Critical-Chains

Collaborative Project

Project Start Date 1st July 2019
Duration 36 Months

Deliverable D7.4 (Public)

Contextual and Situational Description and Benchmark of Events

Published by the Critical-Chains Consortium

Version 7.0 Date: 24-12-2020

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP7

Document Responsible: POSTEIT

Contributors: All

Status: Final

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Abstract

This document, Deliverable D7.4, Contextual and Situational Description and Benchmark of Events describes the Critical-Chains consortium activities with reference to a 7-layer dissemination eco-system which are listed below:

1. Critical-Chains Logo and Branding
2. Critical-Chains Social Media Activities
3. Critical Chains Clustering Efforts
4. Critical-Chains General Awareness-Raising within the Financial Sector Stakeholders
5. Targeted Use-Cases-focused Stakeholder Group Forming
6. Scientific and Technical Publications
7. Project-to-Policy Engagement

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Document History

Version Number	Date	Contributor organisation	Contributions
V.01	30-09-2020	UREAD-POSTEIT	Draft deliverable structuring and section contents
V.02	23-10-2020	RINA-C	Deliverable structure updating
V6.0	27-12-2020	UREAD	Restructuring as required, edits throughout, added several sections; many finalised; some at pre-final stage pending Partner contributions
V7.0	25-12-2021	UREAD	Final edits as required

Internal Review History

UREAD	25-12-2020	Reviewed and identified various improvements to be made
ERARGE	23-01-2021	Reviewed and made suggested edits

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Table of Contents

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Table of Figures

Table of Tables

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Executive Summary

This document, Deliverable D7.4, Contextual and Situational Description and Benchmark of Events, describes the Critical-Chains consortium activities with reference to a 7-layer dissemination eco-system (i.Critical-Chains Logo and Branding, ii. Critical-Chains Social Media Activities, iii. Critical Chains Clustering Efforts, iv. Critical-Chains General Awareness-Raising within the Financial Sector Stakeholders, v. Targeted Use-Cases-focused Stakeholder Group Forming, vi. Scientific and Technical Publications, vii. Project-to-Policy Engagement) in Chapter 6 to 11. The organisation of the deliverable is as follows:

Chapter 1: outlines the Critical-Chains objectives.

Chapter 2: defines the scope of this deliverable.

Chapter 3: presents the methodology for this deliverable – thus setting the analysis-base.

Chapter 4: sets out the ecology of the project touchpoints as the targeted dissemination channels.

Chapter 5: establishes the target audience in terms of the range of sectoral and policy stakeholders.

Chapter 6: motivates the Critical-Chains project logo design and examines its branding messaging impact.

Chapter 7: provides an account of the awareness-raising and dissemination achieved through Critical-Chains Social Media Activities including LinkedIn, Twitter, YouTube Channel.

Chapter 8: reports on the Critical Chains Clustering Efforts with respect to standard event characterisation descriptors, and, tracking and benchmarking metrics.

Chapter 9: describes the Critical-Chains outreach efforts for Stakeholder Engagement and Stakeholder Group building.

Chapter 10: presents the plans for targeted use-case focused Stakeholder sub-group forming as part of innovation management and targeted impact mobilisation strategy.

Chapter 11: sets out the particulars of the scientific and technical publications and provides the abstract of papers.

Chapter 12: describes the Project-to-Policy Contribution of the project through direct input by way of presentations and discussions at the EC project-to-policy workshop, responses to directed questionnaires from the EC Policy Unit as well as the Project-to-Policy presentations and discussions at the clustering over 10 workshops and events that the Critical-Chains project partners have participated in and/or co-organised.

Chapter 13: outlines the major insights informing dissemination efforts in Period II.

Appendix A: project-to-Policy Contributions.

Appendix B: links to presentation PowerPoint.

Appendix C: abstracts and links to scientific and Technical Publications full text.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

1 Introduction

The Project Objectives are to develop an integrated effective, accessible, fast, secure, and privacy-preserving financial contracts and transaction solutions. This is to protect against illicit transactions, illegal money trafficking and fraud that can take place through the banking clearing system and financial transactions settlement process. Thus, the objectives of the project are in the public interest.

The technologies to be deployed consist of:

- Transaction and financial dataflow analytics and modelling of the financial transactions clearing and claim settlement processes.
- Secure and smart use of Blockchain for data integrity checking, by involving financial institutions in the distributed Blockchain network.
- Cyber security protection of Inter-Banks and Internet Banking, insurance, and financial market infrastructures.
- Privacy protection through secure access supported by embedded systems and Internet-of-Things security.
- Critical-Chains is to be validated using four case studies aligned with four critical sectors: banking, financial market infrastructures, the insurance sector, and Highway Toll collection. The validation will include evaluating system reliability, usability, user-acceptance, social, privacy, ethical, environmental, and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy to the rest of the world. The Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector.

To maximise the mobilisation of the impact of project results, it is necessary to plan and execute an effective dissemination strategy. The widest possible dissemination and knowledge and results of the project should be achieved by addressing a wide range of existing or potential stakeholders. International conferences and workshops are being organised to promote the Critical-Chains with:

- the notification of the project results in the scientific sector,
- the promotion of the project in the financial, banking and insurance world,
- the promotion of the project to authorities at national and international level,
- the dissemination to associations and standardization bodies,
- the internal dissemination inside the Critical-Chains consortium.

To further raise the public level of awareness of the project within the scientific and financial communities, the following achievements and work towards the project goals of the first project period (M1-M18) has been performed:

- 11 Peer-reviewed scientific publications;
- 10 Workshops and other external events including partly presentations;
- 18 Logo and Branding messaging actions;
- 51 Tracking of Critical-Chains social media activities.

1.1 Scope of the Deliverable

This deliverable reports on the motivation, mission and results of the dissemination activities undertaken by the Critical-Chains Consortium during the first period of the project M1-M18. It will describe the differing methods and engagement tactics for each of the audiences and stakeholder groups with particular emphasis on the key stakeholders.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

This deliverable includes the description of each activity type in terms of dissemination channel, space, place and focus of the activity and the outcomes as shall be detailed in the following sections.

The aim of this deliverable is to:

- Make an overview of links with relevant projects/initiatives/experts in the field to disseminate project results and facilitate exchange of knowledge in workshops, conferences etc.
- Update the List of all communication and dissemination activities performed to promote the project including a specific analysis of the impacts of the various dissemination activities.

2 Methodology and objectives

The general purpose of the dissemination of European projects is to promote European collaborative research and innovation. This Deliverable is where we report the measured results about the effectiveness of our dissemination campaigns. The Critical-Chains project communication and dissemination objectives are:

- Raise public awareness and ensure maximum visibility of the project key milestones, objectives, activities and findings among EU member states.
- Announce and promote Critical-Chains events, contributing to upgrade its attendance and engagement potential.
- Reach the wider European FinTech and security community

Deliverable Objective: To widen and deepen the awareness-raising re Critical-Chains project Motivation Mission and Innovation results

This objective has been implemented through mutually reinforcing channels and modes of awareness-raising and stakeholder engagement including operations coordinated at 5 levels. In this sense, the deliverable objective is to assess the dissemination actions and to evaluate the impact of these activities on the Critical Chains projects.

The impact could be considered in a short, medium or long period. As a matter of example, the number of participants to one of events organized by Critical Chains is a factor that allows to evaluate a short-term impact; instead, a medium-period impact could be the analysis of the community following (how many people keep following the Critical chains events/workshops/ presentation after participating to the precious one?).

The dissemination assessment is based on indicators that, in turn, are defined through a number of strategic dissemination objectives. The main four dissemination objectives are:

- Strengthening the link to other H2020 peer projects in finance sector
- Ensure robustness of Critical-Chains innovations and results
- Strengthening project positioning in the Research Community
- Making the project “warmer” for the benefit of Project visual identity

The indicators allow to make the abovementioned strategic objectives more evident and useful for the impact assessment. Most of the impact evaluation requires the definition of benchmarks, in this regard different kind of assessment are associated to different kind of benchmarks.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

3 Dissemination channels

In the project period considered, many dissemination actions have been performed in order to raise awareness of the target audience and get interest in the project and its outcomes. To do this, different channels have been used to create and deliver a strategic communications and exploitation campaign across Europe:

- Logo
- Project website
- Social media use
- Promotional content material (video, presentation, brochure, posters, etc.)
- Events participation and Publications

The Promotional and communication material has been tailored for specific audience.

During M1-M18 project period, several dissemination activities including conferences, presentations at relevant 3rd party conferences and workshops has been held. A detailed list of relevant events has been created and regularly updated consisting of major international, national conferences and dedicated networking and clustering events where Critical-Chains participated and shared its achievements. The project website and the social media channels (LinkedIn, YouTube, Twitter) has been maintained and updated accordingly.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

4 Target audience

Critical-Chains aims to impact in six main sectors: A) General Public; B) Industry; C) Policy makers; D) Customers; E) Partners and F) Scientific community.

Table 4-1: Target Audience table

Target audience reference	Examples of target domains	
A. General Public	*Citizen association* *Magazines* *Web* *Conferences*	*Workshops* *Media* *Social media*
B. Industry	*Meetings* *Conferences* *Workshops*	*Social media* *Own events/summits* *Business relations*
C. Policy makers	*Policy reports* *Meetings* *Conferences* *Workshops*	*Social media* *Own events/summits* *Suggestion papers for common standards*
D. Customers	*Media* *Social media*	*Business relations* *Own events/summits*
E. Partners	*Meetings* *Conferences* *Workshops*	*Own events/summits* *Business relations*
F. Scientific community	*Research in blockchain technologies* *Research in FinTech technologies*	*Research in AI based fraud detection applications* *Research in cybersecurity*

Within this perspective, the commercial focus for all dissemination activities is to enlarge opportunities within these six main markets, exploiting the network capabilities of the Consortium.

Clearly, in order to raise awareness on the project, contribute to decrease any potential non-technological barrier to the market uptake and last but not least, share the research advancements and project innovations also with the general public and the scientific community have been fully considered as target audience of dissemination activities.

The dissemination activities are presented for each dissemination channel, referring to the main target audience with a specific reference, as indicated in the **Error! Reference source not found.**.

The scientific community will be addressed by presentations and publications presenting new technological achievements, methodologies developed, and algorithms designed, introduction of cyber security aspects into lectures and practical courses for students.

Industry representatives, Policy makers and Customers from Banking, financial infrastructure, and assurance sectors will be addressed by presentations and demonstrations of developed concepts, methods, technologies, processes and tools, lessons learned reports from developments, experimentation and demonstration.

Public authorities will be addressed by presenting workflows defined and system capabilities implemented within demonstrators and describing additional capabilities achievable by a fully blown system implementation when to exploit Critical-Chains results to a major extend.

The Critical-Chains partners will be addressed by technical workshops, general information sharing and training workshops (e.g. UI-REF, STRIDE, and synthetic DATASET CREATION).

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

5 Motivation and Results of the Critical-Chains Logo design and Branding messaging

5.1 Use of Critical-Chains Logo and Branding messaging

In order to make the project stand out and to build a solid and long-lasting visual identity that can be easily recognised by potential stakeholders, a project identity has been developed by RINA C. The logo was re-designed and simplified to attract a wider community with a more simplified direct messaging.

Designed logo at proposal phase

Re-designed logo

Figure 1 Critical-Chains logo evolution

As seen in Figure 1, the first logo was quite complex and there was no harmony in colours. There were many gears with different types which were supposed to address many application areas by including the industrial context and harmony. This was representing interoperability in various areas but also causing much diversification and sparse presentation. The chain trying to link the gears was not in a good shape as it was resembling prisoning and locking the chains. The triangles at backend were supposed to represent the "triangular accountability model" which is one of the core conceptual ideas of the Critical-Chains. However, these triangular shapes were very sharp pointed giving the sense that something is dangerous and harmful behind.

In order to address the project objectives, the logo is redesigned by keeping the gears in chain, symbolising the technologies and their actual use in Fintech industry, working properly and interoperable. Gears are drawn as if they are the parts of a blockchain with peaceful and charming colours of blue and green. The new logo is more simplified and directly addressing any chain in critical infrastructures each resembled by a gear. Green gives a peaceful message indicating a hopeful future which is also addressed in the new Horizon Europe programme. Blue colour symbolises the harmony which is a key concern in finance domain as well. Thus, Critical-Chains logo indicates the technological advancements addressing the needs of Fintech industry aiming to contribute to a peaceful future coping with financial crime and a harmonised collaboration to improve the finance industry.

The evolution in logo design also reflects the main rationale behind the project identity which is made of Critical-Chains Logo and the promotional payoff presented at every chance. Table 5-1: Tracking of Critical-Chains Logo and Branding messaging actions presents the top dissemination actions where the consortium used Critical-Chains Logo and brand. Social media and web channels played a crucial role to increase the visibility of the logo and present the promotional payoff to a wider community. The scientific and networking events, workshops and conferences provided many opportunities to present the project innovations. The Covid-19 outbreak was an unforeseen obstacle. But this misfortune was mitigated by organising or participating in H2020 project workshops in related areas. In spite of the hitches related to Covid-19 outbreak and the heavy workload at the

project ramp-up phase, the branding message was created, evolved and has reached to a community at thousands scale.

Table 5-1: Tracking of Critical-Chains Logo and Branding messaging actions

Action	Type of channel	Involved partner	When	Target audience	A	B	C	D
Sharing of the Video	RINA Twitter account	RINA-C	08/06/2020	General Public	88	7	5	1
Sharing of the CC Case Study	RINA Twitter account	RINA-C	27/07/2020	General Public	NA	5	4	1
Sharing of the Video	RINA Vimeo account	RINA-C	30/03/2020	General Public	37	NA	NA	1
Roll-Up for Digitalization and Blockchain workshop attended by JR	Roll-up	RINA-C/JR	24/09/2020	End Users Financial Authorities	25	NA	NA	NA
Agenda and Announcement of 3rd Webinar 'Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop'	Project website, webinar channel, research project website guest, project partner social media accounts	RINA-C/ UREAD/ POSTE-IT	14/12/2020	Financial sector network security and training, transactions monitoring managers, European Commission regulatory policy, other standardization stakeholders	288	NA	18 first share	4
Project & Consortium presentation for 'Cybersecurity in Finance' workshop organized by SOTER	Presentation	RINA-C	30/10/2020	Banking, financial infrastructure, assurance sectors	50	NA	NA	1
Project presentation for Project to Policy workshop.	Presentation	UREAD	22/01/2020	Banking, financial infrastructure, assurance sectors	45	NA	NA	0
Project presentation for FINTECH Webinar	Presentation	UREAD	19/05/2020	Banking, financial infrastructure, assurance sectors	60	NA	NA	1
Registration page in GoToWebinar for the 3rd Webinar 'Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop'	GoToWebinar	RINA-C	14/12/2020	Financial sector network security and training, transactions monitoring managers, European Commission regulatory policy, other standardization stakeholders	288	NA	16	1
Creation of project mini site in Indra´s web page	Web page	INDRA	30/07/3030	General Public	NA	NA	NA	NA
Short project report for the Fraunhofer Annual Report	Report	FHG	01/05/2020	General Public	NA	NA	NA	NA
Announcement on the Fraunhofer EMI homepage	Web page	FHG	01/04/2020	General Public	NA	NA	NA	1

including the Critical-Chains promotion video								
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on Fraunhofer EMI Website and LinkedIn page	Web page, LinkedIn	FHG	01/12/2020	General Public	NA	3	NA	2
Sharing of the Critical-Chains promotional Video	JR Twitter and LinkedIn accounts,	JR	May and October 2020	General Public	135	9	3	2
Visibility over ERARGE's social media accounts and web site	Web page & LinkedIn	ERARGE	May-December 2020	General Public	117	39	4	1
Presentation in 7 scientific events	Scientific conferences	ERARGE	August 2019 – September 2020	Scientific Community	~250 (participants)	(8 citations)	14	7
EY EMEIA BLOCKCHAIN Virtual SUMMIT 2020	Video, social media	EY	October 2020	General Public	~1000	NA	NA	3
Sharing the Critical-Chains workshop of December 14 2020	Twitter and LinkedIn	IMEC	December 2020	General Public	NA	9	3	2

LEGEND:

A	People who viewed
B	Number of likes
C	Number of re-postings/con-divisions
D	Number of channels used for the event

6 Critical-Chains Social Media Activities including LinkedIn, Twitter, YouTube Channel

6.1 Dissemination tracking of Critical-Chains social media activity

Critical-Chains project website constitutes a key communication tool to increase the project visibility and impact. During M1-M18, it has been constantly updated with all relevant information about the project (project objectives, information, news, event announcements, public reports, and analysis) and it also served as a communication tool.

The Critical-Chains Project Consortium has decided to open a project Twitter account (https://twitter.com/ChainsH2020). All strategic hashtags were included in project tweets (such as #H2020, #Cyberattacks etc.) in order to give more visibility to the project. In addition, trending hashtags of the day relevant for Critical-Chains (#CyberSecurityDay) have been exploited to maximise the impact of this project on Twitter community. Other accounts (partners, events' account, h2020 accounts, journalists, etc.) have always been mentioned in the project tweets to promote social engagement. Last but not least, images or videos to attract were always included in the project tweets in order to catch the followers' attention more easily.

