

## D8.1

### Initial results of the clustering, platforms, and ecosystems activities

<b>Project number</b>	830892
<b>Project acronym</b>	SPARTA
<b>Project title</b>	Strategic programs for advanced research and technology in Europe
<b>Start date of the project</b>	1 <sup>st</sup> February, 2019
<b>Duration</b>	36 months
<b>Programme</b>	H2020-SU-ICT-2018-2020

<b>Deliverable type</b>	Demonstrator
<b>Deliverable reference number</b>	SU-ICT-03-830892 / D8.1/ V1.0
<b>Work package contributing to the deliverable</b>	WP8
<b>Due date</b>	January 2020 – M12
<b>Actual submission date</b>	10 <sup>th</sup> February 2020

<b>Responsible organisation</b>	CNR
<b>Editors</b>	Fabio Martinelli
<b>Dissemination level</b>	PU
<b>Revision</b>	V1.0

<b>Abstract</b>	This document describes Partnership activities performed by the SPARTA ecosystem in the first year.
<b>Keywords</b>	Clustering, community building, Joint Competence Centre Infrastructure





## Editor

Fabio Martinelli (CNR)

## Contributors

Florent Kirchner (CEA)

Christian Derler (JR)

Philippe Massonet (CETIC)

Raimundas Matulevicius (UTARTU)

Dimitris Kavallieros (KEMEA)

Cristina Martínez, Ana Ayerbe Fernandez-Cuesta (TEC)

Ines Goicoechea, Raul Orduna (VICOM)

Joost Geurts, Thomas Jensen (INRIA)

Fabio Martinelli, Artsiom Yautsiukhin (CNR)

Egidija Versinskiene (L3CE)

Bertrand Lathoud (SMILE)

Armands Meirans (LMT)

Adam Kozakiewicz (NASK)

## Reviewers

Florent Kirchner (CEA)

Ana Ayerbe Fernandez-Cuesta (TEC)

## Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.



## Executive Summary

This document describes Partnership activities performed by the SPARTA network in the first year in several directions.

We promoted the collection and identification of the available platforms and tools from participants contributing to build a catalogue of the existing assets. We started at the same time the analysis of the possible integration mechanisms of these tools within the Joint Competence Centre Infrastructure (JCCI). We currently identified 30 platforms and tools from 16 partners.

We also performed activities related to the consolidation of the national and European ecosystems. We enhanced the SPARTA partnership with associates and friends organizations (pulling together in addition to the 44 SPARTA partners more than 60 organizations willing to contribute and interact with our network).

We bootstrapped the SPARTA monthly workshops in the European countries of the SPARTA partners to increase cooperation and visibility with local ecosystems. In particular, we run 8 workshops in the first year and planned already 11 for the second one.

We cooperated with several EU organizations and EU projects. In particular, when possible, we tried to build and consolidate existing initiatives in the realm of the SPARTA network.

A specific attention is devoted to the cooperation with the other fellow Pilot projects for the competence network.

We report the progresses on those activities and highlight some future plans.



# Table of Content

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
<b>Chapter 2</b>	<b>Joint Competence Centre Infrastructure .....</b>	<b>2</b>
2.1	Purpose.....	2
2.2	JCCI components.....	2
2.2.1	WorkBench.....	3
2.2.2	Virtual Learning Centre.....	3
2.2.3	Cyber Range .....	3
2.3	Tentative usage workflow.....	5
2.4	Next steps .....	7
2.4.1	State of the Art .....	7
2.4.2	Hands-on tasks.....	7
<b>Chapter 3</b>	<b>Clustering activities at national, European and international level .....</b>	<b>8</b>
3.1	SPARTA ecosystem.....	8
3.2	National level.....	11
3.2.1	France .....	11
3.2.2	Belgium .....	12
3.2.3	Greece .....	14
3.2.4	Austria.....	14
3.2.5	Poland.....	15
3.2.6	Germany.....	16
3.2.7	Czech Republic .....	18
3.2.8	Lithuania.....	19
3.2.9	Spain .....	21
3.2.10	Luxemburg .....	25
3.2.11	Portugal.....	26
3.2.12	Latvia.....	27
3.2.13	Italy.....	27
3.2.14	Estonia .....	28
3.3	European level .....	30
3.3.1	Cooperation with EU Organisations.....	30
3.3.2	Cooperation with EU Projects .....	31
3.4	Monthly workshops .....	35
3.4.1	SPARTA Workshop in Madrid, Mundo Hacker.....	35
3.4.2	SPARTA Workshop in León, Mundo Hacker.....	37



3.4.3	SPARTA Workshop in Rennes, part of CominLab „Security and Privacy” ws .....	40
3.4.4	SPARTA Workshop in Vilnius .....	41
<b>Chapter 4</b>	<b>Clustering with other pilots .....</b>	<b>45</b>
4.1	Operational programme management .....	46
4.2	Operational cooperation .....	47
4.3	Substantive cooperation .....	48
4.4	Concerted communications .....	49
<b>Chapter 5</b>	<b>Summary and Conclusion .....</b>	<b>51</b>
<b>Chapter 6</b>	<b>Appendix – Asset Inventory .....</b>	<b>52</b>
6.1	L3CE’s SENTER .....	52
6.1.1	Functional Components Description .....	52
6.1.2	Services provided .....	53
6.1.3	Current Usage .....	53
6.1.4	Resources .....	54
6.1.5	Request of use .....	54
6.2	INRIA’s LHS NGE .....	55
6.2.1	Functional Components Description .....	55
6.2.2	Services provided .....	56
6.2.3	Current Usage .....	57
6.2.4	Resources .....	58
6.2.5	Request of use .....	59
6.3	INRIA’s LHS RBA .....	59
6.3.1	Functional Components Description .....	59
6.3.2	Services provided .....	61
6.3.3	Current Usage .....	61
6.3.4	Resources .....	61
6.3.5	Request of use .....	62
6.4	Tecnalia’s IDSOTER .....	62
6.4.1	Functional Components Description .....	62
6.4.2	Services provided .....	63
6.4.3	Current Usage .....	63
6.4.4	Resources .....	65
6.4.5	Request of use .....	66
6.5	Tecnalia’s OPENCERT .....	66
6.5.1	Functional Components Description .....	67
6.5.2	Services provided .....	68
6.5.3	Current Usage .....	69



6.5.4	Resources .....	70
6.5.5	Request of use .....	71
6.6	Tecnalia's SABOTAGE .....	72
6.6.1	Functional Components Description .....	72
6.6.2	Services provided .....	73
6.6.3	Current Usage .....	73
6.6.4	Resources .....	74
6.6.5	Request of use .....	75
6.7	Tecnalia's Smart Grid Facilities .....	76
6.7.1	Functional Components Description .....	76
6.7.2	Services provided .....	78
6.7.3	Current Usage .....	78
6.7.4	Resources .....	80
6.7.5	Request of use .....	81
6.8	Tecnalia's Industrial Blockchain Facilities .....	81
6.8.1	Functional Components Description .....	82
6.8.2	Services provided .....	82
6.8.3	Current Usage .....	83
6.8.4	Resources .....	84
6.8.5	Request of use .....	86
6.9	Tecnalia's Automotive Cybersecurity Facilities .....	86
6.9.1	Functional Components Description .....	86
6.9.2	Services provided .....	87
6.9.3	Current Usage .....	88
6.9.4	Resources .....	89
6.9.5	Request of use .....	90
6.10	Tecnalia's Cyber-Ranges Facilities .....	90
6.10.1	Functional Components Description .....	91
6.10.2	Services provided .....	91
6.10.3	Current Usage .....	92
6.10.4	Resources .....	92
6.10.5	Request of use .....	93
6.11	INOV's BP-IDS .....	94
6.11.1	Functional Components Description .....	94
6.11.2	Services provided .....	97
6.11.3	Current Usage .....	97
6.11.4	Resources .....	98
6.11.5	Request of use .....	99





6.12	CESNET's Nemea .....	99
6.12.1	Functional Components Description .....	100
6.12.2	Services provided .....	100
6.12.3	Current Usage .....	100
6.12.4	Resources .....	100
6.12.5	Request of use .....	101
6.13	CESNET's IPFIXcol .....	101
6.13.1	Functional Components Description .....	101
6.13.2	Services provided .....	101
6.13.3	Current Usage .....	101
6.13.4	Resources .....	102
6.13.5	Request of use .....	102
6.14	CESNET's Warden .....	102
6.14.1	Functional Components Description .....	103
6.14.2	Services provided .....	103
6.14.3	Current Usage .....	103
6.14.4	Resources .....	103
6.14.5	Request of use .....	104
6.15	CESNET's NERD .....	104
6.15.1	Functional Components Description .....	104
6.15.2	Current Usage .....	105
6.15.3	Resources .....	105
6.15.4	Request of use .....	106
6.16	LIST's Node in Infrachain Blockchain .....	106
6.16.1	Functional Components Description .....	106
6.16.2	Services provided .....	106
6.16.3	Current Usage .....	106
6.16.4	Resources .....	107
6.16.5	Request of use .....	107
6.17	UKON's Visual Computing Center for Cyber Security .....	107
6.17.1	Functional Components Description .....	108
6.17.2	Services provided .....	108
6.17.3	Current Usage .....	109
6.17.4	Resources .....	110
6.17.5	Request of use .....	115
6.18	UBO's IT-Security Awareness Pentesting Framework .....	115
6.18.1	Functional Components Description .....	115



6.18.2	Services provided .....	115
6.18.3	Current Usage .....	116
6.18.4	Resources .....	116
6.18.5	Request of use .....	117
6.19	TUM's Malware Zoo .....	117
6.19.1	Functional Components Description .....	117
6.19.2	Services provided .....	118
6.19.3	Current Usage .....	118
6.19.4	Resources .....	119
6.19.5	Request of use .....	121
6.20	LEO's Cyber Threat Intelligence Services .....	121
6.20.1	Functional Components Description .....	121
6.20.2	Services provided .....	121
6.20.3	Current Usage .....	122
6.20.4	Resources .....	122
6.20.5	Request of use .....	123
6.21	LEO's Intelligence Enabled Next Gen SOC .....	123
6.21.1	Functional Components Description .....	123
6.21.2	Services provided .....	124
6.21.3	Current Usage .....	125
6.21.4	Resources .....	125
6.21.5	Request of use .....	126
6.22	LEO's Security Evaluation Facility .....	126
6.22.1	Functional Components Description .....	126
6.22.2	Services provided .....	127
6.22.3	Current Usage .....	127
6.22.4	Resources .....	128
6.22.5	Request of use .....	128
6.23	CNR's CyberSecurity Osservatorio .....	128
6.23.1	Functional Components Description .....	129
6.23.2	Services provided .....	129
6.23.3	Current Usage .....	132
6.23.4	Resources .....	133
6.23.5	Request of use .....	133
6.24	JR's CTTC .....	134
6.24.1	Functional Components Description .....	134
6.24.2	Services provided .....	135
6.24.3	Current Usage .....	136



6.24.4 Resources .....	136
6.24.5 Request of use .....	138
6.25 VICOM's Secure Industry 4.0 .....	138
6.25.1 Functional Components Description .....	138
6.25.2 Services provided .....	139
6.25.3 Usage .....	140
6.25.4 Resources .....	140
6.25.5 Request of use .....	144
6.26 fortiss' AutoFOCUS3 .....	145
6.26.1 Functional Components Description .....	146
6.26.2 Services provided .....	146
6.26.3 Current Usage .....	147
6.26.4 Resources .....	148
6.26.5 Request of use .....	149
6.27 UniLU's TSOPEN .....	149
6.27.1 Functional Components Description .....	149
6.27.2 Services provided .....	150
6.27.3 Current Usage .....	150
6.27.4 Resources .....	152
6.27.5 Request of use .....	153
6.28 UniLU's SafeCommit .....	153
6.28.1 Functional Components Description .....	153
6.28.2 Services provided .....	153
6.28.3 Current Usage .....	154
6.28.4 Resources .....	155
6.28.5 Request of use .....	156
6.29 CETIC VaCSInE .....	156
6.29.1 Functional Components Description .....	157
6.29.2 Services provided .....	157
6.29.3 Current Usage .....	157
6.29.4 Resources .....	158
6.29.5 Request of use .....	158
6.30 CINI's APPROVER .....	158
6.30.1 Functional Components Description .....	159
6.30.2 Services provided .....	159
6.30.3 Current Usage .....	159
6.30.4 Resources .....	160
6.30.5 Request of use .....	161



## List of Figures

Figure 1: Components of the Joint Cybersecurity Centre Infrastructure. ....	2
Figure 2: Conceptual draft of usage workflow. IdP = identity provider, SDL = service description language. ....	6
Figure 3: Example draft of a list of available resources on the web app. ....	6
Figure 4: Expanded details of an available resource. ....	6
Figure 5: SPARTA ecosystem.....	8
Figure 6: SPARTA associates.....	10
Figure 7: NeCS winter school.....	32
Figure 8: PhD students and young researchers Forum .....	33
Figure 9: SPARTA workshops.....	35
Figure 10: SPARTA workshop in Madrid disseminated through TecNALIA's social network .....	36
Figure 11: SPARTA workshop included in the Agenda of the 13ENISE Program.....	37
Figure 12: SPARTA workshop in León (Spain). ....	38
Figure 13: Agenda of the SPARTA workshop in León (Spain).....	38
Figure 14: SPARTA workshop in León disseminated through TecNALIA's social network .....	40
Figure 15: SPARTA workshop in Vilnius .....	42
Figure 16: Potential points of synergy between the four pilots.....	46
Figure 17: Pilots Cooperation Handbook.....	47
Figure 18: Pilots Associates Incentives .....	48
Figure 19: Technical and Industrial challenges .....	49
Figure 20: HSL global architecture and trust zone.....	56
Figure 21: Faustine platform .....	60
Figure 22: MoM platform. ....	60
Figure 23: Functional decomposition of OpenCert platform.....	67
Figure 24: Facilities of Cybersecurity for the Smart Grid Laboratory.....	77
Figure 25: Composition of the Cybersecurity for the Smart Grid Laboratory .....	77
Figure 26: Industrial Blockchain Laboratory. ....	82
Figure 27: Fleet of 3 Model Cars (Velox Cars). ....	87
Figure 28: Cyber-Ranges Facilities in TecNALIA. ....	91
Figure 29: Example of a BP-IDS deployment. ....	94
Figure 30: Software architecture of the several modules that comprise the BP-IDS system.....	95
Figure 31: Setting up the monitoring core analysis module with business information using the Administration application. ....	96
Figure 32: Configuration Manager.....	96



Figure 33: Forensic analysis of an incident reported by BP-IDS using the Monitoring Interface. ...	97
Figure 34: Leonardo's NexGen SOC overview.....	124
Figure 35: Leonardo's NexGen SOC Service Lines. ....	125
Figure 36: Leonardo's LVS activities. ....	127
Figure 37: Data collection and storage system.....	129
Figure 38: Threat detection tools.....	130
Figure 39: Cyber risk analysis. ....	130
Figure 40: Cybersecurity terminology representation. ....	131
Figure 41: 3D representation of attacks. ....	131
Figure 42: Vulnerability reports. ....	132
Figure 43: Initial setup of JR Cyber Test and Training Centre. ....	134
Figure 44: Network topology of VICOM's Secure Industry 4.0.....	145
Figure 45: Overview of TSOOpen.....	150
Figure 46: CETIC portable edge simulator .....	157
Figure 47: Approver SAST Architecture .....	159

## List of Tables

Table 1: Contributed assets and learning contents from partners.....	5
--	---



## Chapter 1 Introduction

SPARTA partnership activities wish to strengthen and consolidate the existing ecosystems and help those fruitfully cooperate at local, national, European and international level.

Similarly, SPARTA resources can be an instrument to enhance the coordination at European level, consolidating European Digital Strategic Autonomy also through strong capabilities of its Member States.

There is a clear understanding that the limited budget available in SPARTA can only be considered as a catalyst to develop and consolidate the national/local ecosystems (considering the different levels of integration that each Member State aims at).

In particular, we believe we structured the networking activities to maximize the impact of the available resources.

We found several activities could benefit from clustering as well as integration efforts. We considered the work around several pillars:

- **Infrastructures.** We plan to integrate the tools available in SPARTA among partners. The Joint Competence Centre Infrastructure will be the basis for supporting research and innovation capabilities as well as to extend the services that can be offered to third parties.
- **People.** We integrate the organizations in SPARTA with other organizations as associates that aim to actively contribute to the SPARTA activities. This will strengthen the ecosystem. This is done starting from local needs as well as global ones.
- **Networking.** The SPARTA community needs to interact with the other stakeholders at National, European and International level. This is particularly true of the cooperation with the three other pilots and ECSO.

When dealing with the infrastructure the plan is to have a list of tools available to the SPARTA partners with a certain level of integration. The infrastructure consists at least of a workbench with the development tools, a virtual education centre and a cyber range.

When dealing with the people and organizations, SPARTA considered that we need strong national ecosystems, well connected and integrated at European level.

In each country we plan to make growth a coherent hub for cyber security with the main players are active and cooperating, involving as much as possible governmental institutions, industry stakeholders, academic references, and user associations.

Special attention is also given to young researchers and practitioners that represent the research and innovation workforce of the future.



## Chapter 2 Joint Competence Centre Infrastructure

### 2.1 Purpose

One of the objectives for SPARTA is to strengthen cybersecurity capabilities across the EU and closing the cyber-skills gap. In order to boost fundamental capacities and to lower the said skill gap, the Joint Competence Centre Infrastructure (onwards, JCCI) will offer leverage and horizontal domain synergies among organizations. The idea for JCCI is to become a reference location for companies and a research experimentation platform. Start-ups and SMEs will have infrastructure and technologies available through a catalogue, managed by local clusters and authorities.

### 2.2 JCCI components

The JCCI will be formed by 3 main components: a workbench for a shared and distributed testbed where computation and communication resources can be shared, a virtual learning centre to share and spread knowledge for learning purposes, and a federated cyber range with different scenarios to gain skills in cyber-attacks and defences (Figure 1). The different components will consist of integrations of existing means of SPARTA partners, but clustered and available through a web application that either will give direct access or will redirect to the corresponding access site. The aim of the JCCI would be to ease collaboration among them and to allow external organizations to access these shared facilities.

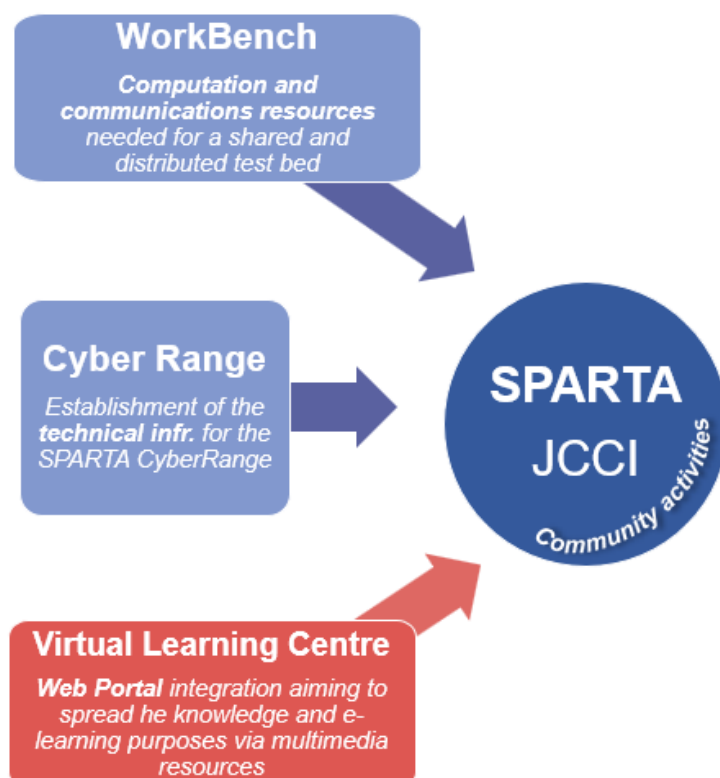


Figure 1: Components of the Joint Cybersecurity Centre Infrastructure.



### 2.2.1 WorkBench

The WorkBench will gather computation and communication resources needed for a shared and distributed test bed. As mentioned before, the WorkBench will be a compound of already existing assets from the partners, and they will be offered through a common platform. So far, **16 partners have contributed 30 assets' information** to the common asset inventory. For that, a document template was prepared with specific parameters that each partner had to fill in about the resources they owned, and how they could be shared and utilized by others. Among these assets, there are solutions for co-creation processes, secure hosting/storage, collaborative platforms, large scale experimentation equipment, intrusion detection systems, cyber-incident detection, monitoring systems, standards compliance, benchmarking, evaluation/certification, etc. Moreover, partners have contributed extensive information about their computing equipment. The integrated document can be found in the Annex.

### 2.2.2 Virtual Learning Centre

The Virtual Learning Centre will be a web portal integration aiming to spread the knowledge and e-learning purposes via multimedia resources. This will be available through a web portal, either openly or with specific requirements for access. These requirements will be detailed in the web application on the details area.

