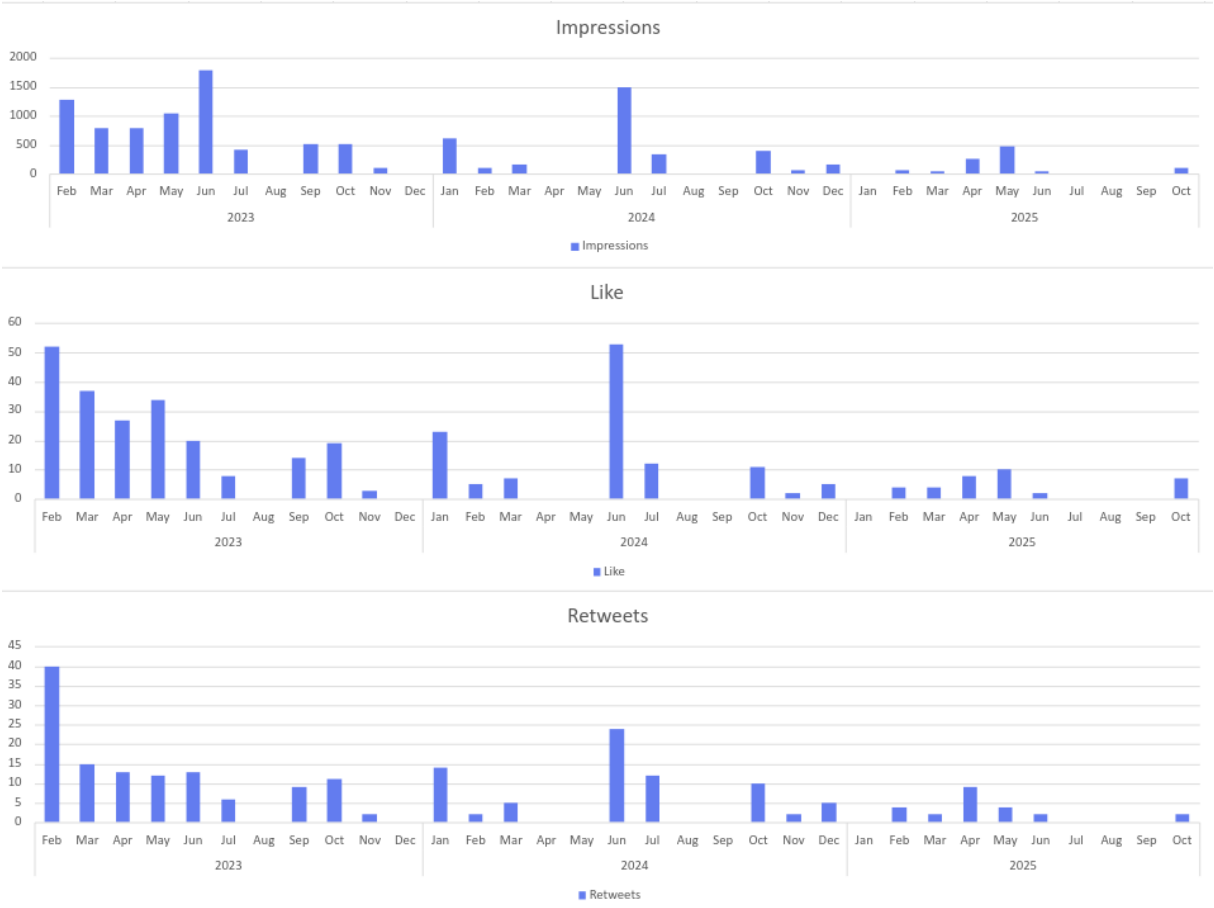


Figure 8: CROSSCON Twitter/X impressions, likes and retweets.

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 82 followers by the end of the project, as depicted in the following Figure 9.

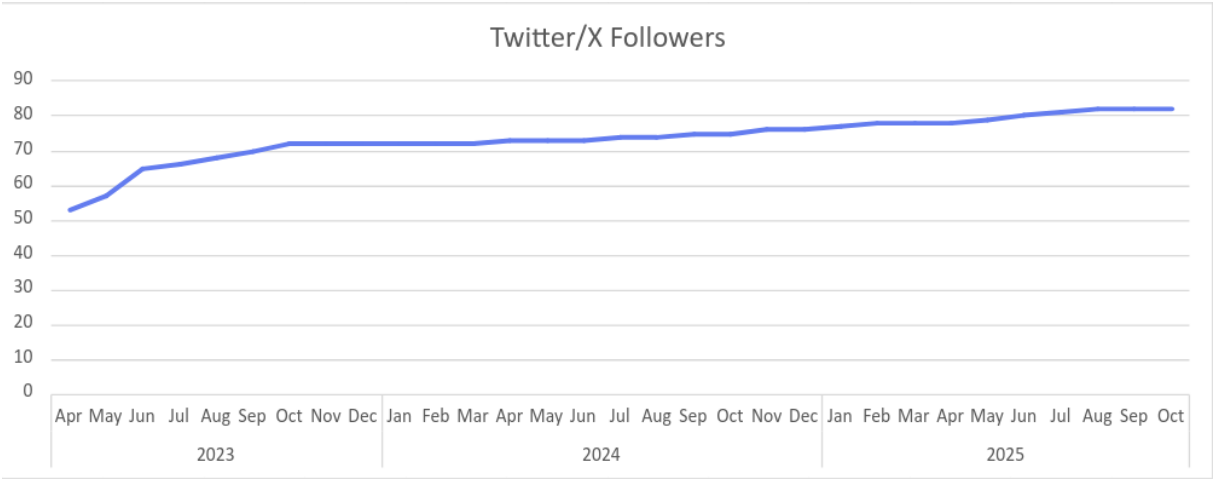


Figure 9: CROSSCON Twitter/X followers

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 280 connections.

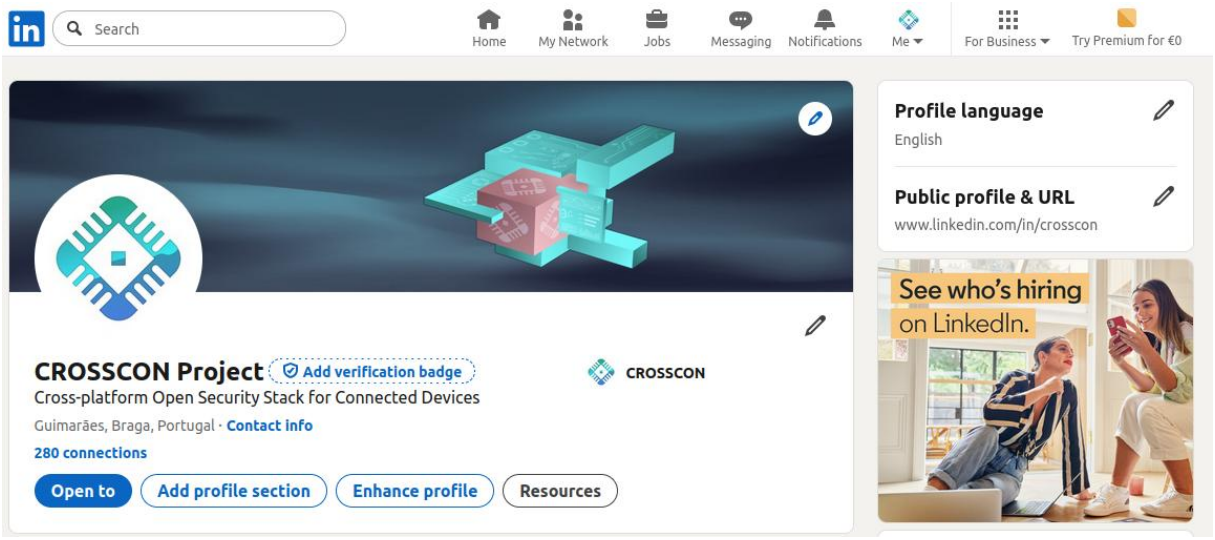


Figure 10: CROSSCON LinkedIn homepage.

Figure 11 illustrates the impressions generated over the last 14 months in LinkedIn. We were unable to collect statistics for the entire project duration due to limitations in LinkedIn's analytics tools, which do not allow retrieval of data covering the full project timeline.

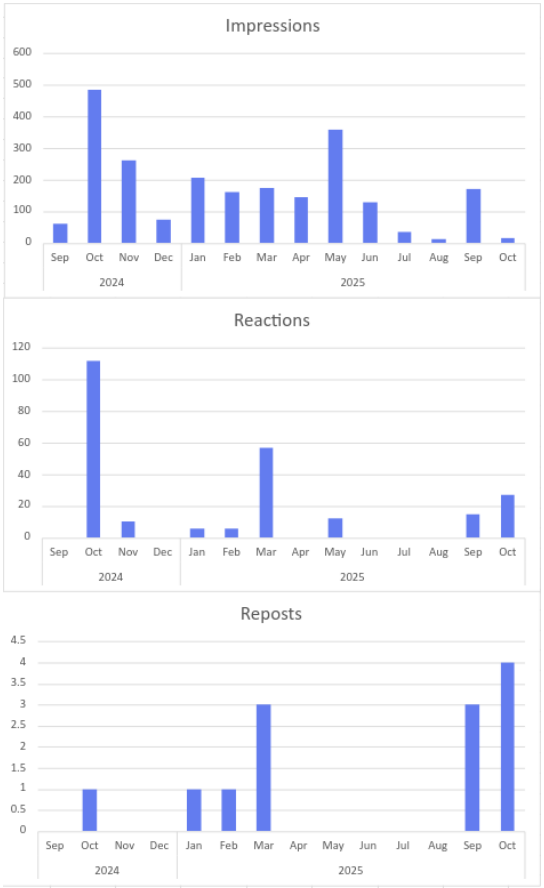


Figure 11: CROSSCON LinkedIn impressions, reactions and reposts.

October of 2024 (484 views) and May of 2025 (360 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. Additionally, month of May also had a high number of impressions, which can also be justified with RISC-V Europe Event publications. Notwithstanding, the month of August presents a low number of impressions, justified by the lack of social media publications. As expected, the likes closely align with the results. A cumulative total of 245 reactions were acquired, which expanded our reach and amplified the impact of our publications.

Regardless of the number of original publications on the CROSSCON LinkedIn profile, the number of followers increased with a constant pace until reaching 296 followers in October 2025, as depicted in the following Figure 12.