Critical-Chains can be found on LinkedIn at https://www.linkedin.com/in/critical-chains-project-55a3501a3/, the profile page includes information about the project, and the partners involved.

Critical-Chains promotional project video can be found on YouTube at:

https://www.youtube.com/watch?v=7NUIdjFHMhI

A project presentation has been made available for all project partners. A project brochure to disseminate Critical-Chains to general public has been developed. A Project poster with technical content has been prepared for fairs, exhibitions, workshops, etc. The dissemination activities over social media are presented in Table 6-1.

Table 6-1: Tracking of Critical-Chains social media activities

Action	Type of social media channel	Involved partner	When	Target audience
Sharing of the project Video	RINA LinkedIn account	RINA-C	08/06/2020	General Public
Sharing of the CC Case Study	RINA LinkedIn account	RINA-C	20/08/2020	General Public
Promotion of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	RINA LinkedIn account	RINA-C	11/12/2020	General Public
Sharing of the CC Case Study	RINA website	RINA-C	26/02/2019	General Public
Promotion of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	RINA website	RINA-C	03/12/2020	General Public
Sharing of the Video	RINA Twitter account	RINA-C	08/06/2020	General Public
Sharing of the CC Case Study	RINA Twitter account	RINA-C	27/07/2020	General Public
Sharing of the Video	RINA Vimeo account	RINA-C	30/03/2020	General Public
Project Introduction and Sharing of the project website link	Twitter Project Account	RINA-C	06/03/2020	General Public
Sharing of the project Video	Twitter Project Account	RINA-C	31/03/2020	General Public
Sharing of the project Video	Twitter Project Account	RINA-C	02/04/2020	General Public
Announcement about Guardtime sharing news item about Critical chains	Twitter Project Account	RINA-C	22/04/2020	General Public
Sharing of the project Video	Twitter Project Account	RINA-C	22/04/2020	General Public
News about First Fintech Workshop on AI where the project has been presented by the coordinator Prof. Atta Badii	Twitter Project Account	RINA-C	19/04/2020	General Public
Retweet SOTER project post with the link to SOTER project website	Twitter Project Account	RINA-C	03/02/2020	General Public
Retweet FORESIGHT post about 2-day meeting held at UniStrathclyde	Twitter Project Account	RINA-C	11/02/2020	General Public
Retweet Guardtime news about the implementation of an immutable audit for the financial services industry	Twitter Project Account	RINA-C/ GT/ EY/ FHG/ INDRA/ CEA	17/04/2020	General Public
Retweet of RINA-C post sharing the project video	Twitter Project Account	RINA-C	08/06/2020	General Public
Retweet of SOTER post about how Cybersecurity habits at home threaten corporate network security	Twitter Project Account	RINA-C	08/06/2020	General Public
Retweet NETAS news about *A Holistic Approach to Cybersecurity*	Twitter Project Account	RINA-C/ NETAS	06/06/2020	General Public
Retweet of SOTER post about online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th Nov 2020	Twitter Project Account	RINA-C	25/11/2020	General Public

Action	Type of social media channel	Involved partner	When	Target audience
Announcement of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	LinkedIn Project Account	RINA-C	09/11/2020	General Public
Post about the online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th Nov 2020	LinkedIn Project Account	RINA-C	24/11/2020	General Public
News about the participation of the coordinator Atta Badii to 'Cybersecurity in Finance' workshop on 30th October	LinkedIn Project Account	RINA-C/ UREAD	25/10/2020	General Public
Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop 14th December	Twitter and LinkedIn account	IMEC	9/12/2020	General Public
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on Fraunhofer EMI LinkedIn page	LinkedIn Account	FHG	01/12/2020	General Public
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on NETAS TR Twitter Page	NETAS Twitter Account	NETAS	11/12/2020	General Public
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on NETAS EN Twitter Page	NETAS Twitter Account	NETAS	11/12/2020	General Public
Announcement of the global promotional video of the Critical-Chains project on NETAS TR Twitter Account	NETAS Twitter Account	NETAS	25/09/2020	General Public
Announcement of the global promotional video of the Critical-Chains project on NETAS EN Twitter Account	NETAS Twitter Account	NETAS	25/09/2020	General Public
Announcement of the kickstart of the Critical-Chains project on NETAS TR Twitter Account	NETAS Twitter Account	NETAS	21/03/2019	General Public
Announcement of the kickstart of the Critical-Chains project on NETAS EN Twitter Account	NETAS Twitter Account	NETAS	03/04/2019	General Public
Re-sharing of the global promotional video of the Critical-Chains project on NETAS YouTube Channel	NETAS YouTube Channel	NETAS	21/09/2020	General Public
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on NETAS LinkedIn Page	LinkedIn Page	NETAS	11/12/2020	General Public
Promote online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	JR LinkedIn account	JR	11/12/2020	General Public
Announced online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020 on JR web page	JR Web page	JR	16/12/2020	General Public
Promote Critical-Chains promotional video in LinkedIn post	JR LinkedIn account	JR	01/10/2020	General Public

Action	Type of social media channel	Involved partner	When	Target audience
Send invitation E-Mail to approx. 600 recipients for participation in online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	From JR company E-Mail account	JR	18/11/2020	General Public
Send reminder E-Mail to approx. 600 recipients for participation in online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	From JR company E-Mail account	JR	25/11/2020	General Public
Reshared Critical-Chains promotional video from NETAS account	JR LinkedIn account	JR	01/10/2020	General Public
Promote Critical-Chains promotional video in Twitter post	JR Twitter account	JR	01/05/2020	General Public
Retweeted Critical-Chains promotional video from NETAS account	JR Twitter account	JR	01/10/2020	General Public
Published News about the project Critical-chains presentation at CONECT Informunity in Vienna - Digital Transformation and Blockchain in FinTech.	JR web page	JR	01/10/2020	General Public
Send Thank you for participation E-Mail to 52 registered participants in online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	From JR company E-Mail account	JR	03/12/2020	General Public
Published News at JR Web page about online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	JR web page	JR	11/12/2020	General Public
Announced Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop, hold on 14th December on JR web page	JR web page	JR	07/12/2020	General Public
Announced Critical-Chains interest on new regulations in Turkey related to the use eGovernment in Financial operations and combat against financial crime	ERARGE LinkedIn Page	ERARGE	13/04/2020	General Public
Announced Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop, held on 14th of December 2020 on ERARGE's LinkedIn account	ERARGE LinkedIn Page	ERARGE	09/12/2020	General Public
Published News, Calls and Awareness-Raising content on the Critical-Chain project website	Critical-Chains Project Website	UREAD	1/7/19-31/12/21	General Public
Published public deliverables of the project on the Critical-Chain project website	Critical-Chains Project Website	UREAD	1/7/19-31/12/21	General Public

6.2 Dissemination relevance of Critical-Chains social media activity

Among the dissemination actions previously presented, the most relevant ones are in the following so that it will be possible to make general performance considerations in relation to the indicators reported in the following table.

Table 6-2: Relevance of Critical-Chains social media activities

Event Name	Type of social media channel	Why this action?	Audience Size	Feedback / Results	Relevance
Sharing of the project Video	RINA LinkedIn account	Reach industrial stakeholder	697 impressions, 9 video views, 11 clicks, 3 reactions, 8 shares	Raise awareness and visibility about project	Medium
Sharing of the CC Case Study	RINA LinkedIn account	Reach industrial stakeholder	10593 impressions, 81 clicks, 66 reactions, 8 shares	Raise awareness about project topics. Create a link between CC project and RINA.	Medium
Promotion of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	RINA LinkedIn account	Reach research community	1308 impressions, 8 clicks, 36 reactions, 8 shares	Expand networking with financial stakeholder. Enlarge project visibility	Medium
Sharing of the CC Case Study	RINA website	Reach industrial stakeholder	108 views	Raise awareness about project topics.	Medium
Promotion of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	RINA website	Reach industrial stakeholder	36 views	Expand networking with financial stakeholder	Medium
Sharing of the project Video	RINA Twitter account	Reach industrial stakeholder	7 likes, 5 Retweets, 88 views	Raise awareness and visibility about project	High
Sharing of the CC Case Study	RINA Twitter account	Reach industrial stakeholder	5 likes, 4 Retweets	Raise awareness about project topics. Create a link between CC project and RINA.	High
Sharing of the project Video	RINA Vimeo account	Reach industrial stakeholder	83 Impressions	Raise awareness and visibility about project	Medium
Project Introduction and Sharing of the project website link	Twitter Project Account	Reach research community	388 Impressions	Drive traffic to project website. Launch project	High
Sharing of the project Video	Twitter Project Account	Reach research community	29 views	Increase project visibility and awareness	

Event Name	Type of social media channel	Why this action?	Audience Size	Feedback / Results	Relevance
Sharing of the project Video	Twitter Project Account	Reach research community	16 views	Increase project visibility and awareness.	Medium
Announcement about Guardtime sharing news item about Critical chains	Twitter Project Account	Reach research community	3 likes	Network expansion Enlarge knowledge about project topic	Medium
Sharing of the project Video	Twitter Project Account	Reach research community	5 likes, 3 Retweets, 126 views	Increase visibility and awareness	Medium
New about First Fintech Workshop on AI where the project has been presented by the coordinator A.Badii	Twitter Project Account	Reach research community	3 likes	Engagement of stakeholder in FINTECH domain.	Medium
Retweet SOTER project post with the link to SOTER project website	Twitter Project Account	Reach research community		Support a project Critical Chains collaborates with. Consolidate a network with financial stakeholder.	Medium
Retweet FORESIGHT post about 2-day meeting held at UniStrathclyde	Twitter Project Account	Reach research community	5 likes, 8 retweets	Increase visibility	Low
Retweet Guardtime news about the implementation of an immutable audit for the financial services industry	Twitter Project Account	Reach research community	8 likes, 4 Retweets 34 engagements 1216 impressions	Network enlargement Increase visibility Enlarge knowledge about project topic	Medium
Retweet of RINA-C post sharing the project video	Twitter Project Account	Reach research community	7 likes, 5 Retweets	Network enlargement Increase visibility	Medium
Retweet of SOTER post about how Cybersecurity habits at home threaten corporate network security	Twitter Project Account	Reach research community	1 like, 1 Retweet	Enlarge knowledge about project topic Engagement of new stakeholder in financial sector.	Medium
Retweet NETAS news about A Holistic Approach to Cybersecurity	Twitter Project Account	Reach research community	2 likes, 2 Retweets	Enlarge knowledge about project topic	Medium
Retweet of SOTER post about online symposium on Emerging Cybersecurity Standards for the	Twitter Project Account	Reach research community	1 like, 1 Retweet 17 engagements	Expand networking with financial stakeholder. Enlarge project visibility	Medium

Event Name	Type of social media channel	Why this action?	Audience Size	Feedback / Results	Relevance
Finance Sector in Europe, hold on 27th Nov 2020					
News about the participation of the coordinator Atta Badii to 'Cybersecurity in Finance' workshop on 30th October	LinkedIn Project Account	Reach research community	7 likes	Raise awareness and visibility about project Engagement of new stakeholders in financial sector.	Medium
Announcement of a Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop on 14th Dec 2020.	LinkedIn Project Account	Reach research community	6 likes	Expand networking with financial stakeholder. Enlarge project visibility	Medium
Post about the online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th Nov 2020	LinkedIn Project Account	Reach research community	1 like	Engagement of new stakeholders in financial sector. Enlarge project visibility	Medium
Sharing the "Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop" 14th December	LinkedIn account imec Nederland	Reach research community	1 like	Engagement of new stakeholders in financial sector. Enlarge project visibility	Medium
Sharing the "Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop" 14th December	Twitter account imec Nederland	Reach research community	3 retweets 6 likes	Engagement of new stakeholders in financial sector. Enlarge project visibility	Medium
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on Fraunhofer EMI LinkedIn page	EMI LinkedIn Account	Reach research community	3 likes	Engagement of new stakeholders in financial sector. Enlarge project visibility	Low
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on NETAS TR Twitter Page	NETAS Twitter Account	Reach industrial stakeholder	1 Retweet / 8 likes	Engagement of new stakeholders in financial sector. Enlarge project visibility	Medium
Announcement of the 3rd Financial Sector Cyber Security & Regulatory	NETAS Twitter Account	Reach industrial stakeholder	1 Retweet / 0 likes	Engagement of new stakeholders in financial sector. Enlarge project visibility	Low

Event Name	Type of social media channel	Why this action?	Audience Size	Feedback / Results	Relevance
Challenges Workshop on NETAS EN Twitter Page					
Announcement of the global promotional video of the Critical-Chains project on NETAS TR Twitter Account	NETAS Twitter Account	Reach industrial stakeholder	3 Retweet / 10 likes	Network enlargement Increase visibility Enlarge knowledge about project topic	High
Announcement of the global promotional video of the Critical-Chains project on NETAS EN Twitter Account	NETAS Twitter Account	Reach industrial stakeholder	1 Retweet / 3 likes	Network enlargement Increase visibility Enlarge knowledge about project topic	High
Announcement of the kickstart of the Critical-Chains project on NETAS TR Twitter Account	NETAS Twitter Account	Reach industrial stakeholder	6 Retweet / 17 likes	Network enlargement Increase visibility Enlarge knowledge about project topic	Low
Announcement of the kickstart of the Critical-Chains project on NETAS EN Twitter Account	NETAS Twitter Account	Reach industrial stakeholder	1 Retweet / 2 likes	Network enlargement Increase visibility Enlarge knowledge about project topic	Low
Re-sharing of the global promotional video of the Critical-Chains project on NETAS YouTube Channel	NETAS YouTube Channel	Reach industrial stakeholder	158 views / 4 likes	Network enlargement Increase visibility Enlarge knowledge about project topic	High
Announcement of the 3rd Financial Sector Cyber Security & Regulatory Challenges Workshop on NETAS LinkedIn Page	Netas LinkedIn Page	Reach industrial stakeholder	39 likes	Engagement of new stakeholders in financial sector. Enlarge project visibility	Medium
Online symposium on Emerging Cybersecurity Standards for the Finance Sector in Europe, hold on 27th 2020	JR LinkedIn account, JR web page, JR company E-Mail account, JR Twitter account	Reach research community and general audience	More than 5000 followers and directly connected email addresses	Raise awareness and visibility about project	Very high
Promote Critical-Chains promotional video in LinkedIn post	JR LinkedIn account	Reach research community	3280 followers, 5 likes	Raise awareness and visibility about project	Very high

Event Name	Type of social media channel	Why this action?	Audience Size	Feedback / Results	Relevance
Reshared Critical-Chains promotional video from NETAS account	JR LinkedIn account	Reach research community	3280 followers	Raise awareness and visibility about project	Very high
Promote Critical-Chains promotional video in Twitter post	JR Twitter account	Reach research community	1515 followers, 135 views, 2 retweets, 1 like	Raise awareness and visibility about project	Very high
Retweeted Critical-Chains promotional video from NETAS account	JR Twitter account	Reach research community	1515 followers, 1 retweet, 3 likes	Raise awareness and visibility about project	Very high
Published News about the project Critical-chains presentation at CONECT Informunity in Vienna - Digital Transformation and Blockchain in FinTech	JR web page	Reach research community	General public	Raise awareness and visibility about project	Very high
Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop, hold on 14th December	JR web page	Reach research community	General public	Raise awareness and visibility about project	Very high
Reshared Critical-Chains promotional video in Linkedin	ERARGE web page	Reach research community and general audience	General public	Raise awareness and visibility about project	Very high

6.3 Assessment of Critical-Chains social media activity and considerations

The assessment of the social media activity of Critical Chains was carried out by evaluating proper key performance indicators on the social channels used by the project (Twitter and LinkedIn):

- Project awareness: website traffic
- Engagement: social media metrics
- Target loyalty: percentage of content consumed by target groups

The visits on the page and the correlated searches have been monitored, therefore the number of users that have interacted with the Critical Chains social pages. In the following as example some indication of the audience size and the relevance of the project on social media channels.

Twitter

Currently, 35 users follow Critical-Chains Twitter account, a parameter to be considered is the number of impressions. The term "impression" means the number of times that the content is displayed to the users. The graph below reports three-month impressions:

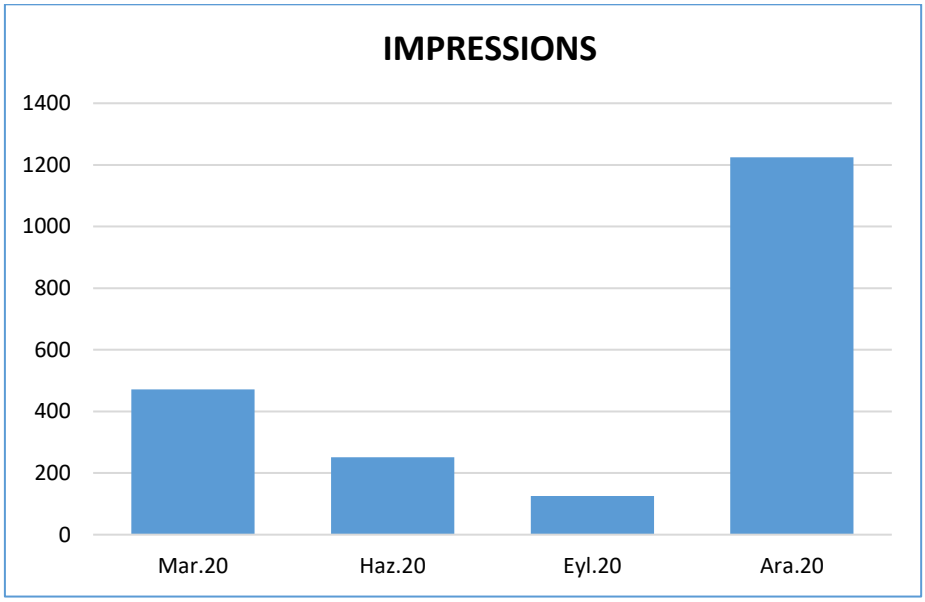


Figure 2: Audience size vs. relevance of social media action

Peaks of impressions occurred when online events have been attended and promoted. In May 2020, 1735 impressions have been reached, a considerable amount, if we consider that the mean value of the impressions on the year 2020 is 490.