So far, **7 partners** have contributed their learning contents to the common learning catalogue. For that, a document template was prepared with specific parameters that each partner had to fill in about the learning resources they owned, and how they could be shared and utilized by others. Among the learning contents, there are online courses, in-person courses, hackathons, competitions and practical courses, which will offer a variety of resources available to share or access under certain conditions.

This integrated document can be found in Annex. The catalogue will be expanded as more contributions are gathered in the following action steps.

### 2.2.3 Cyber Range

Based on the asset inventories from Section 2.1, and once the WorkBench is outlined, it will be possible to select a subset of the testbed to be included in the cyber-range of SPARTA. These already existing cyber-range facilities will be united in a federated and distributed way. Moreover, based on the hands-on section of the Virtual Learning Center, different scenarios will be built for cyber-range training. So far, these testbeds have been pre-selected for the CyberRange: VICOM's Secure Industry 4.0 and TECNALIA's Smart Grid Facilities, Industrial Blockchain Facilities, Automotive Cybersecurity Facilities and Cyber Range Facilities, and the KYPO cyber-range.

A quick summarized overview of all contributed assets and learning contents can be seen on Table 1.

Partner	Assets for workbench	Keywords	Learning contents	Cyber-range?
L3CE	SENER	Center of excellence	-	
INRIA	LHS NGE	Data collection, secure hosting/storage, large-scale experimentation	4 online courses	
	LHS RBA	HW security evaluation, ransomware IDS		
TEC	IDSOTER	IDPS, electrical network and equipment		



Partner	Assets for workbench	Keywords	Learning contents	Cyber-range?
	OPENCERT	Assurance cases, Standards Compliance, Assurance Accountability, GSN	5 in-person courses	✓
	SABOTAGE	Fault Injection, Simulation, Safety		
	Smart Grid Facilities	Machine Learning, Honeypots		
	Industrial Blockchain Facilities	DLT, Blockchain		
	Automotive Cybersecurity Facilities	ECUs, V2V, V2I		
INOV	BP-IDS	Intrusion detection, Incident detection, Business processes	1 online course	
CESNET	Nemea	Flow traffic analysis, Network monitoring	1 CTF competition	
	IPFIXcol	Flow record collector		
	Warden	Network security, event sharing platform		
	NERD	Network entity reputation DB		
LIST	Node in Infrachain Blockchain	Blockchain, smart contracts	-	
UKON	Visual Computing Center for Cybersecurity	Powerwall, Control Room, Machine Learning Infrastructure	1 visual analytics competition	
UBO	IT-Security Awareness Pentesting Framework	Employee awareness assessment, Intrusion Detection, Phishing	-	
TUM	Malware Zoo	Large-Scale Malware Analysis	4 in-person courses	
LEO	Cyberthreat Intelligence Services	Vulnerability detection, attack detection, monitoring, Darknet, real-time analysis, Fraud detection	-	
	Intelligence enabled Next Gen SOC	Security operation center, dynamic risk assessment		
	Security Evaluation Facility	Security evaluation		
CNR	Cybersecurity Osservatorio	Cyber threats, risk assessment, malware detection, CVE, CWE, spam analysis, security reports	-	
JR	CTTC	Data collection, data analysis, IoT security, intrusion detection, APT	-	



Partner	Assets for workbench	Keywords	Learning contents	Cyber-range?
CEA	DeepRed	Security evaluation, Software verification, Binary analysis	3 in-person courses, 1 hackathon	
VICOM	Secure Industry 4.0	Equipment and process monitoring, flexible robotics, big data analytics	-	✓
KYPO	-	-	-	✓
CETIC	VaCSinE	Adaptive continuous security orchestration, heterogeneous hardware, edge, fog, NFV, SFC, TOSCA	-	
Fortis	AutoFOCUS3	Mode-Based Engineering Tool, Safety and Security, Embedded Systems	-	
UniLU	TSOPEN	Logic bomb detection, Android Security	-	
	SafeCommit	Vulnerability Detection Tool For DevOps Communities	-	
CINI	Approver	Mobile Security, Mobile Application Risk Assessment, Vulnerability Analysis, SAST, DAST		

Table 1: Contributed assets and learning contents from partners.

## 2.3 Tentative usage workflow

As mentioned, the three components of the JCCI will be available through a web application that can be accessed by any organization. A first conceptual draft of how the usage workflow will be can be found on Figure 2. Different customers (either partners or external organizations) could access a list of all available resources. This index would be available through SDLs that would return the existing labs and learning equipment, contents and datasets, as well as workbench resources and how to access them. These could either be directly accessed or the site would redirect the organization to the corresponding place.

When requested, the list of available resources could appear with just a few hints of what is available. These could be filtered by different parameters or tags, and a button for either directly downloading or requesting access to the resource (Figure 3). Then, a particular entity from the list could be expanded when clicking on it (Figure 4).



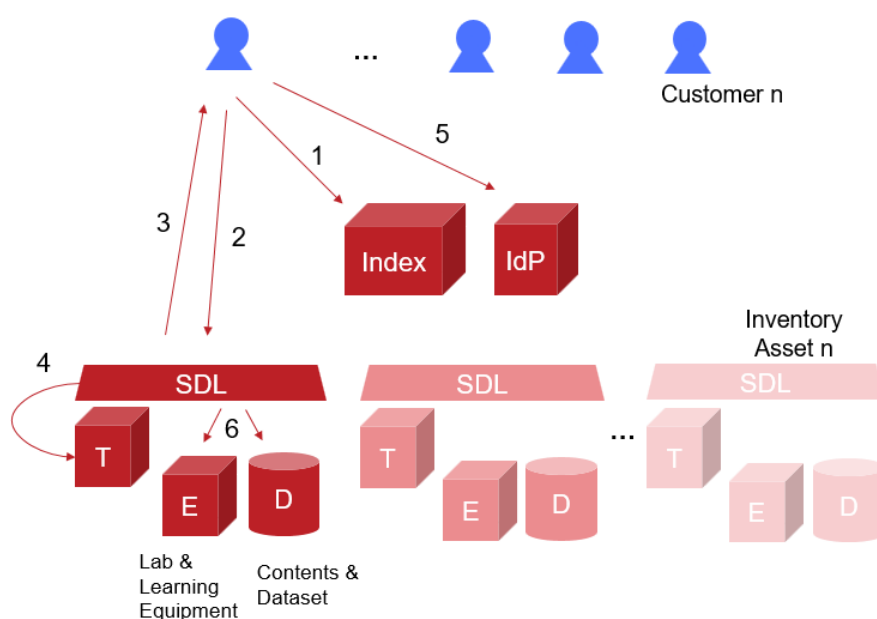


Figure 2: Conceptual draft of usage workflow. IdP = identity provider, SDL = service description language.

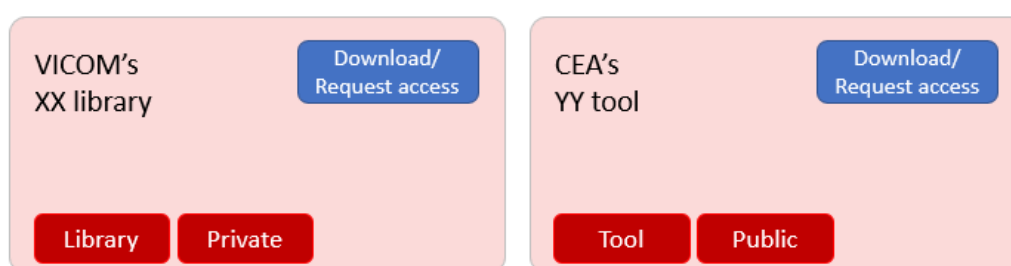


Figure 3: Example draft of a list of available resources on the web app.

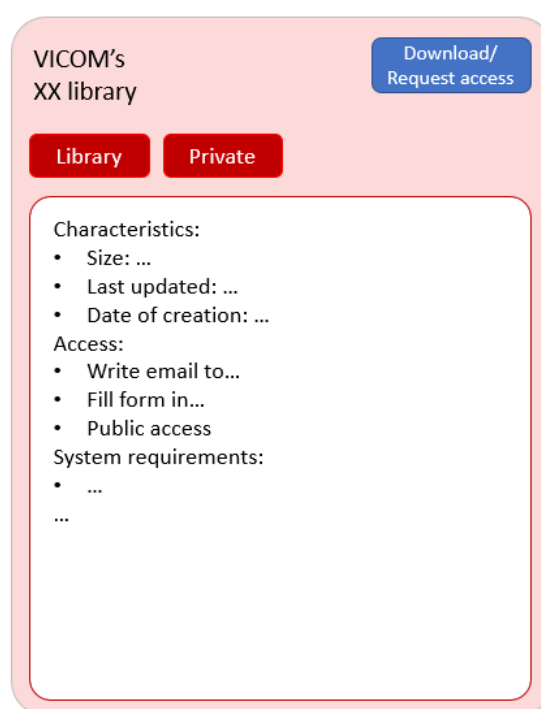


Figure 4: Expanded details of an available resource.



## 2.4 Next steps

For steering the creation of the SPARTA JCCI, our tentative next steps are:

### 2.4.1 *State of the Art*

In order to consider some possible solutions or approaches for our final goal, firstly an overview will be obtained on a few matters:

1. Cybersecurity information sharing protocols (considering CSIRT standards, as information should also be available to them).
2. Best practices for federation mechanisms and their different scopes.
3. Analysis of business models (including ticketing and renting schemes).
4. Analysis of Service Description Languages, considering also the interactivity issue of SDLs.

### 2.4.2 *Hands-on tasks*

Once the state of the art has been reviewed, partners will start building the JCCI by:

1. Analysing the features of the Asset Inventory:
  - a. Characterization of possible common services
  - b. Common language for assets definition
  - c. Suggested integration levels
2. Selecting and uploading the assets catalogue in a web application as main index.



## Chapter 3 Clustering activities at national, European and international level

### 3.1 SPARTA ecosystem

SPARTA is a Pilot for a network of competence centres. SPARTA has an initial set of 44 partners joining the grant agreement.

In most of the 14 countries represented in SPARTA, we ideally collected a core set of partners from research (RTO), academia, governmental agencies and industries.

The picture below describes the partners in SPARTA (per country, per typology)

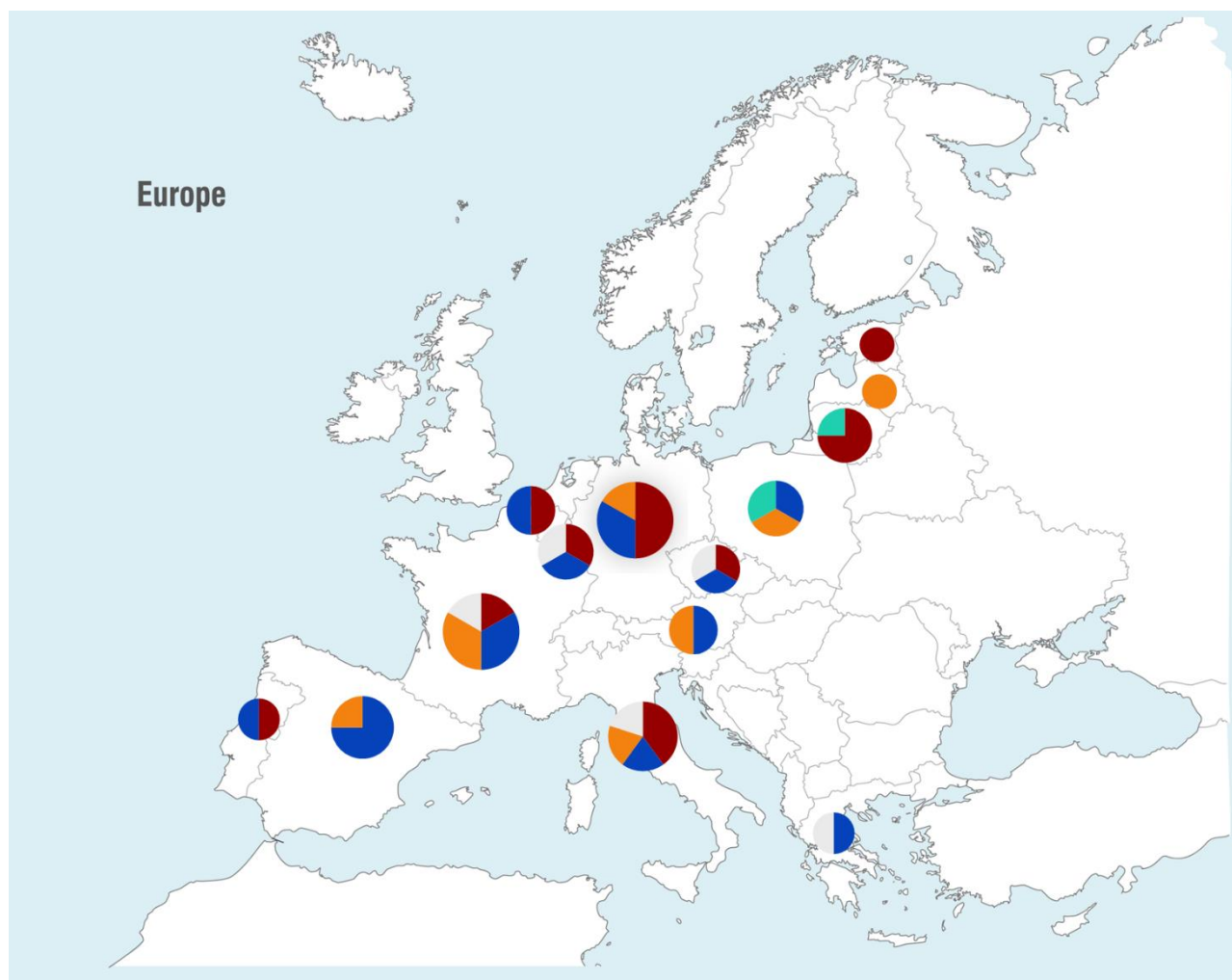


Figure 5: SPARTA ecosystem



This seems to be the optimal size w.r.t. manageability and creation of the critical mass to achieve its objectives. Being community building, one of the main goals, it is useful for several reasons to consider also other forms of involvement in the Network.

In particular, we consider the notion of associates/friends, not formally bounded by the Grant Agreement, yet with the possibility to have active roles in the Network activities.

This allows to create a wider research community, strongly linked to the Network with several levels of involvement. The notion of associate researcher will be also useful to cover research expertise that could be necessary due to the changing of the technologies and research priorities during the Network. Indeed, Network researchers plan to continuously monitor the progress of the Network as well as the excellence and appropriateness of the Activities and Programs. This will allow the Network to better adapt and evolve, and thus reducing the risks of not achieving the stated research goals. The benefits/duties for associated partners are the followings.

Benefits for associated partners:

- Associate partners will be invited to attend open SPARTA meetings.
- Associate partners will be able to use, connect to and experiment with and contribute to the facilities of the JCCI (see the specific rules after)
- There will be a dedicated page on SPARTA web portal which lists all associate partners.
- Associate partners are invited to use the SPARTA Associates logo.
- Associate partners are invited to attend the training and educational activities.
- Associate partners are invited to contribute to roadmapping activities.
- Associate partners can be funded to attend the SPARTA thematic workshops.
- Associate partners will be included in the appropriate SPARTA mailing lists upon request.
- Associate partners will be granted access to the project collaboration platform and the SPARTA Web Portal (based on certain conditions)

Duties for associated partners:

- Associated partners can actively participate into the Programs and Activities of SPARTA.
- Sign a Non-Disclosure Agreement (NDA) for seeing confidential information of the SPARTA Core partners or of other associated partners.
- Associate partners are required to deliver reports documenting their involvement in the SPARTA activities in which they participate.
- Associate partners should acknowledge the SPARTA project if they receive funding for those activities.
- Associated partners need to produce original invoices/receipts when claiming for the refund (the actual reimbursement method will be defined for each partner).
- Associated partners should in any case not harm the SPARTA consortium partners with their activities.

SPARTA might provide a symbolic funding for associate partners (a few thousands EUROS). This funding is only for reimbursement of expenses for travel and accommodations, for attending SPARTA monthly events.

In the following figure, we list the current associates.



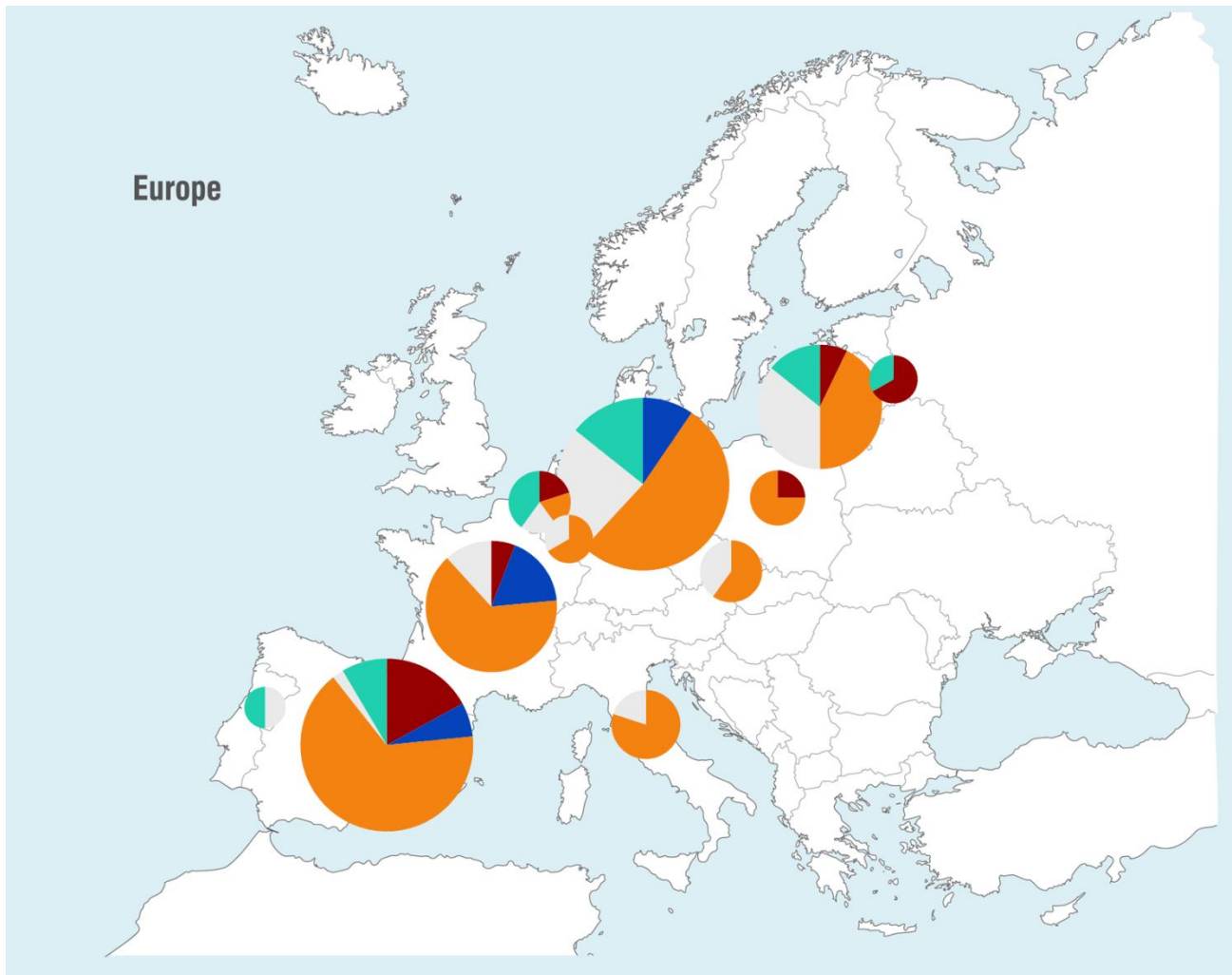


Figure 6: SPARTA associates

We also designed a lighter form of participation called Friends. This does not entail active commitment to specific activities in the Network, still allows the friends to provide/receive benefits for the Network.

This will allow the Network to better adapt and evolve, and thus reducing the risks of not achieving the stated goals.

Benefits for SPARTA friends for:

- Events:
  - SPARTA friends are allowed to attend SPARTA Days.
  - SPARTA friends are allowed to attend SPARTA Workshops upon invitation from Coordinator
- Roadmap and Programs
  - SPARTA friends can provide inputs to the Roadmap
  - SPARTA friends are entitled to receive late information on Roadmap outputs
  - SPARTA friends are entitled to receive late information on programs outputs
- Communication:
  - SPARTA friends logo will appear in the main Sparta web site (Sparta.eu)
  - SPARTA friends are invited to use the SPARTA Friends logo
  - SPARTA friends will be included in the appropriate SPARTA mailing lists upon request.



