H2020-DS-2015-1-Project 700581

Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures

D8.10 - Exploitation Management and business model interim report

General information

Dissemination level	Public
State	Final
Work package	WP8 Project dissemination and commercial strategy
Task	Task 8.3
Delivery date	31/10/2017
Version	1.0

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700581.

Editors

Name	Organisation
M. Aubigny	ITRUST

Authors

Name	Organisation
Maria -Angeles Grado-Caffaro	SAPIENZA SL
M. Aubigny	ITRUST

Reviewer

Name	Organisation	Date
Tiago Cruz	UC	30/10/2017

Executive summary

It is well known that the exploitation of results of the research activity is increasingly gaining both attention and weight in the technology/industry and scientific scenario. For the meaning of exploitation, it will be used the one delivered by the European IPR Help Desk, fact sheet entitled "*The Plan for Exploitation and Dissemination of Results in Horizon 2020*" where it is stated that exploitation "*means the use of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities*".

The present document should be considered as an updated version of the D8.4. It describes the main guidelines defined by the project Consortium regarding the exploitation of the results and describe the preliminary path of each partner to define a reliable business plan. At this stage of the project, a real business plan could not be designed in reliable manner as most tools defined in the project requirements are still in development and their potential marketable value cannot be defined.

Table of Contents

1 Introduction

1.1 Motivation and context

Applied research is one of the most crucial factors in strengthening industrial and scientific competitiveness, enabling the exploitation of innovative technologies and state-of-the-art advances for the common benefit of all the involved partners. By promoting the creation of partnerships between academic/research institutions and industrial organizations, it harnesses their collaborative potential, mobilizing the expertise of each domain towards the creation of innovative solutions.

For the meaning of exploitation it will be used the one delivered by the European IPR Help Desk, fact sheet entitled “The Plan for Exploitation and Dissemination of Results in Horizon 2020” where it is stated that exploitation “means the use of results in further research activities other than those covered by the action concerned, or in developing, creating and marketing a product or process, or in creating and providing a service, or in standardisation activities”.

In this document it is explained which actions are planned to undertake in terms of exploit the results/outcomes of ATENA project, that is, said it broadly, the knowledge and understanding produced by ATENA. These actions refer to a joint effort during the lifetime of the project, meaning the analysis of the exploitation value of the outcomes of the project, including the intermediate steps and also once the project will be finalized.

1.2 Objectives and scope

The objective of the present document is to present an updated version of the D8.4 [8] regarding the context and the overall plan for the exploitation of the results of ATENA project at consortium level.

1.3 Document Structure

This document is made of several chapters, which respectively deal with:

- Chapter 1 is the present introduction.
- Chapter 2 presents a series of general considerations about exploitation and business plan
- Chapter 3 is devoted to explaining key aspects on ATENA applications potential
- Chapter 4 relates to exploitation environment of the project in a go-to-market strategy
- Chapter 5 describes the partners strategy in terms of exploitation
- Chapter 6 contains bibliographic references

1.4 Glossary

A glossary of the main terms adopted in the project is available in deliverable D2.1 [14]. For the sake of maintenance, manageability and completeness, the reader is invited to refer to the project-level separate glossary document (i.e., D2.0 ATENA glossary) that we are also placing on ATENA web-site (https://www.atena-h2020.eu/) for public use.

1.5 Acronyms and symbols

Acronym or symbols	Explanation
CORDIS	COmmunity Research & Development Information Service
DHS	Department of Homeland Security
ECAS	European Action Citizen Services
EECSP	Energy Expert Cyber Security Platform
ENISA	European Union Agency for Network and Information
ENTSOE	European Network of Transmission System Operators for Electricity
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
IADS	Intrusion and Anomaly Detection System
IACS	Industrial, Automation and Control Systems
IPR	Intellectual property rights
IT	Information technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards & Technology
OT	Operational technology
OTA	Other Transaction Agreement
QoS	Quality of Service
RAO	Resource-Action-Operation
SCADA	Supervisory Control And Data Acquisition
SME	Small Medium Enterprise
SWOT	Strengths, Weaknesses, Opportunities and Threats
WP	Work Package

2 Exploitation management and business model development

2.1 General considerations

Since the start of the project, several actions have already been undertaken to exploit the results/outcomes of ATENA – i.e. the knowledge and understanding produced by ATENA, which consists, said broadly, on a prototype. These actions constitute a joint effort during this first period of the project which will be continued and reinforced during the rest of its lifetime and also after its finalization. As a matter of fact, one of the goals of the exploitation work in the final stages of the project is to shed light on how to enter into the scenario using different strategies and tools, how to reach the market and, in this line of market, building a business plan. All these actions will complement and enhance the individual initial exploitation plans of each partner as a function of the project advances. The goal is to devise a strategy that delivers information to the partners to actually exploit the project results obtained, always with optimisation in mind, that is, taking the best option.

The opportunities for exploitation of the results in the market is being studied on a continuous basis though emerging literature review, analysis of projects and cases, field research, interviews and tracking news articles and materials published in professional media.

In a first stage, information about exploitation opportunities has been related to collecting and compiling information and following technological developments to finally analyse the business potential of ATENA and commercial routes, as well as other routes of exploitation as education, training, networking, investigation of further research work, advice to policy makers and more which will be clearly identified in a second stage of this work. In-depth analysis and insight on opportunities and bottlenecks – and how to address them - to introduce the results into the industry and user scenario, technology transfer tactics and commercial routes, opportunities for collaboration and networking, and analysis of technology & market dynamics trends have been initiated and will be reinforced in this second stage of the project lifetime.

In the second stage work the dissemination backing exploitation will be reinforced: reporting scientific project outcomes in scholarly publications; media-based activities will be strengthened since the project outcomes in terms of exploitation will appear more clearly; networking will be enhanced through both, direct interfacing and research–related event as workshops and other research related events as industry briefings; a go-to-market series of strategies will be devised; and, finally, a business analysis will be built.