The most successful months have been April 2020, May 2020 and December 2020. Dec 2020 was so brilliant, with 1225 impressions, thanks to the promotion of the webinar the Critical chains *Financial Sector Infrastructure Cyber-Physical and Regulatory Standards Workshop.* Critical Chains account has been also mentioned by Cyberwatching.eu in its post about the webinar.

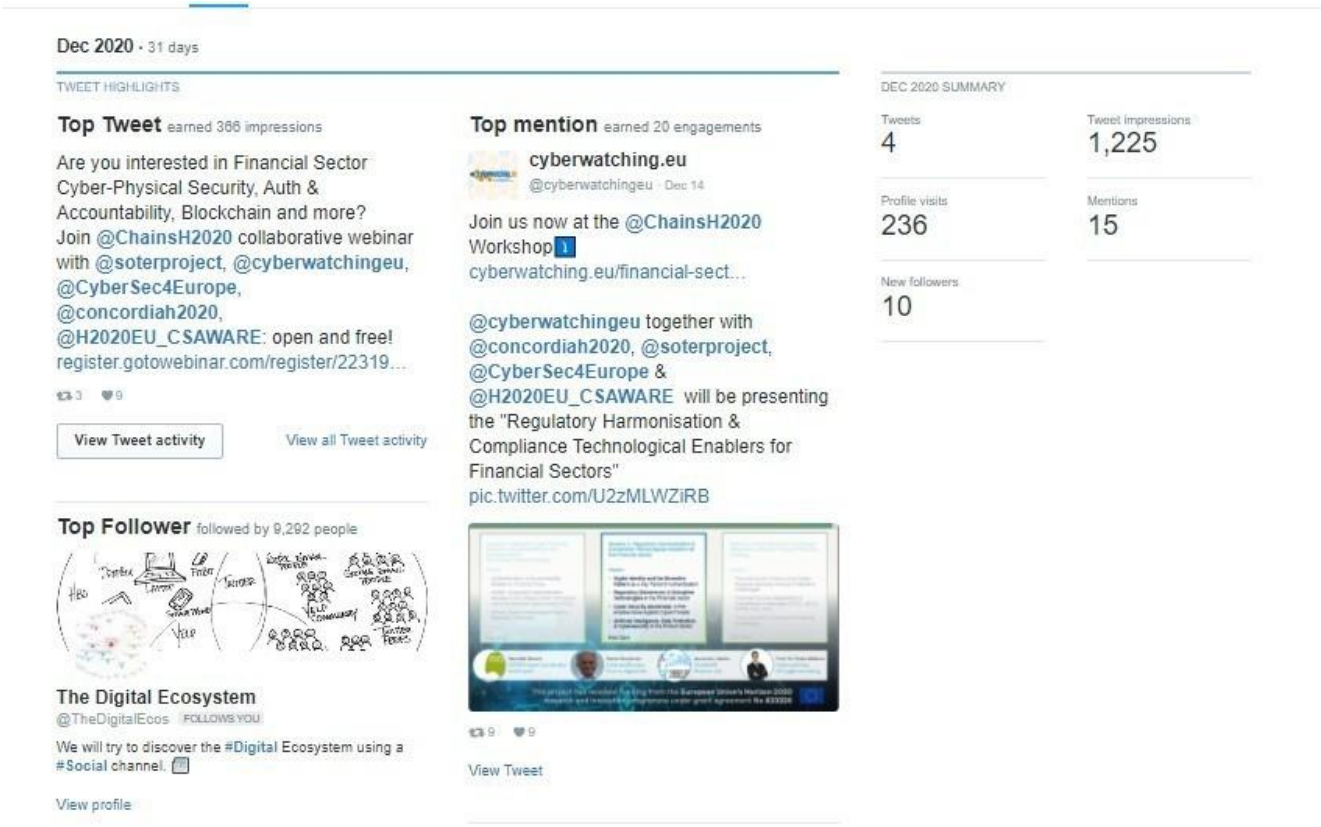


Figure 3: Twitter Analytics - December 2020

May 2020 was even more successful, while in April the project account earned popularity thanks to the sharing of project video.

LinkedIn

Critical-Chains LinkedIn account has reached 41 followers. The analysed metrics are as follow:

- VISITORS: Total number of daily page views and unique visitors over time. Data is measured across desktop and mobile for logged in LinkedIn members.
- IMPRESSIONS: number of times that the content is displayed to the users
- FOLLOWERS: Number of new followers

The popularity of Critical-Chains LinkedIn account grew mainly during the last months of the year 2020, as a matter of fact, the maxim value of the three metrics, shown in the table below, has been reached in December 2020 for each metric.

Table 6-3: Metric max values

METRICS	Max Value
Visitors	18 per day
Impressions	463 impression per month
Followers	22 follower per month

7 Critical-Chains Clustering Efforts

7.1 Dissemination tracking of Critical-Chains Clustering Efforts

In the following table are reported all the actions for liaising with relevant projects/initiatives/experts in the field, to disseminate project results and facilitate exchange or knowledge in joint workshops, conferences, for mutual innovations, news updates from the projects and sharing insights.

Benchmarking the Dissemination Activities

Due to restrictions on holding physical meetings, from early 2020, all the events contributed to or organised by the Critical-Chains Consortium had to be held as virtual workshops (webinars). This to some extent curtailed the range/mode of the dissemination activities particularly in recruitment of new Stakeholder Group members. However the extent and scope of the networking and clustering was maintained as far as was possible in the circumstances and this led to successful delivery of substantive community dissemination activities, notably clustering workshops and joint publications (within the Consortium and across the cluster, already realised and/or formally in progress) -achieved to-date despite the restrictions.

The Critical-Chains consortium thus continued to demonstrate community contributions at the level of a leading member of its cluster within a network-of-networks (e.g. CyberWatching, LSEC) and including its own emerging Stakeholder Group to be extended in Period II. Thus, overall, the Critical -Chains project dissemination activities have reached sufficient momentum to constitute a robust collective effort to continue in period II to motivate our stakeholder community towards the adoption of the Critical-Chains vision and mission for our transformative innovation to support enhanced security and accountability in the financial service sector infrastructure.

Deliverable D7.1 (section 9.1 "*Performed events and Outcomes"*) provided a description of the dissemination events over the period of M1-M12. In this section we provide an outline of those events as a preface to setting out their respective tabularised benchmarking information. However, for each dissemination event that has been performed after M12 to the end of period 1 (M18) we include both a description as well as their respective benchmarking information tabularised as a standard for all dissemination events as shown below.

Workshop 1: Responsible Research & Innovation 11-12 July 2020 - Socio-Ethical Project Kick-off

This workshop was held in two sessions integrated with the project kick-off meeting; respectively focused on **i)** socio-ethical responsible design, and, **ii)** socio-technical design implementation methodology. The first session was delivered by Dr Julian Stubbe, a member of the Critical-Chains Ethical Advisory Board (EAB). The second session was delivered by the Coordinator Prof. Atta Badii, focused on the UI-REF methodology to support accountability and ethical and legal compliance by design as also described in Deliverables D2.3, D2.7 and D6.1.

Workshop 1 -Metrics and Description

Title: Responsible Research & Innovation		
Particulars	**Metrics**	**Description**
Date & Place		11-12 July 2019
Host- Organisers		University of Reading, Critical-Chains Consortium
Number of persons registered	18	Partners' Research staff
Number of the audience who participated	18	Blockchain and Responsible Research & Innovation (RRI)
Number of sessions delivered	2	Dr Julian Stubbe and Prof. Atta Badii
Number of speakers and panellists	2	Limited as being an internal project awareness-raising workshop
Number of channels used for event publicity	1	Direct invitation mailshot to project Partners
Number of projects which contributed to the presentations and/or panel	1	Critical-Chains, plus ethical compliance experience from several other projects e.g. MOSAIC, and VideoSense

Number of countries represented	7	UK, France, Italy, Germany, Spain, Austria, Estonia
Number of sectors represented	4	Financial Sector, IT Security Companies, Security Research Organisations, Blockchain Provider
Main themes discussed	4	Social Acceptability & Impact Analysis of Disruptive Technologies, in particular Blockchain. Accountability-by-design Responsible Research & Innovation

Workshop 2: Ethics of Blockchain, 17th December 2019

This workshop was organised and hosted by the University of Reading, Department of Computer Science. It considered the ethical issues relating to the large-scale take-up of blockchain technology and viewed the main issues as arising from the challenge to ensure accountability and healthy governance over the blockchain layers and the need for accountability but also avoiding or mitigating any longer-term adverse impacts of large-scale blockchain adoption

The presentations from the workshop for which we were able to receive permission to publish have been included on the Critical-Chains website as follows:
https://research.reading.ac.uk/critical-chains/the-ethics-of-blockchain-workshop-17th-december-2019/

Workshop 2 -Metrics and Description

Title: Ethics of Blockchain		
Particulars	**Metrics**	**Description**
Date & Place		17th December 2019, University of Reading
Host- Organisers		Critical-Chains Consortium
Number of persons registered	24	Including Critical Chains Consortium, researchers from 3 UK universities, ORCID Project, InnovateUK
Number of the audience who participated	24	Project Partner staff pls representatives from: Vizidox UK, InnovateUK, ORCID Network https://orcid.org/, Nottingham University, De Montford University, York University, Brunel University
Number of sessions delivered	2	Presentations followed by Panel discussion and Q&A
Number of speakers and panellists	7	Speakers from the Consortium and above external organisations: Mr James King, Dr Neil McBride, Dr Alper Kanak, Mr Kristo Klesment, Mr Bakhtiyor Yokubov, Mr Vincent Bryce, Professor Atta Badii
Number of channels used for event publicity	2	Project websites plus mailshot to the Responsible Research & Innovation RRI research community
Number of projects which contributed to the presentations and/or panel	4	Critical Chains, Vizidox, Exploitation of Genetic Sequencing for Blockchain, ORCID
Number of countries represented	9	Austria, UK, France, Italy, Germany, Spain, Estonia, Turkey, Romania
Number of sectors represented	5	Financial Services, ICT Cybersecurity, Regulatory Compliance and Certification Consultancy Services, Security Research Organisations, Public Sector (InnovateUK)
Main themes discussed	4	Scalability and Security Challenges with Blockchain and Smart Contracts in particular, Authentication and Accountability Models, Embedding Ethical Reflection in Design, Social Acceptability by Design

Workshop 3: Project-to-Policy Kick-Off Workshop, Friday 31st January 2020, REA, Brussels

Professor Atta Badii represented the Critical-Chains Consortium for the Policy Workshop held at the REA, Brussels. His presentation highlights the project objectives and the need for examining the regulatory and certification framework responsive to the evolutionary trends in the Fintech and the emergent forms of

payment systems and intermediation the Critical-Chains presentation was included within D7.1 and also on the Critical-Chains project website, as follows:
https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/Critical-Chains-833326-Policy-Workshop-15PPset-Atta-Badii-22-01-2020.pdf

The agenda included an introductory plenary meeting outlining the proposed Project-to-Policy framework. This was followed by three parallel sub-group meetings. Within the sub-groups, proceedings continued with a presentation by the EC Policy Unit staff followed by presentations by individual projects and the workshop concluded with group discussion including a final statement from each Coordinator of the participating projects regarding the policy perspectives as had emerged through the work of their respective Consortia.

Workshop 3 - Metrics and Description

Title: Project-2-Policy Kick-off Workshop		
Particulars	**Metrics**	**Description**
Date & Place		31st January 2020, Brussels
Host- Organisers		EC, Research Executive Agency (REA)
Number of persons registered	~45	EC-funded security projects
Number of the audience who participated	~45	Subgroup of around 15 delegates
Number of sessions delivered	3	EC Policy Staff Briefing, Individual Project Presentations, Panel Discussion and QA
Number of speakers and panellists	10-12	Coordinators of relevant projects and EC Project and Policy Advisors
Number of channels used for event publicity	2	EC Portal, direct mail invitation
Number of projects which contributed to the presentations and/or panel	~10	EC-funded security projects with applications to financial sector
Number of countries represented	28	EC Countries
Number of sectors represented	5	Financial Services, ICT Cybersecurity, Regulatory Compliance and Certification Consultancy Services, Security Research Organisations, Public Sector (EC Policy Unit, REA)
Main themes discussed	10	Regulatory Mechanisms, Standardisation, Compliance Monitoring, Certification, Blockchain, IoT, Crypto-currencies, Authentication and Accountability Models, eIDAS, PSD2

Workshop 4: AI, Financial Automation and Market Risk, FIN-TECH Project Webinar (https://www.Fintech-ho2020.eu/) **- 19th May 2020**

At the invitation of the FIN-TECH workshop organising committee Professor Badii delivered a presentation on the Critical-Chains project research and innovation objectives for this workshop within the following agenda

Agenda- AI, Financial Automation and Market Risk, FIN-TECH Project Webinar 19th May 2020
Welcome: Tomaso Aste (University College London)
FRM@Europe: The Financial Risk Meter for European Assets Wolfgang Karl Haerdle (Humboldt University of Berlin)
Topic Sentiment Asset Pricing with DNN Supervised Learning Ying Chen (National University of Singapore)
Networking with Peers: Evidence from a P2P Lending Platform Bihong Huang (Asian Development Bank)
Neural Network Middle-Term Probabilistic Forecasting of Daily Power Consumption Michele Azzone (Polytechnic University of Milan)
Social media forecasting of COVID-19 Jeremy Turiel (University College London)
Digital money: the tension between technology and regulation Daniel Heller (University College London)

Project Aegis: The Money Laundering Regulations Sam Hastings (Financial Conduct Authority London)
Explain ability of a Machine Learning Granting Scoring Model in Peer-to- Peer Lending Javier Arroyo (Computense University of Madrid)
Flagship Project for Digital Finance, potential collaboration with FIN-TECH Ernesto Troiano (GFT Italy)
Potential European cloud computing for the FIN-TECH, e.g. AI projects Fabian Placht & Max Guhl (T-Systems Germany)
IoT- & Blockchain-enabled Security Framework for New Generation Critical Cyber-Physical Systems in Finance Sector Atta Badii (University of Reading)
Libra or Librae? Basket based stable coins Paolo Giudici (University of Pavia)
EU Blockchain Strategy Rapolas Lakavicius (European Commission)
Regulatory versus industry risk perspectives Dror Kennett (FINRA)
Using clustering ensemble to identify banking business models Bernardo Marques (University of Porto)
Market States and COVID-19 Pier Francesco Procacci (University College London)
XAI and Exploitation Strategy Jochen Papenbrock (Firamis)
Option Price Forecasting using Multilayer Neural Networks Shatha Qamhieh Hashem (An Najah National University)
The impact of AI and emerging technologies on the operation of Legal and Compliance functions of Financial Institutions Victoria Thompson (Barclays)

Workshop 4 -Metrics and Description

Title: FINTECH, AI Financial Automation and Market Risk		
Particulars	**Metrics**	**Description**
Date & Place		19th May 2020,
Host- Organisers		University College London, FINTECH Consortium
Number of persons registered	~60	Including representatives of Partners of EC-funded security projects with applications to financial sector and respective stakeholders
Number of the audience who participated	~50	
Number of sessions delivered	7	AI-Assisted Options pricing, P2P Lending, European Fintech Cloud, Basket-based Stable Coins, Blockchain, Cyber-physical Security
Number of speakers and panellists	20	As listed in the agenda above
Number of channels used for event publicity	10	Including all Partners' websites and social networks
Number of projects which contributed to the presentations and/or panel	5	FIN-SEC, FIN-TECH, Critical Chains, FRM@Europe, Project AEGIS
Number of countries represented	10	Germany, UK, Italy, Austria, Estonia, France, Turkey, Spain Singapore, Palestine
Number of sectors represented	8	Financial Services, ICT Cybersecurity, Regulatory Compliance and Certification Consultancy Services, Security Research Organisations, Public Sector (EC), Stock Market and Commodities Trading, Cloud Services providers, Blockchain developers.

Main themes discussed	7	AI-Assisted Options Pricing, P2P Lending, European Fintech Cloud, Basket-based Stable Coins, Blockchain, Cyber-Physical Security

Workshop 5: the ECSCI workshop (European Cluster for Securing Critical Infrastructures) held on June 24-25, 2020.