- JCCI:
  - SPARTA friends will be granted access to the project collaboration platform and the SPARTA Web Portal based on general conditions

Duties for SPARTA friends:

- When requested, sign a Non-Disclosure Agreement (NDA) for seeing confidential information of the SPARTA partners or of other SPARTA friends.
- SPARTA friends are required to deliver reports documenting their involvement in the SPARTA activities in which they participate.
- SPARTA friends should acknowledge the SPARTA project if they receive funding for those activities.
- SPARTA friends need to produce original invoices/receipts when claiming for the refund (the actual reimbursement method will be defined for each partner).
- SPARTA friends should in any case not harm the SPARTA consortium partners with their activities.

## 3.2 National level

This section describes the clustering situation at national level, the SPARTA actions taken and future plans from SPARTA partners and associates.

### 3.2.1 France

#### 3.2.1.1 Current status

In France the national authority for cybersecurity is ANSSI. Under its auspices, several clustering activities had been put in place before 2019. SPARTA, has been reaching out to a wide variety of them:

- **System@tic cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects. Link with FUI, FSN and PIA French funding schemes.
- **Image et Réseaux cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects.
- **SAFE cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects.
- **CNRS:** major host for academic research in joint units with universities or own units (e.g. LAAS), contribution to programmes and research output. The Pré-GDR Security created by «l'Institut des sciences de l'information et de leurs interactions » has launched several working groups to address security-related scientific challenges (secure coding, cryptography, formal methods for security, privacy, multimedia security, network & infrastructures & Software & Systems security)
- **IRT SystemX:** research and demonstration/communication platform, additional funding and hosting for dedicated specific projects and/or teams for collaborative work. Link with ANR funding schemes.
- **Ile de France region:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level.
- **Brittany region:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level



- **Pole d'Excellence Cyber:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level. Link with the military ecosystems and the French military procurement agency.
- **Direction Générale de l'Armement (DGA):** for additional funding of specific programmes, with a focus on PhDs. Link with the military ecosystem, both for research and use, and large development programmes. Link with RAPID and ASTRID French funding schemes.
- **COFIS:** French industrial security sector committee, aiming at developing the competitiveness of companies and SMEs, and defending their position in the international markets.

### 3.2.1.2 SPARTA's actions

SPARTA project has established contact with the following organisations to further develop the national cluster for France:

- Paris Region
- AdaCore
- Irisa
- Loria
- Cybersecurity Institute, Univ Grenoble Alpes
- LAAS
- Quarkslab
- AMOSSYS
- Airbus
- UTAC-CERAM

Several interactions have also taken place with the newly-founded CSF industry cluster, and its proposed French Cyber Campus report<sup>1</sup> directly cites SPARTA as a “major initiative”.

SPARTA partners are strongly committed to consolidate the France ecosystem and SPARTA would be the main instrument.

## 3.2.2 Belgium

### 3.2.2.1 Current status

In Belgium network cybersecurity is overseen by the Centre for Cybersecurity Belgium (CCB). CCB is the central authority for cybersecurity in Belgium and manages the Computer Emergency Response Team (CERT) for the purpose of carrying out activities relating to the detection, observation and analysis of online security problems. CCB has the following network related responsibilities:

- Monitoring, coordinating and supervising the implementation of Belgian cyber security;
- Managing the various projects on the topic of cybersecurity using an integrated and centralized approach;
- Ensuring coordination between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
- Formulating proposals aimed at adapting the regulatory framework in the field of cybersecurity;
- Ensuring crisis management in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;

---

<sup>1</sup> <https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport.pdf>



- Preparing, disseminating and supervising the implementation of standards, guidelines and security standards for the various information systems of the governments and public institutions;
- Coordinating the Belgian representation in international cybersecurity forums, coordinating the monitoring of international commitments and national proposals on this subject;
- Coordinating the security evaluation and certification information and communication systems;
- Informing and raising awareness among users on information and communication systems.

CERT.be is as a neutral specialist in Internet and network security that is responsible for:

- coordination in the event of cyber incidents;
- advice about finding a solution when cyber incidents arise;
- support to prevent these security incidents occurring

CCB is working on the definition of a cybersecurity scheme for SME at the federal level in Belgium. It is called Cyber Fundamentals and aims to support SMEs in building achievable cyber security. It will contain many basic components of ISO 27001, albeit with an important focus on cyber security and a specific focus on: "Current and effective measures, which are generally accepted as minimum measures, an average company can implement, within acceptable budgets, which can achieve the best possible results, and are measurable".

In the Walloon Region of Belgium the "Agence du Numérique" (ADN), responsible for digital public policy, is preparing a cybersecurity label for SME called Keep it Secure (KIS) based on CIS 20 controls and the NIST cybersecurity framework version 1.1. Although the cybersecurity label is very general, some of the CIS 20 controls are network related such as "limitation and control of network ports, protocols and services", "secure configuration for network devices such as firewalls, routers and switches", or "wireless access control". The KIS initiative is led by "Agence du Numérique, but CETIC is responsible for defining the contents of the KIS label and evaluating auditors that will carry out KIS evaluations. ADN is also involved in the CYBER interreg project on Regional policies for competitive cybersecurity SMEs. CETIC is acting as a sub-contractor in this project especially related to the KIS label. A presentation of the SPARTA project was made at one of the CYBER consortium meetings.

### 3.2.2.2 SPARTA's actions

SPARTA project has established contact with the following organisations to establish the national cluster for Belgium:

- CCB: collaboration is progressing in two areas. The first area is the cybersecurity competence network that is being followed by CCB. We are keeping them informed of SPARTA activities with respect to the competence network. The second area is collaboration to align the regional KIS label with the federal Cyber Fundamentals certification scheme. The two initiatives are complementary: KIS is lightweight approach aimed at helping SME understanding how to protecting themselves, whereas the federal Cyber Fundamentals is a certification scheme. This is described in more detail in D11.1.
- Agence du numérique: A presentation of the SPARTA project was made at one of the CYBER consortium meetings for ADN.
- INFOPOLE Cluster TIC: partners of the grappe cybersécurité are regularly informed of SPARTA activities
- UNiversité de Namur/CRIDS: we have regular collaboration between CETIC and UNamur/CRIDS on the topic of privacy.

We have already identified a few key cybersecurity actors that could become associate partners of SPARTA: Multitel research center, Université Catholique de Louvain, LSEC, BlueKrypt and Guardis.

Here are some of the planned activities:

- Organisation of the SPARTA week in Brussels end of February



- Collaboration with ADN, CCB and BELSPO of the cybersecurity competence network
- Adding some Belgian companies/organisations are SPARTA associates
- Collaborating with ECSO on the cybersecurity initiatives for SME

### 3.2.3 Greece

#### 3.2.3.1 Current status

In Greece the National Cyber Security Authority (NCSA) was established in the Ministry of Digital Policy Telecommunications and Media following a Presidential Degree. NCSA is responsible for coordinating all competent Ministries and independent authorities of Greece, in order to take all necessary steps towards a secure Greek Cyber space. In close cooperation with the National CERT and National Cyber Security Incident Response Team (NCSIRT is also the Cyber Defense Directorate of the Hellenic Armed Forces), NCSA will have to handle all national critical incidents. NIS directive takes effect in Greece although there is a lot of mandatory steps need to be completed, e.g. identification of essential services. There is also a published National Cyber Security Strategy, referring to the establishment of a national incident notification procedure and legislation regarding rules and penalties. In Greece there is also established the Greek Cybercrime Centre. Among other activities, in the Centre deals, ([www.cybercc.gr/en/](http://www.cybercc.gr/en/)), with the DG-HOME funded project which is aimed primarily at improving research and education, maintained by Center for Security Studies and Hellenic Police. The objectives of GCC are to i) advance cyber security training and University education in Greece, ii) improve research in focused areas of cyber security and crime, iii) mobilize the Greek constituency in the area of cyber security and crime and iv) collaborate with similar centres so as to maximize the uptake of the results. Furthermore, there are several other cyber security activities such as the Annual Cyber defence national exercise “PANOPTIS” the KEMEA annual conference on CI protection, and the Hellenic Team of European Cyber Security Challenge.

#### 3.2.3.2 SPARTA's actions

- SPARTA plans the organization of a monthly workshop in year two.

### 3.2.4 Austria

#### 3.2.4.1 Current status

In Austria there is no single national authority responsible for cyber security matters, instead competences are split mainly between the three entities Bundeskanzleramt (BKA) which is the federal chancellery, the Bundesministerium für Innern (BMI) [ministry of interior], and the Bundesministerium für Landesverteidigung (BMLV) [ministry of defence]. In the national Cyber Security Strategy<sup>2</sup> (dated from 2013), a so-called operative coordinating structure is defined. Its goal is to constantly monitor and assess the situation in cyber space and collaboratively define actions whenever necessary. The BKA also runs the CERT.AT. It is the central point of contact in case of cyber incidents. Within the so-called Austrian Trust Circle security experts of different sectors are connected. An energy CERT is also established; other sector CERTs are being in preparation.

The BMLV is organiser of the yearly IKT-Sicherheitskonferenz, the largest conference of that kind in central Europe and the most important regular meeting point for the Austrian cyber security community.

---

<sup>2</sup> Austrian Cyber Security Strategy

<https://www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21>



The Austrian Cyber Security Platform CSP-AT is a networking initiative triggered by BKA with two working meetings per year.

The WKO (Chamber of economy) runs the so-called Cyber Security hotline. In case of cyber incidents, companies quickly can get help from experts listed there.

### 3.2.4.2 SPARTA's actions

SPARTA has established contact with the following organisations to support the community building within Austrian Cyber Security stakeholders:

- Bundeskanzleramt (BKA)
- BMLV (MoD)

We have already received a sign of interest in joining SPARTA from:

- Bundesministerium für Innern (BMI)

Partner JOANNEUM RESEARCH gave a presentation introducing SPARTA at IKT-Sicherheitskonferenz 2019. A SPARTA workshop in Austria is planned to be organised in May/June 2020 together with the presentation of the Austrian Cyber Security Study 2020.

SPARTA will establish and maintain contacts to relevant parts of the cyber security community in Austria, like authorities, universities, universities of applied science, research and competence centers, industry as well as SMEs. Special attendance will be given to the recently established Cyber Security Campus Graz.

## 3.2.5 Poland

### 3.2.5.1 Current status

The key objective of the National Framework of Cybersecurity Policy of the Republic of Poland is to expand the national cybersecurity system and ensure a consistent approach taken across the Republic of Poland. National Framework of Cybersecurity Policy requires involvement of different actors who are either public sector, telecommunications sector as well as Trust Service Providers and competent ministers responsible for preparing proposals of legal changes in the field of cybersecurity.

Development of the cybersecurity system at the national level also entails the further development of structures dealing with cybersecurity at the operational level, including the national level CSIRTs, sectoral incident response teams (sectoral CSIRT), information exchange and analysis centres (ISAC). To make these developments possible the Government introduced new legislation setting out the revised competencies of the relevant institutions. In particular, three national level CSIRTs have been assigned to civilian, military and government sectors. The civilian sector forms the constituency of CSIRT NASK, which operates within the structures of NASK (Research and Academic Computer Network) — a SPARTA consortium member and a research institute which conducts scientific studies, operates the national “.pl” domain registry and provides advanced IT services.

**CERT Polska** (<https://www.cert.pl/en/>) is a core part of CSIRT NASK and the oldest CERT in Poland. Since its creation in 1996, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. CERT Polska also conducts extensive security-related R&D, supported by the research staff of the institute, particularly the Network and Information Security Methods Team.

In the framework of cooperation between the central government administration and the local government administration, the national government strongly supports development of security clusters:



**Poznan Supercomputing and Networking Center (PSNC)** <http://www.man.poznan.pl/online/en/>. Since 1993 integrating and developing the information infrastructure for science has been the mission of Poznan Supercomputing and Networking Center (PSNC) affiliated with the Institute of Bioorganic Chemistry at the Polish Academy of Sciences.

**CYBERSEC HUB** (<http://cybersechub.eu/>) is a network of integrated activities supporting and promoting companies in Malopolska Region from cybersecurity sector.

### 3.2.5.2 SPARTA's actions

SPARTA project has established contact with the following organisations to establish the national cluster for Poland:

- AGH
- ENERGA Group
- The John Paul II Hospital in Krakow
- PKP Informatyka

In 2020, NASK will be organizing a SPARTA workshop collocated with SECURE 2020 – one of the largest cybersecurity conferences in Poland, organized by NASK/CERT Polska. This event is expected to disseminate information about SPARTA in the cybersecurity community and lead to further growth of the cluster.

## 3.2.6 Germany

### 3.2.6.1 Current status

In Germany there are multiple competence centres for cybersecurity, with activities in a wide range of research topics. For instance, Center for Research in Security and Privacy (CRISP) has a core topic "Security at Large", focusing on security of large systems consisting of multiple interacting components. They bring together experts from multiple areas: engineering, philosophy, physics, psychology, law and economics through interdisciplinary projects. CISA Helmholtz Center in Saarbruecken combines theoretical topics with innovative application-oriented research projects in cybersecurity and privacy. Some of their core research topics are: Secure and Privacy-Friendly Information Processing, Threat Detection and Defenses, Secure Mobile and Autonomous Systems and Empirical and Behavioral Security. Furthermore, this Center has an additional focus on technology transfer and societal outreach. In addition, Competence Center for Applied Security Technology (KASTEL) addresses security problems of the interconnected systems under a motto "Comprehensible security in the networked world". Their goal is to "develop a widespread approach instead of isolated partial solutions". This network pays special attention to critical infrastructures, such as industrial production, energy and networked mobility.

The above mentioned centres focus on basic research whereas the security hub in the metropolitan area of Munich comprises security research, security industry as well as big companies which use security products like automotive and aeroplane OEMs, healthcare sector, telecommunication as well as industrial automation or electricity. The Munich hub already established different cluster initiatives to connect academic research (institutions) with industrial partners or provide consulting services in case of cybersecurity related incidences (incident response):

- The Munich Center for IT-Security (Münchner Sicherheitsnetzwerk) coordinates a lot of (around 100) global and local partner companies and research institutions located in the metropolitan area around Munich.
- Platform for Cybersecurity of the Center of Digitalisation Bavaria (ZD.B), a Bavarian cooperation- and research network, funded by the Bavarian government. The goal is to support different projects between industry, research and governmental partners. An additional goal of ZD.B is to fund and support young scientists.



- The working group “Trust and Cybersecurity” of the “Münchner Kreis” connects even more organizations and enterprises spread around Germany.
- The Bavarian Landesamt für Sicherheit in der Informationstechnik (LSI) aims to protect and defend governmental IT infrastructures and acts as a council in case of security breaches of local authorities.
- ZITIS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) aims to enable law enforcement to use and enhance their technical capabilities to defend against cybercrime and cyberespionage. ZITIS is a branch of the German Federal Ministry of the Interior.
- CODE, funded by the German Ministry of Defence, is a research activity located at the university of armed forces in Munich to educate soldiers in cybersecurity topics.

Munich was already a strong security hub within Germany and became even stronger benefitting from the close collaboration with SPARTA. During the first year, SPARTA activities have influenced this particular hub considerably, e.g. by discussing and elaborating SPARTA Roadmap topics within the different above mentioned institutions, or by starting new cluster R&D activities which will be funded by the Bavarian government, like AI certification, or by establishing new research clusters which applied for governmental funding for SPARTA Roadmap topics like trusted electronics and post quantum computing.

Another regional hotspot for cyber security in Germany is the Bonn/Rhein-Sieg area which is the home of

- research and education institutions working in cyber security (University of Bonn, several Fraunhofer Institutes, Hochschule Bonn-Rhein-Sieg, University of Applied Sciences (H-BRS))
- industry players like Deutsche Telekom, DHL / Deutsche Post
- Governmental agencies like the Federal German Office for Information Security (BSI).

The development and integration of science, research & education, business, authorities and public institutions, as well as other aspects of cyber security in the Bonn/Rhein-Sieg region are promoted by the Cyber Security Cluster Bonn e.V.

### 3.2.6.2 SPARTA's actions

Besides the above already mentioned activities to strengthen the existing Munich hub (one SPARTA PI is the spokesperson of the Munich security network, as well as of the Platform for Cybersecurity and the Security Working group of the Münchner Kreis.) SPARTA members have established contact with the following organisations to build the national cluster for Germany:

- With the three national funded security research centres KASTEL, CRISP (now called ATHENE) and CISPA
- With the security initiatives within the metropolitan area of Munich: SNM, ZD.B. Münchner Kreis, ZIZIS, Code
- With national Cybersecurity Agencies: BSI, Agency for innovation in Cybersecurity (just started funded by the ministry of the Interior and Defense), with the National Cybersecurity Council
- With new clusters, started in 2019: Cyber Security Cluster Bonn e.V.
- With industrial associations: bitkom, BDI, ASW Bundesverband, IHK Bonn/Rhein-Sieg

We have already received a sign of interest in joining SPARTA from:

- UNIVERSUM Business GmbH
- KASTEL

The plan is to keep on working on the SPARTA project level, developing more collaborations with other cybersecurity initiatives within Bavaria and Germany.



### 3.2.7 Czech Republic

#### 3.2.7.1 Current status

Cybersecurity networking in Czech Republic appears and is being developed at several levels. At the national and governmental level, the Czech Republic's National Cyber Security Strategy and the associated Action Plan were drafted by the Czech National Security Authority (NSA) and adopted by the Government in 2015. Both cover the years 2015 to 2020. CERT & CSIRT Capacity Building Strategy defined in the Action Plan 2015-2020 propose enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security and in developing an effective cooperation model at the national level among the cyber security actors – CERT and CSIRT teams. Namely, the most relevant teams, the CSIRT.CZ (operated by CZ.NIC) and govCERT.CZ (operated by NCISA) establish various partnerships with academic as well as industrial partners (e.g. Microsoft, Cisco) via Memoranda of understanding or via joint projects. Building of national competence centres is also supported by the Czech government through Technology Agency of the Czech Republic and the Security Research Program of the Ministry of the Interior. At the industrial level, there exist Czech ICT alliance and ICT union, however these consortia cover whole ICT and do not specifically focus on cybersecurity.

The private cyber security cluster operates through the Network Security Monitoring Cluster (NSM Cluster; <http://www.nsmcluster.com/en/>) covering the region of South Moravia. In 2019, National Cybersecurity Competence Centre (NC3) was established to connect partners from various research and industry sectors. SPARTA participates in NC3 through its members CESNET and Brno university of technology.

At the academic level, CESNET acts as a common platform where various research centres and universities meet and cooperate on joint cybersecurity projects utilizing their specific competences. In parallel to the above levels, various cybersecurity players meet at the local cybersecurity conferences such as C2S2, QuBit, ISS world.

#### 3.2.7.2 SPARTA's actions

SPARTA project has established contact with the following organisations to establish the national cluster for Czech Republic:

- AT&T
- National Cyber and Security Agency (NÚKIB)
- Státní pokladna Centrum sdílených služeb, s. p.
- Ministry of Defence and Armed Forces of the Czech Republic

Ministry of Defence and Armed Forces of the Czech Republic has become an Associate partner as well as a member of Arbitrage group for the T-SHARK programme in WP4. SPARTA member, CZ.NIC is in a close contact with ICT standardization organisations. In this regards, CZ.NIC strives to acquire new SPARTA Associated partners, especially The Electrotechnical Testing Institute (EZÚ), which is among others the Conformity Assessment Body (CAB) for eIDAS certifications as well as ISO/IEC 27001 (Information security management), ISO/IEC 12207 (Software life cycle processes) and ISO/IEC 15288 (Systems and software engineering – System life cycle processes).

SPARTA members, namely CESNET and CZ.NIC participated in C2S2 meeting to discuss national plans in cybersecurity with governmental cybersecurity bodies (govCERT, national CERT, Army CERT, ...).

Brno university of technology got in touch with Masaryk university regarding their Cybernetic polygon to connect the polygon with Brno university of technology network lab and join this infrastructure into SPARTA.

We plan to on-board National Cyber and Security Agency as a SPARTA Associate partner as well as other organisations that we are in touch with as SPARTA friends. We are planning to get in touch with the Czech Accreditation Institute (ČIA), which is active as a national supervisory body for various



certifications, including those according to the Cyber Security Act. We also want to further develop cooperation and support of governmental cybersecurity bodies and include them into the roadmap process organized by SPARTA. Last but not the least we will reach out to other organizations in the Czech Republic through a SPARTA workshop, which we plan to collocate together with one of the CESNET cybersecurity conferences.