2.2 The exploitation strategy in a nutshell

2.2.1 First stage: make the ATENA project known

In this first stage, as preliminary actions, specific efforts are being made to ensure that ATENA appears referenced as much as possible since the exploitation is strongly linked to promotion which is viewed as a supporting tool (the necessity of inform of the existence of the “thing” to exploit), the dissemination and communication efforts through scholarly publications, presentations, press/media activities, website-based and social media operations, networking and directly interfacing, as well as a series of workshops have been implemented. Technology intelligence has been initiated and will continue for the entire duration of the project to keep abreast of industrial and scientific developments in the broad field cyber-security for critical infrastructures and related issues. The dissemination and communication plan has been conceived as a mechanism to strengthen the exploitation issues through a series of efforts addressed to improve

the project visibility across all interested stakeholders in both academia and industries concerned with smart grid, oil and water which are the applications envisaged and where more impact can be found.

2.2.2 Second stage: strengthen the link with potential stakeholders

As said before, the efforts of the first stage will be highly enhanced during the second stage of the project to ensure that all players of interest are reached. In fact, a series of preparation actions have been made during this first stage of the project: collecting information of different nature (actions, policy, resources, players, markets, case studies, scientific research results,…) from a variety of sources, researching and further analysing the scenario dynamics, as well as building databases for further usage. The latter will include information on existing strategies to enter into the market, market figures, a landscape of the market, who are the main players and their movements, new potential emerging players, trends analysis, and more in this strand to obtain a full picture of the environment where ATENA is evolving that could allow to derive opportunities. This work will be an important tool for improving the initial individual exploitation plans and also for possibly a common exploitation plan whose potential will be analysed in-depth, including business activity, further research and networking; education & training; policy advisory actions, as well as for any other use that could find of interest during this research. Also, as a supporting tool (the necessity of inform of the existence of the “thing” to exploit), the dissemination and communication efforts through scholarly publications, presentations, press/media activities, website-based and social media operations, networking and directly interfacing, as well as a series of workshops will be implemented. Technology watch will continue for the entire duration of the project to keep abreast of industrial and scientific developments in the broad field cyber-security for critical infrastructures and related issues. The dissemination and communication plan has been conceived as a mechanism to strengthen the exploitation issues through a series of efforts addressed to improve the project visibility across all interested stakeholders in both academia and industries concerned with smart grid, oil and water which are the applications envisaged and where more impact can be found.

2.2.3 The project assets to be exploited

As a summary, the exploitation work, backed by the dissemination & communication tools, is being conducted with the goal of empowering the impact of the project by boosting the up-take of results – through exploiting its innovation value and business logic, so finally delivering on the innovation value of the technology and knowledge produced. As a matter of fact, in terms of exploitation, the overall objective of the dissemination and communication plan is to ensure that the knowledge and understanding produced by ATENA flows freely to anyone that can made a use of it.

ATENA project is ambitious in terms that it addresses, analyses and develops solutions for a number of key issues in Critical Infrastructure Protection that are still on the research stage since around 15 years. The important matter is that totally satisfactory solutions do not exist; and since ATENA project builds upon proven results and IT components of past projects in the same technology strand; and efficient use of resources and good cost-effectiveness to advance the state of the art, associated to improvement in the industry can be realistically assessed. Further, the dynamics in ICT development requires solutions that are not tailored to the situation as is alone but need to be flexible in application and have the potential of adaptation to the future.

Characteristics and effects of interdependencies in heterogeneous Critical Infrastructure environments comprise one of the most difficult and complex problems in the field of Critical Infrastructure Protection analyses. Huge efforts have been invested in studying and modelling the effects of interdependencies in Critical Infrastructure sectors and between different Critical Infrastructure- sectors when confronted with disruption. This is another positive factor for ATENA exploitation purposes: its uniqueness in a scenario where a demand exists. As a matter of fact, methodologies and tools have reached some maturity status. However, despite those progresses,

the main deficits in the areas of Critical Infrastructure interoperability still seems to comprise two things: (a) there are no sufficient real-live experiments, let alone operations, and (b) there is no sufficient empirical data base on the effects of interdependencies (such as cascading and secondary/ tertiary etc. effects).

The base idea is to have a common platform to be sold to Critical Infrastructure companies, jointly by the consortium. The single components have a value by themselves also, and so they may be individually sold and inserted or marketed in other contexts (ATENA consortium is still in the realm of wide open hypotheses, so no one excludes that the single components may be sold also separately). There is nothing that precludes this in the consortium agreement, but of course will try best to sell the ATENA components – whose power is multiplied when working together - inside a single ATENA bundle.

2.3 Some notes about markets and needs

ATENA prospects for exploitation are good. The activity in the area is hot and increasing. As an example, in the USA, in July 2017 the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) awarded a five-year Other Transaction Agreement (OTA), with a value up to $70 million, to Arlington, Virginia-based Cyber Apex Solutions, LLC, to foster applied research of prototype cyber-defence solutions for critical national infrastructure sectors [6]. According to JRC reports, during year 2016 a series of important facts have happened concerning cyber-security in the broad field of Industrial Control and Critical Infrastructure scenarios. In particular, the 2015 attacks against the Ukrainian electricity distributors have been extremely relevant. These series of attacks have constituted the ignition to raise interest in critical infrastructure protection. However, the vulnerabilities detected in the broad area of ICS equipment by main manufacturers are still increasing.

Other example in the same strand, to what happens in specialized industrial systems, a series of security developments in software that could “spill over” to production environments are also increasing. This has certainly happened in a number of cases where critical infrastructure was adversely affected by general IT security problems” (extracted from [7], page 1).

MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. (USA) is a recent initiative which focus on the need for critical infrastructure cybersecurity since they recognize that much less research in cybersecurity for critical Infrastructure has been done, at the expenses of the advances of Cyber-Physical Infrastructure and IoT (Internet of Things) which, as counterpart, facilitates the vulnerabilities.