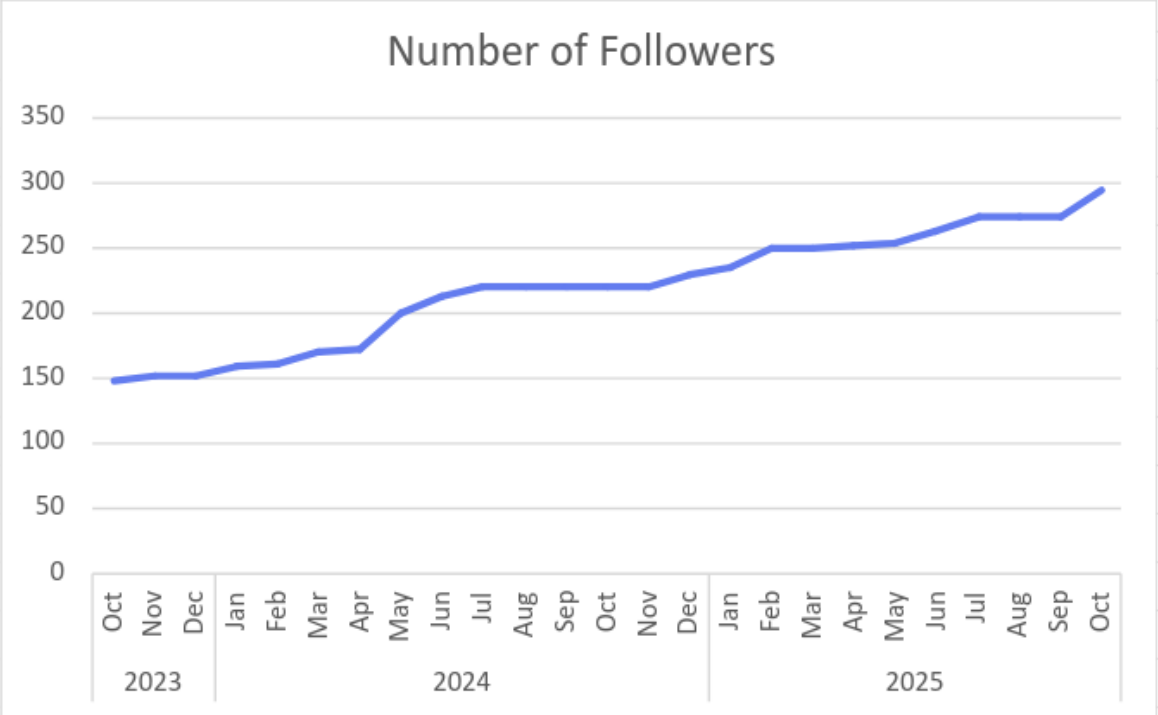


Figure 12: Number of followers of CROSSCON business LinkedIn account.

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, YouTube contains seven CROSSCON related videos:

- **CROSSCON Introduction (link):** In this video, illustrated by Figure 13, 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 46 views and 3 likes. Take into consideration 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 13: Video Introducing CROSSCON on YouTube.

- **Hello Bao World - Virtual Workshop (link)**: In this video, illustrated by Figure 14, CROSSCON propagates the first organized training session, which introduces the Bao Hypervisor, a hypervisor developed by one of the CROSSCON partners, the University of Minho (UMINHO). Since its publication date, this video has achieved a total of 1178 views and 23 likes.

Figure 14: YouTube Video of Bao virtual workshop.

- **CROSSCON Security Stack – CTI Workshop (link):** The video shown in Figure 15 corresponds to CROSSCON's participation in the joint workshop "Cyber Threat Intelligence: Empowering IoT Security", organized by the SecureCyber Cluster. The event gathered over 70 participants and featured presentations and live demonstrations from several EU-funded projects, fostering knowledge exchange and collaboration across research initiatives. Since its publication, the video has reached 489 views and 4 likes, highlighting the community's interest in CROSSCON's contributions.

Figure 15: YouTube Video of CTI workshop.

- **Securing Embedded Systems with fTPM implemented as Trusted Application in TEE" (link):** The video, illustrated by Figure 16, shows the presence of CROSSCON at FOSDEM 2024. It introduces the concept of implementing a firmware Trusted Platform Module (fTPM) as a Trusted Application within a Trusted Execution Environment (TEE). Our talk explores the fundamentals of TPM, its variations, and the advantages of fTPM in embedded systems, particularly leveraging Arm TrustZone. Since its publication, the video has reached 68 views and 2 likes.

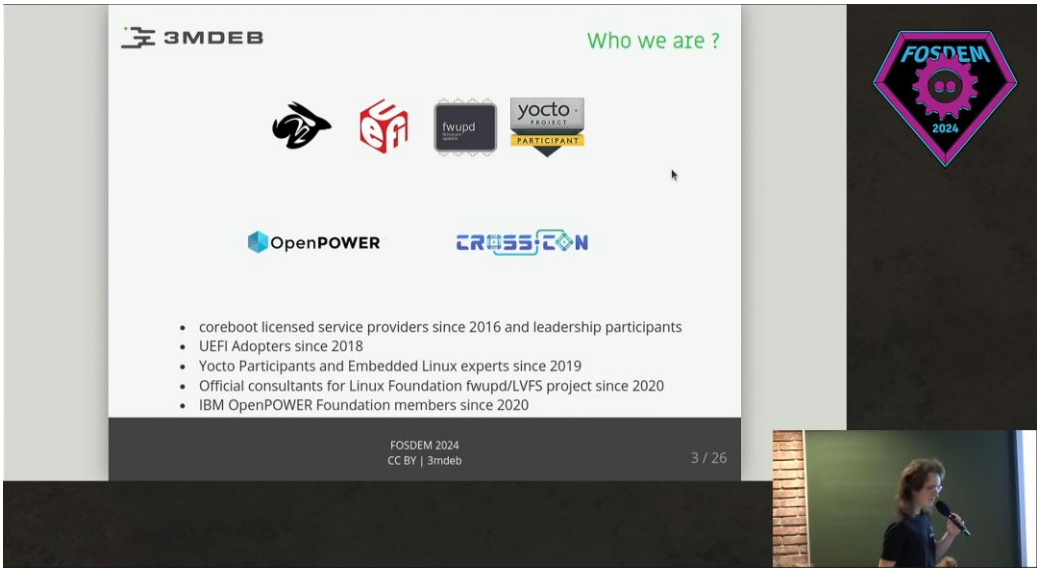


Figure 16: YouTube Video of FOSDEM presentation.

- "**Segurança em dispositivos e aplicações IoT" (link):** This video shown in Figure 17 corresponds to CROSSCON's participation in a webinar organized by OERN, the Northern Regional Section of the Portuguese Engineers' Association. During this event, the CROSSCON project highlighted its role in enhancing security and emphasized its collaborative efforts with academic and industry partners to create a versatile security stack for diverse devices. Since its publication, the video has reached 80 views and 1 like.

Figure 17: YouTube Video of OERN webinar.

- **"ZARHUS Developers Meetup #01" (link) and "ZARHUS Developers Meetup #02" (link),** illustrated in Figure 18 and Figure 19, present two workshop events organized by 3MDEB. Both sessions focused on the CROSSCON Hypervisor, demonstrating its operation on MCU and APU devices. Collectively, the videos have gathered 85 views and 6 likes.

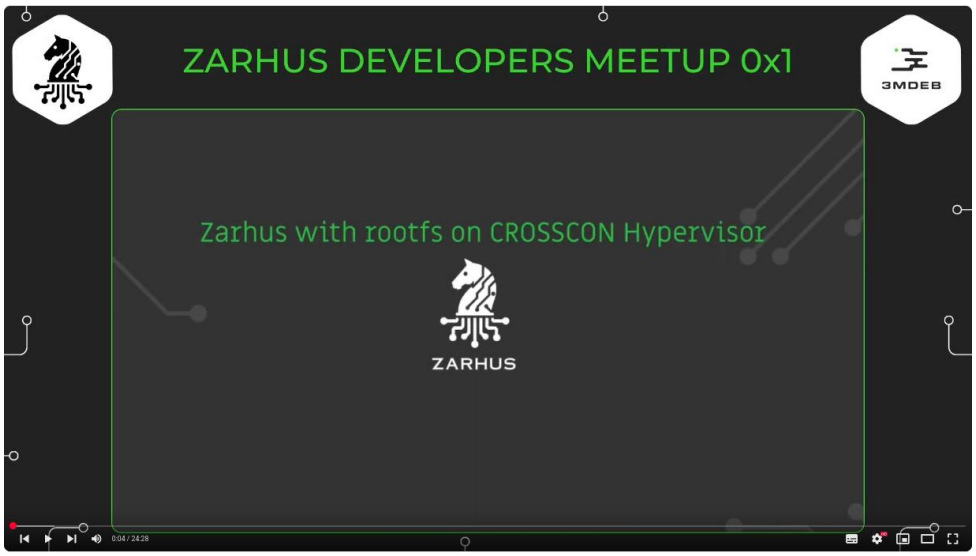


Figure 18: YouTube Video of Zarhus meetup #1.

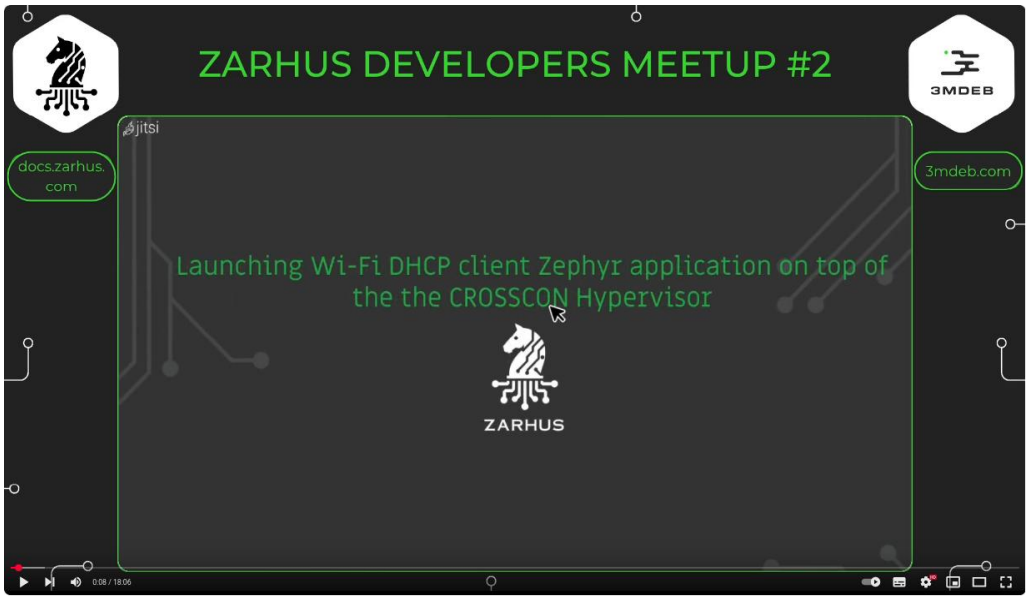


Figure 19: YouTube Video of Zarhus meetup #2.

3.2.4 GitHub

Since the beginning of second half of the project, partners have been contributing their individual implementations to the CROSSCON GitHub page. GitHub was chosen as the central platform because it provides a collaborative environment for code sharing, version control, and community engagement, making it ideal for fostering both transparency and innovation within the project.

By releasing our work as open source, we not only promote the visibility of our components but also enhance their quality, as the wider community can contribute by identifying issues, suggesting improvements, and integrating the solutions into their own projects.

The CROSSCON GitHub page currently hosts 37 repositories. Table 3 lists four repositories with high number of stars, a metric that reflects how many users have marked a repository as a favourite. Among them *"CROSSCON Hypervisor"* is the most stared repo from users with a total of 19 starts, *"CROSSCON-Hypervisor-and-TEE-Isolation-Demos"*, "*CROSSCON SoC*" with 6 starts and "*FPGA_TEE"* with 5 stars.

Table 3: List of most stared GitHub repositories.

Repo Name	Number of Stars
CROSSCON-Hypervisor-and-TEE-Isolation-Demos	7
crosscon_soc	6
CROSSCON-Hypervisor	19
FPGA_TEE	5

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. These meetings typically required a standardized presentation template, used both for project updates and for dissemination to general or specialized audiences.