### 3.2.8 Lithuania

#### 3.2.8.1 Current status

Lithuanian is currently on the process of implementation of national cybersecurity strategy (hereinafter Strategy) under the lead of the Prime Minister's Office and the Ministry of National Defence (MoND). The Strategy defines the most important pillars of the national cyber security policy and is aimed at:

- strengthening the development of the state's cyber security and cyber defense capabilities preventing and investigating cybercrimes
- promoting cyber security culture and the development of innovations
- enhancing close private-public partnership (PPP) and international cooperation, and
- ensuring the fulfilment of international cyber security obligations within the country until 2023

The Strategy meets the provisions of the Program of the Seventeenth Government of the Republic of Lithuania, which was accepted by Resolution No. XIII-82 of the Parliament of the Republic of Lithuania of 13 December 2016

The Strategy is a key document which sets the aims and objectives of Lithuania's public and private sectors as well as research and educational institutions for the next five years. The Strategy takes a holistic approach, where cyber security is seen as an integral part of digital ecosystem rather than an independent national goal or as a set of tools designed for responding to challenges of the digital age.

Stressing the need for enhanced efforts to build national cybersecurity ecosystem Lithuanian government attracted key players in the field:

- **The National Cyber Security Centre at the Ministry of National Defence (NCSC)** (<https://www.nksc.lt>) is the main Lithuanian cyber security institution, responsible for unified management of cyber incidents, monitoring and control of the implementation of cyber security requirements, accreditation of information resources. NCSC mission to be the centre of cyber security expertise for effective cyber security incidents and a strong cyber security prevention system in the country. NCSC approved regulations provide for the following main operational goals of the institution:
  - implement a national cyber security policy
  - perform the functions of the Security Service
  - perform the functions of the national communications protection service
  - perform information dissemination, research and analysis on cyber security issues

Since the year 2018, the one-stop-shop principle of the NSCS provides assistance to the state and businesses institutions and residents. Within the limits of its competence, the NCSC makes decisions along with the state institutions and organizations and other economic entities on the issues of state information resources and critical information infrastructure of cyber security. NCSC is the main coordination body that takes leading role and responsibility for the successful implementation of national cybersecurity strategy.

- **The National Lithuanian Computer Emergency Response Team (CERT-LT)** under the Communication Regulation Authority The purpose of CERT-LT is to promote security by preventing, observing, and solving cybersecurity incidents and disseminating information on threats to information security. Its concrete tasks include the provision of capability to deal with network and information security incidents in Lithuanian public electronic networks and



it is further responsible for coordinating security and incident response measures across all Lithuanian networks. CERT-LT is additionally tasked with managing the reporting of cybersecurity incidents. Coordinates and collaborates with sub-national/sectorial incident-response organisations and reports to other authorities as required regarding the national level issues.

- **The Ministry of the Interior (Mol)** is responsible for the preparation of the Critical Infrastructure (CI) identification methodology and for presenting the list of CI to the Government for approval. Moreover, an officially approved list of critical objects and equipment is included in the Law on Enterprises and Equipment of Strategic Importance to National Security, which was originally passed in 2002. A detailed audit of CI assets was performed at least every two years with the possibility to update the list in response to any actual or expected changes in the threat environment. The last assessment and identification of CI assets took place in July 2016, including vulnerability/asset management plans and processes.
- **The Lithuanian Armed Forces Strategic Communications Department** is responsible for advice and coordination of military information activities by executing monitoring, detection and prevention of Information Operations and Psychological Operations directed to influence perceptions, attitudes and behaviour of targeted audiences in order to achieve political or military objectives.
- **The Cybersecurity Information Network.** Network was established in response to malicious attacks on strategic information systems and critical infrastructure, communication and coordination between relevant public and private sector actors. In the event of a communications disruption, mechanisms are in place to maintain the operational functionality of the national emergency communications network. That is why Ministry of National Defense has identified and mapped redundancy measures, both readily available digital networks and non- digital means for communication. This includes the Cybersecurity Information Network mentioned above.
- **The Safer Internet Center (SIC)** a multi- stakeholder consortium whose activities are:
  - awareness-raising;
  - hotline
  - helpline activities
  - promotion of youth's initiatives as well.

Since 2005, the European Commission sponsors a programme by SIC for raising awareness among school children. It brought together the private sector, the Ministry of Education and Science (currently leading) and the Communications Regulatory Authority.

- **The Lithuanian Research and Education Network (LITNET)** (<https://www.litnet.lt/lt/>) connects computer networks of all research, study and education institutions of Lithuania. LITNET CERT is the Computer Emergency Response Team of LITNET, targeting the fields of computer security incident response, forensics, detection and prevention and is devoted to attracting and retaining successful and responsible development to provide novel technology solutions to target groups.
- **The INFOBALT association** (<https://infobalt.lt>) is a locally and internationally recognized representative of Lithuanian ICT industry. INFOBALT Cyber Security Committee organizes and coordinates the activities of the Lithuanian ICT companies in the field of cyber security.

### 3.2.8.2 SPARTA's actions

SPARTA project has established contacts with the following organisations:

- INFOBALT association
- National Cyber Security Center at the Ministry of National Defence Republic of Lithuania)
- Strategic Communications Department (Lithuanian Armed Forces)
- JSC "Lithuanian Railways"
- LITNET Computer Emergency Response Team
- Debunk.eu



- DELFI
- NRD Cyber Security
- NCC Group Lithuania
- TELECENTRAS (Lietuvos Radijo ir Televizijos Centras)
- State Data Protection Inspectorate
- Vilnius Gediminas Technical University
- Lithuanian Defence and Security Industry Association
- Information security cluster

Lithuania is a small country in a population size and has limited human and financial resources to invest in a wide spectrum of technological advancement aimed at building cybersecurity capabilities. Nonetheless, Lithuania faces same number of security challenges as other EU countries do therefore the innovations have to play a critical role to ensure necessary protection of our society.

International collaboration putting stakeholders in the area together is essential for the small countries. Thus, SPARTA project brings new opportunities for the national clusters enabling them to benefit from SPARTA research programs results and latest developments of SPARTA network partners.

During the 2020 -2021 period, we are planning to implement national information security and information threats' detection and analysis research and education platform (hereinafter NAAS) that will enable to make a strong contribution in to development of modern national research and education ecosystem. NAAS business model is based on practitioners' competence and is founded on the portfolio of national research projects focused on the comprehensive threats intelligence application.

National cluster that unites four research organizations (Mykolas Romeris University, General Jonas Žemaitis Military Academy, Vilnius Gediminas Technical University, and Lithuanian Cybercrime Center of Excellence for Training, Research & Education) will take a leading role in coordination and implementation of NAAS activities:

- Training of professionals
- Scientific research / new concepts, methods development
- Collaboration with different groups of stakeholders (national institutions, EU bodies, end-users, EU clustering platforms and ecosystems)
- Innovation uptake/ EU research projects results exploitation
- Awareness

The initiative places a particular emphasis on the innovations uptake and results exploitation in the end- user operational environment therefore collaboration with SPARTA network and other CCN pilots (CONCORDIA, CyberSec4Europe and ECHO) is critical for the national clusters to address the access to the EU knowledge base that is the foundation for innovations and ability to sustain national clusters in the future.

During the 2020 period, we are planning to implement some collaboration actions at national and EU level. L3CE will lead organization of several workshops at national level aimed to showcase SPARTA project important results to national stakeholders (MoND, NCSC, Ministry of Education & Science, Data Privacy Agency, INFOBALT association)

L3CE analyses the possibility to organize SPARTA workshop aimed to improve T-Shark program visibility and approach new members for Arbitrage Group.

### **3.2.9 Spain**

#### **3.2.9.1 Current status**

Spain counts since 2013 with the National Cybersecurity Strategy that provides a basis for developing the provisions of the National Security Strategy (reviewed in 2017) on the protection of



cyberspace in order to implement cyber threat prevention defence, detection, response and recovery actions against cyber threats.

The [National Security Strategy 2017](#) has consolidated the fact that cyber security must have a differential and own space, taking into account both the impact of the digitalization as an engine of change with implications for cybersecurity beyond the field only the technological Heritage into the political, economic and social, such as the nature of cyberspace as a vector of strategic communication, that can be used to influence public opinion and in the thinking of people through the manipulation of information, misinformation campaigns or actions of hybrid nature. The Strategy sets a new framework, with five general goals running across all fields. Crisis management, National Security Culture, global common spaces, technological development and international projection for Spain shape a strategic grid where cybersecurity is used to open up new paths leading to Spain's present and future security model.

The [National Cybersecurity strategy 2019](#) published in the BOE (Spanish Government Gazette) April 30th 2019 develops forecasts of the National Security Strategy 2017 in the field of cyber security, according to the general objectives, the target of area of cybersecurity and lines of action set to achieve this. Responds well to the mandate of the National security council of 16 July 2018 published in the BOE August 10th.

The overall objective is to ensure a safe use and reliable of the cyberspace in Spain, protecting the rights and freedoms of citizens and promoting economic partner progress. Further objectives are:

- security and resilience of networks and information and communications systems of the public sector and essential services,
- safe and reliable use of cyberspace against illicit or malicious use,
- protection of business and social ecosystem and citizens,
- culture and commitment to cyber security and empowerment of the human and technological capacities, and
- security of cyberspace in the international arena.

The document is structured in five chapters:

- **Cyberspace:** beyond a common global space, which provides an overview of the scope of cybersecurity, the progress made in this area since the adoption of the 2013 Strategy, the reasons which support the development of the 2019 National Cybersecurity Strategy, as well as the main features, which drive its development.
- **Threats and challenges in cyberspace:** it determines the main threats to cyberspace which derive from its status as a common global space, the high level of technology and the great connectivity that makes it possible to amplify the impact of any attack.
- **Purpose, principles and objectives for cybersecurity:** it applies the guiding principles of National Security Strategy 2017 (Unity of Action, Anticipation, Efficiency and Resilience) to the five specific objectives above.
- **Lines of action and measures:** where seven lines of action are established and the measures for the development of each of them identified: (1) strengthen capabilities to deal with threats from cyberspace; (2) guarantee security and resilience for Spain's strategic assets; (3) reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace; (4) boost cybersecurity for citizens and companies; (5) Strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy; (6) contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests; and (7) Develop a cybersecurity culture.
- **Cybersecurity in the National Security System:** it defines the organic architecture of cybersecurity. Under the direction of the President of the Government, the structure is composed of three organs: the *National Security Council*, as the Government's Delegate Commission for National Security; the *National Cybersecurity Council*, which supports the National Security Council and assists the President of the Government in the direction and



coordination of national security policy in the area of cybersecurity, and fosters relations of coordination, collaboration and cooperation between public administrations and between these and the private sector, and the *Situation Committee* which, with the support of the National Security Department, will support the management of crisis situations in any area which, due to their transversality or dimension, exceed the response capacities of the usual mechanisms.

Concerning the **Spanish Cyber Security Ecosystem**, it's mainly formed by:

- [INCIBE](#) as the **Cyber Security National Institute** works in public-private policy initiatives to raise cybersecurity levels in Spain, the follow-up and review of emergent risks in order to be able to anticipate needs, adopt pre-emptive measures and have recourse to early warning mechanisms.
- The [National Center for the Protection of Infrastructures and Cybersecurity \(CNPIC\)](#) is the organism in charge of promoting, coordinating and supervising all critical infrastructure protection-related activities for which the Secretariat of State for Security is competent at national level.
- The [INCIBE-CERT](#) is the National CERT responsible for the prevention and mitigation of, and the response to, cyber-incidents in the corporate, citizen and critical infrastructure operator spheres. In the case of incident management affecting critical private sector operators, INCIBE-CERT is jointly operated by INCIBE and CNPIC, the National Center for Infrastructure Protection and Cybersecurity of the Ministry of the Interior. INCIBE-CERT is one of the reference incident response teams that coordinates with the rest of the national and international teams to improve the efficiency in the fight against crimes involving networks and information systems, reducing their effects on public security
- The CCN-CERT is the Information Security Incident Response Team of the [National Cryptologic Centre, CCN](#), accountable to the [Spanish National Intelligence Centre \(CNI\)](#), to ensure protection from cyber-attacks on classified systems and systems belonging to Public Administrations, and to companies and organizations of strategic interest (those essential for Spanish security and economy).
- The Spanish [Network of Excellence on Cybersecurity Research \(RENIC\)](#) is a membership based sectoral association that includes research centres and other agents of the research cybersecurity ecosystem in Spain. RENIC mainly aims to promote scientific research, technological development, innovation, knowledge and technology transference to industry and the development of R&D in the field of cybersecurity in Spain.
- The Spanish [Cybersecurity Innovation Cluster \(AEI Ciberseguridad y Tecnologías Avanzadas\)](#) brings together companies, research centres, universities, public and other private organizations interested in promoting new technologies in the industrial sector and other related stakeholders, wishing to contribute to the objectives of the Association regarding Security Technologies, at national and international level.
- The ecosystem is completed with regional agencies whose objective is to generate a culture of cybersecurity in the region, like the [Basque Cybersecurity Center \(BCSC\)](#) in the Basque Country, the [ICT Security Centre of the Valencian Community \(CSIRT-CV\)](#), or the [Cybersecurity Agency of Catalonia \(CESICAT\)](#).

### 3.2.9.2 SPARTA's actions

SPARTA project has established contact with the following organisations to build the national cluster for Spain:

- AEI Ciberseguridad
- SPRI
- INCIBE
- Ingeteam
- Schneider Electric
- CCI



- Artech
- PESI
- Ertzaintza
- Cluster Energia
- Mondragon
- Atos
- BCSC
- IKERLAN

We have already received a sign of interest in joining SPARTA from:

- GRADIANT

The following companies have been identified as potential members of the SPARTA Partnership program:

- S21SEC
- ACCENTURE
- CSIC
- Universidad de Granada
- Universidad Politécnica de Madrid
- Universidad de la Laguna
- ITS
- EUROCYBCAR
- IDIADA
- NATURGY
- Panda Security
- Universidad de León
- Innotec - Entelgy
- CounterCraft
- Enigmedia
- CITIC
- IMDEA Software
- Universidad Carlos III de Madrid
- Universidad de Castilla La Mancha
- Universidad de Vigo
- Universidad Rey Juan Carlos
- S2 Grupo
- SGSS
- APPLUS-LGAI o IDIADA
- GMV
- Bit4id
- ClilckAlba
- Integrasys
- Leet Security
- BBVA
- i2CAT
- Ziur

During the 2020 period, we are planning to implement some collaboration actions at national level. Some workshops will be organized, supported by INCIBE and BCSC, in collaboration with the other CCN pilots (CONCORDIA, CyberSec4Europe and ECHO). Concretely, we are planning to organize 4 workshops in the Basque Country, León, Catalonia and Galicia.



We will also analyse, together with INCIBE, the possibility to organize a new SPARTA workshop in Spanish Cybersecurity Research Conference (JNIC), Ciudad Real, June 2020 (<http://2020.jnic.eu>) or in any thematic workshops related to Cyber Ranges.

### 3.2.10 Luxembourg

#### 3.2.10.1 Current status

In Luxembourg, the cybersecurity ecosystem has radically evolved within the last 20 years, a shift actively supported by the Ministry of the Economy, with a vision of inclusion and access to security services and products for all parties of society. The OECD papers from 2002 [1] as well as the more recent one from 2015 [2] significantly inspired this development.

Today, the Luxembourg cybersecurity ecosystem is dynamic, vibrant and represents a strong diversity of innovative products and services, involving players like public entities, administrations, companies, associations, independents as well as start-ups.

The “Cybersecurity Board (CSB)”, chaired by the Prime Minister and involving all relevant ministries and State bodies, represents the highest level of the Luxembourg cybersecurity public governance. On a strategic level, the “Interministerial Coordination Committee for Cyberprevention and Cybersecurity (CIC-CPCS)” strengthens, sustains and facilitates the implementation of the National Cybersecurity Strategy (the third revision was published in May 2018 [3]).

The responsible for security of government, public entities and operators of critical value for the nation is the “High Commissioner for National Protection (HCPN)”. The ANSSI Luxembourg (the national agency, a department of the HCPN) establishes security policies and recommendations. Finally, the GOVCERT Luxembourg (a department of the HCPN) gives a response and support in case of a cyber incident.

Complementarily, Security made in Lëtzebuerg (SMILE) is turned towards the private sector, communes and stakeholders from the economy addressing all questions related to cybersecurity via its three departments: CASES (risk governance and compliance) ; CIRCL (the CSIRT for the private sector) and C3 (Competencies management and economics related to security).

Besides HCPN and SMILE, is the CIC-CPCS composed of the “Luxembourg defence department”, the Media and Communication Unit, the state IT centre, the State Intelligence Service as well as the Foreign Affairs Department.

On the regulatory side, Luxembourg has 5 regulators strongly involved in cybersecurity: CSSF (banking sector), ILR (telecom and NIS), CNPD (GDPR), ILNAS (specific e-archiving law), HCPN (critical infrastructure protection) striving in a continuous effort to harmonise cybersecurity requirements and as such the compliance burden for private and public entities.

To combat cybercrime, the national prosecutor’s office as well as the police forces have dedicated units to deal with « cyber » cases. They collaborate and are supported on an operational level by the CERT.LU [4] community, composed of the 5 public and 5 private CSIRTs from Luxembourg.

Finally, the national safer internet awareness centre is called BEE SECURE [5] and is dedicated to inform citizens and especially youngsters about the dangers and opportunities of the Internet.

In addition to all this, there are several associations and clusters like CLUSIL [6], ISACA [7], CPSI [8], APDL [9], OWASP [10]... as well as the interdisciplinary institute for security, reliability and trust (SnT) of the University of Luxembourg [11] and other research centres, dedicated to topics around cybersecurity.

[1] Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security (OECD 2002 ; <https://www.oecd.org/sti/ieconomy/15582260.pdf>)

[2] Digital Security Risk Management for Economic and Social Prosperity (OECD 2015 ; <http://www.oecd.org/sti/ieconomy/Digital-Security-Risk-Management.htm>)



- [3] National Cybersecurity Strategy III / Stratégie nationale en matière de cybersécurité III ([https://gouvernement.lu/fr/publications.gouv\\_hcpn%2Bfr%2Bpublications%2Bstrategie-nationale-cybersecurite-3%2Bstrategie-nationale-cybersecurite-3.html](https://gouvernement.lu/fr/publications.gouv_hcpn%2Bfr%2Bpublications%2Bstrategie-nationale-cybersecurite-3%2Bstrategie-nationale-cybersecurite-3.html))
- [4] Luxembourg Cyber Emergency Response Community (<https://cert.lu/>)
- [5] <https://bee-secure.lu/>
- [6] Information Security Association Luxembourg (<https://clasil.lu/>)
- [7] ISACA Chapter Luxembourg (<https://www.isaca.org/chapters2/Luxembourg/>)
- [8] College of Information Security Professionals (<https://cpsi.lu/>)
- [9] Data Protection Association Luxembourg (<http://apdl.lu/>)
- [10] OWASP Chapter Luxembourg (<https://www.owasp.org/index.php/Luxembourg>)
- [11] <https://snt.uni.lu/>

### 3.2.10.2 SPARTA's actions

SPARTA project has established contact with the following organisations to establish the national cluster for Luxembourg:

- Luxinnovation
- HCPN

We have already received a sign of interest in joining the SPARTA community from:

- Silent breach

SMILE intends to organise a SPARTA event during the 2020 CyberSecurity Week of Luxembourg (19th to 29th of October).

## 3.2.11 Portugal

### 3.2.11.1 Current status

With currently 35 members, including representatives from the CNCS, military, finance, telecom, government, academia, cybersecurity national industry and cloud providers, the Portuguese National CSIRT Network (RNCSIRT) is the main operational forum for CSIRT's in Portugal, as well as the "key" cybersecurity forum in the country. The RNCSIRT aims to build trusted, direct communication channels among its members, facilitate incident response and disseminate best practices on computer security incident handling. INOV is an active member of RNCSIRT.

### 3.2.11.2 SPARTA's actions

SPARTA project has established contact with the following organisations to establish the national cluster for Portugal:

- CNCS

We have already received a sign of interest in joining SPARTA from:

- Município do Barreiro



### 3.2.12 *Latvia*

#### 3.2.12.1 Current status

The vision of cybersecurity Latvia is a safe, open, free and reliable cyberspace that enables reliable and continuous delivery of services essential to the State and society.

Latvia needs to take advantage of the digital environment in order to ensure economic and social welfare, while reducing the overall level of cybersecurity risks, without unnecessary limitation to the flow of technology and information.

The cybersecurity policy target for the period 2019-2022 is

- strengthening and developing cyber-defence capabilities,
- increasing resilience to cyber attacks,
- promoting public awareness to threats in cyberspace,
- fight against cybercrime.

The following priorities are defined in the implementation of the cyber security policy: cyber-defence, deterrence and growth.

Cyber-defence - developing and improving capacity, and knowledge to defend against growing cyber threats and respond effectively to cyber security incidents a protection and capacity to function.

Deterrence – detect, investigate and stop malicious activities in cyberspace, identifying offenders and call them justice, thereby deterring others from taking such actions.

Growth: continuous development of cybersecurity skills in different sectors and promoting specialization in cybersecurity.