This event was organised by the FINSEC project Consortium (https://www.finsec-project.eu/) as the Coordinator of ECSCI cluster. Professor Badii participated as a contributor to the Q&A session. This workshop presented the different approaches to cyber-physical security as applicable to the seven most significant critical infrastructure sectors i.e. healthcare, energy, gas, water, financial services, air transport and communications.

The particular challenges of critical infrastructure protection in each of the above sectors were addressed by the different projects of the ECSCI cluster that presented their results, discussing the technical, ethical, and societal aspects and the underlying technologies. Specifically, novel techniques were presented for integrated security modelling, IoT security, artificial intelligence, distributed ledger technologies for secure information sharing and increased automation for detection, prevention and mitigation measures.

As can be seen below, the agenda consisted of keynote speeches from the EC, ENISA, ECSO, and on the 10 ECSCI H2020 project results including presentations, roundtable, panel discussions and thematic presentations. The audience included experts in several field related to security protection e.g. critical infrastructure protection, cyber and physical, CERTs, CSIRTs, CISOs, CIOs CSOs, and regulatory and policy authorities.

Agenda -the 1st ECSCI Workshop June 24-25, 2020.
Day 1
Opening remarks by Habtamu Abie and Andrea de Candido, Head of Unit of DG HOME B4 Innovation and Industry for Security
Critical Information Infrastructure Protection: The role of ENISA in the new EU policy context Kostantinos Moulinos, ENISA
DEFENDER: Energy infrastructure protection Gabriele Giunta of Engineering Ingegneria Informatica S.p.a.
SAFECARE: Safeguarding critical health infrastructure by
FINSEC: Securing critical financial infrastructure by Ernesto Troiano of GFT Philippe Tourron of APHM – Hôpitaux universitaires de Marseille and Isabel Praça of ISEP – Institut Superior de Engenharia do Porto
InfraStress: Improving resilience of sensitive industrial plants & infrastructures Lorenzo Franco Sutton of Engineering Ingegneria Informatica S.p.a.
RESISTO: Resilience enhancement and risk control for communication infrastructures Bruno Saccomanno of Leonardo – Società per azioni
STOP-IT: Protection of critical water infrastructures Rita Ugarelli of SINTEF
Thematic session 1: Physical and Cyber security integration and modelling
Thematic session 2: Standardization in Critical Infrastructure Protection
Thematic session 3: Collaborative Risk Assessment
Panel discussion: ELSI
Thematic session 4: Protect Industry 4.0
Conclusions and Collaboration Planning of Day 1
Day 2
Invited talk: Moving towards a trustworthy and resilient European cyber security ecosystem Roberto Cascella from ECSO
Thematic session 1: Resilience of Critical Infrastructures
ANASTACIA: Security and trust assessment in CPS / IOT architectures Stefano Bianchi of AlgoWatt Spa

SATIE: Security of air transport infrastructure of Europe Kelly Burke of DGSSPA
SecureGas: Securing the European gas network Ilias Gkotsis of KEMEA
SPHINX: Cyber-security protection in healthcare IT ecosystem Evangelos Markakis of Hellenic Mediterranean University-HMU
SmartResilience Aleksandar Jovanovic and Bastien Caillard of EU-VRi
Thematic session 2: Automation
Thematic session 3: Legal and Ethical issues
Panel Discussion: Artificial Intelligence
Thematic session 4: Predictive Analytics
Thematic session 5: Anomaly detection
Conclusions and Collaboration Planning of Day 2

Workshop 5 Metrics and Description

Title: European Cluster for Securing Critical Infrastructure (ECSCI)		
Particulars	**Metrics**	**Description**
Date & Place		24th-25th June 2020, Webinar
Host- Organisers		GFT Technologies, Italia SRL
Number of persons registered	~200	Including Partners' representatives from the 10 ECSCI security projects with applications to any of the 7 critical infrastructure application domains and respective stakeholders, EC Project Advisors
Number of the audience who participated	~150	
Number of sessions delivered	12	As set out in the agenda above
Number of speakers and panellists	23	As set out in the agenda above
Number of channels used for event publicity	>20	Including the websites of over 12 ECSCI Partner Projects and affiliated project websites
Number of projects which contributed to the presentations and/or panel	~12	Including 10 ECSCI Partner Projects and related projects
Number of countries represented	>12	Plus European Commission
Number of sectors represented	12	Financial Services, ICT Cybersecurity, Regulatory Compliance and Certification Consultancy Services, Security Research Organisations, Public Sector (EC), Cloud Services, Energy Providers, Gas Supply Sector, Water Supply Sector, IoT Services Sector, CERTs, CSIRTs, CISOs, CIOs CSOs, and regulatory and policy authorities
Main themes discussed	7	Critical infrastructure security protection, cyber-physical security, regulatory and policy evolution, integrated security modelling, IoT security, artificial intelligence for automation for detection, prevention, and mitigation measures, distributed ledger technologies for security information sharing

Workshop 6: Cybersecurity in Financial Sector

Joint Clustering workshop Co-organised with the SOTER Project (**https://soterproject.eu/**) **30th October 2020.** This workshop, hosted by the SOTER project and co-organised with the Critical-Chains with support by other Cluster projects, focused on 5 specific themes as follows:

- Cyber Security Training
- Authentication and Access Control
- Regulatory and Standardisation Monitoring
- Cyber Security Network of Competence
- Regulatory and Standardisation Coherence

Agenda - Cybersecurity in Financial Sector Joint Clustering Workshop – 30th October 2020
Welcome **Corinna Pannofino Trilateral Research (SOTER)**
Cybersecurity Optimization and Training for Enhanced Resilience in finance
Miren Karmele Garcia Garcia, Everis, Martin Griesbacher, RISE (SOTER)
Critical-Chains - IOT- & Blockchain-Enabled Security Framework for New Generation Critical Cyber-Physical Systems in the Financial Services Sector Atta Badii, University of Reading (Critical-Chains)
FIN-TECH - A FINancial supervision and TECHnology compliance training Programme
Anca Mirela Toma, Thomas Leach, Università di Pavia (FIN-TECH)
Predictive and Collaborative Security of Financial Infrastructure
Fabrizio Di Peppo, GFT Italia (FINSEC)
CyberSec4Europe - Cyber Security Network of Competence Centres for Europe
David Goodman, Trust in Digital Life (CyberSec4Europe)
SPARTA - Strategic programs for advanced research and technology in Europe - *CAPE program*
Herve Debar, Insitute Mines Télécom (CAPE – SPARTA)
CONCORDIA - Cyber security cOmpeteNce fOr Research and Innovation
Ramon Martin De Pozuelo, Genis, Caixa Bank (CONCORDIA)
Panel Session
Topics: Regulations, Cybersecurity, Digital Identity, & Training
Moderator: Christian Derler, Joanneum Research (SPARTA), (Critical-Chains)
Critical-Chains: Atta Badii, University of Reading **FIN-TECH:** Anca Mirela Toma, Thomas Leach, Università di Pavia **FIN-SEC:** John Soldatos, Innov-acts **CyberSec4Europe:** David Goodman, Trust in Digital Life **SPARTA:** Herve Debar, Insitute Mines Télécom **CONCORDIA:** Ramon Martin De Pozuelo Genis, Caixabank

Workshop 6 Metrics and Description

Title: Cybersecurity in Financial Sector		
Particulars	**Metrics**	**Description**
Date & Place		30th October 2020, Webinar
Host- Organisers		SOTER-Critical-Chains Consortia
Number of persons registered	~50	Including representatives of Partners of EC-funded security projects with applications to financial sector and respective stakeholders
Number of the audience who participated	~38	
Number of sessions delivered	2	Presentations from individual projects followed by Panel Session
Number of speakers and panellists	13	As listed in the agenda above
Number of channels used for event publicity	>15	Contact list invitation through Mailchimp, Project and Partner websites, Twitter, LinkedIn, Cyberwatching Research Hub, Cybersecurity month website
Number of projects which contributed to the presentations and/or panel	6	SOTER, Critical Chains, SPARTA, FIN-TECH, Concordia, Cybersecurity4Europe,
Number of countries represented	>12	Austria, France, Germany, Italy, Spain, Ireland, UK, Cyprus, Turkey, Estonia
Number of sectors represented	5	Financial Sector, ICT Cybersecurity, Security Research organisations, Socio-technical and human factors research Groups, eTraining Sector
Main themes discussed	6	Financial Sector, Cybersecurity, Authentication, Accountability, Modelling, Cybersecurity training, Regulatory Tensions

Workshop 7: Online Symposium Emerging Cybersecurity Standards for the Finance Sector in Europe: 27th November 2020

Organisers: Martin Griesbacher (RISE- Research Industrial Systems Engineering), Christian Derler Joanneum Research (Critical-Chains), Ronald Hochreiter (University of Vienna), Tina Ehrke-Rabel (University of Graz)

This online symposium included: **i)** presentations of research insights from selected European cybersecurity projects in the finance sector, as well as i**i)** stakeholders discussing their current challenges and needs with regard to cybersecurity and standardisation; followed by **iii)** panel discussion.

Agenda - Online Symposium Emerging Cybersecurity Standards for the Finance Sector in Europe: 27th November 2020
Introduction -Christian Derler (JOANNEUM RESEARCH), **Oana Mitrea** (Silicon Alps)
Challenges of new Technologies – Distributed Ledger and Cybersecurity Branka Stojanovic (JOANNEUM RESEARCH) – Discussant: Tina Ehrke-Rabel (University of Graz)
Understanding the Role of Human Behaviour for Cybersecurity in the Finance Sector Martin Griesbacher (Research Industrial Systems Engineering, RISE). – Discussant: Atta Badii (University of Reading)
Cybersecurity Issues in Fin-Tech Artificial Intelligence & Machine Learning Systems Ronald Hochreiter (Vienna University of Economics and Business) – Discussant Robin Renwick (Trilateral Research Ireland)
Stakeholder-Discussion: What new Standards are needed in the European Finance Sector? -Moderators Christian Derler (JOANNEUM RESEARCH), Martin Martin Griesbacher (RISE), Oana Mitrea (Silicon Alps)

Workshop 7 Metrics and Description

Title: Emerging Cybersecurity Standards for the Financial Sector in Europe		
Particulars	**Metrics**	**Description**
Date & Place		27th November 2020, Webinar
Host- Organisers		Joanneum Research, RISE, UGraz, UEconomicsWien
Number of persons registered	~35	Including representatives of Partners of EC-funded security projects with applications to financial sector security, banking sector, financial crime law enforcement, public sector
Number of the audience who participated	~28	
Number of sessions delivered	3	Presentations from individual projects, stakeholder observations, Panel Discussion
Number of speakers and panellists	10	As set out in the agenda above
Number of channels used for event publicity	6	Including project websites and direct mailshot invitations
Number of projects which contributed to the presentations and/or panel	3	Critical-Chains, SOTER, FinTech,
Number of countries represented	~20	The countries listed in the participating consortia above
Number of sectors represented	5	Financial Services Sector, ICT Cybersecurity, Security research organisations, Security Training Sector, Financial crime detector and prosecution
Main themes discussed	5	Blockchain, Human Factors and Cybersecurity Training, Secure Deployment of Machine Learning Models (Adversarial Training Considerations), Standardisation & Regulatory Mechanisms

Workshop 8: Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop, 14th December 2020 - 10:00- 13:30 CET (Webinar)

The thematic focus of this workshop included the following challenges:

- Risk-based Cyber-Physical Security by Design

- Financial Sector Cyber-Physical Security Protection
- Authentication & Accountability Models across the Financial Sector Flows, IOT & Blockchain
- Regulatory Harmonisation & Compliance Challenges: Tensions, Technological & Policy Enablers
- (PSTD 2, eIDAS, AML, GDPR, NIS)
- Training Harmonisation: e-Portfolio & Workplace-based Incident-Responsive Security Training

https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/2020/12/Financial-Sector-Cyber-Security-Regulatory-Challenges-Workshop-14th-Dec2020-v15.pdf

Agenda- Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop, 14th December 2020 - 10:00- 13:30 CET (Webinar)
Welcome and Overview of the Workshop, Ivan Tesfai – RINA Consulting S.p.A., Critical-Chains
Session 1: Integrated Cyber-Physical Security & Accountability for the Financial Sector: The Critical-Chains Paradigm
Authentication & Accountability Models in Financial transaction Flows Prof. Atta Badii & Dr Alper Kanak, University of Reading, ERARGE, Critical-Chains
Fintech Cloud Environment Trust & Security Challenges Kristo Klesment, Guard Time, Critical-Chains
eiDAS- Compliant Authenticated Access to the Critical-Chains Framework using the National Digital Identity (SPID), Massimiliano Aschi, Poste Italiane, Critical-Chains
Q&A
Session 2: Regulatory Harmonisation & Compliance Technological Enablers for the Financial Sector
Digital Identity and the Biometric Pattern as a Key Factor in Authentication Karmele Garcia, EVERIS, SOTER
Regulatory Disharmony & Disruptive Technologies in the Financial Sector David Goodman, Trust in Digital Life, CyberSec4Europe
Cyber Security Awareness: A Pre-emptive Move Against Cyber-Threats Laurentiu Vasiliu, Peracton, CS-AWARE
ICT Legal Consultants: Dealing with Regulatory Tensions (PSTD2, GDPR) Pablo Balboni, ictlegalconsulting, Cyberwatching
Q&A
Session 3: Financial Sector Challenges (Regulatory, Security-Privacy Protection, Training)
Panel Discussion: Stakeholders (Poste Italiane, Caxia Bank, Cyber-Security Project Coordinators, Subject Matter Experts) **Moderator: Atta Badii (Critical-Chains)** **Themes:** • Financial Sector Infrastructure Cyber-Physical Security-Privacy Protection Challenges • Financial Services Regulatory & Compliance Challenges (PSTD2, eiDAS, GDPR, AML, NIS) • Cyber Security & Compliance Training Challenges

Workshop 8 -Metrics and Description

Title: Financial Sector infrastructure Cyber-physical Security and Regulatory Standards		
Particulars	**Metrics**	**Description**
Date & Place		14th December 2020, Webinar
Host- Organisers		Critical Chain Consortium
Number of persons registered	69	

Number of the audience who participated	46	Including representatives of Partners of EC-funded security projects with applications to financial sector and respective stakeholders, EC project & policy advisors
Number of sessions delivered	3	Individual Presentations, Panel Discussion, Q&A
Number of speakers and panellists	13	As set out in the agenda above
Number of channels used for event publicity	>20	Including Critical-Chains Partner websites, Consortium Partners' websites, Twitter, Project LinkedIn channel, EC News Channel, Consortium Partners LinkedIn channel, Sectorial Research Project LinkedIn channels/website/Twitter, RINA VIMEO Channel https://research.reading.ac.uk/critical-chains/ Critical Chains H2020 Project LinkedIn @ChainsH2020 https://www.youtube.com/channel/UCa3QA5cOLRMR8bPGIvsVWg
Number of countries represented	>20	Including the countries of the participating Consortia Partners
Number of sectors represented	7	Financial Services, ICT Cybersecurity, Security research organisations, Human Factors and Cybersecurity Training, Cloud Services, Legal and Data Protection, Public Sector (Regulatory and Policy authorities)
Number of Project-to-Policy contributions made	4	Regulatory Harmonisation, Cybersecurity Impact of Disruptive Technologies in the Financial Sector, Security-Privacy Protection Challenges, Regulatory tensions, and Compliance Issues
Main themes discussed		Authentication, Accountability Engineering, Authentication as a Service, Blockchain as a Service, Secure Cyber as a Service, Transaction Flow Modelling as a Service, Regulatory Mechanisms and Standardisation issues (Harmonisation, PSD2, GDPR, *AML,NIS)*, Application Domains (FINTECH, Open Banking, Insurance, Highway toll, Cybersecurity Awareness, Agile Incident Responsive Training.

Workshop 9 -Metrics and Description

Title: ISICAS 2020 (International Symposium on Integrated Circuits and Systems)		
Particulars	**Metrics**	**Description**
Date & Place	29-30 August 2020 Shangai /China (Online)	This conference is one the flagship events of IEEE in the fields of hardware-based cyber-physical systems, circuits and systems.
Host- Organisers	IEEE Circuits & Systems (CAS) Society	
Number of persons registered	150	
Number of the audience who participated	400	
Number of sessions delivered	17	
Number of speakers and panellists	100	

Number of channels used for event publicity	2	Linkedin, web site
Number of countries represented	NA	This is a worlwide scientific ogranisation. No specific country or sector was represented.
Number of sectors represented	NA	
Number of Project-to-Policy contributions made	NA	
Main themes discussed		Paper presented: "A Reconfigurable Random Number Generator Based on the Transient Effects of Ring Oscillators" By B Acar, S Ergun (ERARGE) and this paper was decided to be published in IEEE Transactions on Circuits and Systems II: Express Briefs (67 (9), 1609-1613). The results of this study have been used in HwSaaS and reported in D5.5.