This section aims at showing the CROSSCON presentation template. Figure 20 demonstrate the first and last slide of the presentations. Each presentation should include the project name, presentation date, presenter's name, presentation title, and, when applicable, the event name. The final slide should display the project logo, presenter contact information, EU acknowledgements, and partner logos. This template has been used in various contexts, for example, the CROSSCON presentation at the Sentinel Cluster Meeting in Lisbon, Portugal (M12).

Figure 20: Template of the first and last slide to be presented in a general or specialized presentation.

3.3.2 CROSSCON Newsletter Templates

Throughout the project, it is important to report key activities to the CROSSCON community by leveraging communication materials such as newsletters.

Figure 21: CROSSCON newsletter template.

Anyone subscribed to the project website automatically receives each newsletter by email upon its release. Up to now, CROSSCON delivered four newsletters, all 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 21). 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.

The second page takes the form of an introduction and summary, where a specific author (the one mentioned in the front page) contextualize the project's stage, highlights some key events, 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.

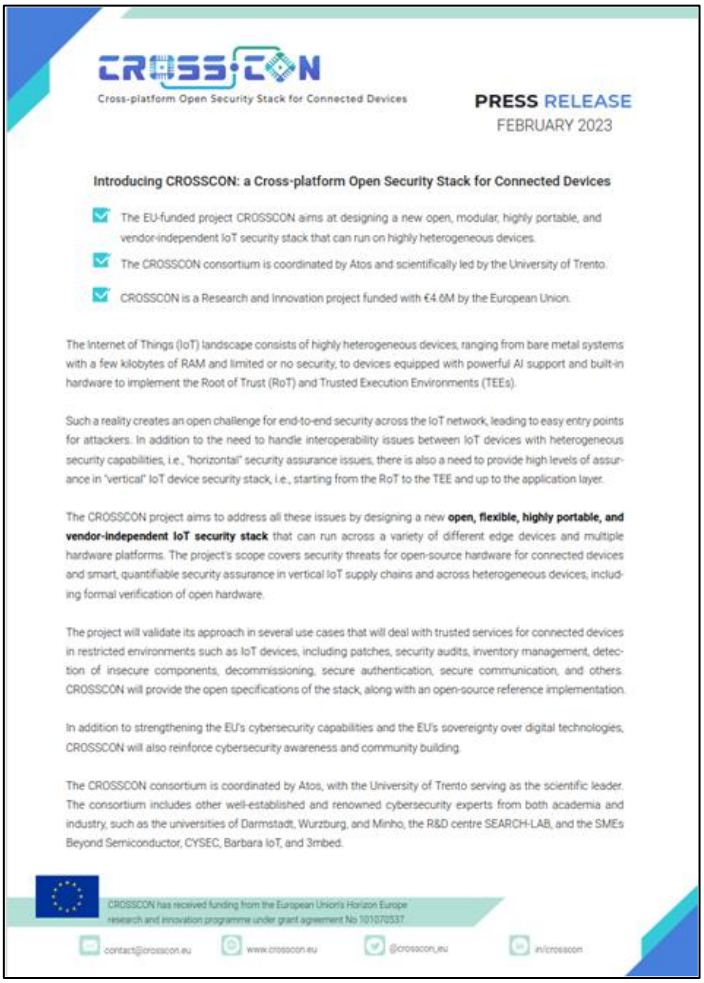
3.3.3 CROSSCON Blog Post Templates

To disseminate project results and share personal perspectives with a broader audience, while also updating readers within the project updates, blog posts are an effective communication tool, which published regularly. Figure 22 shows a website screenshot illustrating an example of a blog post. All blog posts follow the the same template, featuring an engaging title, the CROSSCON logo, the project's social media handles, and a photo of the author.

Figure 22: Blogpost banner example.

3.3.4 CROSSCON Press Release Template

A press release is a short, official piece of writing that organizations use to share important news with the public through the media. It's often used to announce things like project updates, new partnerships, product launches, or major achievements. The goal is to get journalists or media outlets to pick up the story and publish it, so the message reaches a wider audience. Like other communication materials, press releases follow a specific template, as illustrated on the page shown in Figure 23. The template includes the publication date, the project logo, and a brief summary of the milestones achieved and the progress made within the project.



CROSS:CON

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 23: First CROSSCON press release template.

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

Table 4 presents all scientific publications released under the CROSSCON project up to the date of this report. It lists each publication's title, venue, KPI type (conference or journal), contributing partners, and corresponding access link. All publications acknowledge the project in compliance with EC guidelines [4]. The last four entries do not include links, as they were accepted for presentation at upcoming conferences. Additionally, one scientific paper on TEE vulnerability analysis was submitted but rejected; it will be resubmitted shortly.

Table 4: List of scientific publications.

Title	Venue	Type	Partner	Link
Virtualization today, Virtualization tomorrow	Embedded World 2023	Conference	UMINHO	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	TUD	link
Interoperable IoT Security Stack: The RISC-V Opportunity	RISC-V Summit Europe 2023	Conference	ALL	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
The Nonce-nce of Web Security: an Investigation of CSP Nonces Reuse	ESORICS 2023	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 /TUD	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
A Novel Trusted Execution Environment for Next-Generation RISC-V MCUs	Embedded World 2024	Conference	UMINHO / BEYOND	link

HSP-V: Hypervisor-less Static Partitioning for RISC-V COTS Platforms	IEEE Access	Journal	UMINHO	link
PUF-based Authentication in IoT against Strong Physical Adversary using Zero-Knowledge Proofs	SafeThings 2024	Conference	UWU	link
Lost and Found in Speculation: Hybrid Speculative Vulnerability Detection	IEEE DAC	Conference	TUD	link
WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors	USENIX 2024	Conference	TUD	link
One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices	S&P 2024	Conference	TUD	link
Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems	IEEE GPECOM 2024	Conference	ATOS	link
Securing Embedded and IoT Systems with SPMP-based Virtualization	RISC-V Summit Europe 2024	Conference	UMINHO | BEYOND	link
FLAShadow: A Flash-based Shadow Stack for Low-end Embedded Systems	ACM Transactions on Internet of Things	Journal	UNITN	link
BiRtIO: VirtIO for Real-Time Network Interface Sharing on the Bao Hypervisor	IEEE Access	Journal	UMINHO	link
CVA6 MMU-less Virtualization – From Hardware to Software, and Vice Versa!	Embedded Word 2025	Conference	UMINHO	link
Certified Secure Updates for IoT Devices	ICT Systems Security and Privacy Protectio	Conference	UNITN	link
An open-source Trusted Execution Environment for Resource-Constrained RISC-V MCUs	RISC-V Summit EU 2025	Conference	UMINHO	link
Open-source SPMP-based CVA6 Virtualization	RISC-V Summit EU 2025	Conference	UMINHO	link
RLFuzz: Accelerating Hardware Fuzzing with Deep Reinforcement Learning	IEEE HOST	Conference	TUD/UWU	link
Firmware Secure Updates meet Formal Verification	ACM Transactions	Journal	UNITN	link

	on Cyber-Physical Systems			
AnyTEE: An Open and Interoperable Software Defined TEE	IEEE Access	Journal	UMINHO	link
AuthentiSafe: Lightweight and Future-Proof Device-to-Device	ACM ASIACCS 2025	Conference	UWU	link
Bridging the Interoperability Gaps among Trusted Architectures in MCUs	ICICS	Conference	UNITN | UMINHO	link
Valkyrie: A Response Framework to Augment Runtime Detection of Time-Progressive Attacks	DSN 2025	Conference	TUD	link
VoiceRadar: Voice Deepfake Detection using Micro-Frequency and Compositional Analysis	NDSS Symposium 2025	Conference	TUD	link
SafeSplit: A Novel Defense Against Client-Side Backdoor Attacks in Split Learning	NDSS Symposium 2025	Conference	TUD	link
Fuzzerfly Effect: Hardware Fuzzing for Memory Safety.	IEEE S&P	Journal	TUD	link
LightShed: Defeating Perturbation-based Image Copyright Protections	Usenix Security Symposium 2025	Conference	TUD	link
HFL: Hardware Fuzzing Loop with Reinforcement Learning	DATE 2025	Conference	TUD	link
GenHuzz: An Efficient Generative Hardware Fuzzer	Usenix Security Symposium 2025	Conference	TUD	link
GoldenFuzz: Generative Golden Reference Hardware Fuzzing	NDSS Symposium 2026	Conference	TUD	No link
Light2Lie: Detecting Deepfake Images Using Physical Reflectance Laws	NDSS Symposium 2026	Conference	TUD	No link
NeuroStrike: Neuron-Level Attacks on Aligned LLMs	NDSS Symposium 2026	Conference	TUD	link

Fuzzilicon: A Post-Silicon Microcode-Guided x86 CPU Fuzzer	NDSS Symposium 2026	Conference	TUD	link
Misbehavior Detection and Mitigation on 5G Core Services in Kubernetes	MSWiM 2025	Conference	ATOS	link
Towards a formal verification of the Bao Hypervisor	FPS 2025	Conference	UNITN	link

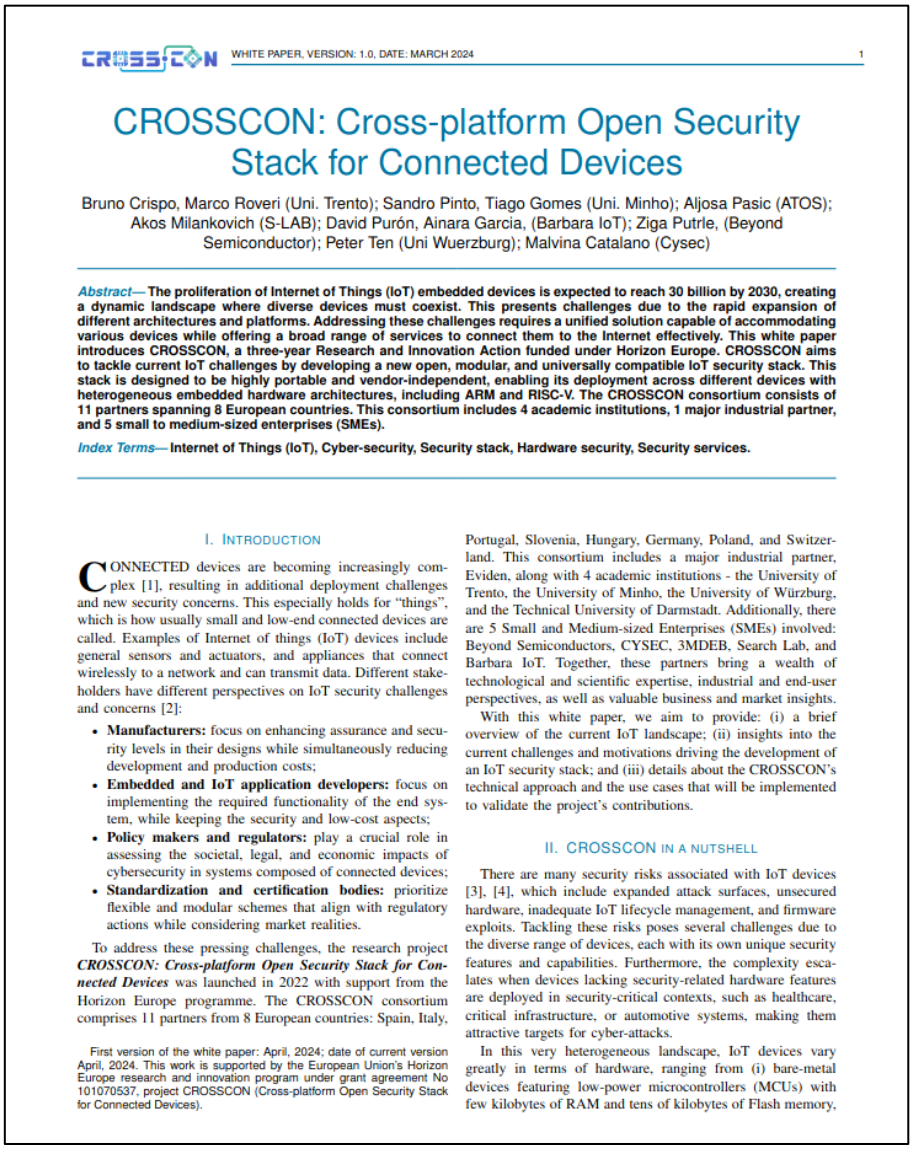
The collected information, summarized and represented in Table 5, includes data from various publications, distinguishing between journal and conference papers. We also categorized the publications by partner, with UMINHO, TUD, and UNTN standing out in terms of the number of contributions throughout the project. Among these publications, some were co-authored across partners. For these cases, we included a column clarifying how many publications were shared.