The global market for critical infrastructure protection is growing, and it is projected to reach $94 billion by 2020, according to Global Industry Analysts, Inc.

Much more information exists about the importance of critical infrastructure protection in terms of cybersecurity which is being gathered, analysed and digested to connect it with ATENA purposes and results.

3 A spotlight on applications

3.1 Introduction

Oil, gas, water and smart grids are the fundamental applications envisaged by ATENA. As a consequence, the exploitation activities will focus on these applications, which will be the fundamental recipients of the knowledge produced by ATENA, apart, of course, and very important, of other fields in the cybersecurity area. Speaking in terms of technology segments, ATENA tackles aspects such as telecommunication networks, , SCADA security, managed security & services, and to the following vertical segments: energy & power (smart grids, nuclear, solar, thermal, hydro and geothermal), IT and communication, secured communication and network security solutions.

The consortium is backed by specific knowledge and experience on these applications and technologies since it counts with partners whom are from the industry and also end users. All partners have the necessary demonstrated background to undertake the exploitation of ATENA knowledge and results. In this section we focus on the exploitation concerning the applications. Additionally, since this is also very important fundamentally due to the interdisciplinary nature of ATENA, other potential unexpected applications that can be tackled by the knowledge produced by ATENA during its lifetime will be also investigated and analysed, in the search of the so-called spin-applications.

3.2 The exploitation background of ATENA

It is important to notice that presently, critical infrastructures evaluation, their simulations and their threats examination are attracting a high attention from governments, policy makers, stakeholders and also from the market since they constitute an opportunity for the latter (the market). The state of the art and the challenges in terms of exploitation relating to cyber-security of critical infrastructures as water, gas and electrical grids are viewed as extremely important, particularly because of their strong inter-dependencies and their impact in society and business continuity in case of major outage, malicious takeover or even loss of control due to a blindness attacks.

Furthermore, since ATENA, is a project leveraging the outcomes of previous European Research activities – the CockpitCI [9] and MICIE [10] projects – also related to the critical infrastructure domain,, its value for exploitation is particularly relevant. MICIE fundamental outcome was an alerting system for assessing the risk level inherent to critical infrastructures-provided services: the proof-of-concept critical infrastructure interdependency models obtained, risk predictor and secure mediation gateway paved the way for the CockpitCI project (which ATENA project follows up). One of the ATENA goals is to continue this strand through exploiting the advanced features of ICT algorithms and components, so as to bring them at operational industrial maturity level; concerning this, the knowledge and understanding produced by ATENA will be tailored and validated in the above mentioned selected use cases: water, smart grid, oil and gas. As a matter of fact, ATENA project aims at addressing the area from “lab to market”, by leveraging research, innovation and prototypes developed in the previous MICIE and CockpitCI projects.

3.3 Water sector

Water is a particularly relevant topic as being one of the most important critical infrastructures for the society and highly dependent of the grid. In terms of exploitation, the role of the partner La Société Wallonne des Eaux from Belgium is highly significant. They use their big portfolio of contacts to present and analyse the opportunities to exploit the results of ATENA. Also, the industry partner MULTITEL whom has been partner of the project GreenRail2 from Belgium has got valuable information in terms of electricity consumption optimisation in railways and electrical traction network and since they coordinate the Smart Water project (Wallonia, Belgium) which is

devoted to small-medium power pumped hydro energy storage integration in smart electrical grids focusing on operational optimisation of services portfolio is an important actor in delivering knowledge for ATENA exploitation purposes. ENEA is contributing to exploit ATENA in the water scenario with their experience gained through SINERGREEN project [11], funded by the Italian government, which aim is to improve the energy efficiency and to develop renewable energies by means of monitoring, optimization and integration in the electricity system of other distribution networks, as gas and water networks. The exploitation and dissemination team actively cooperate with these partners to coordinate efforts; to reinforce their actions; to discuss the results obtained in these mentioned projects and in the development of ATENA; to make an in-depth research of what is happening and expected in the full water scenario in terms of markets and needs; to dig information on its dynamics and to obtain and analyse any other information which would provide understanding of how the market for ATENA in the water scenario can be tackled; the goal is once all this knowledge be acquired, to analyse it in order to develop a go-to-market strategy. Also, dissemination and communication actions will actively be performed in the water arena, as an essential tool for exploitation, making ATENA visible in the specific water scenario.

3.4 Electrical sector

Smart grid is another application of ATENA, with a particular weight, since both water, gas and oil are strongly dependent of the grid. In this case, IEC is the end-user partner whom will be a source of information about exploitation potential; also ENEA is an important industry partner for this application: the knowledge gained through their AFTER (FP7) [12] and ASTROM (EPCIP) deal with electric transmission systems will be of very help to investigate the exploitation potential of ATENA in the smart grid sector. The industry partner CREOS LU will be also an important player for the exploitation activities since they are well positioned as distributors of gas and electricity with access to industrial control system vendors as well as to its peer in the distribution and transmission sector as ENTSO-E and EUTC. UC (Coimbra University) will be also instrumental for exploitation purposes since they are engaged in collaborations with electricity utilities, and also oil refineries, another application envisaged by ATENA; further, since they are also involved in other collaborations addressing further applications as telecommunications operators and hardware producers they can be useful to contribute to investigate spin-off applications for ATENA outcomes. FNM (Leonardo spa) is particularly well positioned to exploit the ATENA results in terms of helping advance the Homeland Security market in both domestic and international arena, which is considered an increasing priority all over the world. The know-how of these partners who are the closest to the market will be managed for exploitation purposes as said before in the case of water. Below it is included a summary of the actions.