Workshop 10 -Metrics and Description

Title: ICHMS 2020 (IEEE International Conference on Human-Machine Systems)		
Particulars	**Metrics**	**Description**
Date & Place	7-9 September 2020, Rome – Italy (Online)	This is one of the leading conferences of IEEE covering a wide range of technologies touching directly to the humans.
Host- Organisers	IEEE	IEEE Systems, MAn & Cybernetics Society Univ. Of Calabria, Italy CNR, Italy Sapienza Univ. Di Roma Associazione Italiana di Systems Engineering IEEE Italy Section
Number of persons registered	NA	
Number of the audience who participated	600	
Number of sessions delivered	28	
Number of speakers and panellists	128	
Number of channels used for event publicity	2	Linkedin, web site
Number of countries represented	NA	This is a worldwide scientific organisation. No specific country or sector was represented.
Number of sectors represented	NA	
Number of Project-to-Policy contributions made	NA	
Main themes discussed		Paper presented: "Diamond Accountability Model for Blockchain-enabled Cyber Physical Systems". This paper raised a strong interest on the blockchain-enable accountability models where hardware-based IoT security is used in digital twin environments.

7.2 Assessment of Critical-Chains clustering efforts

All the events related to the Critical-Chains clustering efforts for the reference period are listed in Table 7-1.

Table 7-1: Tracking of Critical-Chains clustering effort

Action	Type of cluster	Involved partner	When	Target audience
ECSCI virtual workshop	ECSCI	UREAD	24-25 June 2020	
Virtual conference	SOETER H2020	RINA-C	20 Nov. 2020	SOTER Project's partners
Stakeholder Engagement	Financial sector company			Ub-Technologies NL B.V.
Activities Planning with the FIN-TECH Project	FIN-TECH SOTER	UREAD		FIN-TECH project's partners; SOETER Project's partners
Activities Planning with the FINSEC Project	FINSEC			FINSEC project's partners
''Training on Cyber-Risk and Security-by-design'' WEBINARS	POSTEIT internal employees and managers	POSTEIT	05-21 Oct. 2020	POSTEIT internal employees and managers
'Cybersecurity in Finance' workshop organized by SOTER	SOTER H2020	RINA-C/UREAD	30 Oct 2020	Fintech and cybersecurity sector
SDX engagement	Stakeholder engagement	RINA-C	23 Nov 2020	Project partners
3rd Webinar *'Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop'*	Financial Sector	RINA-C/POSTE-IT/UREAD	14 Dec 2020	Financial sector network, security and training, and transactions monitoring managers, European Commission regulatory policy and other standardization stakeholders
Cyberwatching Engagement	Stakeholder engagement	RINA-C/UREAD	13 Nov 2020	Project partners
UB technologies engagement	Stakeholder engagement	RINA-C	June 2020	Project partners
Emerging Cybersecurity Standards for the Finance Sector in Europe	Finance sector, industry	JR, UREAD	27/11/2020	scientific community
Digital Transformation and Blockchain in FinTech	Austrian industry and service sector	JR	24/09/2020	industry
Cybersecurity in Finance	European research community	UREAD, JR, RINA-C	30/10/2020	scientific community
Cyber Security in Österreich 2020: Ein- & Ausblicke für Studierende	Austrian Cybersecurity ecosystem	JR	28/05/2020	general public

Technologiegespräche des Europäischen Forums Alpbach, Breakout Session 08 „Wie sicher ist sicher? Leben und Wirtschaften im Spannungsfeld zwischen Komfort – Geschwindigkeit – Sicherheit“	Applied Research community, Industry	JR	23/08/2019	policy makers
IKT Sicherheitskonferenz 2019	Austrian/German Security community	JR	01/10/2019	policy makers
GRAZ SECURITY DAYS FOR INDUSTRY 2019	Industry	JR	18/09/2019	industry
9. Arbeitssitzung der Cyber Security Plattform Austria	Austrian Cybersecurity community	JR	03/10/2019	policy makers
FORTE und KIRAS Einreichertag (National Security and Defence research programs)	Security Research community	JR	21/10/2019	scientific community
MILIPOL Paris 2019, Workshop on AI for LEAs	European Security Research community, Law enforcement agencies	JR	20/11/2019	industry
SMI2G Meeting 2020	European Security Research Community	JR, UREAD, ERARGE, CEA, RINA-C	30/01/2020	scientific community
KIRAS Fachtagung (National security research program)	Security Research community	JR	21/09/2020	scientific community
Fintech Week Vienna 2019	Fintech community	JR	18/11/2019	industry
First Israeli Winter School on Biometrics	Students	JR	11/02/2020	scientific community
ICHMS 2020 (IEEE International Conference on Human-Machine Systems)	Security Research community	ERARGE	7-9/09/2020	industry scientific community

7.3 Dissemination relevance of Critical-Chains clustering efforts

Among the dissemination actions previously presented, the most relevant ones are in the following so that it will be possible to make general performance considerations in relation to the indicators reported in Section 2 Methodology and objectives.

Table 7-2: Relevance of Critical-Chains clustering efforts

Event Name	Why this cluster?	Audience Size	Feedback / Results	Relevance	A	B	C	D	E	F	G	H	I	J	K
SDX engagement	SDX is a company working in AI and security and some of their projects are focused on finance. Stakeholder network enlargement	7	SDX becomes a Critical Chains stakeholder	High	NA	7	1	7	1	NA	NA	NA	NA	3	NA
3rd Webinar 'Financial Sector Infrastructure Cyber-Physical Security and Regulatory Standards Workshop'	Visibility raising/ stakeholder network expansion	46	Strengthen the collaboration and interaction of Critical Chains project with other relevant financial projects and enhancement	High	69	46	3	13	1	8	5	5	NA	5	3
Cyberwatching engagement	Cyberwatching has a network of 50 projects focused on cybersecurity. Visibility raising.	NA	Co-Organization of Workshops Critical-Chains project description has been included in Cyberwatching project hub	High	NA	NA	1	NA	1	NA	NA	NA	NA	3	NA
UB Technologies engagement	stakeholder network expansion	3	Inclusion in CC stakeholder community Participation at critical chains workshop Availability to provide feedback for supporting CC.		NA	3	1	3	1	NA	NA	NA	NA	3	NA
Emerging Cybersecurity Standards for the Finance Sector in Europe	Identify synergies and complementary approaches	30	Raised attention to Critical-Chains in the international FinTech scientific community; Started planning cooperation steps between FinTech research projects, including SOTER and FINTECH EU projects, and organisations including RISE, Vienna University of	Very high	52	30	2	6 + 6	1	4	2	3	5	5	4

			Economics and Business, UNI Graz, SILICONALPS; Received positive feedback.												
Digital Transformation and Blockchain in FinTech	Disseminate to Austrian community	25	Raised attention to Critical-Chains in Austrian blockchain and FinTech industry community; Received positive feedback.	Very high	NA	25	2	8	1	4	2	NA	1	6	4
Cybersecurity in Finance	Learn about relevant projects	NA	Raised attention to Critical-Chains in the international FinTech scientific community; Started clustering activities with other projects in the same area; Exchanged ideas of potential cooperation between projects; Received positive feedback.	Very high	NA	NA	2	7	1	4	2	7	NA	NA	4
Cyber Security in Österreich 2020: Ein- & Ausblicke für Studierende	Disseminate to Austrian student communities	85	Raised attention to Critical-Chains and related H2020 projects in the Austrian student's community and among the Austrian Cybersecurity ecosystem	Medium	NA	85	1	4	1	4	2	NA	2	5	4
Technologiegespräche des Europäischen Forums Alpbach, Breakout Session 08 „Wie sicher ist sicher? Leben und Wirtschaften im Spannungsfeld zwischen Komfort – Geschwindigkeit – Sicherheit"	Raise awareness among applied research stakeholders	30	raised awareness to Cybersecurity research on national and European level within stakeholders and policy makers by organising this breakout session within this top conference for applied research in Austria	High	NA	30	1	6	1	4	2	NA	4	6	6
IKT Sicherheitskonferenz 2019	Raise awareness among security community and policy makers	2000	Raised attention to Critical-Chains in international cybersecurity policy-makers community; Business talks with stakeholders about potential cooperation;	High	NA	2000	12	40	1	4	2	NA	15	NA	20
GRAZ SECURITY DAYS FOR INDUSTRY 2019	Raise awareness among security community and industry	150	Raised attention to Critical-Chains in the international cybersecurity policy-makers community; Business talks with stakeholders about potential cooperation;	High	NA	150	6	18	1	4	2	NA	6	NA	10
9. Arbeitssitzung der Cyber Security Plattform Austria	Raise awareness among security community and policy makers	60	Raised attention to Critical-Chains in the Austrian cybersecurity policy makers' community; Business talks with stakeholders about potential cooperation;	High	NA	60	3	8	1	4	2	NA	2	NA	5

FORTE und KIRAS Einreichertag (National Security and Defence research programs)	Raise awareness among security community and policy makers	80	Raised attention to Critical-Chains in the Austrian scientific community; Business talks with stakeholders about potential cooperation;	High	NA	80	2	10	1	4	2	NA	2	NA	8
MILIPOL Paris 2019, Workshop on AI for LEAs	Raise awareness among security community and policy makers	30	Raised attention to Critical-Chains in the international cybersecurity industry community; Business talks with stakeholders about potential cooperation;	Medium	NA	30	4	4	NA	NA	NA	NA	NA	NA	NA
SMI2G Meeting 2020	Brokerage between H2020 research partners	400	Raised attention to Critical-Chains in the international scientific community; Presented proposal ideas building on planned work of Critical-Chains; Business talks with stakeholders about potential cooperation;	Medium	NA	400	6	60	1	4	2	NA	27	NA	40
KIRAS Fachtagung (National security research program)	Raise awareness among security community and policy makers	80	Raised attention to Critical-Chains in the Austrian scientific community; Business talks with stakeholders about potential cooperation;	High	NA	80	2	10	1	4	2	NA	2	NA	8
Fintech Week Vienna 2019	Raise awareness within Fintech sector	200	Raised attention to Critical-Chains in the Austrian FinTech industry community; Business talks with stakeholders about potential cooperation;	Very high	NA	200	4	20	1	4	2	NA	6	NA	10
ISICAS 2020 (International Symposium on Integrated Circuits and Systems)	A flagship IEEE conference	400	Raised strong attention on the reconfigurable RNG design approach and the users can choose the RNG working mode (See D5.5 for technical details).	High	NA	400	17	101	2	1	2	NK	NK	NK	0
ICHMS 2020 (IEEE International Conference on Human-Machine Systems)	A conference led by a distinguished community of IEEE related to smart systems	600	Raised strong attention on the hardware-based security schemes in IoT and blockchain environments + paper presentation	Medium	NA	600	28	128	2	1	2	NA	NA	NA	0
MWSCAS 2019 (Midwest Symposium on Circuits and Systems)	A very renowned worldwide symposium in cyber-physical systems and circuits	1000	Raised strong attention on the use truly random number generation, cryptographic solutions and their applications in Fintech + paper presentation	High	NA	1000	68	300	1	1	1	NA	NA	NA	0

ISICAS 2019 (International Symposium on Integrated Circuits and Systems)	A prestigious conference on integrated solutions covering the secure embedded systems	350	Raised strong attention on cryptanalysis that can be applied to Fintech security + paper presentation	High	NA	350	17	36	1	1	1	NA	NA	NA	0
APPCAS 2019 (IEEE Asia-Pacific Conference on Circuits and Systems)	A worldwide conference with special sessions for IoT security and blockchain	320	Raised strong attention on the true random number generation schemes, their test and validation in security schemes + paper presentation	Medium	NA	320	19	71	1	1	1	NA	NA	NA	0
AsianHOST 2019 (Asian Hardware Oriented Security and Trust Symposium)	One of the renowned organisations in cyber-physical security and trust solutions in many areas	50	Raised strong attention on the true random number generation schemes, their test and validation in security schemes + paper presentation	Medium	NA	50	4	16	1	1	1	NA	NA	NA	0
2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)	IEEE's flagship conference on systems and cybernetics	1750	Raised strong attention on block-chain accountability and digital twin concept + paper presentation	Medium	NA	1750	84	504	1	1	1	NA	NA	NA	0
Blackhat Conference	Worldwide conference on cyber security	800	Raised strong attention on hardware-based security, cyber-physical security, blockchain accountability	High	NA	800	16	250	1	1	1	NA	NA	NA	0

LEGEND:

A	Number of persons pre-registered	G	Number of projects who participated
B	Number of audiences who attended	H	Number of EC Countries represented in &-OR
C	Number of sessions (talk on same or related topic=a session)	I	Number of sectors represented
D	Number of speakers	J	Number of project-to-Policy talks/papers presented
E	Number of channels used for the event (e.g. webinar, twitter)	K	Number of channels used for pre-publicity of the event
F	Number of channels used for post-publicity of the event (e.g. pictures or videos)		

8 Targeted Use-Cases-focused Stakeholder Awareness Raising

POSTE arranged a set of 6 Webinars during the period between 05/10/2020 and 21/10/2020 titled ''Training on Cyber-Risk and Security-by-design'', during the event the promotional video of the Critical-Chains Project was shown to the audience. Below has been reported the main information relating to the webinars.

The country addressed is Italy and the target consists of all employees in Directorate General of Bancoposta (bank), including top management. 481 people participated to 6 different webinars totalling 25 hours of presentations. Top level managers (decision-makers), experts from every area in the financial sector, engineers, cyber-security experts were involved.

Critical-Chains was introduced to the audience and project's objectives and expected results were presented including the Pilot developed by Poste Italiane. Feedback reported from the audience were positive.

BancoPosta is one of Italy's biggest financial service providers, a major player that is constantly expanding its range of services for households. It is mainly engaged in:

- the active management of the banking book, consisting of public and private customer deposits and relative lending activities;
- promotion and management of the postal savings instruments issued by Cassa Depositi e Prestiti (bonds and savings books);
- transaction banking services (payments and collections), such as postal payment slips, F24 tax forms, national and international postal money orders, Moneygram and Eurogiro services;
- promotion and distribution, through its own distribution platform, of financial products issued by third parties or other group companies, such as:
    - asset management products (units of open-ended mutual funds established by BancoPosta Fondi SGR);
    - asset administration products;
    - Poste Vita and Poste Assicura insurance policies.
- third-party financing products and credit cards. As concerns asset management, BancoPosta Fondi SGR manages open-ended mutual investment funds, delivering significant returns over the years. It is also specialised in the management of Eurozone sovereign bonds and corporate bonds. Asset management is a business we are targeting to drive our future growth, with a view to offering simple, clear and well-structured products, building on the relationship of trust we have with our customers. To this end, Poste Italiane has forged partnership agreements with ANIMA Holding over 2017–2018. Under the Deliver 2022 Plan, BancoPosta Fondi SGR has become a competency centre for the management of all group financial investments.

Poste operates also in the insurance business through PosteVita, a leading life insurance company in Italy, now active in the casualty insurance segment. Poste Vita additionally offers investment and savings products, promoted through our distribution platform.

9 Targeted Use-Cases-focused Stakeholder Group Forming

Stakeholder Engagement

Stakeholder Group members are encouraged to participate in our workshops as speakers and/ or panellists and in addition to access to public deliverables, they are invited to contribute to the requirements revision by expressing their opinion regarding the various aspects of the design and deployment of Critical-Chains services. Stakeholder Group members are welcome to offer trialling opportunities and/or datasets for consideration of further engagement by the Steering Committee on a case-by-case basis.

The engagement the potential stakeholder group member companies started early in 2020. The Consortium has been seeking opportunities to reach out to organisations and enterprises operating in the Financial Sector or within the regulatory standardisation and security organisations to join our stakeholder group and despite the restrictions re holding physical meetings, the dissemination manager RINA-C has continued to pursue the available opportunities for networking and has managed to enrol two organisations with well-matched interests and keen interest in the Critical-Chains area of innovation. Preliminary discussions with RINA-C have led to formal meetings which have included the following steps for both members who have since joined the Stakeholder Group.

1. The senior management and R&D staff of the companies have made presentations to members of the Consortium followed by Q&A and discussion of their technological capabilities, business model and service provision focus and possible areas of related Critical-Chains innovation.
2. The Critical-Chain Coordinator and Dissemination Manager have presented the project objectives, clarified the terms of engagement with the Stakeholder Group members consistent with the Critical-Chains Consortium Agreement and in particular the project security policy.
3. Accordingly, the companies have confirmed acceptance of the offer of association with the Critical-Chains project as Stakeholder Group members.
4. The draft Engagement Roadmap and the Next Steps have been developed by the Dissemination Manager for consideration of the Steering Committee.

Accordingly, the following two organisations have been duly invited to participated as a panellist within workshop 8, as presented above and further collaboration is planned to be implemented during period ii) as shall be determined by the Steering Committee.

It is expected that the two Stakeholder Group members will support our networking within the financial sector to further expand the Stakeholder Group particularly from amongst the organisations providing cloud-based services to the financial sector. A brief outline of the profile of the two organisations is follows:

1) SDX Network

https://www.sdx.network/

Product and Business model focus: Provider of a **Secure Compute Data Platform**

- **Providing insights for the clients derived from raw data they do own and will not need to access**
- Applying SQL or ML algorithms to compute on top of one or multiple third-party data sources without accessing and owning the raw data. – obtaining the data insights to clients without the need to purchase the whole dataset.
- **No need to move the data from its initial storage**

- The computation is performed directly on the client premises where the data is securely stored. The data provider would not need to move the data from its original location, leaving the custody of the targeted raw data intact whilst enabling its data processing – trust agnostic regime
- **privacy preserving & algorithm IP protection**
- Deploying federated learning, multi-party computation and private blockchain network to protect the security of the computation, privacy, and IP protection of algorithms.