Table 5: List of number of publications per partner throughout the project duration.

Partner	Number of Conferences	Journals	Total	Shared
UMINHO	12	3	14	5
TUD	18	2	14	3
UNITN	8	3	10	3
UWU	5	0	5	3
BEYOND	3	0	3	3
ATOS	3	0	3	1
SLAB	1	0	1	1
CYSEC	1	0	1	1

3.4.2 White Papers

To disseminate the project's objectives, CROSSCON released two white papers, both available on the CROSSCON website. The first white paper outlines the project's key ideas and explains how they contribute to advancing the state of the art in building secure IoT devices. Additionally, it provides: (i) an overview of the current IoT landscape; (ii) insights into the challenges and motivations behind developing a dedicated IoT security stack; (iii) details of CROSSCON's technical approach; and (iv) the use cases selected to validate the project's contributions. Figure 24 presents the opening page of the white paper.



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 24: First page of the first white paper.

The CROSSCON project contributed to the joint white paper Gain Insights into the Latest Cybersecurity Trends from Horizon Europe Funded Projects (front page on Figure 25). This document is the result of a collaborative effort between eight EU-funded projects (AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, KINAITICS, REWIRE, TRUMPET, and TRUSTEE) and aims to consolidate knowledge and highlight emerging trends in cybersecurity. The white paper presents the vision, objectives, use cases, and core technologies of each project, addressing critical challenges related to data protection, privacy, and resilience against digital threats in domains such as healthcare, finance, and critical infrastructures.

CROSSCON's contribution focused on its proposal of a Cross-platform Open Security Stack for Connected Devices, an open, portable, and vendor-independent IoT security stack. The white paper outlines how CROSSCON seeks to overcome the architectural heterogeneity of the IoT ecosystem (including ARM, RISC-V, and different TEE implementations), by providing a security stack capable of delivering trusted services, strong isolation, and interoperability. Such collaborative dissemination reinforces the project's visibility, promotes knowledge exchange among European initiatives, and contributes to shaping the future of cybersecurity in Europe.

Figure 25: First page of the second white paper.

The joint white paper “Gain Insights into the Latest Empirical Cybersecurity Trends and Results from Horizon Europe Funded Projects” represents a collaborative effort between six European research initiatives: AI4CYBER, CERTIFY, CROSSCON, ENCRYPT, REWIRE, and TRUSTEE; all devoted to strengthening Europe’s cybersecurity capabilities. The publication highlights each project’s main objectives, research directions, architectures, and empirical results, focusing on technologies such as AI-driven cybersecurity, privacy-preserving computation, Trusted Execution Environments, and secure IoT frameworks. Together, these initiatives address critical challenges in data protection, regulatory compliance, and cyber resilience across diverse sectors, including healthcare, finance, and mobility. By promoting collaboration and knowledge exchange among Horizon Europe projects, the white paper contributes to advancing privacy-preserving technologies, enhancing trust and interoperability, and shaping a more secure and sovereign digital future for Europe.

Figure 26: First page of the third white paper.

3.5 Conferences, Workshops and Industry-Related Events

Through the project duration, 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 T6.1, 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 in Table 6, the events are grouped into three main categories: total number of events, summer schools, and other training events.

- **Total number of events:** This category includes all events, distinguishing between those organized by CROSSCON and those in which CROSSCON participated. It covers workshops (e.g., cluster meetings and specialized workshops), summer schools (e.g., educational programs and academic gatherings), training events (e.g., webinars and sessions designed for educational purposes), as well as other conferences not fitting into the previous categories.
- **Summer schools:** This category refers specifically to educational programs, school events, and academic gatherings hosted by institutions.
- **Others:** This category encompasses a broader range of events, including conferences and talks where CROSSCON partners were involved.

To describe all CROSSCON events participation and organisation during the last months, Table 6 and Table 7 include a list of each of them, respectively. Each event in the list we include a classification type, the corresponding event name, location, date, and the CROSSCON partner attendance. To classify the type, we adopt the following description: "Conf." for other events; "TE" for Training Event; "W" for workshop; and "SS" for summer school events.

Table 6: List of CROSSCON participated events.

Type	Event Name	Location	Date	Partner/s
Conf.	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
Conf.	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
Conf.	Embedded World 2023	Nuremberg, Germany	14-16 Mar 2023	UMINHO
Conf.	High-Tech Women	Darmstadt, Germany	30 Mar 2023	UWU
TE	CYSAT	Paris, France & Online	26-27 Apr 2023	CYSEC

Type	Event Name	Location	Date	Partner/s
Conf.	RISC-V Summit Europe 2023	Munich, Germany	05-09 Jun 2023	UMINHO
W	Encrypt - Clustering Workshop	Procida, Italy	6 Jun 2023	UNITN
W	ERATOSTHENES - 2nd Workshop: Trust and Identity Management for IoT	Online	16 Jun 2023	UMINHO
Conf.	European Symposium on Research in Computer Security	The Hague, Netherlands	25-29 Set 2023	UNITN
TE	Allpros Webinar	Online	20 Jun 2023	ATOS
W	EU-CIP Conference	Brussels, Belgium	20-21 Sep	ATOS
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 | TE	Bao Hypervisor Virtual Workshop	Online	15 Nov 2023	UMINHO
Conf.	ENLIT EUROPE - Making the Intelligent Power Grid Happen	Paris, France	28-30 Nov 2023	BIOT
SS |TE	NECS - PHD WINTER SCHOOL 2024	Cortina d'Ampezzo,Italy	8-12 Jan 2024	TUD, BEYOND, UWU
W	CROSSCON Workshop - Security Services for Connected Devices	Cortina d'Ampezzo, Italy	12 Jan 2024	TUD, BE3YOND, UWU
TE	TEE Course (SLAB)	Online	17 Jan 2024	SLAB

Type	Event Name	Location	Date	Partner/s
TE	FOSDEM 2024	Brussels, Belgium	Q1'2024 (Feb)	3MDEB
W	CTI Workshop	Online	6 Mar 2024	UMINHO
Conf.	Embedded World 2024	Nuremberg, Germany	9-11 Apr 2024	UMINHO, BEYOND
TE	CYSAT	Paris	24-25 Apr 2024	CYSEC
W	IEEE Workshop on SafeThings 2024	San Francisco	23 May 2024	UWU
Conf.	RISC-V Summit EU 2024	Munich, Germany	24-28 June 2024	UMINHO, BEYOND
W	WISP 2024	Salamanca, Spain	26-28 June	ATOS
TE	CyberSecurity Day	Pise, Italy	10-13 Oct 2024	UNITN
Conf.	The 10th Annual IoTSF Conference	London	23 Oct 2024	UNITN
TE	NXP Tech Days Milan 2024	Milan, Italy	22 Oct 2024	UNITN
W	WB3C: New Technologies and Cybersecurity	Podgorica, Montenegro	5-8 Nov 2024	Beyond
Conf.	SWII 2024 I Transformational Technologies for Net-Zero Societies	Empa. Dubendorf	11 Dec 2024	CYSEC
SS	NeCS Winter NECS - PHD WINTER SCHOOL 2025	Cortina d'Ampezzo (Italy)	20-24 Jan 2025	UNITN
Conf.	Embedded World 2025	Nuremberg, Germany	11, 13 Mar 2025	UMINHO
TE	Crypto-Chipset Security	Online	28 Aprl 2025	SLAB
W	Zarhus Developers meetup #1	Online	6 May 2025	3MDEB
W	RISC-V Summit EU	Paris, France	12 May 2025	UMINHO

Type	Event Name	Location	Date	Partner/s
W	SecRIot 2025	Tuscany, Italy	9-11 Jun 2025	UNITN
W	Cyber Security Workshop: Empowering NREN Institutions: Generative AI Training for Network Monitoring and Cyber Security	AIT, Thailand	25 Jul 2025	UMINHO, UNITN
W	Zarhus Developers Meetup #2	Online	5 Aug 2025	3MDEB

Table 7: 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 | 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
W	RISC-V Summit EU	Munich, Germany	28 Jun 2024	CROSSCON
W	WISP 2024	Salamanca, Spain	26-28 Jun 2024	ATOS
SS	NeCS Winter NECS - PHD WINTER SCHOOL 2025	Cortina d'Ampezzo, Italy	20-24 Jan 2025	UNITN
TE	Crypto-Chipset Security	Online	28 April 2025	SLAB
W	SecRIoT 2025	Tuscanny, Italy	9-11 Jun 2025	UNITN

Figure 27 illustrates the involvement of individual partners in events during the first half of the project, as well as an overview of the countries where these events took place. The statistical analysis shows that online events were the most frequent, with 11 occurrences, followed by Italy, which hosted five events and became the most visited country by the CROSSCON consortium.

Figure 27: Analysis on event participation by CROSSCON in first half of the project.

In the second half of the project, as illustrated in Figure 28, CROSSCON partners significantly increased their participation in events. UMINHO recorded the highest number with 14 participations, followed by UNITN with 10, and both Beyond and ATOS with 6 each.

In terms of geographical distribution, events participation became more widespread, with CROSSCON disseminating its work across multiple regions. Online events remained the most attended (11 in total), followed by Italy with 11 events and Germany with 6. This broader international presence likely contributed to the increased number of visits to the project website.

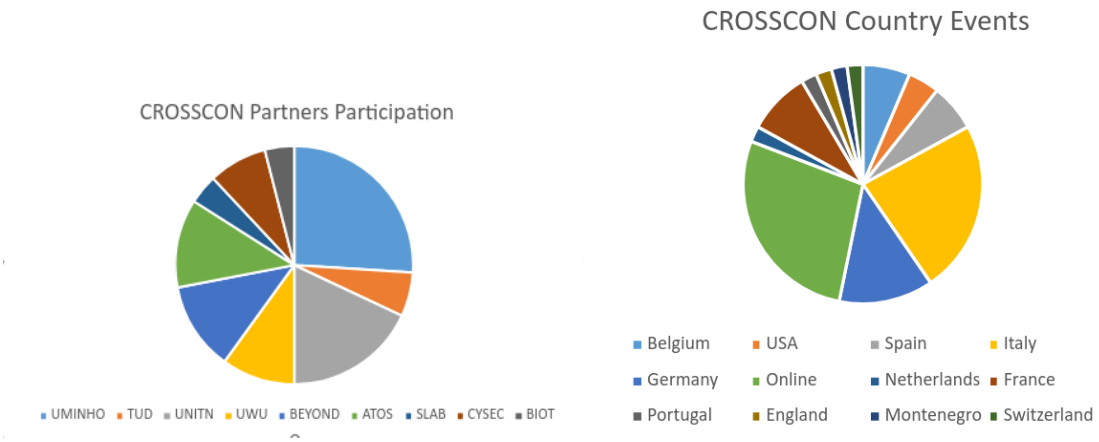


Figure 28: Analysis on event participation by CROSSCON in the end of the project.