3.5 How to reach this potential

Again and as with any other application studied, the exploitation and dissemination team will actively cooperate with partners to coordinate efforts; to reinforce their actions; to discuss the results obtained in their previous and present projects related to the goals of ATENA, to discuss the actual efforts and results within the development of ATENA; to make an in-depth research of what is happening and what is expected (trends) in the full different scenarios to tackle (oil, gas, water, grid) in terms of markets and needs; to dig information on these scenarios dynamics and to obtain and analyse any other information which would shed light and provide understanding of how the market for ATENA in the different scenarios can be tackled. The goal is, once all this knowledge be acquired, to analyse it in order to develop a series of go-to-market strategies. Also, dissemination and communication actions will actively be performed in the three application scenarios envisaged by ATENA, as an essential tool for exploitation, making ATENA highly visible in the different specific scenarios & markets under study. Dissemination will also tackle other related disciplines that could benefit from the work being done (the so mentioned spin-off applications).

As a final remark, since exploitation of research results is contemplated nowadays within the broad area of Knowledge Transfer, which goes ahead from actually reaching markets and make dissemination and communication, activities concerned with improving and enlarging curricula (academic partners) including the involvement of industries as targets are being prepared. Also, further networking with peers and/or industry to undertake new related projects is contemplated as exploitation and will be assessed so as to produce a series of recommendations. Apart from this, the academic partners constitute a knowledge pool where spin-off applications can derive from the technology developments to reach the final outcomes, as for example, modelling, advances in SCADA security, and more in this strand which is being studied for exploitation purposes and which final results will be available in the second stage of the project.

Training, strongly related with curricula development, is also important for exploitation, particularly in a project of this nature, where strong research efforts are required and where also a strong need of trained personnel exists. As a matter of fact, for example Forbes reported in 2016 that there were over one million cyber security jobs at international level and that more than 209,000 cybersecurity jobs in the USA were unfilled in the same year 2016. Now, in 2017, 350,000 jobs are still unfilled, according to CyberSeek [13]; Cyberseek is a project of the National Initiative for Cybersecurity Education (NICE), under the umbrella of the National Institute of Standards and Technology (NIST) in the USA. The trend is rapidly growing, to 6 million globally till 2019 according to Symantec.

4 Go-to-Market Strategies

4.1 General considerations

This chapter, consists of a series of strategies that are being investigated and devised for ATENA results enter into the market. Here the introduction of the initial individual exploitation plans of each partner already outlined in the proposal, is being used to refine these plans as well as to provide a guide for the full consortium.

ATENA final outcome is an integrated solution, a tool suite made up of models, methods and software tools. In order to adequately exploit this outcome and other potential spin-off outcomes that could have been detected during the project development, a research is being made to elaborate different strategies to reach the market.

Key drivers for ATENA market are the growing dependency of critical infrastructures on information and communications technologies, including Internet of Things, as well as the increasing automation processes across all verticals segments (energy & power, IT and communication, secured communication and network security solutions), growing requirements for cost effective security solutions and the market trend of deploying best practices for a better response in the event of emergencies. In that market there are still not commercial solutions specifically designed for an integrated approach to the needs of the emerging OT / IT scenarios. This is the reason why ATENA aims at developing an integrated solution starting from the valuable results of European research projects, based on the most modern field specific standards and methodologies (NERC, NIST, ENISA) and exploits heavily up to a market-ready technology offering: a tool suite composed by: models, methods and software tools.

Studying and analysing potential go-to-market strategies will give raise to the necessary information for helping partners to build their own business models based on ATENA outcomes. IPR (Intellectual Protection of Rights) will be studied so as the partners be able to build their business plans in a fair and legal way; a detailed contract will be elaborated, in the final stages of the project development as a result of making a deep insight to ascertain to whom pertain the different results obtained, as it is usual in the IPR arena: ATENA consortium, in particular those partners who would have rights on the results, will study also the convenience of using the input of legal advisors specialized in IPR, whom may come from the universities or big organizations working in ATENA. Also, given the nature of ATENA (an attractive product for Governments) special attention will be given, not only to markets and academic peers but also to Governments both in Europe and in the international arena.

4.2 SWOT ANALYSIS for ATENA

A strategic analysis about Strengths, Weaknesses, Opportunities and Threats (SWOT) has been developed for specific scope of the ATENA project, whose summary appears below. This effort was undertaken in order to better understand how the ATENA value proposition can be efficiently leveraged in the scope of the objectives and domains for which it was designed.

Strength: strong points of ATENA solution	Weaknesses of the ATENA solution
▪ The solution follows the good security practices and lesson learned during the State of the Art analysis ▪ Most of the component has been based on open source which ensures easy deployment, transparency and low price ▪ Not linked to commercial solution ▪ Based on multiple expertise of the consortium	▪ Not recognised in industrial world such as Siemens, ABB, PSI solutions ▪ No huge financial support to promote the solution and to ensure the end-users of the financial stability of the providers. ▪ No real leader in the solution exploitation strategy.
Opportunities: potential for development	**Threats: obstacles in the development**
▪ The solution could be deployed for other type of CIs such as financial, health etc. ▪ The solution could be used in smallest organisation to monitor the risk. ▪ Each component has its own life cycle and could be easily developed as stand-alone product.	▪ Dependency of the industrial operator and manufacturer knowledge: e.g. for the industrial protocol. ▪ Size (SME) or status (University) of the partners: unable to fight big provider in that type of solution. ▪ Lack of confidence of such solution from industrial side.

The future action regarding the exploitation of the project results should consider this SWOT analysis to strengthen the project asset and limit its weaknesses as much as possible.

In that aim, the study on the future, prospects and trends is also being made with the goal of making a compilation on published information (and again some interviews) about what is expected for critical infrastructures protection in terms of markets, technologies, and other matters of interest that are being researched within ATENA. This information will be valuable not only for ATENA exploitation but also for policy makers.

The investigation, at international level, of the evolution of existing projects , players, the analysis of cases of study, and other happenings in the field is considered important to learn, making technology watch for business purposes and for study networking possibilities; that is why efforts are being continuously doing made, through digging information so as to build a comprehensive list of targets which will be useful for ATENA exploitation, with a view of Knowledge Transfer purposes, which include all kind of tools to make use of scientific & technological work.