While every institution in Latvia is responsible for its own part of cybersecurity in cabinet of ministers cybersecurity is represented by Minister of defence. Ministry of defence is also chairing National Cybersecurity council. As leading agency for civil defence and disaster relief Ministry of interior is coordinating Critical infrastructure protection program. National CERT team CERT.LV is located in University of Latvia in institute of Mathematics and informatics(LUMII), but is reporting to MOD. Latvia has three universities active in cybersecurity area BA School of Business and Finance, Vidzeme University of Applied Sciences and University of Latvia.

Latvia has developed cybersecurity industry ranging from hardware producers at Mikrotikls to communication security products to different cybersecurity services including e-signature and digital id services from LVRTC to NOTAKEY.

NGO and civic activity field in cybersecurity is well developed as there are active local and international NGO like ISACA, United cyber-defence league, LIKTA, NETSAFE active in country.

#### 3.2.12.2 SPARTA's actions

SPARTA project has established contact with the following organisations:

- CERT.LV (the Information Technology Security Incident Response Institution of the Republic of Latvia)
- Vidzeme University of Applied Sciences
- PIKC SALDUS TEHNIKUMS

### 3.2.13 *Italy*

#### 3.2.13.1 Current status

The Italian community started already time ago a process of cooperation and clustering of the rich competences in cyber security present in the research and academia landscape.



- CINI has set up the largest laboratory in Italy on cybersecurity (CINI Cybersecurity National Laboratory) that puts together 44 universities and collects expertise from more than 300 researchers actively working in Cybersecurity. It contributed to create the Italian Cyber security Framework<sup>3</sup> and several successful initiatives as CyberChallenge.IT, the Italian cybersecurity challenge.
- CNR had an interdepartmental security project and later a cyber security one putting together the expertise and resources of more than 100 researchers in the field and contributed with Leonardo to set up the Italian Technological Platform in Security Research (SERIT).
- CNIT has a rich competence in networking and cyber security aspects.

All together, these created on Feb 2017 the National Committee for Research in Cyber Security under the auspices of Italian Department of the Information for Security (DIS). This is a successful example of national cooperation.

All these actors are part of the SPARTA Consortium that is also complemented by the main Italian industry in the defence sector, i.e. Leonardo, and the Italian CERT run by MISE-ISCOM in SPARTA.

### 3.2.13.2 SPARTA's actions

The SPARTA clustering is thus representative of the Italian Cybersecurity ecosystem and the clustering activities of SPARTA in the sector. Nevertheless, the plan is to enlarge also to other partners especially in vertical sectors.

SPARTA has established contact with the following organisations to establish the national cluster for Italy:

- Sogei
- ENEL

We have already received a sign of interest in joining SPARTA from:

- Poste Italiane
- TERNA
- IDS
- Torino wireless foundation

The plan is to continue to work at SPARTA project level as well as at national one. CNR and CINI have a major role in the Tuscan Cyber security centre and we would be pleased to embody also this in the SPARTA activities.

### 3.2.14 Estonia

#### 3.2.14.1 Current status

In 2010, by a decision of the Government of the Republic, the Estonian Informatics Centre was given government agency status. The Estonian Information System Authority (RIA) (<https://www.ria.ee/en/>) received additional powers and resources for organizing protection of the state's ICT infrastructure, and exercising supervision over the security of information systems. For the purposes of organizing the protection of infrastructure, the Department of Critical Information Infrastructure Protection (CIIP) (<https://www.ria.ee/en/ciip.html>) was formed within the RIA. The creation of the Estonian Defense League's Cyber Unit (EDL CU) (<http://www.kaitseliit.ee/en/cyber-unit>), which took place as a result of collaboration between the public, private and third-sector, has been instrumental in ensuring national defense. The EDL CU is also engaged to support civilian institutions and protect critical infrastructure in a crisis situation. The main provider of training and awareness-raising in the field of cybersecurity is Information Technology Foundation for Education

---

<sup>3</sup> <https://www.cybersecurityframework.it/>



(HITSA) (<https://www.hitsa.ee>) formerly known as the Tiger Leap Foundation. HITSA training is offered to pre-schoolers well as older children, while also involving parents and teachers in the process.

In 2019, Estonia released its third National Cyber Security Strategy for the period of 2019 – 2022 ([https://www.mkm.ee/sites/default/files/kyberturvalisuse\\_strateegia\\_2022\\_eng.pdf](https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf)). In this document there are four strategic objectives stated for the next four years.

- **A sustainable digital society.** Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness.
- **Cybersecurity industry, research and development.** Estonian cybersecurity industry is strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia.
- **A leading international contributor.** Estonia is a credible and capable partner in the international arena.
- **A cyber-literate society.** Estonia is a cyber literate society and ensures sufficient and forward-looking talent supply.

In order to achieve these four strategic goals, Estonia is going to focus on developing technological resilience, ensuring cyber incident and crisis prevention, preparedness and resolution, fostering comprehensive governance and development of a cohesive cybersecurity community, supporting and promoting Estonian cybersecurity R&D and research-driven industry, advancing substantial cooperation on cyber issues with strategic international partners, promoting sustainable cybersecurity capacity building across the globe, raising cybersecurity awareness among citizens, state and private sector, and finally developing talent to meet the needs of both state and private sector.

Cyber security issues continue to be governed horizontally, meaning each public institution is responsible for their own area. The central cyber security agency in Estonia continues to be the Estonian Information System Authority (RIA). The most significant action in cyber security took place in summer, when Information System Authority signed a contract with the European Commission to establish EU-CyberNET, a new cyber security center of excellence for the duration of four years. EU-CyberNET initiative focuses on global cyber security capacity building.

Secondly, the Estonian Ministry of Defence launches a Cyber Security Training Centre CR14. It will serve the needs of the Estonian Defence Forces and NATO's Cyber Range as well as Allies and Partners.

Finally, the NATO Cooperative Cyber Defence Centre of Excellence keeps up with its high-level work. Within 2019, five additional countries joined the CCD COE: Bulgaria, Denmark, Norway, Ireland and Romania. In 2019, we also saw major events organized by the CCD COE like the Locked Shields 2019 exercise and the CyCon 2019 conference.

### 3.2.14.2 SPARTA's actions

SPARTA project has established contacts with several organizations and plan to organize a SPARTA monthly workshop in year 2.



### 3.3 European level

SPARTA partners interacted with several EU and international bodies in several forms. We recall here some of the main organizations and EU project we cooperated with.

#### 3.3.1 *Cooperation with EU Organisations*

##### 3.3.1.1 ECSC

The European Cyber Security Organisation (ECSC) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSC represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSC members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

SPARTA partners are fully involved in ECSC in several roles including in the Board of ECSC, e.g., CEA, CNR, Thales).

Cooperation with ECSC is at several levels, in particular, SPARTA coordinator has been invited to serve in the scientific and technical committee of ECSC. SPARTA representatives are invited in several ECSC meetings, as the ECSC WG6 ones.

The cooperation is strong and is going to be re-enforced by a MoU between SPARTA and ECSC.

##### 3.3.1.2 ENISA

ENISA was created in 2004 by EU Regulation No 460/2004 under the name of European Network and Information Security Agency. The Agency works closely together with the EU Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises and since 2019, it has been drawing up cybersecurity certification schemes.

ENISA assists the Commission, the member states and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA ultimately strives to serve as a centre of expertise for both member states and EU Institutions to seek advice on matters related to network and information security.

SPARTA partners cooperate in several forms with ENISA officers in many activities. In particular, SPARTA researchers cooperated with activities on roadmapping and certification that are currently two hot topics.

SPARTA project has established contact with the following organisations to establish the European ecosystem:

- EOS (EU)
- ENLETS (EU)
- ESA (EU)



### **3.3.2 Cooperation with EU Projects**

#### **3.3.2.1 Cyberwatching**

Cyberwatching aims at defining and promoting a pragmatic approach to implement and maintain an EU Observatory to monitor R&I initiatives on cybersecurity & privacy, throughout EU & Associated Countries. These initiatives will be clustered, with a cluster tool, and themes identified, leading to an online catalogue of services for cybersecurity & privacy, showcasing market uptake and advancing EU sustainable competitiveness. A supply & demand marketplace of EU cybersecurity products & services, as well as the inclusion of an end-users' club, ensures that perspectives of SMEs as well as other relevant stakeholders are properly taken account of. Ultimately, a cybersecurity & privacy ecosystem will be created, offering prime and guided access to the cyberwatching.eu catalogue of services & marketplace & ensuring feedback in terms of effectiveness & usability of research results.

Main Outputs: Continuously updated observatory & R&I online catalogue, cluster tool, 4 concertation meetings, 4 annual workshops, 10 regional SME workshops, 10 webinars, 4 cluster reports, 2 white papers, 2 roadmaps, sustainability through cybersecurity & privacy marketplace

SPARTA project is listed among the project in Cyberwatching and SPARTA researchers are often called in meetings organized by Cyberwatching, several events were attended by CNR.

#### **3.3.2.2 NECS**

The European Network for Cyber Security (NECS) addressed the training and development of a European talent pool to help implement and support the European Cyber-security strategy as highlighted in the EC's Digital Agenda. NeCS developed a new generation of researchers that combine a strong academic foundation with practical experiences, technological expertise with awareness of the socio-economic and legal context and conviction to furthering research with an entrepreneurial spirit. The 4-year NECS project ended in Sept 2019 and worked for a cyber-security research and training network makes a significant contribution towards meeting the increased demand of human expertise in this critical field. NECS fosters a multi-sector/multi-disciplinary approach that is absolutely necessary for tackling coherently all cyber-security needs as recognized by the Network and Information Security (NIS) platform that has been established by the EU in order to develop a public/private cooperation strategy.

NeCS winter school (<https://necs-winterschool.disi.unitn.it/>) has been inherited by SPARTA in cooperation with the other 3 Pilot networks and will continue as joint effort with an interesting governance model that sees equally involved all the 4 Pilot networks, in particular in the organizing committee 25% is represented by SPARTA researchers (i.e. Fabio Martinelli (CNR) and Paolo Prinetto (CINI)). The 2020 edition is described in the following brochure.





The **European Network(s) for Cybersecurity (NeCS) PhD School** was launched three years ago, in response to the increase need of highly qualified experts in cyber-security. The School addresses the issues of training and development of talented junior researchers as indicated in the European Cyber-security strategy and highlighted in the EC's Digital Agenda.

This year the School is supported by the four most important EU initiatives in this area: the Cyber-security Competence Networks. They have been launched last year, within the H2020 framework, and are , **CONCORDIA**, **CyberSec4Europe**, **ECHO** and **SPARTA**. All of them, put emphasis on the crucial role of education for cyber-security, proposing new educational and training programmes and new methods of teaching.

The NeCS PhD School is an opportunity for the four pilots to presents to young researchers, and most importantly, to put in practice, some of their innovation and results. Scope of the NECS PhD Winter School is to present advances on both attacks and defenses in the realm of cyber-security. In this year programme, compared to previous editions, a good part of the lectures is dedicated to hands-on experiences and exercises, such that students can put in practice the theoretical principles and lessons learned during the more classical lectures.

#### Speakers:

Jane Henriksen-Bulmer, Bournemouth University  
Jorge Cuellar, SIEMENS  
Florent Kirchner, List Institute, CEA  
Mattijs Jonker, University of Twente  
Wim Mees, Royal Military Academy  
Kai Rannenber, Goethe University Frankfurt  
Burkhard Stiller, University of Zurich  
Konstantinos Votis, CERTH/ITI

Jeroen van der Ham, Dutch NCSC  
Simone Fischer-Hübner, Karlstadt University



#### Organizers:

Bruno Crispo, Univ. Trento (CSE4EU)  
Javier Lopez, Univ. Malaga (CSE4EU)  
Fabio Martinelli, CNR (SPARTA)  
Matteo Merialdo, RHEA Group (ECHO)

Paolo Prinetto, CINI (SPARTA)  
Anna Sperotto, U. Twente (CONCORDIA)  
Burkhard Stiller, Univ. of Zürich (CONCORDIA)  
Wim Wees, Royal Military Accademy (ECHO)

<http://necs-winterschool.disi.unitn.it/>

Figure 7: NeCS winter school

NeCS also contributed to the SPARTA partnership by passing its PhD students and young researchers Forum on Facebook (<https://www.facebook.com/groups/184586768722967>), more than 400 subscribed. This is a main tool among the European PhD community to stay tuned on the latest advancements.





Figure 8: PhD students and young researchers Forum

### 3.3.2.3 StandICT

StandICT.eu, “Supporting European Experts Presence in International Standardisation Activities in ICT”, addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene. Through a Standards Watch, StandICT.eu will analyse and monitor the international ICT standards landscape and liaise with Standards Development Organisations (SDOs) and Standard Setting Organisations (SSOs), key organisations such as the [EU Multistakeholder Platform for ICT Standardisation](#) as well as industry-led groups, to pinpoint gaps and priorities matching EU DSM objectives. These will become the topics for a series of 8 Open calls focused on priority domains and a continuous cascading grants process, launched by StandICT.eu from March 2018, providing support for European specialists to contribute to ongoing standards development activities, and attend SDO & SSO meetings.

SPARTA partner Fabio Martinelli (CNR) worked on the External Advisory Group and contributed to spread the standICT opportunities in SPARTA as well as to spread SPARTA expertise in StandICT. The project coordinator of StandICT is actually also a SPARTA associate. The need to foster standardization activities is clear and well acknowledged in SPARTA.

### 3.3.2.4 SAPPAN

SAPPAN is a new project and aims to develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. SAPPAN will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. SAPPAN will enable this within a single organization as well as across organisations through novel models for privacy-preserving data processing and sharing. It will enable utilizing external experts for intrusion detection and sharing of knowledge on response and recovery actions while respecting the privacy and confidentiality requirements of individuals and organizations. SAPPAN will enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches.



SPARTA partner CESNET participates in SAPPAN. At one point the project looked for a sharing platform and we presented there the results of T4.4, MISP demo, PROTECTIVE/IDEA demo, C3ISP demo during of the face to face meeting. It is worth noticing that Masaryk university (member of CONCORDIA) participates also in this project and they presented what CONCORDIA figured out to use as a sharing platform.

### 3.3.2.5 AEGIS for US cooperation

AEGIS aims to strengthen dialogues between Europe and the US, in order to facilitate exchange of views, policies and best practices to stimulate cooperation around cybersecurity and privacy R&I, and contribute in shaping the future global cybersecurity and privacy landscape.

AEGIS proposes a multi-stakeholder approach to engage relevant communities more actively and strategically in supporting dialogues and creating a common and orchestrated vision and strategy to accelerate EU-US cooperation in cybersecurity and privacy R&I. At the core of the AEGIS strategy is the Cybersecurity Reflection Group EU-US that will be established as a multi-stakeholder collaboration platform. The Cyber-RG EU-US, through its Working Groups, will address specific issues on international, technical trends, policy and legislation challenges in cybersecurity and privacy, and will facilitate the effective collaboration of a wide range of interested parties including policy makers, researchers, technology experts, business leaders, cyber policies experts and influencers and civil society. Under the leadership of the AEGIS consortium, these key groups will come together to decisively tackle cybersecurity and privacy related problems and to provide opinions and recommendations to policy dialogue. AEGIS will also provide a mapping of the cybersecurity and privacy landscapes in EU and US, benchmark relevant legislation and policies and promote innovation partnerships and opportunities for future EU-US cooperation in cybersecurity and privacy areas of mutual strategic interest.

The AEGIS consortium is in a privileged position to generate significant impacts in both sides of the Atlantic, by leveraging the partnership's network multipliers with a wide-ranging access to cybersecurity and privacy stakeholders, including researchers, think tanks, business and political decision makers, and thus to contribute significantly to deepen cybersecurity and privacy R&I cooperation between Europe and the US.

### 3.3.2.6 EUnity for Japan cooperation

EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions.

Among EUNITY objectives there are:

- Encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges by organizing at least two workshops, ensuring a broad participation of the relevant stakeholders (policy groups representatives, industry representatives, academia representatives) in the workshops and by feeding back the collected information into EU-based groups such as ECSO, EOS, NIS, and the CSA.
- Identify potential opportunities for future cooperation between European and Japanese R&I ecosystems and policy makers by identifying and mapping the relevant legislation, policies and cybersecurity agendas, roadmaps and timelines at the EU level (NIS platform, cybersecurity cPPP) and at the National level, as well as in Japan, clearly identifying and prioritising the joint topics in a proposed EU-Japan Cybersecurity and Privacy Strategic Research and Innovation Agenda (EUJ-C&P-SRIA) and ensuring that the collected information is made widely available through modern communication means.
- Foster and promote European cybersecurity innovation activities and increase the international visibility of EU activities in cybersecurity, by showcasing important results of



projects and including key European research actors (companies and researchers) in the project's workshops.

EUnity is managed by SPARTA partner IMT and the follow up activities of this project will be also conducted in cooperation with SPARTA.

### 3.4 Monthly workshops

SPARTA workshops have the goal to integrate associates and the wider SPARTA and national communities. The information flow should be bidirectional from SPARTA to attendees and from attendees to SPARTA. Mainly related to Roadmaps, Research programs and community based activities (partnership and JCCI). We created with WP12 and WP3 a handbook for running SPARTA monthly workshops as well as a report form.

In the first year we run 8 workshops (listed below) and 11 are already planned for year two.

Country	Location	month	dates	Organizers
France	Paris	feb-19	18/02/2019	French Cluster (CEA)
Italy	Rome	sept 219	26/09/2019	Italian Cluster (LEO)
Italy	Pisa	oct 2019	11/10/2019	Italian Cluster (CNR)
Germany	Bonn	set-19	30/09/2019	UBO
Lituania	Vilnius	apr-19	30/04/2019	L3C
Spain	Leon	oct 2019	23/10/2019	VICOM/TEC/EUT
Spain	Madrid	apr-19	24/04/2019	YWH
France	Rennes	sept 2019	13/09/2019	INRIA

Figure 9: SPARTA workshops

We give some excerpts of the reports of these meetings.

#### 3.4.1 SPARTA Workshop in Madrid, Mundo Hacker

The workshop was framed in the 6th edition of Mundo Hacker Day, an event organized by the popular Spanish TV show Mundo Hacker focused on the dissemination of cybersecurity in an entertaining way. Mundo Hacker Day was held at Kinopolis Madrid, on 24 April 2019. The event featured several tracks and round tables with large companies in the ICT sector where they addressed the most current issues in the digital security sector.

Bearing in mind that each year, Mundo Hacker Day brings together thousands of people, which resemble a very heterogeneous audience (cybersecurity practitioners, researchers, students, industry, etc.), and the fact that the SPARTA partner YesWeHack was going very active throughout it (as both participant and golden sponsor), they preliminarily suggested to Indra the possibility of taking advantage of this occasion to disseminate SPARTA, subsequently involving the partners Vicomtech and Tecnalia.

The activities carried out during the workshop assumed the following **objectives**:

- To make the SPARTA project known to attendees by introducing its view for a European network of competences in cybersecurity, objectives, research programs and the challenges to be faced.
- To acquire feedback and know the opinion of the attendees (ranging from experts to students) about the topics covered and the project approaches.
- Since the workshop was the first SPARTA event held in Spain, it was expected to serve as a preliminarily meeting point for local partners (not excluding the rest).



- To disseminate the possibility of cooperating as associate partners aiming on attracting the attention of new ones.

The workshop was divided into two tracks. The first of them focused on the presentation to the attendees of the overall SPARTA view, as well as the particular role/view of the attending partners. The track was coordinated by Indra (Jorge Maestre Vidal and Sebastián Laiseca Segura), which presented the project background, objectives, organization approach, roadmap and research programmes. They also introduced the Indra's view of the project and its role. Then each attending partner (YesWeHack (Nicolas Diaz), Vicomtech (Raul Orduna Urrutia), Tecnalía (Concepcion Cortes)) presented its contribution to the project and particular view about the forthcoming work.

The second track was coordinated by YesWeHack (Nicolas Diaz), where the Coordinated Vulnerability Disclosure (CVD) process was presented and its main challenges were introduced to the attendees, covering the discussion of tools and means that facilitate CVD for a safer Internet. This facilitated the participation of the audience, triggering an open debate on various related topics of interest.

Despite the facts that the workshop was organized with short notice (due to the attempt of taking rapid advantage of the influence of Mundo Hacking Day in Spain) and that it has had little audience, it served to meet part of the established objectives. Firstly, in the context of the workshop, the project was disseminated in a public event and through social networks, thus contributing to the understanding of the SPARTA's view for a European network of competences in cybersecurity. Second, the topics covered by the SPARTA research programme were discussed in-depth, thus facilitating the attendee participation and providing very valuable feedback. On the other hand, one-third of the Spanish partners was present, which served as preliminarily step towards triggering further joint local initiatives. Unfortunately, the workshop was not able to recruit new associated partners in situ; but the related dissemination actions in social networks and between the Mundo Hacker Day assistants may encourage new partnership requests in the short/medium term.