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.
- **Zenodo:** Zenodo ensures accessibility, credibility, and sustainability, while also meeting the dissemination and open science obligations of CROSSCON.

3.6.1 CROSSCON Brochure

Figure 29 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.

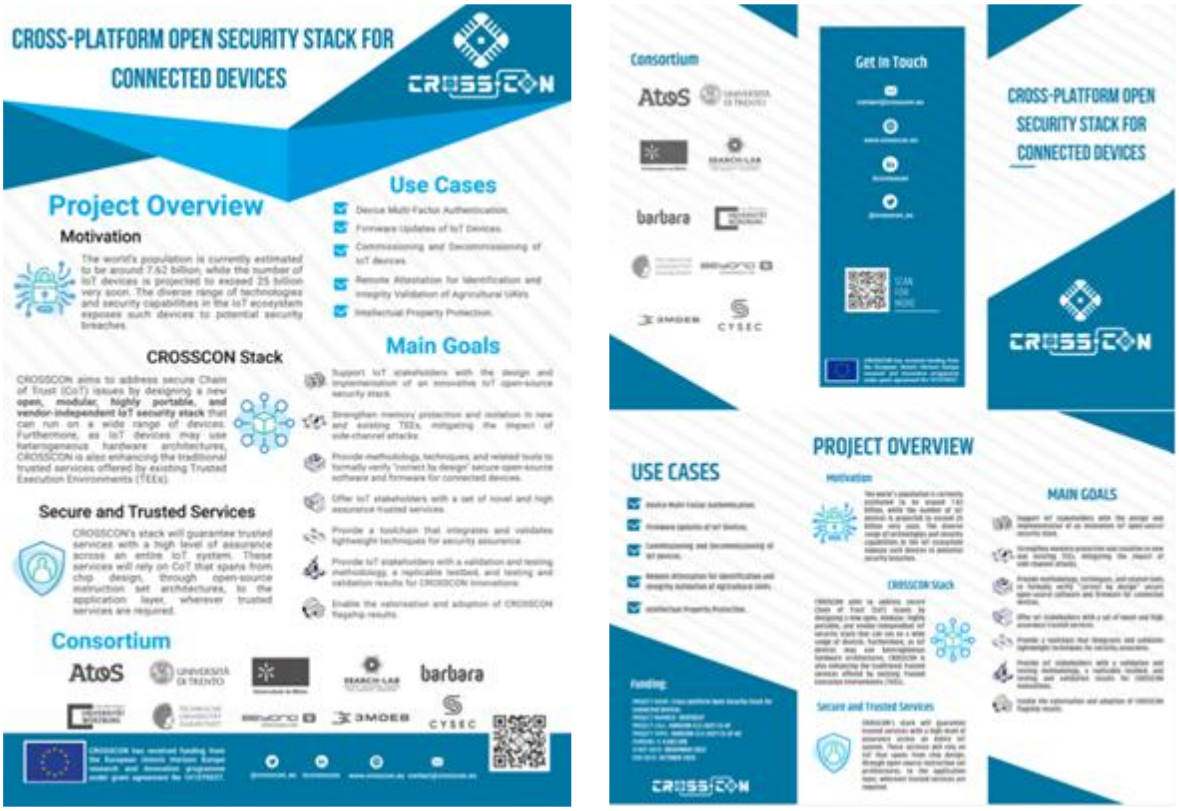
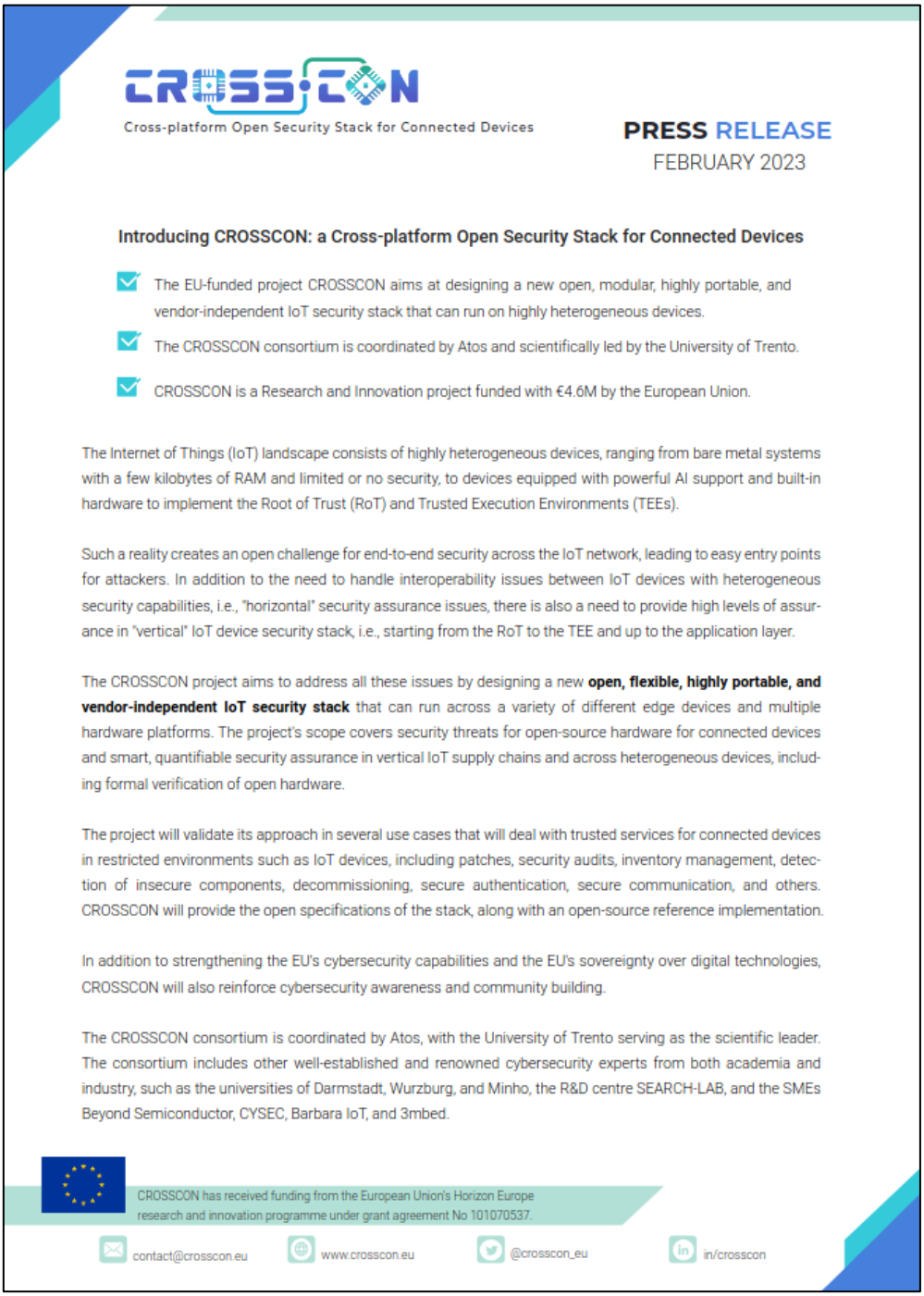


Figure 29: One-page and tri-fold brochures.

3.6.2 CROSSCON Press Release

Just as mentioned before. A press release is a brief official statement used to share important news, such as updates, partnerships, launches, or achievements, with the public through the media to reach a wider audience. Until date of writing CROSSCON launched 2 press releases. Figure 30 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).



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.

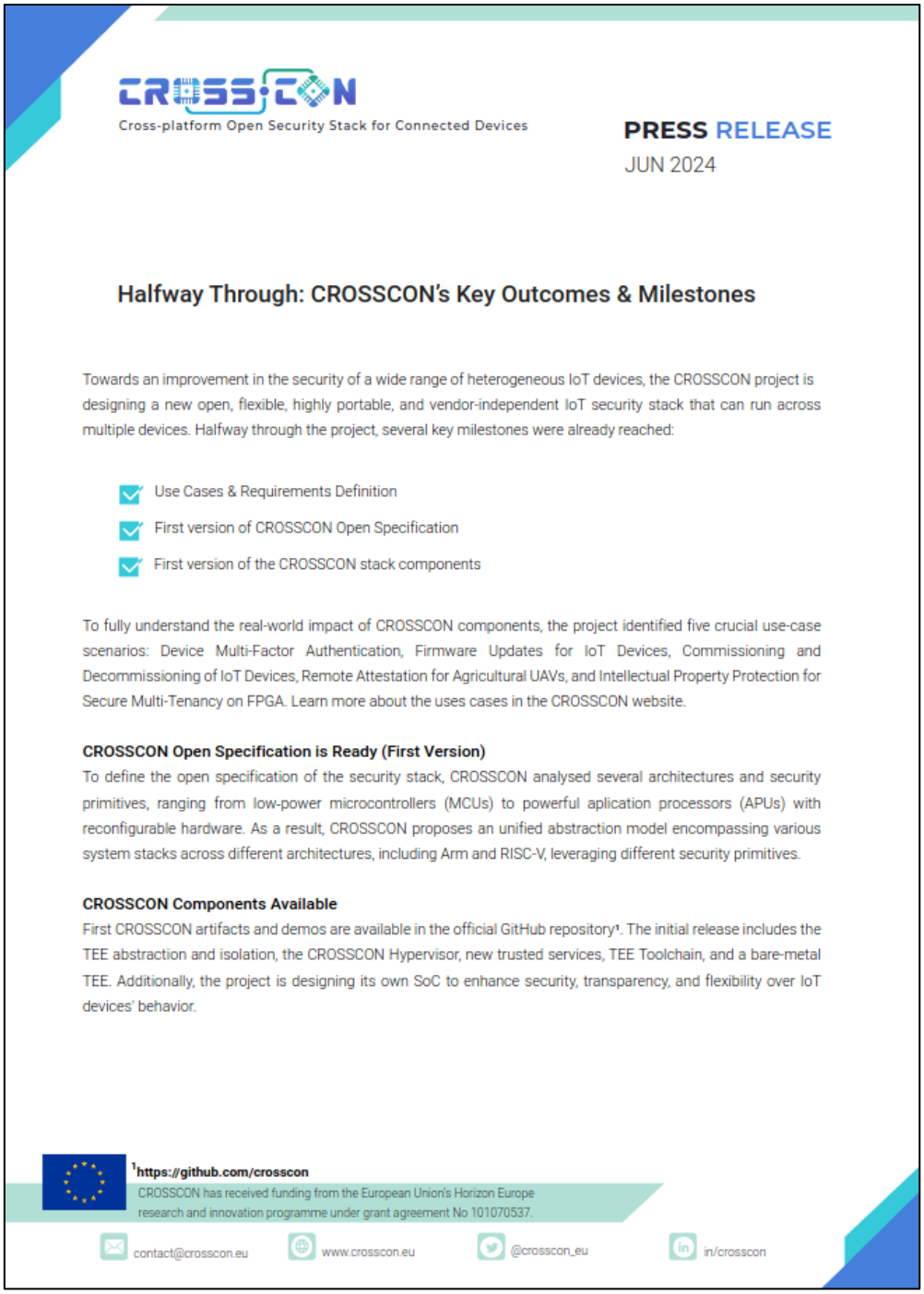
The CROSSCON consortium is coordinated by Atos, with the University of Trento serving as the scientific leader. The consortium includes other well-established and renowned cybersecurity experts from both academia and industry, such as the universities of Darmstadt, Wurzburg, and Minho, the R&D centre 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 30: First CROSSCON press release.