5 Partner exploitation survey

In this part of the deliverable, considering the progress of the project and the trends of the potential markets for the ATENA tools suite, each partner tried to answer the three fundamental question:

1. Which exploitable results do the project partner (each partner) aim to generate?
2. What form(s) can the exploitation of these results take? How to enable it?
3. What is each partner contribution to the project, what are their different exploitation strategies, are the expectations of partners compatible and coherent?

These issues are taken from EU – extracted by a schedule proposed by experts in exploitation inside EU - are included to pinpoint which are the most relevant questions to answer after 12 months of a project. This is also to put in evidence – by difference - that more ambitious answers (e.g., a business plan) will be treated in the future.

5.1 CRAT

Which exploitable results does the project partner aim to generate?

CRAT expects to reinforce and develop its collaboration with the consortium's members, in particular with end users and other research centres. The collaboration with the end users, in particular, will enable CRAT to acquire familiarity with real, field deployed, facilities and high-end testbeds.

Additionally, CRAT intends to exploit the results of this project for didactic and teaching purposes. Several master courses and PhD theses will exploit the results coming from the research activities of ATENA, either as teaching material or as research fields and directions. Seminars on the methodologies and results coming from the project will be held at the Universities in the CRAT consortium and in the surrounding companies/universities. New generation researchers and engineers working for CRAT will acquire important know-how on cyber-physical security and Control Theory, control strategies for mitigation in CIs, and in preventive control schemes for composable security in the CI domain.

Finally, CRAT intends to sponsor the technology transfer of the most promising results produced by CRAT during the 36 months of the project, by fully supporting start-ups in the field and SME in Europe. The final aim of these collaborations will be the development of commercial solutions.

What form(s) can the exploitation of these results take? How to enable it?

Most results of the project coming from CRAT's effort will be published in international journals and conferences, enabling a peer confrontation with other researchers in the field, additionally enhancing the know-how acquired by CRAT.

The technology transfer of these results can take the form of collaboration with SME and startups active in the field to develop/enhance products ready for market.

Future collaborations in research projects with members of the ATENA consortium are envisaged for the further development of the methodologies and results of CRAT's ATENA activities.

What is the partner contribution to the project, what are their different exploitation strategies?

CRAT main activities consist of the following:

- Leading the ATENA system requirement and architectural activities

- Development of new, CI contextualised, approaches to composable security for preventive control of cyber-physical systems.
- Development of mitigation strategies for adversarial events in CIs
- Contribution to anomaly detection algorithms based on control theory and machine learning and big data analysis for forensics.

The exploitation of most activities is focused on know-how improvement and didactic purposes. More market-friendly results, such are those coming from WP5 and WP3, will be exploited collaborating with SME and startups for prototyping purposes and technology transfer.

5.2 IBS

For IBS, the main exploitable result will be the new knowledge developed in the course of ATENA project.

IBS is a non-profit research entity and main exploitation occurs either in the form of publishing.

Knowledge obtained in ATENA serves also as an important background for future research projects.

5.3 MULTITEL

Which exploitable results does the project partner aim to generate?

Multitel is developing simulation models of interdependent CIs. These models are possibly to be used in the risk predictor module to calculate on-line the consequences of possible scenarios on quality of service indicators (QoS) for final customer (of electricity, water,...). The models are developed in The Intelligent RAO Simulator.

Based on this, transformation into a marketable version would include (1) developing software modules to automatically customize the RAO model with client's CIs data stored in format used by client, (2) further optimizing RAO model to increase calculation speed, (3) developing software to encapsulate the RAO model in an API to be used by risk predictor developers (the API shell insure data exchange with the model, results processing and model execution control) and (4) writing documentation on API. All this can be estimated now in 6-12 man/months. A RAO license will also be needed to run models. RAO belongs to Multitel and is not commercialized in regular way. So, license cost right costs cannot be still provided now.

They are essentially simulation models and potentially some results of their exploitation in the frame of Task 2.5 "Risk assessment to increase resilience and awareness", if we succeed to get some generalizable conclusions about how to increase interdependent CIs resilience by structural and operational measures.

What form(s) can the exploitation of these results take? How to enable it?

Use of models developed in ATENA operational tool, namely as a part of risk predictor (for damage estimation), so the form of results exploitation for Multitel is the same as for all partners contributing in ATENA tool; We can enable it by developing software modules allowing the use of simulation models by developers of risk predictor (see above).

What is the partner contribution to the project, what are their different exploitation strategies?

Multitel's contribution is simulation models for risk assessment, more precisely for damage estimation in terms of QoS indicators under different scenarios of adverse events (WP2); simulation models development (adaptation) for using them in validation process to simulate various scenarios of adverse events to feed ATENA tool with current simulated system state for testing (WP7).

5.4 UL

Which exploitable results does the project partner aim to generate?

For UL, the main exploitable results are scientific publications in strong journals and conferences related to security, SCADA systems and critical infrastructures. Moreover, Patents could be also envisioned within the context of ATENA.

What form(s) can the exploitation of these results take? How to enable it?

Algorithms and techniques proposed within ATENA project can be used for building prototypes and demos. To this end, an engineering work is required to transform these scientific publications into concrete prototypes.

What is the partner contribution to the project, what are their different exploitation strategies?

The main contribution of UL in ATENA is the design of security agents for intrusion detection. In addition, UL will be involved in the Software Defined Security task to build a framework that is able to dynamically and proactively react to the evolving threats.

For the exploitation plan, UL aims at improving R&D activities in Critical infrastructure protection and SDN, therefore enrich related didactic activities.

5.5 SAPIENZA SL

Which exploitable results does the project partner aim to generate?