2) UB Technologies (www.ubtechnologies.nl)

Product and Business model focus: Provider of a **Portfolio and Risk Analytics and Forecasting Platform**

The platform provides rapid end-to-end risk analysis for bankers, asset managers and quants to run huge simulations at large scale, resulting in enhanced insights into the drivers of financial performance. This enables the clients to radically improve, accelerate and democratise their risk/return decision-making.

The GPU-supercharged platform leverages established technologies and a compute-optimised codebase. The technology provides users - both technical and non-technical – to deploy the analytics core with output accessible via both cutting edge APIs or a convenient user interface.

9.1 Assessment of Stakeholder Group Engagement Process and Results

In order to ensure the robustness of Critical-Chains innovations, one of the core elements of dissemination strategy was building a stakeholder community that able to be engaged for feedback aimed at the improvement of project results and support to validation.

In this sense, dissemination actions towards Critical-Chains target stakeholders have been done in order to identify relevant entities, assess and eventually include them in the so-called Critical-Chains stakeholder community.

The general evaluation process followed is below reported:

- The potential stakeholders are identified by each partner
- The Dissemination manager evaluates the value of the stakeholder (in terms of the target audience and fit with project scope)
- If the stakeholder is considered relevant, the dissemination manager communicates the possible engagement of the entity to the Consortium.
- In case none disagrees, the dissemination manager organizes an interview with the new stakeholder, the coordinator, and the interested partners.
- After a briefing among the project coordinator, dissemination manager, and/or interested partners, the new stakeholder could be considered a member of the community.

So far, two entities have been selected as the candidate of the stakeholder community. In the following details:

- Ub-technologies b.V. (https://www.ubtechnologies.nl/): The company offers a portfolio risk optimization platform to banks and insurance exploiting AI technologies. Since it is strongly verticalized in the Fintech/banking/insurance sector, it is considered as the target user of Critical-Chains. The company has been duly approved to join the stakeholder community (first representative). The company contributed with feedback and information useful to draft user requirements and attended as a guest speaker on the Critical-Chains workshop held on December 14th.
- SDX Network (https://www.sdx.network/): The company offers a secure computing data platform based on federated learning strategies. The company presented a comprehensive overview of the main solution, key technologies, and a series of privacy-preserving relevant use cases, which one specifically

verticalized on the financial sector. After a briefing, and without disagreement of Critical-Chains consortium, the entity can be considered a member of the Critical-Chains community

Additionality, in 2020, Critical-Chains Partner IMEC from Nederland announced that they have been working together with ERARGE from Turkey to integrate the Secure Distance Bounding solution with the secure stick. For further integration with the use cases in early 2021, they will align with the use of case owners and make a decision on which use cases to join in which the stakeholder community will be consolidated in terms of the user-experience aspect of the integration.

Accordingly, in 2020, Stakeholder Group members are invited to our public workshops and can have access to the public deliverables but are also will be invited to contribute to the revision of the requirements through special sessions to be held alongside our planned public workshops whereby following presentations of project results to stakeholders they would be invited to express their opinion regarding the various aspects of design and deployment of Critical-Chains services.

10 Scientific and Technical Publications

Scientific and technical achievements have been disseminated by producing and publishing publications below, and also included in the Appendix:

Paper 1: #1 by IMEC-NL

TITLE	Paper: Secure, Accurate, and Practical Narrow-Band Ranging System (IACR TCHES)
Abstract	Relay attacks pose a serious security threat to wireless systems, such as contactless payment systems, keyless entry systems, or smart access control systems. Distance bounding protocols, which allow an entity to not only authenticate another entity but also determine whether it is physically close by, effectively mitigate relay attacks. However, secure implementation of distance bounding protocols, especially of the time critical challenge-response phase, has been a challenging task. In this paper, we design and implement a secure and accurate distance bounding protocol based on Narrow-Band signals, such as Bluetooth Low Energy (BLE), to particularly mitigate relay attacks. Narrow-Band ranging, specifically, phase-based ranging, enables accurate distance measurement, but it is vulnerable to phase rollover attacks. In our solution, we mitigate phase rollover attacks by also measuring Time-of-Flight (ToF) to detect the delay introduced by such attacks. Therefore, our protocol effectively combines the best of both worlds: phase-based ranging for accuracy and Time-of-Flight (ToF) measurement for security. To demonstrate the feasibility and practicality of our solution, we prototype it on NXP KW36 BLE chips and evaluate its performance and relay attack resistance. The obtained precision and accuracy of the presented ranging solution are 2.5cm and 30cm, respectively, in wireless measurements.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	NA

Paper 2: #2 by ERARGE

TITLE: A Reconfigurable Random Number Generator Based on the Transient Effects of Ring Oscillator (ISICAS2020)	
Abstract	This brief presents a reconfigurable Random Number Generator (RNG) based on transient effect of ring oscillators. Users can select a method based on the irregular sampling of a regular waveform or on the regular sampling of an irregular waveform to obtain a random bit sequence to be used in different applications, such as lightweight cryptography or high-security communication. The entropy is acquired by exploiting Transient Effect Ring Oscillators (TEROs). The proposed fully-digital RNG structure is firstly implemented on a Zynq-7000 FPGA (Field Programmable Gate Array) without any post-processing method such as the Von Neumann. In addition to the RNG structure, an on-the-line test module based on FIPS 140-2 is also implemented to check the randomness of the produced data statistically in real time. Users can change the statistical test parameters according to their desired security levels. Finally, an ASIC (Application Specific Integrated Circuits) implementation of the proposed RNG is done following the Cadence digital design flow for the TSMC 180 nm CMOS process. The implemented ASIC design occupies an area of 0.85 mm x 0.85 mm and the estimated power required is 11.827 mW.
H-Index	111
Current Impact factor	2.814
Historical Impact Factor or SNIP	NA

Paper 3: #3 by ERARGE

TITLE **Diamond Accountability Model for Blockchain-enabled Cyber Physical Systems (ICHMS2020)**	
Abstract	Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This letter presents a Diamond Accountability Model (DAM) where a public or private authority is included in the blockchain transactions providing non-repudiation of digital transactions, holistic security and effective governance. The proposed technique aims to present a decentralized solution for multi-agent applications where many partnering organizations have to collaborate without suffering from the security, accountability, maintenance, scalability, and integrity problems over distributed cyber-physical systems (CPS). The proposed scheme positions authorities also in the chain that enables additional accountability and trust. The scheme proposes a verification mechanism where the authorized organizations are also included in the verification of transactions over the blockchain. In order to elucidate, a conceptual use case is presented where at least two partnering organizations collaborate with each other within a decentralized but also authorized blockchain-enabled scheme.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	NA

Paper 4: #4 by ERARGE

TITLE: A Non-autonomous Balanced Chaotic Circuit Based-on A Bipolar Differential-pair (MWSCAS19)	
Abstract	A novel cross-coupled bipolar transistor-based non-autonomous chaotic oscillator is proposed. The derivation methodology of this novel chaotic oscillator is based on integrating two of existing chaotic oscillators symmetrically and employing a differential-pair stage. Simulation and experimental results, verifying the feasibility and the correct operation of the circuit are also given.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	NA

Paper 5: #5 by ERARGE

TITLE: Random Number Generators Based on Irregular Sampling and Fibonacci–Galois Ring Oscillators (ISICAS2019)	
Abstract	This brief presents a random number generator (RNG) based on irregular sampling of regular waveform method where the irregular signal is obtained by combining Fibonacci-Galois ring oscillators with an XOR gate. The RNG is implemented on a FPGA (field-programmable gate array). The regular waveform generated by the digital clock manager of the FPGA, is sampled at times corresponding to certain number of rising edges of the irregular signal, and the resulting bit stream is subjected to statistical tests of randomness. It is demonstrated that the resulting bit sequence from the proposed RNG satisfies NIST 800-22 test suit and Rabbit and SmallCrush batteries from TestU01 library without any need for post-processing such as Von Neumann or XOR. A comparison between the methods regular sampling of irregular waveform and irregular sampling of regular waveform is given in terms of robustness against external interference. The impact of selection of Fibonacci-Galois polynomials is discussed. Using digital design flow for TSMC 65nm process, an asic implementation of the proposed RNG is given having 1115 gates and 4.811 mW estimated power.
H-Index	111

Current Impact factor	2.814
Historical Impact Factor or SNIP	NA

Paper 6: #6 by ERARGE

TITLE: A Comparative Study on the Robustness of Chaos-Based Random Number Generators (APCCAS)	
Abstract	This paper presents a comparative study on continuous-time chaos-based random number generation methods regarding their robustness against changes in chaos controlling parameters and external interference. Chaotic systems suggest enabling high throughput random data without need for postprocessing and with less complex hardware. However, due to effects of aging or fabrication process variations, the chaos controlling parameters of the random number generator may change. Furthermore, external interference can be applied on the chaotic oscillator to manipulate its output. Therefore, in a chaotic RNG, the bit generation method should be immune to parameter variation and external interference. In this study, two widely used methods for random number generation have been compared: 1) Regular sampling of chaotic waveform (RSCW), and 2) Chaotic sampling of regular waveform (CSRW). A double-scroll chaotic system is chosen as the chaotic oscillator and it is numerically simulated in normalized time domain to generate random bit sequences using both methods. Applying the concepts of autocorrelation and approximate entropy to the output bitstreams, the robustness of the two-bit generation methods against parameter variation and external interference have been compared. It is demonstrated that chaotic sampling of regular waveform method provides more robustness against parameter changes and external interference compared to regular sampling of chaotic waveform method.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	25

Paper 7: #7 by ERARGE

TITLE: Attack on a Microcomputer-Based Random Number Generator Using Auto-synchronization (AsianHOST)	
Abstract	A novel attack system is proposed to reveal the security weaknesses of a microcomputer-based random number generator (RNG). Convergence of the attack system is proved using auto-synchronization. Secret parameters of the microcomputer-based RNG are revealed where the available information are the structure of the RNG and a scalar time series observed from the chaotic system used as the seed of the RNG. Simulation results verifying the feasibility of the attack system are given such that, next bit can be predicted while the same output sequence of the RNG can be generated.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	6

Paper 8: #8 by ERARGE

TITLE: A Visionary Model on Blockchain-based Accountability for Secure and Collaborative Digital Twin Environments (IEEESMC2019)	
Abstract	With the recent advancements in blockchain technology, it has become obvious that this technology is not just for crypto-currencies but instead can be used as a decentralized tool for better accountability. Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This paper presents a blockchain-based model for distributed and collaborative digital twin environments which is becoming indispensable in new "Any 4.0" era. The proposed model includes a public or private authority in the digital twin ecosystem providing non-repudiation of blockchain transactions, holistic security and privacy preservation. The proposed technique is based on the "X-by-design" and "X-as-a-service" principles which can be discussed as a novel model for better security, accountability and integrity in decentralized mechanisms. In order to elucidate, two case studies are described where the digital twin operations, stakeholders' activities and regarding transactions are stored on a blockchain.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	120

Paper 9: #9 by JR

TITLE	**APT datasets and attack modelling for automated detection methods: A review**
Abstract	Automated detection methods for targeted cyber-attacks are getting more and more prominent. In order to test these methods properly, it is crucial to have a suitable dataset. This paper provides a review on datasets and their creation for use in APT detection in literature. A special focus is placed on feature engineering, including construction, selection and dimensionality reduction. Two use cases based on the underlying infrastructure are distinguished, large enterprise networks and Cyber Physical System, additionally including cloud computing systems, financial technology networks and Internet of Things networks. These datasets are usually based on an attack model. A description of different stages including approaches and goals of such attacks are given. The major achievement is the description and analysis of existing feature extraction methodologies and detailed overview of datasets used in APT detection related literature. This shows that the large enterprise network use case, has incorporated a much more frequent use of datasets with quite short periods of time. In the case of Cyber Physical System, a realistic dataset is publicly available.
Index	
ırrent Impact factor	579
storical Impact ıctor or SNIP	756

Paper 10: #10 by JR, UREAD

TITLE	**Cyber-Attack Taxonomy of Distributed Ledger- and Legacy Systems-based Financial Infrastructures**
Abstract	Nowadays, virtually all products and services offered by financial institutions are backed by technology. While the frontend banking services seem to be simple, the core-banking backend systems and architecture are complex and often based on legacy technologies. Customer-facing applications and services are evolving rapidly, yet they have data dependencies on core banking systems running on ancient technology standards. While those legacy systems are preferred for their stability, reliability, availability, and security properties, in adapting the frontends and services many security and privacy issues can occur. Clearly, these issues are arising as those systems have been designed decades ago,

	without considering the enormous amounts of data that they are required to handle and also considering different threat scenarios. Moreover, the trend towards using new technologies such as Distributed Ledger Technologies (DLT) has also emerged in the financial sector. As the nodes in DLT systems are decentralized, additional security threats come to light. The focus of this work is the security of financial technologies in the FinTech domain. We provide relevant categorization and taxonomies for a better understanding of the main cyber-attack types, and suitable countermeasures. Our findings are supported by using security-by-design principles for some selected critical financial use-cases, and include a detailed discussion of the resulting threats, attack vectors and security recommendations.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	NA

Paper 11: #11 by JR, FHG, UREAD

TITLE	Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications
Abstract	Financial technology, or Fintech, represents an emerging industry on the global market. With online transactions on the rise, the use of IT for automation of financial services is of increasing importance. Fintech enables institutions to deliver services to customers worldwide on a 24/7 basis. Its services are often easy to access and enable customers to perform transactions in real-time. In fact, advantages like these make Fintech increasingly popular among clients. However, since Fintech transactions are made up of information, ensuring security becomes a critical issue. Vulnerabilities in such systems leave them exposed to fraudulent acts, which cause severe damage to clients and providers alike. For this reason, techniques from the area of Machine Learning (ML) are applied to identify anomalies in Fintech applications. They target suspicious activity in financial datasets and generate models in order to anticipate future frauds. We contribute to this important issue and provide an evaluation on anomaly detection methods for this matter. The experiments are conducted on several fraudulent datasets from real-world and synthetic databases, respectively. The obtained results confirm that ML methods contribute to fraud detection with varying success. Therefore, we discuss the effectiveness of the individual methods with regard to the detection rate. In addition, we provide an analysis on the influence of selected features on their performance. Finally, we discuss the impact of the observed results for the security of Fintech applications in the future.
H-Index	NA
Current Impact factor	NA
Historical Impact Factor or SNIP	NA

10.1 Dissemination tracking of Critical-Chains Scientific and Technical Publication

The following Table 10-1: **Tracking of Critical-Chains publications** shows the dissemnation tracking of scientific and technical publications together with publications metrics as well as journal specifications. Eight publications have been published, one is already accepted and two publications are under revision. The publications types range from Journal Paper to Conference Paper, Review and Article.

Table 10-1: Tracking of Critical-Chains publications

ID	Type of Publication	Date	Journal	Status	Open Access	Involved Partner	Target audience	Current Impact factor	Historical Impact Factor or SNIP
1	Journal Paper	15.01.2021	IACR TCHES	Accepted	Yes	IMEC-NL	Academic/International	NA	NA
2	Journal Paper	31.07.2020	IEEE TCAS-II	Published	No	ERARGE (ISICAS)	Academic/International	111	NA
3	Conference Paper	30.09.2020	Proceedings of IEEE ICHMS	Published	No	ERARGE	Academic/International	NA	NA
4	Conference Paper	31.10.2019	Proceedings of IEEE MWSCAS	Published	No	ERARGE	Academic/International	NA	NA
5	Journal Paper	09.08.2019	IEEE TCAS-II	Published	No	ERARGE	Academic/International	111	NA
6	Conference Paper	09.01.2020	Proceedings of IEEE APCCAS	Published	No	ERARGE	Academic/International	NA	25
7	Conference Paper	24.02.2020	Proceedings of AsianHOST	Published	No	ERARGE	Academic/International	NA	6
8	Conference Paper	28.11.2019	Proceedings of IEEE SMC	Published	No	ERARGE	Academic/International	NA	120
9	Review	29.01.2020	Computers & Security, Volume 92, 2020	Published	No	JR	Scientific community	3.579	3.756
10	Article	NA	NA	Under Revision	NA	JR, UREAD	Scientific community	NA	NA
11	Article	NA	NA	Under Revision	NA	JR, FHG, UREAD	Scientific community	NA	NA

10.2 Dissemination relevance of Critical-Chains Scientific and Technical Publication

Among the dissemination actions previously presented, the following Table 10-2: Relevance of Critical-Chains publications provides for each publication the relevance as number of citations, downloads/views as well as feedback/results. The goal is to assess with these metrics the positioning of Critical-Chains in the research community. The positioning in terms of the overall number of citations needs to be improved in Period II. Papers #5 and #9 have been cited 7 times whereas all other publications have not yet been cited. The overall number of downloads/ views with well above 1,000 could be an indication for a possible increase in future citations of papers.