The second CROSSCON press release (June 2024), shown on the first page in Figure 31, highlights the project's progress at its halfway point. It first announces the release of the initial version of the CROSSCON Open Specification, which introduces a unified abstraction model for security stacks across heterogeneous architectures, including Arm and RISC-V, from low-power microcontrollers to high-performance processors with reconfigurable hardware. It also confirms five key use-case scenarios: (i) multi-factor authentication, (ii) secure firmware updates, (iii) commissioning and decommissioning of IoT devices, (iv) remote attestation for agricultural UAVs, and (v) intellectual property protection for FPGA-based secure multi-tenancy. Lastly, it announces the availability of the first version of CROSSCON stack components on GitHub, including the CROSSCON Hypervisor, new trusted services, a TEE toolchain, a bare-metal TEE and CROSSCON SoC.



Cross-platform Open Security Stack for Connected Devices

PRESS RELEASE

JUN 2024

Halfway Through: CROSSCON's Key Outcomes & Milestones

Towards an improvement in the security of a wide range of heterogeneous IoT devices, the CROSSCON project is designing a new open, flexible, highly portable, and vendor-independent IoT security stack that can run across multiple devices. Halfway through the project, several key milestones were already reached:

- Use Cases & Requirements Definition
- First version of CROSSCON Open Specification
- First version of the CROSSCON stack components

To fully understand the real-world impact of CROSSCON components, the project identified five crucial use-case scenarios: Device Multi-Factor Authentication, Firmware Updates for IoT Devices, Commissioning and Decommissioning of IoT Devices, Remote Attestation for Agricultural UAVs, and Intellectual Property Protection for Secure Multi-Tenancy on FPGA. Learn more about the uses cases in the CROSSCON website.

CROSSCON Open Specification is Ready (First Version)

To define the open specification of the security stack, CROSSCON analysed several architectures and security primitives, ranging from low-power microcontrollers (MCUs) to powerful aplication processors (APUs) with reconfigurable hardware. As a result, CROSSCON proposes an unified abstraction model encompassing various system stacks across different architectures, including Arm and RISC-V, leveraging different security primitives.

CROSSCON Components Available

First CROSSCON artifacts and demos are available in the official GitHub repository[1]. The initial release includes the TEE abstraction and isolation, the CROSSCON Hypervisor, new trusted services, TEE Toolchain, and a bare-metal TEE. Additionally, the project is designing its own SoC to enhance security, transparency, and flexibility over IoT devices' behavior.

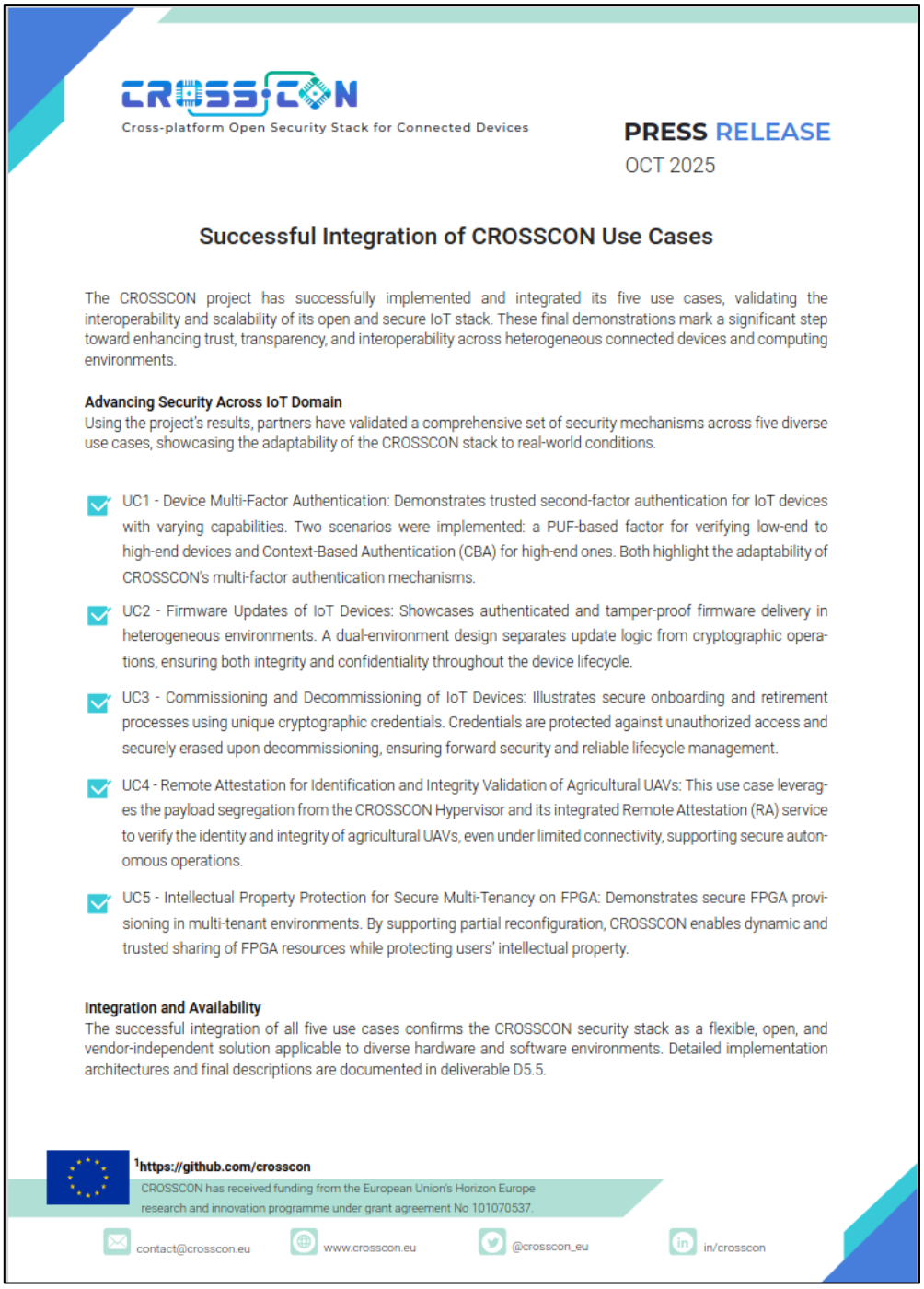
[1] https://github.com/crosscon

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 31: Second CROSSCON press release.

To conclude the project, **a third and final press release** was prepared for publication in M36. This final release will not only mark the official closure of the project but will also highlight the main conclusions from the Use Cases, which demonstrate the functionality and versatility of the CROSSCON stack across different environments, platforms and architectures.



CROSSCON

Cross-platform Open Security Stack for Connected Devices

PRESS RELEASE

OCT 2025

Successful Integration of CROSSCON Use Cases

The CROSSCON project has successfully implemented and integrated its five use cases, validating the interoperability and scalability of its open and secure IoT stack. These final demonstrations mark a significant step toward enhancing trust, transparency, and interoperability across heterogeneous connected devices and computing environments.

Advancing Security Across IoT Domain

Using the project's results, partners have validated a comprehensive set of security mechanisms across five diverse use cases, showcasing the adaptability of the CROSSCON stack to real-world conditions.

- UC1 - Device Multi-Factor Authentication: Demonstrates trusted second-factor authentication for IoT devices with varying capabilities. Two scenarios were implemented: a PUF-based factor for verifying low-end to high-end devices and Context-Based Authentication (CBA) for high-end ones. Both highlight the adaptability of CROSSCON's multi-factor authentication mechanisms.
- UC2 - Firmware Updates of IoT Devices: Showcases authenticated and tamper-proof firmware delivery in heterogeneous environments. A dual-environment design separates update logic from cryptographic operations, ensuring both integrity and confidentiality throughout the device lifecycle.
- UC3 - Commissioning and Decommissioning of IoT Devices: Illustrates secure onboarding and retirement processes using unique cryptographic credentials. Credentials are protected against unauthorized access and securely erased upon decommissioning, ensuring forward security and reliable lifecycle management.
- UC4 - Remote Attestation for Identification and Integrity Validation of Agricultural UAVs: This use case leverages the payload segregation from the CROSSCON Hypervisor and its integrated Remote Attestation (RA) service to verify the identity and integrity of agricultural UAVs, even under limited connectivity, supporting secure autonomous operations.
- UC5 - Intellectual Property Protection for Secure Multi-Tenancy on FPGA: Demonstrates secure FPGA provisioning in multi-tenant environments. By supporting partial reconfiguration, CROSSCON enables dynamic and trusted sharing of FPGA resources while protecting users' intellectual property.

Integration and Availability

The successful integration of all five use cases confirms the CROSSCON security stack as a flexible, open, and vendor-independent solution applicable to diverse hardware and software environments. Detailed implementation architectures and final descriptions are documented in deliverable D5.5.

[1]https://github.com/crosscon

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 32: Third 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 8 summarizes the blogposts available on the website, highlighting the title, partner, and date of publishing.

Table 8: List of CROSSCON blog posts.

Title	Partner	Planned Date	Published Date
We are open, but formal	ATOS+UNITN	M6	M6
TEEs are not Silver Bullets	UMINHO	M7	M7
Enhancing Security in Agricultural UAVs: The Power of Remote Attestation	CYSEC	M8	M9
Cybersecurity is a Community Effort	BIOT	M9	M9
Enhancing IoT Security through Device-to-Device Authentication	3MDEB	M10	M11
Information Flow Tracking: Enhancing Data Security and Privacy	BEYOND	M11	M12
FPGA-based Trusted Execution Environments and Their Use Cases	TUD	M12	M14
Ensuring the Integrity of IoT Devices: Best Practices for Secure Firmware Updates	SLAB	M13	M14
Trust as a Foundation for Secure Internet of Things Services	UWU	M14	M16
Embracing fTPM on embedded ARM Devices: Insights and Solutions	3MDEB	M15	M17
Stack and Stick are in Stock	ATOS	M16	M17
Using IEC-62443 to Secure Industrial Devices	BIOT	M17	M20
Improving the resilience of trusted applications with control flow integrity	UNITN	M18	M20
Secure-by-formal-design: Towards better software and hardware assurance	BEYOND	M19	M21

Challenges of Embedding Security in IoT Devices	CYSEC	M20	M21
TEE vulnerabilities, are you still there?	UMINHO	M21	M25
Ensuring Memory Safety for Trusted Applications through Secure Compilation	UNITN	M22	M26
AuthentiSafe: A Milestone in the CROSSCON Project for IoT Authentication	UWU	M23	M28
Ensuring Secure IoT Sytems: CROSSCON's Approach to Security Testing	SLAB	M24	M28
Fuzzing the Future: How AI is Transforming Hardware Security Evaluation	TUD	M25	M29
Many TEEs, One Hypervisor: Enhancing Cross-Platform Security and Interoperability	UMINHO	M26	M31
Achieving persistent tagging for robust stack memory error protection	UNITN	M27	M36
Secure Authentication using context	UWU	M28	M36
CROSSCON: from knowhow generation to technology development, maturation and impact creation -- Mission accomplished!	ATOS	M36	M36

This task was successfully completed with contributions from all partners, who worked collaboratively to maintain the website up to date. As a result, the website achieved its final design, as shown in Figure 33. Throughout the project, a total of 24 blog posts were published and further disseminated through other social media platforms, including LinkedIn and X.