To augment and expand their knowledge capital so as to be able to undertake further work of interdisciplinary nature, focusing on strategic views and scenario & market analysis in terms of Internet of Things and Critical Infrastructure protection as well as other matters that can appear showing interest during the investigation. SAPIENZA already has accumulated knowledge assets built from previous participation in international projects and studies: ATENA is an opportunity to acquire new understanding of the topic, scenario dynamics and players as well as to analyse and research cross-disciplinary innovation aspects that can help to shed light on the field and use for further analyses. As a summary, SAPIENZA own exploitation plan is related fundamentally to value extraction, that is, converting the created value into a form that is useful to the organization in terms of strategic positioning which will be used to undertake further work while expanding their fields of expertise and their collaborative networks.

What form(s) can the exploitation of these results take? How to enable it?

Intensive work of digging information of different nature (actions, policy, resources, players, markets, case studies, scientific research results,…) from a variety of sources, research, further analysis, and writing to both publish & disseminate material and building databases for further

usage, including devising strategies to enter into the market, to undertake new research efforts, to devise strategies for improving the exploitation and for training, as well as for any other use that could find of interest during the research.

What is the partner contribution to the project, what are their different exploitation strategies?

Analysis of the state of the art in connexion with other technologies as Wireless Sensor Networks (D8.2); analysis of the validation work with the vision to shed light on exploitation value and opportunities; devise of exploitation strategies following the final results of ATENA and other potential intermediates that could have a value; informing the ATENA consortium on opportunities for dissemination (call for papers, keynotes speakers…) and for exploitation; research on targets apart from the ones already identified at the project initiation (covering both literature and teams/players) so as to build a database to communicate ATENA value and results and establishment of contact; analysis of results obtained through these contacts; dissemination & promotion.

5.6 iTRUST

Which exploitable results does the project partner aim to generate?

One of iTrust main business is to provide security consultancy, organisational and technical guidance to implement security in any type organisation including CIs. In that aim, iTrust assists their customers in risk analysis and risk monitoring including the design and the implementation of countermeasures to reach an acceptable level of risk. In the project, based on their own expertise, iTrust is developing both vulnerability management system and risk analysis system but also some probes to feed the two previous systems with near real-time data: SmartHome IDS, Multi-antivirus system and Security Configuration Checker.

Based on this, moving into marketable version for the different component either as stand-alone product or as service would include: (1) developing software modules to automatically feed topology model with client's CIs data stored in format used by client, (2) further optimizing security metrics to increase reliability of the assessment, (3) developing market software (design interface), packaging (for product) and (4) writing documentation on them. All this can be estimated now in 6-12 man/months. Other cost could be added as licence contract or service contract design or marketing cost (estimated to at least additional 6 man months). When product will be ready, additional cost could be also added as implementation cost for guidance and customer training or maintenance cost for product and software: it could be estimated in 3 man/months/year

What form(s) can the exploitation of these results take? How to enable it?

As previously mentioned, the product and software develop could be exploit as standalone product (maybe for large market as SmartHome IDS) or as service (Vulnerability Management System and Risk Analysis. The results will be also included in the overall architecture of the ATENA system.

What is the partner contribution to the project, what are their different exploitation strategies?

The contribution of iTrust for the project is both to provide new probes for the detection layer contributing to increase the efficiency of the IADS and to provide two important systems for the ATENA system, i.e. the vulnerability management system (providing the vulnerability level of CIs component) and the risk analysis tools (providing the current risk level at CIs service and node level).

As mentioned the operator CREOS, the chance to reach a commercial product for entire tools developed in the ATENA project framework is weak. So, that is the reason why the results of the project could also be envisaged as autonomous product or solution to have a chance to be commercialised. So the consortium shall to articulate these two strategies together.

The expectations of partners are really compatible and coherent. Most of the system designed and developed during this project are in line with lesson learned during the previous project MICIE and CockpitCI and represent a new step in the architecture design of a real solution.

5.7 UC

Mission statement: UC is a reference Portuguese University, with over 22,000 students (including more than 2,500 PhD students and 7,000 Master students). UC is also a reference research institution, with 35 research centres actively involved in top-level pure and applied research. More specifically, the Faculty of Science and Technology presently has approximately 470 Professors/Researchers who draw on an involvement in cutting-edge research to assure the best education at all levels. Fourteen departments offer programs leading to the Bachelor, Master and Doctoral degree programs. The Faculty R&D infrastructures are organized in 16 Units, including the Centre for Informatics and Systems of the University of Coimbra (CISUC), funded in 1995. CISUC, with around 60 PhD researchers, is the research arm of the Department of Informatics Engineering (DEI-UC) – which is more focused on education, offering graduate courses, specialized masters courses, PhD programmes and advanced training services to the industry. These two entities are complemented with Instituto Pedro Nunes (IPN), a non-profit organization controlled by the University of Coimbra which focuses on fostering technology transfer from the University to the community, including advanced applied research services for the industry, advanced technology transfer programs and incubation of technological start-up companies. Over the last 10 years CISUC and DEI-UC were directly involved in the creation of more than a dozen successful start-up companies, which altogether created over 1,500 direct jobs and have an annual turn-over exceeding 120 million Euro. A few examples of such companies include Critical Software (*www.criticalsoftware.com*), WIT-Software (*www.wit-software.com*) and Feedzai (*www.feedzai.com*). Moreover, CISUC and DEI-UC were also involved in technology transfer programs with some of the largest industries in Portugal and many Portuguese and European SME's.

Which exploitable results does the project partner aim to generate?

Exploitable results relevant for UC comprise both acquired/refined expertise on various fields of the ATENA project and specifically developed algorithms, technologies, software platforms and software/hardware components developed specifically in the scope of ATENA.

As such, UC identifies the following exploitable results:

- Advancements on its expertise on security monitoring frameworks for industrial and automation control systems, including anomaly detection algorithms, high performing distributed processing platforms, mixed physical/virtual environments, forensics and infrastructure *softwarization* in the IACS domain.
- The ATENA monitoring and cyber-detection platform, specialized probes such as the SCADA Honeypots and the SSU and specialized meta-management and forensics tools.