Figure 10: SPARTA workshop in Madrid disseminated through Tecnalia's social network



### 3.4.2 SPARTA Workshop in León, Mundo Hacker

The workshop was framed in the 13<sup>th</sup> edition of the ENISE congress in León (Spain), on October 23<sup>rd</sup>, and was organized by Tecnalía, Vicomtech, Eurecat and Indra. “Cybersecurity in the connected industry: from threat to opportunity” is the slogan chosen for this thirteenth edition of the International Meeting on Information Security.



Figure 11: SPARTA workshop included in the Agenda of the 13ENISE Program.

The workshop, organized with the collaboration of INCIBE that has provided the infrastructure for the event within the [ENISE 13 Concept development room](#), has served as an opportunity to disseminate the SPARTA objectives and results, and to connect SPARTA with other CCN pilots (CONCORDIA and CyberSec4Europe). The total number of attendees was 19, being 6 of them SPARTA partners.





Figure 12: SPARTA workshop in León (Spain).

The workshop was divided into three tracks. The first track was focused on the presentation of the objectives of the CCN and the objectives of the three pilots (CyberSec4Europe, SPARTA and CONCORDIA). The second track was dedicated to a Panel on 'Use cases and impact for Spain'. The third track was dedicated to a panel on 'New challenges for cybersecurity and synergies between pilots'. The agenda of the workshop is shown in the Figure 13.

<b>Pilotos de Ciberseguridad Europeos y el Impacto para España</b> <b>JORNADA DE TRABAJO</b> 23 octubre 2019 9:30 am Salón de Desarrollo de Ideas de 13ENISE, León	
<b>Introducción pilotos CCN</b> 9:30 am	Pilotos para la red de Centros de Competencia en Ciberseguridad europea <b>Juan Díez González, INCIBE</b>
<b>CyberSec4Europe</b> 10:00 am	Objetivos del piloto CyberSec4Europe <b>Miembros de CyberSec4Europe</b>
<b>SPARTA</b> 10:30 am	Objetivos del piloto SPARTA <b>Miembros de SPARTA</b>
<b>CAFÉ   11:00 am</b>	
<b>CONCORDIA</b> 11:30 am	Objetivos del piloto CONCORDIA <b>Miembros de CONCORDIA</b>
<b>CASOS DE USOS</b> 12:00 am	Panel de Casos de Usos e Impacto para España <b>CAIXABANK, ATOS, INDRA</b>
<b>NUEVOS RETOS</b> 12:45 am	Panel de Nuevos Retos para la ciberseguridad y sinergias entre pilotos <b>Miembros de CyberSec4Europe, SPARTA, CONCORDIA</b>
<b>CONCLUSIONES</b> 13:30 am	Conclusiones y nuevos pasos en la coordinación <b>INCIBE, Comisión Europea</b>

Figure 13: Agenda of the SPARTA workshop in León (Spain).



The Spanish cluster meeting has concluded the need to identify some synergies between the 4 pilots (CONCORDIA, CyberSecurity4Europe, ECHO and SPARTA) and to work together towards the creation of a common objective: a European network of centres of cybersecurity experience.

- The creation of a **JCCI infrastructure** is present in the 4 pilots, however each pilot follows different point of view and different stages. An alignment is needed to create some interfaces because the EU has expressed the need to work together to provide a common infrastructure.
- The same applies to the **Roadmap** definition. EU's intent is to develop a Roadmap with clear milestones to tackle cybersecurity industrial challenges in selected sectors and implement it through a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.
- The **WP Structure** is also quite similar in the four pilots, with the presence of synergies in: Governance Design; Research & Innovation, Roadmap & Demonstration cases; Education, Training and Standardization; and Communication & Community building.

During the workshop, we received an Expression of Interest to become Associate by Gradiant (<https://www.gradiant.org>). Gradiant R&D Center is a private technology centre located in Galicia (Spain). Gradiant is backed by a board foundation including representatives of the three Galician universities (Vigo, Santiago and A Coruña) and six of the most important companies working in Galicia (AAltia, Arteixo Telecom, Egatel, Indra, Plexus, R, Telefónica and Televés); and INEO business association, which represents most of ICT Galician companies.

Juan Díez (INCIBE) announced that INCIBE will manage the I+D+i of the EU Cybersecurity Competence Network. After some discussion with the CONCORDIA, CyberSec4Europe and SPARTA partners, INCIBE has decided to take the glove and organize private workshops with the Spanish partners of the four pilots, to promote the alignment of the projects, and also to have a clear vision at Spanish level of capacities, synergies, and interests.

The event was widely disseminated through the SPARTA and TecNALIA social networks.







Figure 14: SPARTA workshop in León disseminated through Tecnalia's social network

### 3.4.3 SPARTA Workshop in Rennes, part of CominLab „Security and Privacy” ws

The Sparta workshop was organized by Inria in Rennes on September 13 in the context of the CominLabs event, which is a regional initiative covering the Bretagne region and Pays de la Loire focusing on research and education. A dedicated Sparta session was organized to introduce the Sparta project and its road mapping activity. This was followed by a discussion session to exchange on future challenges in Security and Privacy. The feedback of the session was used to refine the



emerging challenges identified, and shape the roadmap feedback process that is to be introduced in the next version of the roadmap deliverable D3.2. The workshop attracted 27 participants (11 participants are affiliated to a SPARTA partner although not necessarily active in the project).

### 3.4.3.1 Agenda

9h30	Welcome coffee/tea
10h - 12h30	Presentation of on-going projects and actions: <ul style="list-style-type: none"> <li>• HardBlare: Co-processors for information flow control</li> <li>• PrivGen: Privacy-preserving sharing and processing of genetic data.</li> <li>• Profile: Analyzing and mitigating the risks of online profiling (law, computer science and sociology)</li> <li>• Tyrex: Lattice-based cryptography for homomorphic encryption</li> <li>• Watsup: Watermarking outsourced data (start-up project)</li> <li>• JSExplain: Explaining JavaScript executions (standardisation)</li> <li>• Blockchain FM: Formal methods for blockchain and smart contract security</li> </ul>
12h30-13h30	Lunch
13h30-17h00	Sparta Project - Future research actions in security and privacy <ul style="list-style-type: none"> <li>• Presentation Sparta Roadmap</li> <li>• Discussion about challenges and possible research actions.</li> <li>• CominLabs 2.0 Security and Privacy track and its related research structures</li> </ul>

### 3.4.3.2 Main outcomes

The participants were shortly presented the Sparta network and the EU cybersecurity context it is part of. Specifically, the SPARTA roadmap was presented, and discussed between participants. Notably the synergies that exist between education and research were considered an important corner stone to reinforce cybersecurity in the EU. To this end high quality university programmes are necessary to fill the gap of cybersecurity expertise, and ensure the necessary competence is available transversally in EU industry (including programmes for cryptography post-quantique, software security data protection and privacy, security of algorithms (notably for AI), hardware security, malware analysis, reactive security). At the same time, such high quality (master) programmes are also needed to identify and recruit research talents that push research competence and will ensure competitiveness in the long run. Research labs were also identified as ideal environments for industrial cybersecurity specialist to keep at the forefront of possible threats and novel techniques. At the same time, such exchanges may align research interest and industrial relevance.

### 3.4.4 SPARTA Workshop in Vilnius

SPARTA Associates workshop that was held in Vilnius on the 30<sup>th</sup> of April 2019 was organised by the Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE) in cooperation with the Mykolas Romeris University (MRU).





Figure 15: SPARTA workshop in Vilnius

The key objective of the workshop was to disseminate the SPARTA project goals and results between national stakeholders and demonstrate a new approach to international collaboration and networking.

#### 3.4.4.1 Introduction and overview of SPARTA project:

Evaldas Bruze (L3CE) introduced the SPARTA project concept, short, mid and long-term goals and objectives, project structure, governance model, strategic partnerships, and expected results. He provided an overview of its 4 research programs, and elaborated on the expected set of benefits that programs can bring to the national stakeholders.

SPARTA research programs:

- T-SHARK (Full-spectrum cybersecurity awareness)
- CAPE (Continuous assessment in polymorphous environments)
- HAIL-T (High-Assurance Intelligent Infrastructure Toolkit)
- SAFAIR (Secure and fair AI systems)

Specific attention was paid to the T-SHARK program introduction. The program idea, which is based on a comprehensive threats profiling model has been developed with the focus on the specific challenges of the Baltic Sea region, therefore it was well accepted by the national stakeholders. The project team introduced the T-Shark implementation methodology that is based on the Stage Gates approach and an established Arbitrage Group composed of the independent group of experts from academia, industry, end-user and policy maker's organizations.

#### 3.4.4.2 SPARTA associate partners concept and presentation of benefit pack:

Referring to the overall concept of the project, it is expected that SPARTA will be supported by extensive network of Associated Partners. Integration with national clusters and national ecosystems will help build a network that contains the wide spectrum of new knowledge, scientific ideas and creates islands of competence around specific cyber domains.



Round table discussions helped to get a deeper understanding on the challenges and opportunities specific to the Baltic Sea Region and find new ways to link Lithuanian stakeholders with SPARTA network. A list of targeted questions helped to shape the discussions and link them with SPARTA benefits pack.

#### **3.4.4.3 Overview of LT cybersecurity market:**

Over the past four years, Lithuania has strengthened its cyber capabilities and crime prevention and has been developing a lot of international initiatives, as well as paying great attention to innovation development in different fields of cybersecurity. It is worth mentioning that Lithuania ranks fourth on the draft Global Cybersecurity Index 2018 published by the United Nations. This is Lithuania's highest-ever position in the international cybersecurity environment ranking. By comparison, it was ranked 57th in 2017.

To get a deeper insight into the current national capabilities and demand for innovations, L3CE initiated several Face-to-Face (F2F) meetings with different stakeholders groups, aimed to explore possibilities for further collaboration with SPARTA project and expand the network of associated partners.

F2F meetings have been organized with public organizations, critical infrastructure operators, ISP and key industry players-specifically:

- Ministry of Foreign Affairs,
- Ministry of Interior
- Office of Lithuanian Government Crisis Management Center
- Lithuanian Radio and Television Center
- Lithuanian Energy
- IT Industry
- Vytautas Magnus University

Important aspect to mention that the majority of national organizations indicated that collaboration may help to optimize the use of national resources necessary for the developing and maintaining cyber threats detection and prevention capabilities. Additionally, a rapid and shared understanding of threats and incidents would enable a better detection of external threats. T-Shark programme will serve national organizations with a new Threats Intelligence model and collaborative tools. Project team generated considerable interest and high expectations of the national stakeholders for the outcomes of research programmes therefore some of them committed to join Arbitrage Group and contribute to solutions evaluation activities.

Information gathered at these meetings was very useful for the planning of future workshops and shape the questions that will be discussed with participants.

#### **3.4.4.4 The main outcomes of the workshop:**

Workshop participants took an active part in the discussions, shared their views, experiences and expectations in relation to Innovations development, results uptake and exploitation. One aspect that deserves a particular mention, national stakeholders are very interested in SPARTA project results and willing to link national priorities with innovations roadmap developed within the scope of SPARTA project.

Stakeholder's expectations:

- Access to EU knowledge base
- Networking is a great environment for open-minded and collaborative people – those who looking to open up, share experiences and learn from each other
- Access to the competence development programs
- Access to the SPARTA innovations (new methodologies, new solutions)



The key issues that have been raised during the discussions mainly focused on the national cybersecurity capabilities:

- Lack of skilled resources, in particular huge gap in analytical skills
- Lack of partnership experience with national research organizations & international networks
- Huge demand for new approaches merging human and machines capabilities
- Huge demand for real time monitoring and emotion sensing technologies
- Huge demand for market ready innovations

Representatives of NCC Group Lithuania <https://www.nccgroup.trust/> immediately accepted an invitation to join SPARTA Associates Network. The company committed to allocate the necessary resources and to share experience in the field of standardization, certification, competence development (e.g. TIBER EU Compliance) share the data sets for experimentation, contribute to evaluation of T-Shark Threats Intelligence model and technology solutions.

#### **3.4.4.5 Action Points Agreed:**

- Associated partner application will be provided to NCC Group management to formalize SPARTA Associated partner status.
- Regular meetings, workshops and events aimed to inform, update and disseminate SPARTA project results involving SPARTA partners and national stakeholders will be organized at least once a year.
- Customized list of benefits will be developed and disseminated between different groups of stakeholders (e.g. public, industry, ISP etc.). Coordination meeting with 4 SPARTA research programs will be organized.
- Coordination of Associate partners workshops. Share and disseminate SPARTA Associates workshop results with all SPARTA network partners and friends.
- NCC Group proposed to make a demo case on existing comprehensive cyber threat intelligence solutions. Further details on the relevance of the solution must be discussed with T-Shark program team.
- L3CE will introduce Engagement Framework to the potential members of SPARTA Associates and Friends.

The workshop was widely disseminated through the SPARTA and partner's social networks and portals.



## Chapter 4 Clustering with other pilots

The SPARTA proposal had explicitly devoted effort in the cooperation with the other winning projects to promote a truly fair cooperation in the interest of European society through competition among the winning projects. This activity was explicitly requested by the call and was understood early on as instrumental for the success of the pilots.

---

***Specific attention was paid to make sure individualistic agendas did not interfere with the committed, collaborative spirit that is key to the success of the European Competence Network.***

---

This proposed cooperation, initially designed around direct interactions with the two other pilots, has been slightly adapted with the start of the project:

- In addition to the initial two additional pilots Concordia and Echo, a fourth laureate had been funded: Cybersec4Europe. While the first two pilots had an orientation towards cyber-defence and industry, the latter was more balanced towards civilian applications and academia. What is more, additional European stakeholders demonstrated interest in the pilots: JRC, REA and ECSO in particular. Overall this assembled a wide variety of European assets and opportunities in cybersecurity, for which coordination and technical guidance was key.
- The European Commission, through DG CONNECT, proposed to hold monthly meetings between the coordinators of the 4 pilots in Brussels, starting on 6<sup>th</sup> February (M0) – hereafter, *Network meetings*. If time-consuming, this organization has allowed to bootstrap the collaboration process under favourable auspices, focusing on important organizational and alignment topics, and helping information to flow efficiently not only between the pilots, but with the Commission and the aforementioned European institutional stakeholders as well.

Under these conditions, cooperation actions with other pilots has been targeted at 4 major *lines of work*:

1. Operational programme management of the 4 pilots portfolio, with the aim of identifying concrete ways for the pilots to interact on core call topics.
2. Operational cooperation for piloting the Competence Network, with the goal of governing a community including, but not limited to, the 4 pilots.
3. Substantive cooperation for piloting the Competence Network, with the goal of identifying key areas of European collaboration including, but not limited to, the 4 pilots.
4. Concerted communications for piloting the Competence Network, aiming at disseminating common messages online and in specific events.

These objectives, in turn, have largely contributed to frame the work of the 4 pilots, not just under each pilot's purview, but as a key complementary operators of a wider common good: the European Competence Network. With this in mind, SPARTA representatives have made significant, demonstrable, and repeated efforts in the period, as illustrated in the next sections, to actively synchronize and contribute to this common good. Specific attention was paid to make sure individualistic ambitions and agendas did not interfere with the collaborative spirit that is key to the success of this endeavour, while still maintaining a high level of expectations for – and commitment to – the outcome of such collaborations.



## 4.1 Operational programme management

The goal with this objective was to identify focal points across pilots, stemming from the requirements set by their common starting point, the SU-ICT-03-2018 call for proposal. Among initial points: roadmapping, standards and certification, joint infrastructures and capability-building including cyber-ranges, threat intelligence, open tools, or awareness actions. Yet in the initial phases of the 4 pilots, identifying areas of collaboration was not an easy task for a few reasons:

- because in-pilot work had not started yet on all of topics, no initial footing existed from which to build fruitful collaborations on these topics; the pilots teams had to put significant effort in getting work off the ground, which left little concrete resources to establish and maintain cooperation;
- in particular, the terminology and areas of application varied widely between all pilots. An example of this was certification, which encompassed both technical, institutional, multi-sectoral, and sovereignty components;
- this was exacerbated by original approaches taken by some pilots on common topics. Here again, certification is a good example: some pilots focused on exploring technical opportunities for future product certification schemes, others were keen on taking part in standardization discussion groups;
- finally, the expected balance between pilot cooperation and differentiation (value for funding) was hard to define, especially under the circumstances described by first item of this list.

Facing what would be a more long-term alignment process, cooperation started nonetheless with the sharing of the four pilots' Description of Actions (DoA). From this exchange, the coordinator of Concordia extracted potential points of synergy between the four pilots. SPARTA volunteered the names of its Activity and Program leaders as possible contact points, and the idea of sharing common events (reviews, outreaches, etc.).

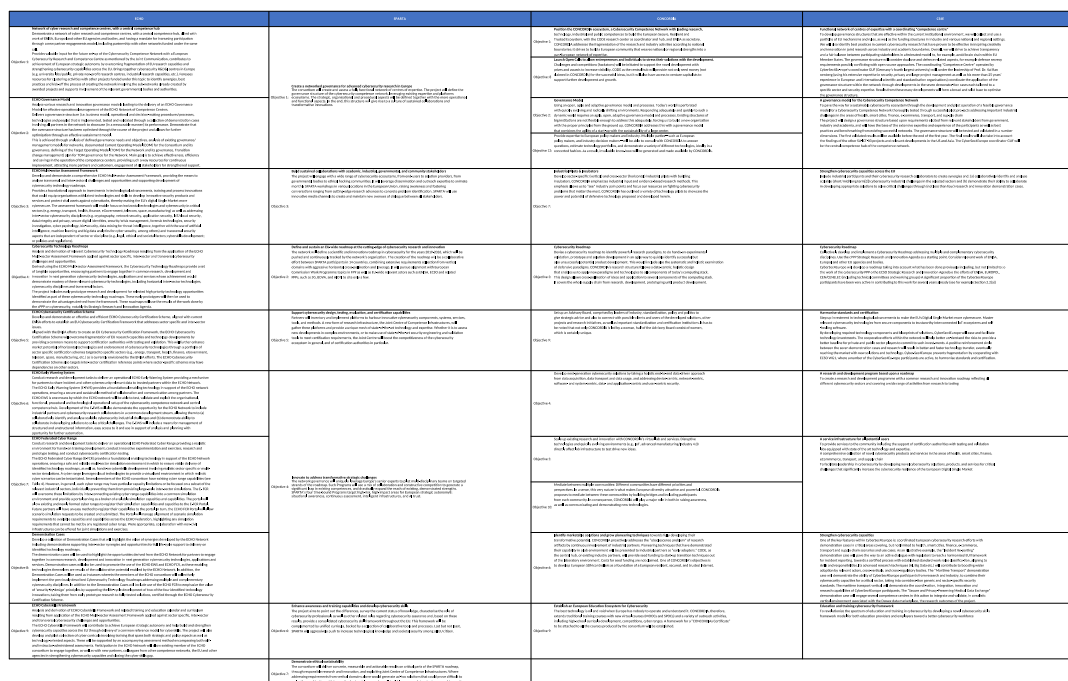


Figure 16: Potential points of synergy between the four pilots

The resulting extraction performed a syntactic comparison between the DoAs – pictured above for instance is the comparison between high-level pilot objectives. However, precise interpretations suffered from misunderstandings induced by the aforementioned reasons. As a result, to this day it could not be leveraged beyond initial discussions toward further cooperation actions. We believe



that further refinement, helped by the maturation of the concrete pilot actions and positioning, will significantly improve its usefulness.

## 4.2 Operational cooperation

From the initial Network meeting, the *operational* cooperation line of work was aimed at setting up procedures for upcoming collaborations. The identification of WP leaders for instance has also discussed under this angle. A particular attention was paid by SPARTA coordinators at the matter of confidentiality of communications: encryption procedures and trusted shared repositories hosted by the Commission were the result of these considerations. These considerations were collected into a Pilots Cooperation Handbook, under the responsibility of the Concordia coordinator, and are regularly updated.



<sup>†</sup> The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No 830927, No 830892 830943, No XXXXX.

Figure 17: Pilots Cooperation Handbook

Beyond inter-pilot collaborations, the question of onboarding new interested parties into the Network has been opened. A particular point of attention has been the incentives for such additional participants. SPARTA has been leading the collection and structuring of pilot contributions, and producing the aggregate “Associates Incentives” document below.