Table 10-2: Relevance of Critical-Chains publications

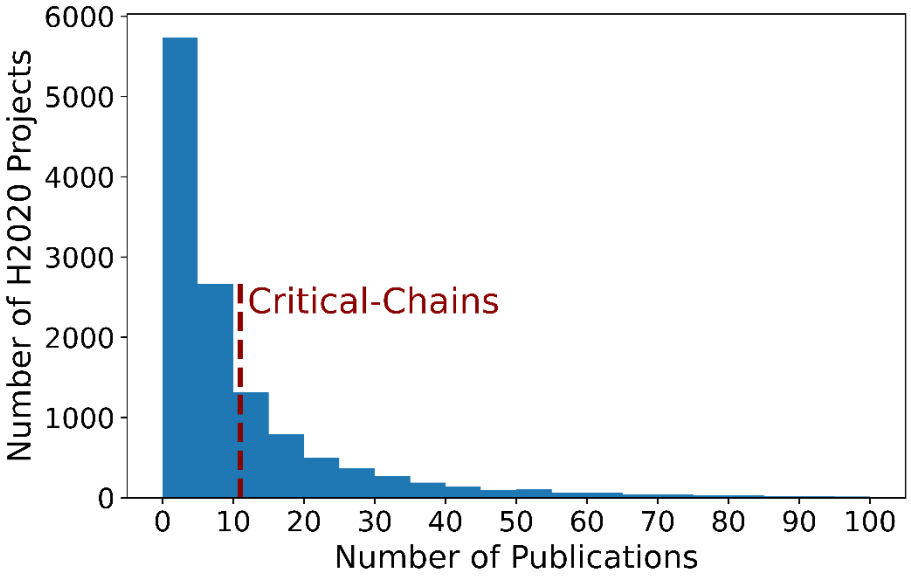
ID	Number of Citations	Number of Downloads / Views	Journal Impact Factor	Feedback / Results	Current Impact factor	Historical Impact Factor or SNIP
1	0	0	NA	NA	NA	NA
2	0	253	2.814	The conference paper accepted to be published in the IEEE Transactions on Circuits and Systems. 15 speakers showed special interest and participated in the technical discussions during or after the session.	NA	NA
3	0	35	NA	12 speakers showed special interest and participated in the technical discussions during or after the session.	NA	NA
4	0	54	NA	14 speakers showed special interest and participated in the technical discussions during or after the session.	NA	NA
5	7	377	2.814	The conference paper accepted to be published in the IEEE Transactions on Circuits and Systems. 17 speakers showed special interest and participated in the technical discussions during or after the session.	NA	NA
6	0	58	NA	13 speakers showed special interest and participated in the technical discussions during or after the session.	NA	25
7	0	76	NA	19 speakers showed special interest and participated in the technical discussions during or after the session.	NA	6
8	0	241	NA	21 speakers showed special interest and participated in the technical discussions during or after the session.	NA	120
9	7	59	3.579	NA	3.579	3.756
10	There is no available statistical information since this paper is still under revision.					
11	There is no available statistical information since this paper is still under revision.					

10.3 Assessment of Critical-Chains Scientific and Technical Publication against benchmark

As a benchmark against which the number of publications of Critical-Chains is evaluated, the publications of all EU research projects under Horizon 2020 are used which can be found under the following URL: https://data.europa.eu/euodp/en/data/dataset/cordisH2020projects.

The list comprises of over 10,000 projects with over 160,000 publications. Figure 4: Distribution of the number of H2020 projects and the number of publications. It can be seen that most projects published between 0 and

10 publications. Critical-Chains with 11 publications is therefore in the upper range of most projects. shows the distribution of the number of publications for each project as a histogram. Most of the projects published between 0 and 10 publications and the number of projects drops roughly exponentially with the number of publications. Therefore, Critical-Chains is with 11 submitted publications in a good position with the goal to further increase the number of publications in Period II.



igure 4: Distribution of the number of H2020 projects and the number of publications. It can be seen that most projects published between 0 and 10 publications. Critical-Chains with 11 publications is therefore in the upper range of most projects.

To further range Critical-Chains within the H2020 landscape some statistical key indicators of the list of scientific publications are listed in Table 10-3.

Table 10-3: Statistical key indicators of scientific publications by H2020 projects

Mean value	Median	Percentile of projects with less than 11 publications
13.77	6	66.9%

The mean value of almost 14 publications per project is rather high due to the fact that some projects have an extensively large numbers of publications. The median of 6 publications means that 50 % of the projects have less than 6 publications and the other 50 % of the projects have more than 6 publications. Therefore, Critical-Chains is with 11 publications in the upper half of all projects. The percentile of projects with less than 11 publications is roughly 67%, which means that two thirds of all H2020 projects have less than 11 publications. All publications of Critical-Chains are targeted at an international audience to maximise visibility and impact.

11 Project-to-Policy Engagement

The Project-to-Policy Engagement has been implemented through the following Critical-Chains Consortium contributions by way of participation in workshops or surveys initiated by the EC as well as inclusion of sessions and themes for workshop presentations and panel sessions (co)organised by Critical-Chains on specialist topics that directly provided project-to-policy insights from a number of projects focused on financial sector regulatory and standardisation related issues.

The workshop events have included critical-chains partners and partners from other related projects, with relevant cross-disciplinary or specialist expertise, providing presentations on a range of standardisation, compliance n ad certification issues relating to regulatory mechanisms, “regulatory tensions and pain-points” (e.g. GDPPR vs PSD2), regulatory deficits (e.g. in relation to harmonisation, emerging mobile money business models and crypto-currencies, authentication, digital signing, blockchain smart contacts etc;

11.1 Dissemination tracking of Critical-Chains project-to-policy engagement

A list of the dissemination activities is provided below with an outline of the focus of the project-to-policy related contributions from each such activity.

1. **Responsible Research & Innovation 11-12 July 2019 University of Reading**

This workshop also discussed the need for regulatory self-audit to ensure all systems, including online services and decision support software and processes adhere to and maintain standards of safety security and integrity to avoid exposing the citizens to risks of harm and hurt. This includes protection against inequitable treatment, bias and integrity breaches through lack of protections against adversarial attacks particularly in decision support systems.

2. **Contributions to policy informing insights re the Security Projects Innovation Focus** Taxonomy questionnaire. This was to support mapping of cybersecurity expertise of existing centres to enable the Impact Assessment of the Proposed Regulation to set up the EC Competence Centres in Cyber Security, critical-chains responded to the invitation to participate in the EU survey 'Cybersecurity-relevant projects classified based on "A Proposal for a European Cybersecurity Taxonomy" (JRC - 2019)" Dec 2019.

3. **Ethics of Blockchain 17th December 2019, University of Reading**

Digital Signing authentication EIDAS

4. **Project-2-Policy Kick-off Workshop 31st January 2020, Brussels**

The Critical-Chains Coordinator Professor Atta Badii represented the Critical-Chains Consortium for the Policy Workshop held at the REA, Brussels and was able to highlight the project objectives and the need to examine the regulatory and certification framework responsive to the evolutionary trends in Fintech and the emergent forms of payment systems and intermediation

.

5. **FINTECH, AI Financial Automation and Market Risk** 19th May 2020

6. **European Cluster for Securing Critical Infrastructure (ECSCI)** 24th-25th June 2020,

7. **The Critical-Chains Consortium Project-to-Policy Responses to EC Policy Unit Questionnaire** relating to Regulatory, Standardisation, Compliance and Certification issues, 21-September 2020

8. **Cybersecurity in Financial Sector,** 30th October 2020

9. **Emerging Cybersecurity Standards for the Financial Sector in Europe** 27th November 2020,

10. **Financial Sector infrastructure Cyber-physical Security and Regulatory Standard**s- 14th-Decembdr 2020

11.2 Dissemination relevance of Critical-Chains project-to-policy engagement

A qualitative assessment of how effective the project-to-policy contributions have been can be inferred by the observation of insights exchanged during the events. The tables below provide for the relevant events specific characterisation for tracking and assessment of the scale of the Critical-Chains Project -y=to-policy efforts for the clustering workshop (co-organised) and/or contributed to. All events can be assumed as held as webinars unless a physical location is specified

Workshop 1 -Metrics and Description

Title: Responsible Research & Innovation **Date:** 11-12 /7/ 2019		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	1	Privacy by design and by default – GDPR Compliance self-audit requirements

Workshop 2 -Metrics and Description

Title: Ethics of Blockchain **Date:** 17/12/2019, University of Reading		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	1	Regulations relating to smart contracts secure and crypto-currencies

Workshop 3 - Metrics and Description

Title: Project-2-Policy Kick-off Workshop **Date:** 31/01/2020 Brussels		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	10-12	Regulatory, standardisation and certification issues relating to the financial services sector

Workshop 4 -Metrics and Description

Title: FINTECH, AI Financial Automation and Market Risk **Date:** 19/05/2020		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	4	Regulatory Mechanisms, Standardisation re Crypto-currencies, Authentication and Accountability Models, eIDAS

Workshop 5 -Metrics and Description

Title: European Cluster for Securing Critical Infrastructure (ECSCI) **Date** 24-25/6/2020		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions	2	Regulatory Mechanisms and Standardisation

Workshop 6 -Metrics and Description

Title: Cybersecurity in Financial Sector **Date:** 30/10/2020		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	3	Regulatory Tensions, Compliance Monitoring, Standardisation

Workshop 7 -Metrics and Description

Title: Emerging Cybersecurity Standards for the Financial Sector in Europe Date: 27/1/2020		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	3	Regulatory Mechanisms, Compliance Monitoring, Enforcement Authorities

Workshop 8 -Metrics and Description

Title: Financial Sector infrastructure Cyber-physical Security and Regulatory Standards- Date: 14/12/2020		
Particulars	**Metrics**	**Description**
Number of Project-to-Policy contributions made	4	Regulatory Harmonisation, Cybersecurity Impact of Disruptive Technologies in the Financial Sector, Security-Privacy Protection Challenges, Regulatory tensions, and Compliance Issues

12 Conclusions and next steps

This deliverable, D7.4, has set out the ecology of the project touchpoints as an integrated mutually re-enforcing system-of-systems and a framework within which the results of the various dissemination efforts have been characterised with benchmarking metrics to map the tracking and assessment of various dissemination actions over the progressive phases of Period I implementation; including:

- Establishing the Critical-Chains Logo and Branding
- Dissemination activities and awareness raising through the website and social media
- (Co)organising and contributing to clustering workshop events
- General Awareness-Raising within the Financial Sector Stakeholders
- Stakeholder Group Building
- Scientific and Technical Publications
- Project-to-Policy contributions

Despite the restrictions re physical meetings, the Consortium has managed to contribute to community building and leading across over 15 related projects and two networks-of-networks (Cyberwatching, LSEC) each of which act as a hub for over 20 relevant projects and stakeholder groups. Accordingly Critical-Chains has co-organised and contributed to over 10 clustering workshops with plans to continue to build on our collaborative efforts to hold further events as a means of engaging our stakeholders by showcasing the results of our innovation as well as to share insight with other consortia and stakeholders on scientific and technical innovation challenges and Project-to-Policy issues. The total number of direct contacts with the Critical-Chains project during Period I via logo views, social media views/likes, or workshop attendance is approximately 4500.

The Consortium efforts in accomplishing its dissemination objectives across the above range of available touchpoints has led to the following priorities set to inform the dissemination agenda for Period II:

i. Continue to build on the active clustering workshop agenda already set.

ii. Increase efforts in tracking the number of views and likes for Critical-Chains Logo and Branding messaging actions.

iii. Attempt to increase joint publications within the consortium and possibly in collaboration with the most closely related projects within the cluster.

iv. Increase efforts in production of demo videos show-casing the performance of the various Critical-Chains X-as-a-Service solution sets in prototypical operational workflow contexts.

v. Use the show-casing demos to focus on engagement with use-case specific stakeholder sub-groups to motivate interest and arrive at insights re impact mobilisation to inform exploitation planning.

In conclusion, our overall dissemination performance has paved the way for widening and deepening the community awareness of our vision and our rigour in pursuit of its realisation. Above all our commitment to socially responsible sustainably successful transformative innovation, Critical-Chains consortium at all has contributed to support the enhanced security of financial transaction systems and services, which is our primary stakeholder arena.

13 Appendices

13.1 Appendix A: Project-to-Policy Contribution

The Critical-Chains Consortium Project-to-Policy Responses to EC Policy Unit Questionnaire relating to Regulatory, Standardisation, Compliance and Certification issues.

Date: 21-09-20

Q1 What *do you consider as the main shortcomings of the cybersecurity legislation and policy that your project has encountered? -Could you propose any workable solutions how these could be tackled?*

Regulatory mechanisms need to support threat-driven, risk-based and operational-context-aware security and privacy-by-design as well as compliance assurance audit including of IT products and cloud services.

The rapid pace of innovations relating to cryptocurrencies and mobile money has opened up new business models some of which have operated in a regulatory void whilst new spaces have emerged in the financial transaction's domain exposed to various types of irregularity and fraudulent conduct. In particular there is no regulatory regime for cryptocurrencies at European level. Some countries of the EU (e.g. Germany) have already put in place legislation relating to the new currencies; thus, there is a vacuum to be addressed by European level directives that will inevitably have to pass through a phase of harmonisation and homogenisation of the regulations already present. A lack of legal certainty is often cited as the main barrier to developing a sound crypto-asset market in the EU -the goal proclaimed by the recent declarations of Valdis Dombrovskis (European Union's Executive Vice President of the European Commission for An Economy that Works for People). (https://www.coindesk.com/eu-bloc-wide-regulatory-regime-crypto-economic-chief).

Personal data and card holder data need to be protected in compliance with the General Data Protection Regulation (GDPR) and the Payment Card Industry Security Standards (PCI – DSS). The application of these regulations should be certified by a Qualified Security Assessor (QSA) to verify correct implementation and adherence to security measures and processes required by each regulation and cover all minimum issues related to applicable directives and standards. Additional applicable local laws also need to be reviewed.

In the wider private sector who are the source of much of the financial transactions and as such constitute one side of the stakeholders involved, security policies range from non-existent to not-so-easily align-able to support business-to-business collaboration - lacking a common security requirements baseline.

This is not helped by the universally shared observation that some cyber privacy-security legislation is not easily translatable to operational implementation actions. This is due to:

- lack of a commonly accepted cost-effective solution requirement (which anyhow would have to be prioritised in each case based on the criticality of any risks to core business operations)
- lack of specific technology standard or prescribed solution for specific sectoral business context
- Lack of clear definitions e.g. the PSD2 provides a guideline as to how to create secure authentication methods, but it lacks a clear definition of what "independent" authentication factors means.

Some companies are well prepared for GDPR compliance and others are more focused on protecting confidentiality and integrity during the exchange of financial data.

Without specific schemas (or guidelines, at least) it is difficult to set-up a properly balanced security audit plan (when needed). The audit level of detail and the extent of evidence must be applicable to business operational context.

Cybersecurity attitudes are not homogeneous across different personnel roles. Usually people are not fully aware of security risks, threats and incidents and may be inadequately trained to identify and respond to them.

A security strategy should integrate all the security requirements, identify relevant context-specific security objectives, and orchestrate all the activities that operate the established security measures responsive to the regulations, and standards.

It is possible to imagine that the advent of transformative technologies may open up new security protection capabilities that may obviate the need for some regulatory mechanisms whilst, as a side-effect, also creating new security loopholes requiring new regulatory mechanisms. In this sense, and particularly given the rapid pace of innovation of systems and business models in the financial sector, the regulatory innovation has to remain closely responsive to the emerging patterns of new security needs and new malicious use-cases to ensure a rapidly learning regulatory eco-system keeping up with the disruptive innovation and resulting business models and putting in place the required regulatory mechanisms to ensure the trustful integration of new technology whilst preventing the new evolving patterns of fraud.

For example, the advantages of DLT and blockchain include greater user control, reduced transaction time and cost, immutability, enhanced efficiency and automation, transparent financial audits, tamper-proof logging, and overall fewer chances of errors or fraud. The general security measures in the financial domain have significant problems because of the trade-off between security and efficiency, privacy and efficiency and trustworthiness. The online transactions, especially at worldwide level are cumbersome which may cause serious latencies in transactions and lack of trust between transactors. Blockchain infrastructure can provide effectively support some of the requirements but as highlighted in the Kaspersky report on DLT cybersecurity[1], the risks associated with DLT and blockchain still remain. As new attack surfaces emerge so do new attacks, finding new vulnerabilities to exploit. However, traditional blockchain implementations do not prioritise time-critical transactions or data while they are waiting to be added to the blockchain. Cumbersome blockchain infrastructures can fail to achieve coherence within an acceptable latency. This may cause serious problems in various sectors such as Industry 4.0, smart health, or transportation where the integrity of processes may be directly or indirect affected by related financial flows. For instance, a typical smart transportation application requires toll collection or the use of city cards where millions of people pay for mobility cards and use them in mobility systems. Hence, there is a strong need to define and elaborate sector-specific security, privacy and even safety measures that should be linked to financial operations covering payment systems, insurance, online banking, and promotional systems.

This points to a dual strategy of parallel innovation in new security paradigms and technological solutions on the one hand, and, a fast-learning regulatory innovation framework on the other hand. For example, supporting digital signing solutions that are scalable and make digital infrastructure more transparent.