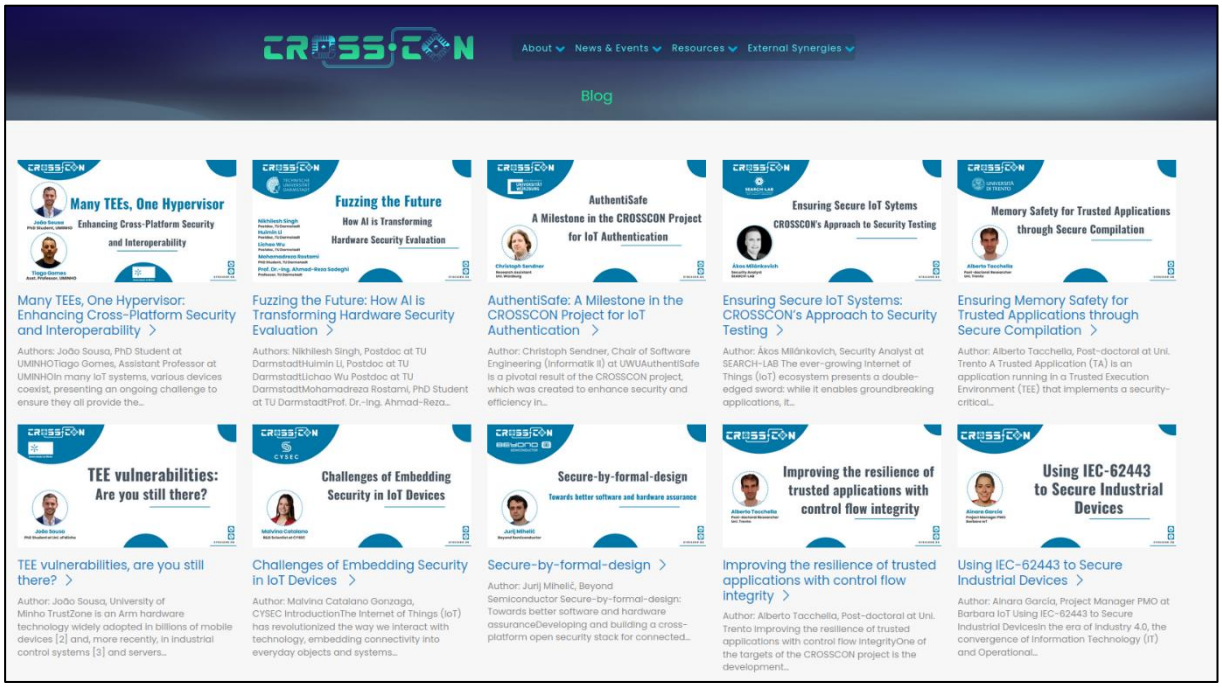


Figure 33: Blog Posts organization in CROSSCON Website.

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 several times 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 dissemination and communication leader Tiago Gomes. Other examples like this were published in Visão. Sapo, etc.

Figure 34: 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.

- **Newsletter #1 (M5) [6]:** Introduced the project by presenting CROSSCON's objectives and initial use cases (UC1, UC2, UC3). It featured the first blog post to increase visibility, reported on the first events attended and organized by CROSSCON, and presented the first synergies created with other initiatives. Additionally, it introduced all partners and described their roles within the project.

Figure 35: First and second CROSSCON newsletters.

The subsequent newsletter, published in November (M13), 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.

- **Newsletter #2 (M13)[7]:** This newsletter issue showcased recent and upcoming events, the first digital media appearances of CROSSCON, new external synergies, and four new blog posts. It also introduced the remaining use cases, contextualizing them within the project, and presented the first scientific publications to share initial results. The newsletter concluded with the announcement of the next release date.

Figure 36: Third and fourth CROSSCON newsletters.

The third newsletter, published in July 2024 (M21), marked an important milestone, following the release of the first version of CROSSCON components. With an introduction authored by the WP3 leader, the edition presented the components through architectural diagrams and explained how users could begin working with them. It also featured updates on key events, introduced the first versions of major components, including the CROSSCON Hypervisor, CROSSCON SoC, and CROSSCON Trusted Services, and reported on the second press release, several blog posts, and new scientific publications. The issue concluded by announcing the date of the next release.

- **Newsletter #3 (M21)[8]:** Focused on presenting the first CROSSCON components with detailed architectural diagrams, highlighting how users could interact with them. It introduced the Hypervisor, SoC, and Trusted Services, while also reporting on events, the second press release, new blog posts, and publications.

The fourth newsletter, released in June 2025 (M32), closely with the final stage of the project, **at a time when specifications had been finalized, components were stable, and demos had been shared with the community.** The introduction, written by a software engineer, highlighted the project's key milestones, its overall significance, and encouraged readers to explore the project's GitHub repository for hands-on engagement with the released components. This edition showcased refined architecture diagrams featuring novel advancements, reported on events attended and upcoming, and presented several blog posts and scientific publications. It concluded with the announcement of the **final newsletter** dedicated to project closure.

- **Newsletter #4 (M32)[9]:** Reflected the maturity of CROSSCON, presenting finalized specifications, stable components, and public demos. It also emphasized community engagement through GitHub, highlighted events, publications, and blog posts, and announced the final newsletter.

To conclude the project, a final newsletter is planned to disseminate the project's closing results, ensuring that the CROSSCON outcomes reach stakeholders, the research community, and the wider public. 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.

3.6.7 Zenodo Platform

The Zenodo platform aligns with both scientific best practices and European project dissemination requirements. Owing to its Open Access nature, publishing CROSSCON outputs on Zenodo ensures that all documents are freely accessible worldwide, thereby increasing visibility among researchers, industry stakeholders, and policymakers. Additionally, each uploaded document (deliverable, presentation, or report) receives a Digital Object Identifier (DOI), making it citable in academic publications and ensuring proper referencing. For these reasons, and to further enhance the visibility of our results, CROSSCON deliverables have been published on this platform, receiving positive feedback in recent months.

Through Zenodo, it is also possible to track document visibility and engagement metrics, including the number of views and downloads for each published deliverable. Table 9 presents these statistics for several CROSSCON deliverables available on the Zenodo platform (link of Zenodo page with CROSSCON content). We intend to upload all deliverables until the end of the project.

Table 9: List publications in Zenodo platform.

Title	Views	Downloads
D1.1 Use Cases Definition Initial Version	18	27
D1.2 Requirements Elicitation Initial Technical Specification	18	34
D1.3 Validation Criteria Initial Version	24	20
D1.4 Use Cases Definition Final Version	15	27
D1.5 Requirements Elicitation Final Technical Specification	16	29
D1.6 Validation Criteria Final Version	12	29
D2.1 CROSSCON Open Specification – Draft	8	54
D2.2 CROSSCON Formal Framework – Draft	7	22
D3.1 CROSSCON Open Security Stack Documentation - Draft	17	23
D3.2 CROSSCON Open Security Stack – Initial Version	9	39
D4.1 CROSSCON Extensions to Domain Specific Hardware Architectures Documentation – Draft	11	43
D4.2 CROSSCON Extension Primitives to Domain Specific Hardware Architectures — Initial Version	5	14
D5.2 Integrated CROSSCON Security Stack - First Version	6	66
D6.1 Project Website	7	15
D6.2 Dissemination and Communication Plan	6	22
D6.4 (MISS)	5	52

D7.2 Data Management Plan	5	16
D7.3 Data Management Plan Revised	7	12

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. For example, we consider as a training activity all demonstrations of CROSSCON components, explanations of how they work, and how can be integrated with other components. Most training events in Table 6, fits in this category.

4.1.1 NECS Winter School

The **European Network for Cybersecurity (NeCS) PhD School** was launched seven years ago to address the growing demand for highly qualified experts in cybersecurity. The scope of the NeCS PhD School is to showcase the latest advances in both cybersecurity attacks and defences. Its program combines traditional theoretical lectures with practical, hands-on sessions, enabling students to apply concepts and consolidate knowledge through direct experimentation. Over the last three editions (2023, 2024, and 2025), the NeCS PhD School has been supported by the CROSSCON project. This collaboration has strengthened the school's role as a hub for presenting innovative research results and emerging technologies to young researchers.

As part of its contribution, CROSSCON has provided specialized training sessions demonstrating the use of the CROSSCON Hypervisor on both APU and MCU devices, as well as the CROSSCON Baremetal TEE. These sessions allow students to gain practical experience with key topics such as virtualization, system security, and trusted execution. Through these activities, participants are exposed to multiple architectures and develop a deeper understanding of cross-platform cybersecurity challenges and solutions.

Figure 37: Banner used for NECS Winter School 2025.

4.1.2 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 38: Banner used for Bao Hypervisor virtual workshop.

4.1.3 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.

Figure 39: Banner used for CROSSCON TEE course event.

4.1.4 Crypto-Chipset Security

The **Crypto-Chipset Security Webinar** focused on the core principles of secure computing, with a particular emphasis on cryptography role. Delivered by **Search-Lab**, the online course provided valuable insights into security protocols, cryptosystem attacks, secure coding best practices, and key cryptographic mechanisms. The event encouraged interactive discussions and Q&A sessions, fostering

knowledge exchange and collaboration among participants. The workshop successfully attracted more than 40 attendees, reflecting strong interest in the topic and the relevance of the content delivered.

Figure 40: Banner used for CROSSCON Webinar event about Crypto-Chipset Security.

4.1.5 CROSSCON & (Secure) Friends

The **CROSSCON & (Secure) Friends** event was organized by CROSSCON as part of the RISC-V Summit Europe. The session offered valuable insights to the RISC-V community, highlighting how CROSSCON components such as the **CROSSCON SoC** and the **CROSSCON Hypervisor** contribute to advancing the ecosystem through practical demonstrations. The demonstrations showcased how the CROSSCON Hypervisor leverages RISC-V Hypervisor extensions to manage multiple VMs on APU devices, and how the CROSSCON SoC integrates a **perimeter guard** component to control non-CPU bus accesses to memory. The event also served as an opportunity to present the CROSSCON GitHub page and share its open components with the wider RISC-V community, fostering collaboration and adoption.

Figure 41: Banner used for CROSSCON &(Secure) Friends event.

4.1.6 Zarhus Developers Meetup #1 & Zarhus Developers Meetup #2

The **Zarhus Developers Meetup #1** and **Zarhus Developers Meetup #2** were held during a more advanced stage of the project, where CROSSCON partners showcased to the community how to run the **CROSSCON Hypervisor**. The sessions demonstrated not only its ability to support multiple VMs across different platforms but also its use on low-end devices. Participants were introduced to advanced capabilities such as **cache mitigation strategies** (using cache coloring) and **per-VM TEE**, including support for running **OP-TEE inside a VM**.

Figure 42: Banner used for Zarhus Developers Meetup 0x1 event.

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 project duration, 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 [10]. 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 10 and Table 11 correlate the projected KPIs set for M36 with the achieved KPI of the corresponding dissemination actions.