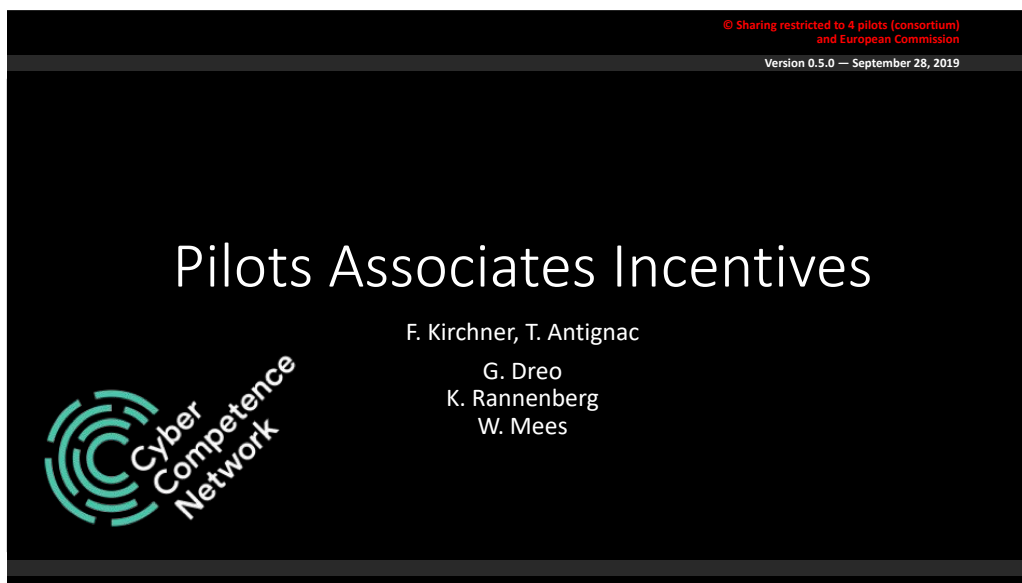
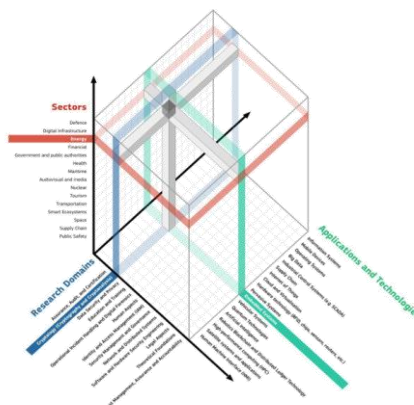


Figure 18: Pilots Associates Incentives

Discussions are still ongoing in this topic, with SPARTA's Partnership Director directly involved.

Finally, JRC's work on the cybersecurity Taxonomy and Atlas provided additional contributions to matters of operational cooperation. The Taxonomy defined a clear reference point for technical interactions, ranging from academic domains to industrial sectors and applications.



This greatly benefitted SPARTA's early Roadmap work, as well as the inter-pilot Technical & Industrial Challenges detailed in the next section.

The Atlas, while still under construction, already has sparked procedural discussions, especially around access rights and strategic intelligence.

### 4.3 Substantive cooperation

While operational cooperation is focused on procedures and support for collaborations, the substantive cooperation line of work tackled the best ways to invest in research and innovation actions to maximize impact. As a first step, SPARTA volunteered to lead the identification and collection of top investment priorities for Europe. Since the roadmapping work for all pilots was just beginning, this started with the identification of the main challenges being addressed by the technical part of the 4 pilots – Technical & Industrial Challenges, aka T&I Challenges. SPARTA coordination



bootstrapped this from an in-depth initial analysis of the pilots' DoAs, then followed by a round of reviews and comments on top of the first draft.



Figure 19: Technical and Industrial challenges

The result was one of the earliest documents compiled from common work, and was used to inform the Commission's suggestions for topics in the next Framework Programme, to update ECSO's SRIA, and to feed Member States research roadmaps.

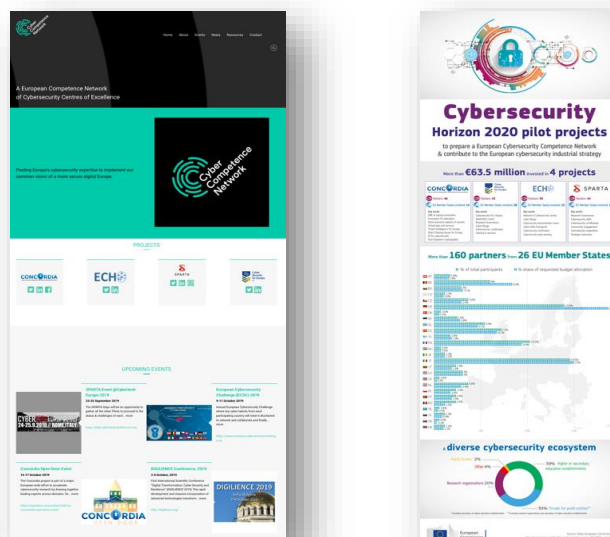
Another facet of this work was to get in touch with public authorities from Member States, and identify their priorities for public investments. To conduct this exercise, the idea was to step away from coordinator presentations of the 4 pilots as presented in the next section. Instead, the Network opted to rely on pilot partners that could present ambitious R&I opportunities, which might generate interest from specific subsets of Member States. SPARTA partners did an outstanding job of proposing "moonshot" topics, and then leading the design, consolidation, and animation of the resulting presentations to the Council's Horizontal Working Party on cyber issues, on 29 Nov 2019. The conclusion of that meeting was to reconduct similar discussions on a regular basis.

## 4.4 Concerted communications

For the Network to succeed, the alignment and efficiency of communication actions was deemed mandatory. A communication taskforce was quickly created at the start between all four pilots and the Commission, under the rotating leadership of the pilots, with the goal to set a framework for such alignment. The initial joint communications also came early, through the official launch of the pilots, and the associated campaign over social networks. Here the SPARTA dissemination team was notably active in efficiently producing flyers and infographics, as well as photo and video content.

This was quickly followed by the launch of a common website <https://cybercompetencenetwork.eu> creating an Internet entry point, redirecting to the respective pilot websites. A significant task from this line of work was the presentation of the pilots to Council, Parliament, and Commission stakeholders. This entailed, not only presenting the 4 pilots, but also exposing the underlying common rationale and results for them. SPARTA took a leading role in this work, organizing content and discussions, and structuring synthetic presentations, with the goal to ensure a fair and honest representation of all 4 pilot actions. These actions were successful in presenting the Network dynamics to Mariya Gabriel on 13 Mar 2019, to the Rapporteur for the proposed regulation (Rasmus Andresen) and Parliament Members (Claudia Gamon) on 5 Nov 2019, and to the SC7 programme committee on 26 Nov 2019.





In addition to the work performed on these 4 major lines of work, it is worth underlining the intrinsic utility of the monthly meetings to ensure a coherent mutual understanding. A notable gain, beyond the previously-mentioned topics, was the ability to follow closely, pilots and Commission together, the progress of the proposed regulation and future framework programme.

In conclusion, we believe the first year of inter-pilot collaboration has been remarkably successful at creating an embryo Competence Network. There is little doubt that this effort will need to be sustained to be successful, and SPARTA will strive to contribute to the best of its resources to that end.



## Chapter 5 Summary and Conclusion

Cyber security challenges are growing covering many if not all aspects of our life. The complexity and size of such challenges is such that single organizations or even nations cannot often cope with those. For many the solution is partnership, working together, taking advantage of powerful collaborative platforms and infrastructures to achieve the common goal security.

SPARTA partnership program aims at strengthening and consolidating the European ecosystem in cyber security stemming from strong national clusters of relevant organizations that pull together merging people, infrastructures (platforms) and knowledge to provide research innovation and advanced services for the European society and economy.

The reduction of the fragmentation at national and European level is one for the aspects SPARTA is going to sort out by recognizing that the 44 initial SPARTA partners cannot cover all cybersecurity domains, applications, and sectors, and that additional competences are necessary. Thus the notion of associate partner – able to interact by sharing information, resources and be part of the ecosystem – has been developed. We happily doubled initial number of partners and we continue to grow.

From a kernel of main RTO, industries, and national agencies we are growing to include further actors useful, first, to consolidate the national ecosystem, and second, to interact as a whole at the European level.

Cooperation with the main stakeholders at European level including agencies, projects and other relevant stakeholders started.

Finally it is worth mentioning that a Joint Competence Centre Infrastructure (JCCI) collecting, federating and integrating partners/associates tools and platforms is undergoing and a set of services available to the interested stakeholders already identified.



## Chapter 6 Appendix – Asset Inventory

The purpose of this document is to provide a template in which to reflect the main characteristics of the candidate assets to be part of the SPARTA JCCI.

The information provided will be used as a basis to establish, in the first place, which assets will be part of the SPARTA workbench. Subsequently will be chosen which of them will make up the SPARTA Cyber Range.

### 6.1 L3CE's SENTER

<b>Name of the asset</b>	SENER
<b>KeyWords</b>	Centers of excellence, collaborative platform
<b>Organization</b>	L3CE
<b>Point of contact</b>	egidija@l3ce.eu
<b>Location</b>	Didlaukio str. 55 LT-08329 Vilnius LITHUANIA

<b>Asset objectives</b>	Structured communication and secure environment for collaborative activities between EU LEA and Research community
<b>Technological Areas of Work</b>	<ul style="list-style-type: none"> <li>• Cybercrime</li> <li>• Dark Web</li> <li>• Open Source Intelligence</li> </ul>

#### 6.1.1 Functional Components Description

Structured communication and secure environment for collaborative activities (password protected area, sharing and storing information, having specialized charts, project and initiatives management capabilities). The portal is available at <https://www.senternetwork.eu/>.

The technical solution was designed to support effective co-creation process.

- Dedicated space for discussions will enable to find a common solution for up to date LEA challenges.
- New ideas sharing space will enable innovative ideas to be turned into technologies addressing end user needs.
- The centralisation of reference documents and templates in a shared space facilitates will support management of new opportunities and sharing of knowledge and best practices
- A new Integrated Calendar of Events which will provide a single entry point of all events organised by interested parties will open wider networking possibilities and access to EU knowledge base.



### 6.1.2 Services provided

- Dedicated space for forums and discussions
- Online document library: Reference documents and templates repository
- Files sharing and storage
- Events management tool

### 6.1.3 Current Usage

- Used by SENTER network partners and Special Interest Groups
- For multi stakeholders projects initiation, implementation and monitoring

#### 6.1.3.1 Past Projects

Name (Funds)	Short description
SENTER	The key objective of the SENTER project was to create a single point of Reference for EU Centers of Excellence (CoE) in the area of Cybercrime by developing further the Network of national CoE into well-defined and well-functioning community.
ECOPOL	The key objective of the project was to create conceptual model for automated information assessment tool.

#### 6.1.3.2 Live Projects

Name (Funds)	Short description
Lion DC	The Lion DC project aims to provide law enforcement agencies with the skills, methods and tools they need to counter drug trafficking on the Internet. The project will improve practitioners' understanding of online drugs crime phenomena (including potential interception and international cooperation points) and build their skills in dealing with the Dark Web. It will explore investigative techniques and tactics and test innovative technologies. It will also test ways to go beyond the "follow the money" principle, which relies on tracking cryptocurrencies and blockchain technologies. By using a wide range of sources, the project hopes to provide better ways of identifying criminals
I-LEAD	I-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-European LEA network.
SPARTA	Sparta is a novel Cybersecurity Competence Network, supported by Europe's H2020 program, with the objective to develop and implement top-tier research and innovation cooperative actions
PRoTEC	The general objective of the project is to provide all members of EFUS actionable European municipalities an actionable perspective on the protection of their public spaces and other soft targets, by providing them with good practices and access to technology concepts, and the knowledge to tailor them to their needs



### 6.1.3.3 Other relevant actions taking place

None.

### 6.1.4 Resources

#### 6.1.4.1 Scientific and Technological Team

**Mr. Evaldas Bruze** holds master's degrees in mathematics & informatics, as well as economics & business. He is an experienced coordinator and contributor to several national and EU-wide research, evaluation and technology projects focused on security issues, particularly on hybrid threats, radicalization, violent extremism and organized crime. His current work is related to the study of innovative methods and techniques to detect rare risks in cyber environments and assessing prevention strategies, for example, through strengthening the role of law enforcement intelligence units. He is an IT expert with a strong technical background as a solution architect & with operational skills in process management, including 15 years' experience in IT systems development projects. He played a significant role in the establishment of MRU's security LAB as a competence gateway for Cyber Security experts, R&D centers and security practitioners, and international networks of academia, as well as LEA in the cybercrime domain.

**Mr. Tomas Tauginas** Head of Analysis Unit, Dep. of Strategic Communication, LT Armed Forces with strong background of analytical skills, practical skills in IO monitoring & analysis and reporting. Strong skills in propaganda techniques, trends and prevention tactics. Leadership and coordination experience (operational monitoring) under high-intensity military action zone. Giving multiple presentations for stakeholders on strategic communication, information operations, and hostile information operations. Coordinator of Establishment of the Lithuanian Armed Forces Center for information Tasks Coordinator of Establishment of LT Armed Forces Center for Information Space Monitoring & Analysis (IO, Hybrid Warfare, Unconventional ops.)

#### 6.1.4.2 Technical Equipment

L3CE is a member of MRU Social Innovations Laboratories network (MRU LAB) and belongs to University research ecosystem that is known for having modern – and some of the best – infrastructure in the country. Auditoriums and lecture halls are equipped with the very latest equipment allowing Internet connectivity and providing for computerized work stations for students and lecturers. When Lithuania was Chairing the Presidency of the Council of the European Union in 2013, there were numerous international education and academic events held at MRU. The MRU LAB has established mobile work stations in two (80-seat and 30-seat) auditoriums in the open spaces with all the necessary equipment. The University Library is among the most modern of academic libraries in Europe. There is active implementation of open access policies and the IT network and infrastructure is well developed. According to "Rotten Wi-Fi", the quality of Wi-Fi at the University places MRU in second place among universities in the world. Mykolas Romeris University has all the human, infrastructure and financial resources, which are essential to accomplish the research project (e.g. 24-hour modern library; huge list of databases). In order to implement the project, the University will provide rooms, library, computer and project administration services. For scientific events of different extent, there is a number of seminar and conferences rooms ranging from 14 to 436 places. In all rooms are available ICT means and network. Therefore, it is able to host project events.

### 6.1.5 Request of use

<b>Ticketing system</b>	Registration
<b>Communication Channels</b>	-
<b>Time management</b>	-
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	Free access with prior registration



## 6.2 INRIA's LHS NGE

<b>Name of the asset</b>	LHS NGE
<b>KeyWords</b>	Data collection, securing hosting/storage, collaborative platform, large scale experimentation
<b>Organization</b>	INRIA
<b>Point of contact</b>	lhs-support@inria.fr
<b>Location</b>	Inria Nancy Grand-Est 615 rue du jardin botanique 54600 Villers-les-Nancy FRANCE

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Internet-wide security monitoring</li> <li>• Internet-wide scanning</li> <li>• Data analysis</li> <li>• Secure Data Hosting</li> </ul>
<b>Technological Areas of Work</b>	Chapter 1      Cyber-security Chapter 2      Machine Learning Chapter 3      Big Data

### 6.2.1 Functional Components Description

The High-Security Laboratory (HSL) is designed to host decisive research activities in order to make networks, Internet exchanges and associated telecommunications equipment safer. It allows to collect and store data while ensuring their confidentiality and integrity, both logically and physically, while offering a safe environment for researchers to work.

The HSL relies on “trust zones”, dedicated and isolated environments with limited and controlled interactions with the Internet. Such an environment benefits from all the services offered by the HSL (network and data protection, automatic backup, local services – APT, DNS, LDAP, NTP...) while been always separated from the outside world by two levels of security from different constructors/technologies (two firewalls from different constructors for the logical aspects, two different biometric authentication mechanisms for the physical ones), as shown in Figure 20.



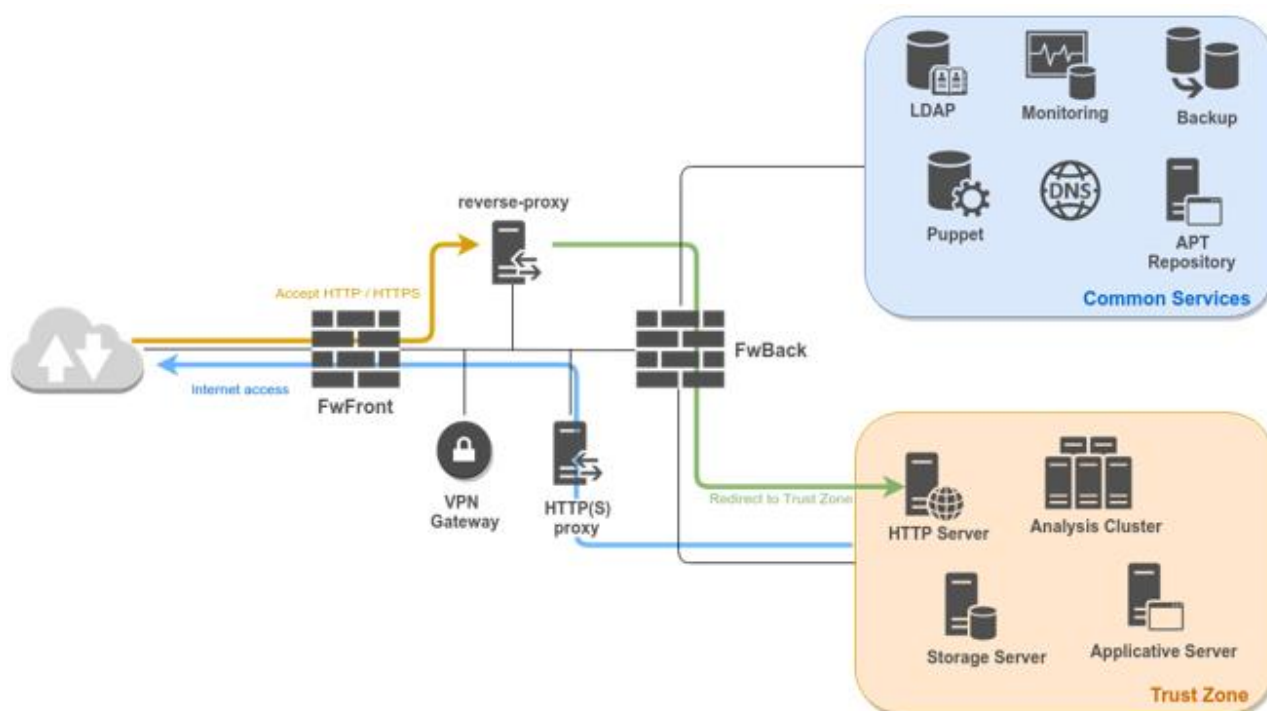


Figure 20: HSL global architecture and trust zone.

Such trust zones are deployed for each hosted project, including its own network and VLAN to ensure it is isolated from other hosted projects, but also user accounts and groups dedicated to the project in the HSL LDAP directory, associated firewalling and users/groups access lists policies (ACLs).

These zones are fully integrated to the automatic configuration and software management solution (puppet). The access to such a trust zone is possible through a dedicated Virtual Private Network (VPN), deployed exclusively for each project, and only limited to the user accounts linked to the project's LDAP groups.

## 6.2.2 Services provided

### Secure hosting

Allow secure hosting and analysis of sensitive data via dedicated trust zones

### Data collection and analysis via security sensors for a long term perspective

Place distributed data sensors and probes on the Internet, collect and enrich data automatically, and allow researchers to work on these datasets in the HSL

### Large scale experiments

Allow researchers to run Internet-wide experiments such as port scanning

### Dissemination and communication

Allow researchers to deploy public services or disseminate results regarding their activities in the HSL



## 6.2.3 Current Usage

### 6.2.3.1 Past Projects

Name (Funds)	Short description
FLAMINGO (EU)	The goals of FLAMINGO are (a) to strongly integrate the research of leading European research groups in the area of network and service management, (b) to strengthen the European and worldwide research in this area, and (c) to bridge the gap between scientific research and industrial application. To achieve these goals, FLAMINGO performs a broad range of activities, such as to develop open source software, establish joint labs, exchange researchers, jointly supervise Ph.D. students, develop educational and training material, interact with academia and industry, organize event, and strongly contribute to (IETF and IRTF) standardization.
HuMa (FR)	This project targets the analysis of Advanced Persistent Threat (APTs). APTs are long and complex attacks which thus cannot be captured with standard techniques focused on short time windows and few data sources. Indeed, APTs may last for several months and involve multiple steps with different types of attacks and approaches. The project addressed such an issue by leveraging data analytics and visualization techniques to guide human experts, which are the only one able to analyze APT, rather than targeting a fully automated approach

### 6.2.3.2 Live Projects

Name (Funds)	Short description
ThreatPredict (NATO)	Predicting attacks can help to prevent them or at least reduce their impact. Nowadays, existing attack prediction methods make accurate predictions only hours in advance or cannot predict geo-politically motivated attacks. ThreatPredict aims to predict different attack types days in advance. It develops machine-learning algorithms that capture spatio-temporal dynamics of cyber-attacks and global social, geo-political and technical events. Various sources of information are collected, enriched and correlated such as honeypot data, darknet, GDELT, Twitter, and vulnerability databases. In addition to warning about attacks, this project will improve our understanding of the effect of global events on cyber-security.
SecureIoT (EU)	SecureIoT is a joint effort of global leaders in IoT services and IoT cybersecurity to secure the next generation of dynamic, decentralized IoT systems, which will span spanning multiple IoT platforms and networks of smart objects, through implementing a range of predictive IoT security services. SecureIoT will architect predictive security services in-line with leading edge reference architectures (RA) for IoT applications (i.e. RAs of the Industrial Internet Consortium, the OpenFog Consortium and the Platform Industrie 4.0), which will serve as a basis for specifying security building blocks at both the edge and the core of IoT systems. SecureIoT will provide concrete implementations of security data collection, security monitoring and predictive security mechanisms, which will be the basis for offering integrated services for risk assessment, compliance auditing against regulations and directives (e.g. GDPR, NIS, ePrivacy), as well as support to IoT developers based on programming annotations. The services will be open and based on the SECaaS (Security-as-a-Service) paradigm.