The major security shortcomings in the Financial Industry may be listed as personal data hijacking, for example theft, usage and/or sale (e.g. on the dark net) of victims' credit cards detail via bank or merchant fraud, and illicit money trafficking. The fully decentralised nature of blockchain may cause vulnerabilities and

[1] https://www.kaspersky.com/enterprise-security/dlt-cybersecurity

weaknesses that can be exploited by fraudsters and criminals. This is not only applicable to financial crimes but also other crimes, such as human trafficking, communication and illegal online material sharing over private chains. For instance, some crime organisations share videos and photos of children for sexual exploitation. The triangular model that is proposed in the Critical-Chains project adds authorities (e.g. banks, governmental organisations) in the loop as an approver, and regulatory needs learning and feedback node, for any transaction between two (or more) transactors (e.g. sender and receiver). This model consisting of transactor 1, transactor 2 and the authority can be standardised for any transactions over any smart application to offer both immutability and accountability. In doing so the distributed ledgers and smart contracts may include the trusted parties (authorities) in the chain which makes for semi-decentralised approval available 24/7 at a global scale

Q2- ***To what extent do you think the general security measures baselines (based for example on ISO27001) are effective at sectoral level and would more sector-specific measures be needed for the financial sector?***
General security measures baselines, for example, ISO27001, are in general able to answer security challenges in traditional financial institutions, with a constraint that all updates to a standard, such as ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines), should be implemented.

The ISO 27001/27002 security measures can identify high level objectives that need to be achieved by specific security measures. PCI and GDPR identify the processes required to determine what specific security measures and processes are most suitable for a specific architecture based on the specific risks and vulnerabilities related to the systems, communications and applications deployed as part of a specific solution.

These standards and other frameworks e.g. COBIT, NIST CSF etc. are multi-purpose schemes applicable in different contexts, but they do not pose specific security requirements that define common security measures for a specific sector (e.g. they do not define that an IT system used in the Financial Sector shall be designed, developed, tested, installed, configured, etc. in a particular way and the system shall meet specific security requirements, the same for the policies, procedures etc. that are part of a management system). Thus, more specific/sectorial security requirements should be identified for network segregation, access control, accounting, logging, integrity checking and so on.

The general security measures baselines such as ISO27001 are thus not very effective when applied to modern applications in the Financial Sector that have specific security requirements and often involve the usage of mobile applications. In these cases, the generic security measure baselines must be integrated and expanded with security controls for other frameworks. In this way significant progress has been made in terms of responding to cyber threats and protecting personal data through specific tools such as the NIS regulation and the PSD2 regulation.

- These regulations have increased the level of cyber security but will require, continuous technological refinement to remain constantly updated responsive to the continuing mutation of cyber threats.
- Sector-specific measures are needed, but it is difficult to publish them as business interests prevail. The financial sector must prove that they can be transparent and have earned the trust needed. Internal auditing and compliance systems have shown monitoring failures, for example, in money laundering cases.

- Specific requirements should be identified also for the risk management process, periodic vulnerability assessment, personnel drills (both for IT and non-IT personnel). Standardised security certification of IT products should be more widely implemented.
- Special attention, and a potential standard review, should be considered for cloud based FinTech services, because they bring in new challenges and threats.
- General signing requirements enable analysis afterwards at a detailed level, of any digital event.

Q3- How do you assess the role of digital service providers and in particular cloud service providers within the financial sector as compared to other critical sectors?

The financial sector is one of the most active sectors investing in digital services and cloud infrastructure. With the recent developments in online systems, for example over the cloud, banking and the insurance sectors have evolved into the digital age. Recent trends such as mobile banking, e-banking, online stores and purchasing over the Internet, e-insurance, e-government, e-payment, e-tax, etc. have shown that the level of technology acceptance in the Financial Sector is high. The service or cloud providers can support the Fintech processes by undertaking some of the most common issues of infrastructure with the highest level of technology at accessible prices.

Accordingly, the rising trend for financial service providers is to move their services to the cloud. Compared to other critical sectors, the Financial Sector is even more exposed to cyber-attacks as its business is totally exposed to the cloud network. In this sense, the sector is moving in the direction of a shared information security model. This move from physical to cloud could make companies increasingly dependent on service providers.

Cloud service providers are crucial for the Financial Sector to establish and maintain worldwide and 24/7 availability of financial services as well as for providing capabilities for crypto services. As the global economy depends highly on a steady money flow, cloud service providers must ensure a safe and easy access to their services for individuals as well as for companies.

However, digital service providers must earn the trust of other Financial Sector partners and customers. Different measures have been used. Payment system providers have been successful in this so far.

One approach to assessing the role of digital service providers and in particular cloud service providers is to add the security measures and processes required as part of the SLA requirements and perform audits to assess the correct management of the information related to the service provided by the third party.

Since the Financial Sector is more sensitive to privacy issues compared to other sectors, digital service providers, and especially cloud service providers, need to focus more on compliance with privacy protection related regulation. Critical infrastructure sectors (energy, water distribution,), for example, should be more focused on safety and availability issues, to protect users and service delivery.

Q4-***Do you observe a specific need for additional or revised policy or regulation in the Financial Sector, which renders it different from other critical sectors?***

One has to wonder whether indeed it was a lack of regulations or poor monitoring that have led to the various reported failures in timely detection and the tracking of money transactions in cases such as the apparent disappearance of over 2 billion Euro from the Wirecard balance sheet.

It may be that there indeed exist sufficient policies and regulatory mechanisms but that monitoring, and enforcement would need to be strengthened. The authorities would need to maintain the focus on existing

policies through constant monitoring of the evolution of cyber security scenarios with a view to periodically updating existing policies in order to achieve the goal of continuous improvement that enables an effective and efficient response to the continuous mutations of the cyber threat scenario (e.g. increasing the use of artificial intelligence for cybercrime).

However given that E-banking is a reality and will be the main banking channel in the near future it can be argued that there is a need for regulation that supports litigation against the bank, using legally admissible evidence based on forensic data intelligence that proves the nature of the digital activities.

Even although the financial sector data exchange does not involve the safety or the health of individuals, it is still the case that specific security and privacy protection requirements and controls should be defined prior, during and after a transaction or data exchange, focusing on security measures which involve data confidentiality, authenticity and integrity both for data in transit and data at rest.

There is a specific need to revise the policies about using blockchain not only in the Financial Sector but also in other sectors as the financial sector provides a cross-sectoral underpinning that influences all other domains. This is not only related to the use of cryptocurrencies in financial transactions, but also regulations related to smart contracting and distributed ledgers, and the participation of a centralised authority or authorities in such financial operations. Such a regulatory revision should also tackle the coordination and collaboration of many centralised authorities; for instance, two different banks or a bank-insurance company.

An instance of this is the type of solution stack that support a critical sector infrastructure (e.g. transportation) that manages cardholder data which needs to be verified and secured in transit and at rest to protect the confidentiality of the information managed without compromising the availability of the service. Such pipelines should be assessed to determine the level of maturity/complexity required over the security measures that should be implemented to protect the critical, sensitive, or personal data managed by the solutions through the pipeline.

13.2 Appendix B: Links to Critical-Chains Presentation PowerPoints

For the Project-to-Policy Workshop held at the REA, Brussels 31-01-2021

https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/Unorganized/Critical-Chains-833326-Policy-Workshop-15PPset-Atta-Badii-22-01-2020.pdf

13.3 Appendix C: Abstracts of Scientific & Technical Papers and Links to full text

Paper#1 by IMEC-NL

Relay attacks pose a serious security threat to wireless systems, such as contactless payment systems, keyless entry systems, or smart access control systems. Distance bounding protocols, which allow an entity to not only authenticate another entity but also determine whether it is physically close by, effectively mitigate relay attacks. However, secure implementation of distance bounding protocols, especially of the time critical challenge-response phase, has been a challenging task.

In this paper, we design and implement a secure and accurate distance bounding protocol based on Narrow-Band signals, such as Bluetooth Low Energy (BLE), to particularly mitigate relay attacks. Narrow-Band ranging, specifically, phase-based ranging, enables accurate distance measurement, but it is vulnerable to phase rollover attacks. In our solution, we mitigate phase rollover attacks by also measuring Time-of-Flight (ToF) to detect the delay introduced by such attacks. Therefore, our protocol effectively combines the best of both worlds: phase-based ranging for accuracy and Time-of-Flight (ToF) measurement for security. To demonstrate the feasibility and practicality of our solution, we prototype it on NXP KW36 BLE chips and

evaluate its performance and relay attack resistance. The obtained precision and accuracy of the presented ranging solution are 2.5cm and 30cm, respectively, in wireless measurements.

Link to full text: Not published yet.

Paper #2 by ERARGE
This brief presents a reconfigurable Random Number Generator (RNG) based on transient effect of ring oscillators. Users can select a method based on the irregular sampling of a regular waveform or on the regular sampling of an irregular waveform to obtain a random bit sequence to be used in different applications, such as lightweight cryptography or high-security communication. The entropy is acquired by exploiting Transient Effect Ring Oscillators (TEROs). The proposed fully-digital RNG structure is firstly implemented on a Zynq-7000 FPGA (Field Programmable Gate Array) without any post-processing method such as the Von Neumann. In addition to the RNG structure, an on-the-line test module based on FIPS 140-2 is also implemented to check the randomness of the produced data statistically in real time. Users can change the statistical test parameters according to their desired security levels. Finally, an ASIC (Application Specific Integrated Circuits) implementation of the proposed RNG is done following the Cadence digital design flow for the TSMC 180 nm CMOS process. The implemented ASIC design occupies an area of 0.85 mm x 0.85 mm and the estimated power required is 11.827 mW.

Link to full text: https://ieeexplore.ieee.org/document/9153808

Paper #3 by ERARGE
Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This letter presents a Diamond Accountability Model (DAM) where a public or private authority is included in the blockchain transactions providing non-repudiation of digital transactions, holistic security and effective governance. The proposed technique aims to present a decentralized solution for multi-agent applications where many partnering organizations have to collaborate without suffering from the security, accountability, maintenance, scalability, and integrity problems over distributed cyber-physical systems (CPS). The proposed scheme positions authorities also in the chain that enables additional accountability and trust. The scheme proposes a verification mechanism where the authorized organizations are also included in the verification of transactions over the blockchain. In order to elucidate, a conceptual use case is presented where at least two partnering organizations collaborate with each other within a decentralized but also authorized blockchain-enabled scheme.

Link to full text: https://ieeexplore.ieee.org/document/9209518

Paper #4 by ERARGE
A novel cross-coupled bipolar transistor-based non-autonomous chaotic oscillator is proposed. The derivation methodology of this novel chaotic oscillator is based on integrating two of existing chaotic oscillators symmetrically and employing a differential-pair stage. Simulation and experimental results, verifying the feasibility and the correct operation of the circuit are also given.

Link to full text: https://ieeexplore.ieee.org/document/8884899

Paper #5 by ERARGE
This brief presents a random number generator (RNG) based on irregular sampling of regular waveform method where the irregular signal is obtained by combining Fibonacci-Galois ring oscillators with an XOR gate. The RNG is implemented on a FPGA (field-programmable gate array). The regular waveform generated by the digital clock manager of the FPGA, is sampled at times corresponding to certain number of rising edges of the irregular signal, and the resulting bit stream is subjected to statistical tests of randomness. It is

demonstrated that the resulting bit sequence from the proposed RNG satisfies NIST 800-22 test suit and Rabbit and SmallCrush batteries from TestU01 library without any need for post-processing such as Von Neumann or XOR. A comparison between the methods regular sampling of irregular waveform and irregular sampling of regular waveform is given in terms of robustness against external interference. The impact of selection of Fibonacci-Galois polynomials is discussed. Using digital design flow for TSMC 65nm process, a basic implementation of the proposed RNG is given having 1115 gates and 4.811 mW estimated power.

Link to full text: https://ieeexplore.ieee.org/document/8789641

Paper #6 by ERARGE

This paper presents a comparative study on continuous-time chaos-based random number generation methods regarding their robustness against changes in chaos controlling parameters and external interference. Chaotic systems suggest enabling high throughput random data without need for post processing and with less complex hardware. However, due to effects of aging or fabrication process variations, the chaos controlling parameters of the random number generator may change. Furthermore, external interference can be applied on the chaotic oscillator to manipulate its output. Therefore, in a chaotic RNG, the bit generation method should be immune to parameter variation and external interference. In this study, two widely used methods for random number generation have been compared: 1) Regular sampling of chaotic waveform (RSCW), and 2) Chaotic sampling of regular waveform (CSRW). A double-scroll chaotic system is chosen as the chaotic oscillator and it is numerically simulated in normalized time domain to generate random bit sequences using both methods. Applying the concepts of autocorrelation and approximate entropy to the output bitstreams, the robustness of the two-bit generation methods against parameter variation and external interference have been compared. It is demonstrated that chaotic sampling of regular waveform method provides more robustness against parameter changes and external interference compared to regular sampling of chaotic waveform method.

Link to full text: https://ieeexplore.ieee.org/document/8953106

Paper #7 by ERARGE

A novel attack system is proposed to reveal the security weaknesses of a microcomputer-based random number generator (RNG). Convergence of the attack system is proved using auto-synchronization. Secret parameters of the microcomputer-based RNG are revealed where the available information are the structure of the RNG and a scalar time series observed from the chaotic system used as the seed of the RNG. Simulation results verifying the feasibility of the attack system are given such that, next bit can be predicted while the same output sequence of the RNG can be generated.

Link to full text: https://ieeexplore.ieee.org/document/9006666

Paper #8 by ERARGE

With the recent advancements in blockchain technology, it has become obvious that this technology is not just for crypto-currencies but instead can be used as a decentralized tool for better accountability. Blockchain has the capacity to transform the industries disruptively as it presents new features like smart contracts, tokenization of content, eliminating counterfeit products, supply chain improvement, digital twins, and end-to-end security. This paper presents a blockchain-based model for distributed and collaborative digital twin environments which is becoming indispensable in new “Any 4.0” era. The proposed model includes a public or private authority in the digital twin ecosystem providing non-repudiation of blockchain transactions, holistic security and privacy preservation. The proposed technique is based on the “X-by-design” and “X-as-a-service” principles which can be discussed as a novel model for better security, accountability and integrity in decentralized mechanisms. In order to elucidate, two case studies are described where the digital twin operations, stakeholders' activities and regarding transactions are stored on a blockchain.

Link to full text: https://ieeexplore.ieee.org/document/8914304

Paper #9 by JR

Automated detection methods for targeted cyber-attacks are getting more and more prominent. In order to test these methods properly, it is crucial to have a suitable dataset. This paper provides a review on datasets and their creation for use in APT detection in literature. A special focus is placed on feature engineering, including construction, selection and dimensionality reduction. Two use cases based on the underlying infrastructure are distinguished, large enterprise networks and Cyber Physical System, additionally including cloud computing systems, financial technology networks and Internet of Things networks. These datasets are usually based on an attack model. A description of different stages including approaches and goals of such attacks are given. The major achievement is the description and analysis of existing feature extraction methodologies and detailed overview of datasets used in APT detection related literature. This shows that the large enterprise network use case, has incorporated a much more frequent use of datasets with quite short periods of time. In the case of Cyber Physical System, a realistic dataset is publicly available.

Link to full text: https://doi.org/10.1016/j.cose.2020.101734

Paper #10 by JR, UREAD

Nowadays, virtually all products and services offered by financial institutions are backed by technology. While the frontend banking services seem to be simple, the core-banking backend systems and architecture are complex and often based on legacy technologies. Customer-facing applications and services are evolving rapidly, yet they have data dependencies on core banking systems running on ancient technology standards. While those legacy systems are preferred for their stability, reliability, availability, and security properties, in adapting the frontends and services many security and privacy issues can occur. Clearly, these issues are arising as those systems have been designed decades ago, without considering the enormous amounts of data that they are required to handle and also considering different threat scenarios. Moreover, the trend towards using new technologies such as Distributed Ledger Technologies (DLT) has also emerged in the financial sector. As the nodes in DLT systems are decentralized, additional security threats come to light. The focus of this work is the security of financial technologies in the FinTech domain. We provide relevant categorization and taxonomies for a better understanding of the main cyber-attack types, and suitable countermeasures. Our findings are supported by using security-by-design principles for some selected critical financial use-cases, and include a detailed discussion of the resulting threats, attack vectors and security recommendations.

Link to full text: https://eprint.iacr.org/2020/1440

Paper #11 by JR, FHG, UREAD

Financial technology, or Fintech, represents an emerging industry on the global market. With online transactions on the rise, the use of IT for automation of financial services is of increasing importance. Fintech enables institutions to deliver services to customers worldwide on a 24/7 basis. Its services are often easy to access and enable customers to perform transactions in real-time. In fact, advantages like these make Fintech increasingly popular among clients. However, since Fintech transactions are made up of information, ensuring security becomes a critical issue. Vulnerabilities in such systems leave them exposed to fraudulent acts, which cause severe damage to clients and providers alike. For this reason, techniques from the area of Machine Learning (ML) are applied to identify anomalies in Fintech applications. They target suspicious activity in financial datasets and generate models in order to anticipate future frauds. We contribute to this important issue and provide an evaluation on anomaly detection methods for this matter. The experiments are conducted on several fraudulent datasets from real-world and synthetic databases, respectively. The obtained results confirm that ML methods contribute to fraud detection with varying success. Therefore, we discuss the effectiveness of the individual methods with regard to the detection rate. In addition, we provide

an analysis on the influence of selected features on their performance. Finally, we discuss the impact of the observed results for the security of Fintech applications in the future.

Link to full text: NA

****