Over the past 36 months, CROSSCON partners have actively contributed to academic research, publishing in 8 journals and 36 conferences. In terms of dissemination activities, the project has organized 11 events and participated in 42 others. Furthermore, CROSSCON has been featured in 3 winter/summer schools and attended 14 additional training events, including webinars, conference sessions, and other educational activities not classified as workshops or schools. In addition, two white papers are currently available on the project website. CROSSCON has also fostered synergies with around 16 EU projects through joint events and collaborations involving multiple partners. Finally, within the scope of demonstrators, the project includes all demonstrations available in its GitHub repositories as well as specific Use Case demonstrations, detailed as follows:

- x8 Demonstrations in *"CROSSCON-Hypervisor-and-TEE-Isolation-Demos"* repo (x6 in Qemu, x1 in RaspberryPi 4B, x1 ZCU 102);
- x1 Demonstration in *"CROSSCON SoC"* repo;
- x1 Demonstration in "*FPGA_TEE*" repo;
- x3 Demonstrations in "uc1-2-integration" repo;
- x1 Demonstration in "uc1-integration" repo;
- x1 Demonstration in "ZK-PUF-Zephyr-Demo" repo;
- x1 Demonstration in "UC5-IP_Protection_for_Secure_Multi-Tenancy_on_FPGA" repo;
- x1 Demonstration in "context-based-auth-crosscon-demo" repo;

Table 10: KPIs report for the dissemination activities.

Dissemination activity - KPI description	Projected KPI Target M36	Achieved KPI Target M36
Scientific publication	>= 32 Publications	47 Publications
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 Events attended/organized	>= 30/3	Events attended: 42 Events organized:11
Winter/Summer schools	3	3
Other training events (courses, webinars)	>=10	14
Liaison with projects	>=15	16
White papers	>=4	3
Demonstrators	>=4	17

We acknowledge that some of the KPIs defined for the project were quite ambitious. However, aside from the target for white papers (two delivered instead of the expected number), all KPIs were successfully achieved on time, with several even exceeding expectations, particularly those related to publications and organized or attended events.

In addition to dissemination activities, the CROSSCON project has implemented a clear communication strategy aimed at maximizing the visibility of its activities and outcomes across diverse audiences. Accordingly, and following the structure of Table 10, Table 11 presents the achieved KPIs compared to the projected targets for M36 under the respective communication actions.

During the past 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 24 blog posts submitted. Regarding multimedia content, CROSSCON has accumulated considerable interactions, with around 2k views on YouTube videos and at least 500 shared brochures across 42 events. Furthermore, the project has issued three press releases and submitted 4 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 11: 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	24	24
Elevator pitch to brief the project to a wide audience (e.g., motion graphics animation and infographics)	Animation (e.g., YouTube)	1000 views	~2000views
	Brochure (events, science fairs)	500 shares	500+
Online press release	Website	3 PRs	2
Interact with companies interested in adopting the CROSSCON platform	Social media, newsletter	50 industrial feedbacks	50+

6 Conclusions

This deliverable, D6.6 - Dissemination, Communication and Community Building – Final 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[3]. While some KPIs were not fully achieved at mid-term, mainly due to the ongoing development and late public release (at M18) of core CROSSCON components, the situation has since improved significantly. By the end of the project, all major KPIs have been successfully met, with several even exceeding expectations, particularly regarding the number of publications, organized and attended events, and social media engagement.

The strategies previously proposed to enhance outreach, such as producing more dynamic and visually engaging content (e.g., animated posts, detailed technical highlights), have proven effective in boosting visibility and engagement. The consortium has continuously assessed and refined its communication and dissemination plan throughout the project, ensuring that actions remained aligned with the project's evolution and impact goals.

Although CROSSCON is now approaching its conclusion, dissemination and communication activities will continue beyond the project's lifetime. Several scientific papers acknowledging CROSSCON are still under review, and a final post-project newsletter is planned to consolidate all outcomes and results. This newsletter will also highlight the demonstrations developed throughout the project and promote new videos and materials shared on CROSSCON's online channels.

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.

[5] SecureCyber Cluster, Linkedin page [Online]. Available: https://www.linkedin.com/company/securecyber-cluster-%E2%80%93enhancing-cybersecurity?trk=public_post-text [Accessed 08-09-2025]

[6] CROSSCON Newsletter #1 [Online] Available: https://crosscon.eu/newsletter/newsletter-1-march-2023

[7] CROSSCON Newsletter #2 [Online] Available: https://crosscon.eu/newsletter/newsletter-2-november-2023

[8] CROSSCON Newsletter #3 [Online] Available: https://crosscon.eu/newsletter/newsletter-3-september-2024

[9] CROSSCON Newsletter #4 [Online] Available: https://crosscon.eu/newsletter/newsletter-4-june-2025

[10] Secure Cyber Cluster [Online] Available: https://www.linkedin.com/company/securecyber-cluster-%E2%80%93enhancing-cybersecurity/posts/?feedView=all

[11] CROSSCON, D6.4 Dissemination, Communication and Community Building First Report., T. Gomes, 2024.

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)

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

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;

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

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;

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


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

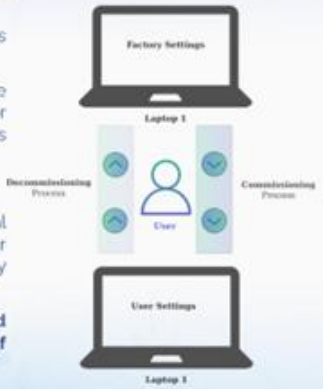
UC3: Commissioning and Decommissioning of IoT devices.

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.

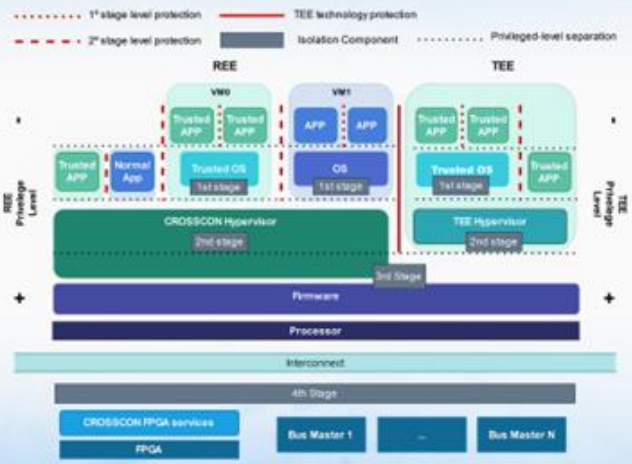
CROSSCON Stack

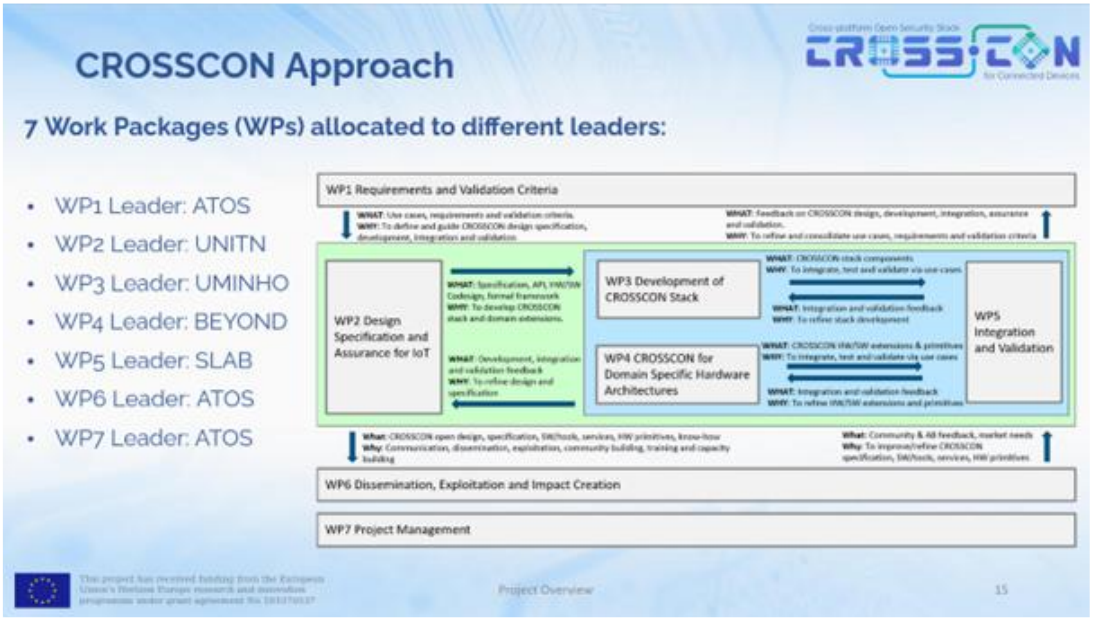
CROSSCON Stack Overview:

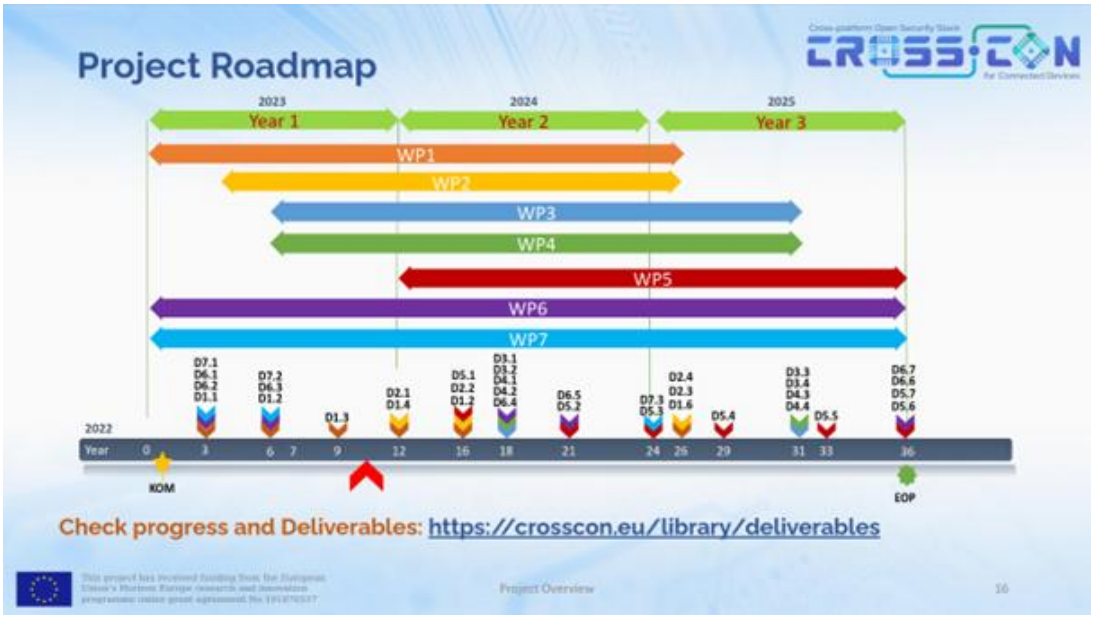
- Extends **interoperability** across heterogeneous devices;
- Offers a unified level of **abstraction** across **multiple hardware platforms**;
- Enriches existing **security** features by adding **new trusted services**;

CROSSCON SOC

- Trusted Services
- CROSSCON Hypervisor
- CROSSCON TEE
- HW Security primitives




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