What form(s) can the exploitation of these results take? How to enable it?

The UC team involved in the ATENA project is actively involved in the three aforementioned UC mission vectors (education, research, technology transfer), and plans to exploit ATENA's results in various ways.

At training level UC will exploit the ATENA results in its educational services, especially at postgraduate level. DEI-UC offers courses on security in several Master programmes (including a specialized Master on Information Security) which will take advantage of ATENA results. Moreover, several Master students are being directly supported by the ATENA framework for preparing their MSc Dissertation – including the access to testbeds, reference scenarios and datasets. At this point, there are at least 5 MSc students that directly used ATENA for their dissertation work. The same thing happens at PhD level, with the usage of ATENA results in a specific course on security integrated in the PhD programme, and the direct involvement of 4 PhD students preparing their thesis.

At research level UC is using ATENA to further expand its expertise in IACS security and related areas. ATENA results are being actively exploited by means of scientific publications – as already mentioned in ATENA dissemination reports – and the scouting of related research areas. This way UC intents to increase its international impact and reputation in areas such as IACS security, virtualization of IACS infrastructures, safety monitoring for complex processes, ICT forensics, IoT and cloud/fog computing. The contributions of UC to the ATENA framework have already seeded a number of follow-up research projects in those areas, at national and international levels, which are expected to kick-off in the next months.

Regarding technology transfer, there were already several contacts with industrial partners (both specialized SME's and large partners such as EDP – the largest Portuguese energy utility) to disseminate the ATENA approach and to identify potential spin-off technology transfer activities. Ongoing discussions already pinpointed two potential opportunities (one in the field of security and safety monitoring, another in the field of IACS network virtualization) and more objective results are expected to follow as ATENA results materialize.

What is the partner contribution to the project, what are their different exploitation strategies?

UC leads the design and development of the cyber-detection layer and is also deeply involved in the validation tasks. Its exploitation plans focus on the components developed by UC – in some cases with the collaboration of other ATENA partners – and on potential synergies with other ATENA components, such as Roma3 tools, the various testbeds involved in the project and the specialized cybersecurity components provided by other partners. Various joint exploitation strategies are being considered or already under implementation. For instance:

- Teaching staff exchange programs with Roma3, in order to reinforce the advanced training courses on security at both institutions (MSc and PhD courses). These exchange programs will start in Q1/2018.
- Preparation of new research projects with ATENA partners (in some cases also involving external partners) in related fields, enabled by ATENA outcomes.
- Discussions on joint productization and joint commercialization (or joint release as open source) strategies for selected ATENA components.

5.8 ENEA

Which exploitable results does the project partner aim to generate?

As ENEA is committed by Italian Government to transfer technology to industry, therefore it will exploit ATENA results for reinforcing the technology transfer activities to national industry and in international contexts.

What is the partner contribution to the project, what are their different exploitation strategies?

ENEA is involved in the development of a unified modelling framework and relevant models to predict the efficiency of CIs physical flow and CI resilience against adverse events (faults, cyber-physical threats, challenges to "normal" operation) of their Industrial Automation and Control Systems (IACS). The unified modelling framework rely on a hybrid modelling approach, in which actual physical devices, emulators and simulators, such as agent-based, discrete event, domain and traversal simulators, co-exist and are composed. That should consent the representation of the heterogeneity of physical flows across CIs and the CIs different capabilities, such as the ability to face cyber threats and faults to IACS and to maintain acceptable levels of flow efficiency and availability

Unified modelling framework and models to predict physical flow efficiency and resilience across CIs against adverse events on IACS, requirements of WP3 IACS for security, distributed awareness and distributed Mitigation and Resiliency, verification, development and components Integration, validation and dissemination of the results.

5.9 CREOS

Which exploitable results does the project partner aim to generate?

Identify new tools and systems to improve Gas and Electricity CI protection against cyber-attacks and infrastructure resilience. Contribute to enhancing CREOS IT security landscape and thus improve the resilience of the European energy distribution sector.

Disseminate project ideas and results to the professional sector of industrial control system vendors as well as to its peer in the distribution and transmission sector (ENTSO-E and EUTC).

What is the partner contribution to the project, what are their different exploitation strategies?

CREOS provides its dual expertise in electricity and gas distribution, and also in security of the Smart Grid. Moreover, it provides testing facilities on electricity and gas test network in order to validate the ATENA tools in the most real environment as possible. It will also able to disseminate in the professional network the results and the standards requirements set up during the project.

5.10 UNIROMA3

Which exploitable results does the project partner aim to generate?

Acquire information, experiences and technology knowledge about risk reduction issues related to some of the most CIs in Europe; Contribute to CIP and CIIP activities. Exploit ATENA results in didactic activities.

What is the partner contribution to the project, what are their different exploitation strategies?

ROMA3 brings his technical experiences in telecommunication and in automation research fields, thanks to new challenges in the CI Protection. Research activities are actually in the field of topological control theory, resilient control algorithms, decision support algorithm and software defined security. ROMA3 is leading WP5, for analysing, developing and implementing mitigation and reaction strategies for the physical infrastructures, their services and their IACS. ROMA3 is updating the CISIApro tool and the Integrated Risk Predictor (IRP) from MICIE and CockpitCI, for

improving the risk assessment procedures and suggesting suitable reconfigurations. ROMA3 delivers support to Leonardo in the improvement of the Secure Mediation Gateway. As university, ROMA3 contributes to scholarly dissemination activities.

5.11 IEC

Which exploitable results does the project partner aim to generate?

To learn on tools and systems that can improve the company's possibilities to protect the energy infrastructure capabilities from cyber-attacks, in particular to real-time Distributed Monitoring and Detection System able to aggregate the filtered and analysed information of potential cyber-attacks induced on SCADA systems or telecommunication systems used to support the operation of CIs and identify the potential unsecured area of the CIs.

Furthermore the project is an opportunity to acquire the know-how and the possibility to exploit the project's results to introduce new possibilities for effective and secure operation of the energy infrastructure, and to acquire know-how on telecommunication, informatics and control systems, and more specifically on ICT security and risk prediction.

What is the partner contribution to the project, what are their different exploitation strategies?

IEC contributes in working on validation; on unified modelling framework and models to predict physical flow efficiency and resilience across CIs against threats of their IACS. In particular they deliver on taxonomies, risk assessment and analysis; IACS design for security; System Requirements; analysis of the Security Matrix; in Distributed Mitigation and Resiliency; mitigation strategy and reaction strategy; System integration -contribution to the integration process.

5.12 FNM-Leonardo SPA

Which exploitable results does the project partner aim to generate?

FNM will contribute to development of some of the ATENA models and prototypes, acting for some of them as the main developer and for other ones as a contributor. In particular, it will have a biggest role in the development of (a) the secure mediation gateway, that acts as a secure service bus that entrusts communications among ATENA modules and to/from external modules (possibly in other CIs), (b) the repository of information related to CI's assets and topology, in the format that is needed to other ATENA modules, (c) the adaptors that let high level ATENA modules cooperate with CI's SCADA, (d) the Composer module that supports the static assessment of the security level of the ICS according to newly defined methodologies and metrics.

All the developed tools in ATENA will be software components with well-defined REST-based interfaces, able to cooperate each other by means of the secure mediation gateway, that acts as a secure service bus that entrusts communications among ATENA modules and to/from external modules. This standard interface enables the easiest interoperability and modifiability of ATENA modules. Instead, the research about methodologies and metrics to assess the security level of the ICS will take the form of documents of rules and criteria.

What is the partner contribution to the project, what are their different exploitation strategies?

FNM is the project coordinator, and takes part to most of the tasks in all the WPs. In particular, FNM is involved in WP6 where it has the double role of developer of some of the tools that compose the ATENA suite and WP leader, coordinating the system integration of the tools of the ATENA suite. In WP3 FNM has a primary role in definition of the methodology and metrics to assess the statically security level of a ICS. In WP2 FNM contributes to definition of interdependency models. In WP5 FNM contributes to the design and development of the Software Defined Security logical subsystem (with a role in the development of Risk Predictor and Orchestration modules). These modules and the related knowledge about the related theory and practice will be exploited by FNM by attempting to commercializing them (in agreement and revenue share with other partners involved in the development). There are various possibilities that at the moment have not been evaluated in a project business plan, that range from (a) integrating ATENA software components inside one or more products in the FNM's portfolio, to (b) licensing or selling the developed software to a different company, to (c) assigning the developed software to an external related company (possibly a spin-off company of one of the partners) that will try to exploit it (maybe building commercial agreements with major ICS producers).
The research about methodologies and metrics to assess the security level of the ICS will be exploited by (a) submitting them to standardisation authorities and proposing to add them to existing metric standards and by (b) using these results to enhance the company's knowledge about this topic, that can be directly sold as a service by FNM, who works also as a certification authority for the assessment of systems security.

5.13 SWDE

Which exploitable results does the project partner aim to generate?

Identify novel solutions and innovative approach to improve Water CI protection against cyber-attacks and enhance supply chain infrastructure resilience.

What is the partner contribution to the project, what are their different exploitation strategies?

SWDE contributes to the project ATENA as SCADA operator and Water distributor. In that aim, it provides expertise especially for the State of the Art and the taxonomies definition regarding control systems and water management. It helps to set up the ATENA tools (requirements, detection and analysis tools design) to be in line with security requirements of water management operators. It contributes to defining security indicators, adapting security detection systems, risk analysis and mitigation strategies, and designing the expert systems usable for water operators. The SWDE is in charge with the FOREM of an Expertise Centre in order to provide a real test platform for new systems but also to provide awareness for public and professional audience. This expertise centre and other IT platforms deployed by SWDE is being used to validate the ATENA tools in real environments.

6 References

[1] Creating values: IP exploitation in Horizon 2020 - IPR Helpdesk. © European Union 2014.

[2] Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future. Legislative Acts for the Energy Sector EECSP Report February 2017.

[3] Critical Infrastructures: Background, Policy, and Implementation John D. Moteff Specialist in Science and Technology Policy June 10, 2015. Congressional Research Service 7-5700 www.crs.gov RL30153.

[4] Paul Theron, Introduction to the European IACS components Cybersecurity Certification Framework (ICCF), doi:10.2760/717579.

[5] Synthesis of existing legislation, guidelines, standards, organisations andprojects related to drinking water safety and monitoring. ERNCIP Thematic Group Chemical and Biological Risks to Drinking Water Task 2, deliverable 2.3, 2015

[6] Homeland Security News Wire," Applied cybersecurity research for better protection of critical national infrastructure sectors" (online), available at: *http://www.homelandsecuritynewswire.com/dr20170727-applied-cybersecurity-research-for-better-protection-of-critical-national-infrastructure-sectors* (last access: October, 2017).

[7] JRC Technical Reports, "Cyber Security Trends and their implications in ICS: Mid-year report 2016" (online), *http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103512/lbna28187enn.pdf*, (last access: October, 2017).

[8] ATENA Consortium, "ATENA Deliverable D8.4 Exploitation plan" 2016

[9] CockpitCI Funded under FP7-SECURITY Project ID: 285647, Cordis Report Summary *http://cordis.europa.eu/result/rcn/173345_en.html*

[10] MICIE Funded under FP7-ICT Project ID: 225353, Cordis Report Summary *http://cordis.europa.eu/project/rcn/88359_en.html*

[11] SINERGREEN project website, *http://www.sinergreen-smargreen.it/*

[12] AFTER project website, *http://www.after-project.eu*

[13] Cyberseek website, *http://cyberseek.org/*

[14] ATENA Consortium, "ATENA Deliverable D2.1 State of Art" 2016