### 6.2.3.3 Other relevant actions taking place

HSL is widely used in internal projects of INRIA.

## 6.2.4 Resources

### 6.2.4.1 Scientific and Technological Team

Frederic Beck (male) is a research engineer at Inria in the Experimentation and Development Department and acts as Technical Director for the High Security Laboratory at the Inria Nancy Grand-Est research center. His main research areas are related to networking and cyber-security, and closely linked to the Inria Resist team's projects, and other HSL related activities.

Jérôme François (male) is a research scientist at Inria in the RESIST team (former MADYNES) and supports the team leader, Isabelle Chrisment, as deputy leader. His main research area are focused on the use of data analytics techniques for security as well as the definition of software-based network monitoring probes both at the data and control planes. In 2019, he received the IEEE Young Professional award in Network and Service Management. He is in charge of different international collaborations of the research team with the University of Luxembourg and the University of Waterloo in Canada. In addition to publications, he started as associate Editor-in-Chief of Wiley IJNM (International Journal of Network Management) and as co-chair of NMRG (Network Management Research Group) at IRTF (Internet Research Task Force) in 2019.

### 6.2.4.2 Technical Equipment

Cyber security oriented datacenter	<p>Around 95 servers, organized in per-project clusters and trust zones:</p> <p>Chapter 1      8 to 40 cores per server</p> <p>Chapter 2      32 to 128 GB memory per server</p> <p>Chapter 3      1 to 20 TB disk space per server</p>
Network Telescope (darknet + honeypots)	<p>Available datasets:</p> <ul style="list-style-type: none"> <li>• Darknet data: passively collecting unsolicited traffic towards unused IP address space (4K addresses), 370GB compressed PCAP since nov. 2014</li> <li>• Honeypot data: various honeypots attack logs and traces (mainly NetFlow data) collected since 2008</li> <li>• Malwares collected through the honeypots</li> </ul> <p>Possibility to access live data streams via message queueing (RabbitMQ) and perform near realtime analysis of these events</p>
Blacklists aggregator	<p>Aggregate, centralize and preprocess (refinement and enrichment) relevant publicly available blacklists (IP, domain, URL) for further use (datasets annotation for example), available via MongoDB or RESTful API</p>
Security Knowledge Base	<p>Knowledge Base containing various security related standards (CPE, CVE, CWE, CAPEC) and their relationships, available through MongoDB or RESTful API</p>



### 6.2.5 Request of use

<b>Ticketing system</b>	Managed by the HSL support team
<b>Communication Channels</b>	On-site and partially VPN access
<b>Time management</b>	Labour days of the HSL support team between 9:00-16:00
<b>Granularity</b>	Access to subsystems can be provided
<b>Type of access (public, free, comm)</b>	Non profit (NDA and/or acknowledgement required)

## 6.3 INRIA's LHS RBA

<b>Name of the asset</b>	RBA
<b>KeyWords</b>	HW security evaluation, ransomware IDS
<b>Organization</b>	INRIA
<b>Point of contact</b>	Jean-louis.lanet@inria.fr
<b>Location</b>	Campus de Beaulieu, 263 Avenue Général Leclerc, 35042 Rennes FRANCE

<b>Asset objectives</b>	Security of the hardware Secure execution and detection of ransomware
<b>Technological Areas of Work</b>	EM Fault injection Bare metal malware execution

### 6.3.1 Functional Components Description

#### FAUSTINE Platform

The Platform Faustine is dedicated to EM fault injection. The EM hardware is controlled through several parameters (power, waveform, ...). It is adapted from low-end microcontroller (e.g. ST32) to high-end multicore SoC (e.g. Raspberry Pi3). Data acquisition is done through a high-speed oscilloscope. The target is inside a Faraday cage to avoid external EM perturbation. The device is mounted on a X-T-Z table allowing a high precision position of the probe. Several probes are available large coverage or precise coverage. Home-made probe for specific usage can also be used. A camera inside the cage allows a visual positioning of the device under the probe.





Figure 21: Faustine platform

### MoM Platform

The Mom platform is dedicated in one hand to grab malware from external database, to execute them on a Windows (7/8/10 operating system 32 and 64 bits) bare metal platform. Then, the platform stores the live samples in a database labelling with a probable identification. In the other hand, MoM can execute anti ransomware solution 24/7 on the slaves, recording several parameters like the number of byte lost before detection, the number of files lost and so on.

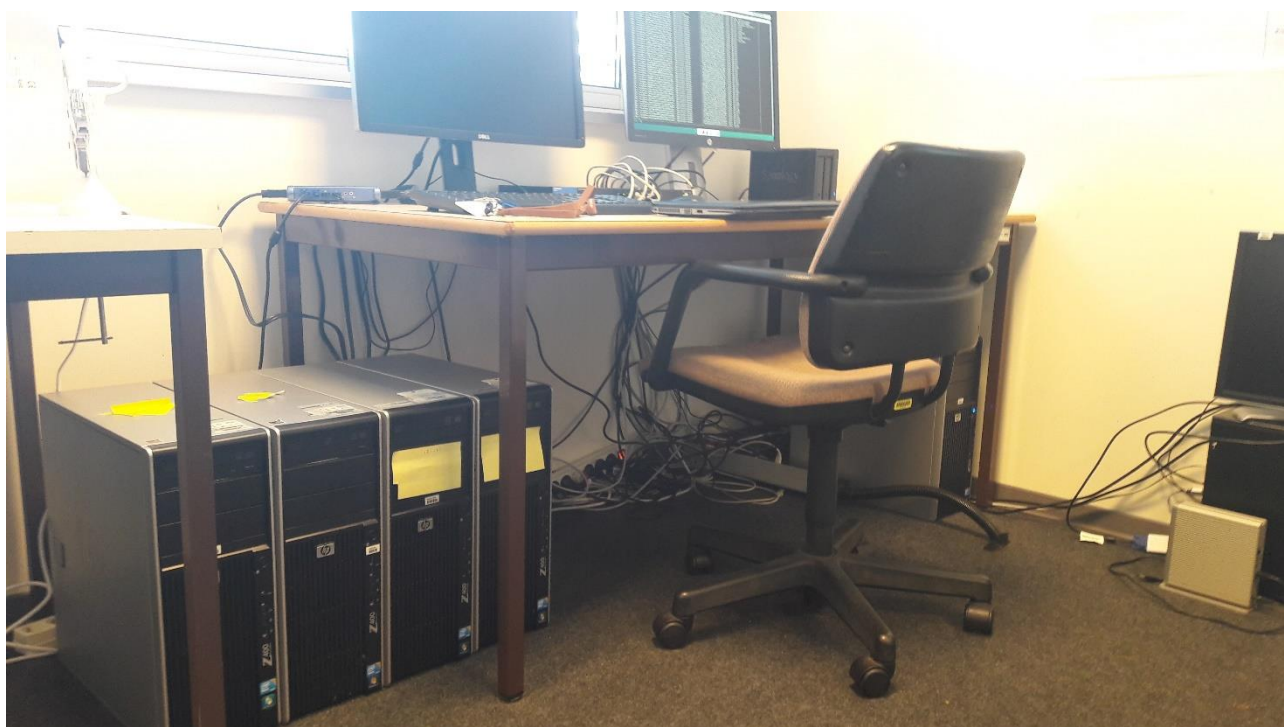


Figure 22: MoM platform.



The automated process is the following: a new image with different is loaded on a slave, a ransomware is sent to the slave, a session is automatically simulated (mouse, keyboard, applications processes...) and the ransomware is executed. If after a 15 minutes delay no activity is detected, a new image is loaded and a new ransomware is tested. If the ciphering activity is detected then the test results are stored in the database.

### 6.3.2 Services provided

Evaluation of the effect of fault into a software stack.

Evaluation of an anti-ransomware solution.

### 6.3.3 Current Usage

#### 6.3.3.1 Past Projects

None.

#### 6.3.3.2 Live Projects

Name (Funds)	Short description
SPARTA (EU)	Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

#### 6.3.3.3 Other relevant actions taking place

HSL is widely used in internal projects of INRIA.
---

### 6.3.4 Resources

#### 6.3.4.1 Scientific and Technological Team

Jean-Louis Lanet, joined <a href="#">INRIA</a> - Rennes Bretagne Atlantique in September 2014 to be involved into the High Security Labs (LHS). He was Professor at the University of Limoges (2007-2014) at the Computer Science department, where he lead the SSD team (Smart Secure Device). He was also associate professor of the University of Sherbrooke and he was in charge of the Security and Cryptology course of the USTH Master (Hanoi). His research interests include the security of small systems like smart cards, but also software engineering, malware analysis, hardware security.
Ronan Lashermé is a research engineer at INRIA Rennes, in the LHS lab. Engineer from Grenoble-INP Phelma, after finishing a Ph.D. with the CEA and the UVSQ in 2014, he worked in a startup to develop physical attack benches for devices evaluation. He later joined INRIA and the LHS lab for a postdoc on fault attacks. He is interested in the security of embedded systems and hardware components and how the abstraction barriers (mathematics/software, hardware/software) can be exploited to compromise a device.
Louis Bida Louis is a software engineer, he is specialized in embedded software and security. He worked for companies developing embedded products for automotive and security solution. At INRIA Louis works on ransomware detection and countermeasure. He manage the MoM platform.



### 6.3.4.2 Technical Equipment

Faustine:	Fault injection platform with EM environment to stress IoT devices and high end SoC. It includes EM probes, Signal generator, RF amplifier, High bandwidth oscilloscope, Faraday cage,... The software stack to design experiment is open source.
MoM:	Platform to evaluate ransomware. It includes a Database, direct access to Internet, baremetal execution on slave PC.

### 6.3.5 Request of use

<b>Ticketing system</b>	Managed by the HSL support team
<b>Communication Channels</b>	On-site and partially VPN access
<b>Time management</b>	Labour days of the HSL support team between 9:00-16:00
<b>Granularity</b>	Access to subsystems can be provided
<b>Type of access (public, free, comm)</b>	Mainly non profit.

## 6.4 Tecnalía's IDSOTER

<b>Name of the asset</b>	IDSOTER
<b>KeyWords</b>	IDPS, electrical network and equipment, machine learning
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	oscar.lage@tecnalia.com
<b>Location</b>	Parque Tecnológico de Bizkaia

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Intrusion detection for OT</li> <li>• Non-intrusive anomaly detection system in industrial environments</li> <li>• Integral monitoring of the infrastructure</li> </ul>
<b>Technological Areas of Work</b>	Cybersecurity, Industry, Intrusion Detection & Prevention Systems, Machines Learning, Energy, Manufacturing, Smart & connected machines

### 6.4.1 Functional Components Description

IDSOTER connected to a network will offer the following functionalities:

- Detection and analysis of sector-specific information and its protocols (Energy, Manufacturing, automotive, etc.)
- Non-intrusive and secure detection of:
  - Cyber incidents, including known cybersecurity attacks and possible Zero-Day attacks.



- Any anomaly in the operation of the process that may be the result of a principle of attack, unintentional errors or even malfunction of any device in the installation.
- Comprehensive, accessible and real-time view of process and system operation.
- Reduction of response times to incidents.
- Registration of all communications for forensic analysis of any cybersecurity incident or the incorrect operation of the system itself in order to identify responsibilities.

The main building blocks that conform the system are:

- Monitoring System: in charge of non-intrusive capture of network traffic and parsing the different domain-specific protocols.
- AI powered correlation engine: the correlation engine will have an overview of the data acquired by the monitoring systems in order to identify any anomalous situation in the infrastructure. The engine combines different techniques and strategies to fulfil its mission: signatures, machine learning, etc.
- Alert Manager: alert configuration system that in the future will also allow the automation of certain preventive actions on the infrastructure.
- Dashboard: control panel that allows the monitoring and even the configuration of the system using an intuitive web interface.

## 6.4.2 Services provided

### 6.4.2.1 Support platform for R + D + I projects

IDSOTER allows to easily capture and analyse the traffic of any industrial infrastructure. Thanks to its modular architecture it can be used to capture and parse industrial protocols for the design of artificial intelligence modules, validate the effectiveness of IDS systems and mathematical algorithms, capture real traffic from an industrial infrastructure in order to train artificial neural network, etc.

It can be used to develop R+D+I projects with a cooperative approach.

### 6.4.2.2 Training

The asset may be used as a platform for offering and developing a wide-range of training activities related to anomaly detection and industrial infrastructure protection, even incorporated to cyber ranges.

### 6.4.2.3 Consultancy

The asset may be used as a platform to support activities performed around consultancy services, allowing an analysis of the infrastructure, inventory of assets, identification of segments and conduits, etc.

## 6.4.3 Current Usage

### 6.4.3.1 Past Projects

Name (Funds)	Short description
SEKUTEK - SEKurtasun TEKnologiak	<p>SEKUTEK objectives were to increase:</p> <ul style="list-style-type: none"> <li>• Availability of installations, manufacturing processes and embedded systems in industrial domains.</li> <li>• Information integrity of the industrial equipment, of the people and the developments and configurations of devices and industrial networks.</li> </ul>



Name (Funds)	Short description
	<ul style="list-style-type: none"> <li>Information confidentiality and the protection of the intellectual property.</li> </ul> <p>In the context of this project, IDSOTER was developed and tested as an IDS for the energy sector.</p>

#### 6.4.3.2 Live Projects

Name (Funds)	Short description
SPEAR – Secure Private Smart Grid	Securing smart grids against cyber-attacks is of vital importance for National Security and Public Safety, since the collapse of an energy production utility may cause human lives, millions of euros, denial of a very important and common good such as energy and days or even months of recovering. To this end, the SPEAR proposal aims at a) detecting and responding to cyber-attacks using new technologies and capabilities, b) detecting threat and anomalies timely, c) developing all-in-one security detection solutions, d) leveraging advanced forensics subject to privacy-preserving, e) confronting Advanced Persistent Threat (APT) and targeted attacks in smart grids, f) increasing the resilience of the smart grid innovation, g) alleviating the lack of trust in smart grid operators and h) empowering EU-wide consensus. Within SPEAR, four proof-of-concept Use Cases are planned in order to validate and assess the implemented security and privacy tools.
ENACT - Trustworthy and Smart Actuation in IoT systems	Smart IoT systems typically operate in a changing and often unpredictable environment, the ability of these systems to continuously evolve and adapt to their new environment is decisive to ensure and increase their trustworthiness, quality and user experience. The DevOps movement advocates a set of software engineering best practices and tools, to ensure Quality of Service whilst continuously evolving complex systems and foster agility, rapid innovation cycles, and ease of use. There is no complete DevOps support for trustworthy smart IoT systems today. The main technical goal of ENACT is to develop novel IoT platform enablers to: i) Enable DevOps in the realm of trustworthy smart IoT systems and enrich it with novel concepts for end-to-end security and privacy, resilience and robustness strengthening trustworthiness, taking into account the challenges related to “collaborative” actuation and actuation conflicts. ii) Facilitate the smooth integration of these to leverage DevOps for existing and new IoT platforms and approaches (e.g., FIWARE, SOFIA, and TelluCloud).
TRAZAK – Monitoring, trazability and response cybersecurity service in Industry 4.0	TRAZAK objectives are related to building technologies for solving monitoring challenges in industrial environments like the effective monitoring of industrial network protocols and industrial devices and the trazability and contro-analysis of a real time industrial attack.
SUCESO – Machine Learning supported Cybersecurity	Compromise Indicators (IOC) requires refinements when talking about applying them in production.



Name (Funds)	Short description
	<p>Such IOCs act as patterns for detecting anomalous behaviors, but require adjustments to each individual case based on each company's data flow.</p> <p>It is intended that this customization and adjustment of indicators will become customized, but at the very least can provide solutions tailored to the most typical parameters of a specific sector.</p>

### 6.4.3.3 Other relevant actions taking place

Live demonstration to local industrial companies in the BDIH Cybersecurity in the Smart Grid Lab.

## 6.4.4 Resources

### 6.4.4.1 Scientific and Technological Team

Mr. Eneko Gómez Ramos (male) is a Telecommunication Engineer, majoring in Telematics, by the University of the Basque Country (UPV/EHU). He works in Tecnia as R&D Engineer for the Cybersecurity & Safety Group of the IT Competitiveness Area on the ICT (TIC) Division. He is currently researching about Blockchain technologies (Hyperledger Fabric, Ethereum, Quorum) applied to industrial systems and processes. During his experience as CyberSecurity senior researcher, Eneko has taken part in public and private projects related to cryptographic tools, vulnerability analysis, secure architecture designs and security anomaly detection through heuristic techniques. Some of the main CyberSecurity-related technologies Eneko deals with are Blockchain, PKI, IAM platforms, IDS, log analysis and network monitoring, having applied some of these technologies in industrial environments in projects such as WHITEZONE, SOTER or PETROLOC. Moreover, Eneko is an expert software developer that deals frequently with languages such as Java, Python or C++, relational databases (MySQL, PostgreSQL), cloud technologies and interoperability formats (XML, JSON, YAML); using them both in web (Django framework...) and mobile (Android...) developments.

Mrs. Erkuden Rios (female) is R&D project manager of Cybersecurity and Safety team within the ICT Division of Tecnia. She is currently coordinator of the H2020 MUSA project on multi-cloud security ([www.musa-project.eu](http://www.musa-project.eu)), and the coordinator of the Data Protection, Security and Privacy in Cloud Cluster of EU-funded research projects, launched by DG-CNECT in April 2015 (<https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/>). She is specialised in trust and security engineering technologies and has coordinated and worked in a number of large European and Spanish national projects on the subject such as TACIT, SWEPT, ANIKETOS, RISC, CIPHER and SHIELDS. Erkuden collaborates with Technology Platforms and Forums relevant to the project such as cPPP - ECSO, AOITI and the Spanish Technology Platform on Trust & Security – eSEC. After obtaining her MSc in Telecommunication Engineering at the University of Basque Country (Spain), she worked for Ericsson Spain for 6 years before joining Tecnia in 2003.

Mrs. Eider Iturbe (female) is a R&D engineer of Cybersecurity and Safety team within Tecnia. She is specialized in trust and security engineering technologies and has broadened its expertise through her participation in different European and Spanish national projects such as ANIKETOS, SWEPT, TACIT, and CIPHER. She is currently leading the architecture and integration work package in MUSA project ([www.musa-project.eu](http://www.musa-project.eu)), on multi-cloud secure applications. Eider graduated in Telecommunication Engineering from the University of the Basque Country (Spain) and in the European Master in project management at the same university. Before joining Tecnia in 2009, she worked for software consultancy firms where she acquired management skills and a great technical expertise in the security field.



Mr. Saturnino Martínez Melchor (male) is a seasoned Computer engineer with more than 20 years' experience in Cybersecurity field. He has worked in Panda Security as a Malware Researcher for 15 years applying Machine Learning Technologies to Cybersecurity now working in Tecnalia in related tasks but more oriented towards Industrial security. He has worked in the development of a Threat Hunting platform and detecting APTs and hacker intrusions on big companies like banks and telecommunications companies. Currently working in two European projects aimed at detecting network traffic anomalies in Smart Grids (Energy) and in IoT systems. He has also been involved as Professor in the Official Security Master's Degree at the University of Deusto.

#### 6.4.4.2 Technical Equipment

Monitoring System	It must be run on a Debian-based OS. In addition, the HW must be compliant with the specific regulations of the industrial infrastructure.
AI Powered correlation engine	A machine with at least 32GB of RAM, 1 TB of SSD Disk and at least 8 cores of CPU.

#### 6.4.5 Request of use

<b>Ticketing system</b>	Managed by TECNALIA TrustTech team
<b>Communication Channels</b>	Either VPN access to infrastructure or inhouse installation
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit

### 6.5 Tecnalia's OPENCERT

<b>Name of the asset</b>	OPENCERT
<b>KeyWords</b>	Assurance cases, Standards Compliance, Assurance Accountability, GSN
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	alejandra.ruiz@tecnalia.com
<b>Location</b>	Parque Tecnológico de Bizkaia

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Monitoring regulation process compliance</li> <li>• Assurance cases evolution</li> <li>• Assurance evidence accountability</li> <li>• Support for compositional certification</li> </ul>
<b>Technological Areas of Work</b>	Cybersecurity, Safety, Automotive, Aerospace, Energy, Medical devices, robotics



### 6.5.1 Functional Components Description

The current features of OpenCert include the management of information from standards and regulations, the management of assurance projects, assurance case management, and compliance management.

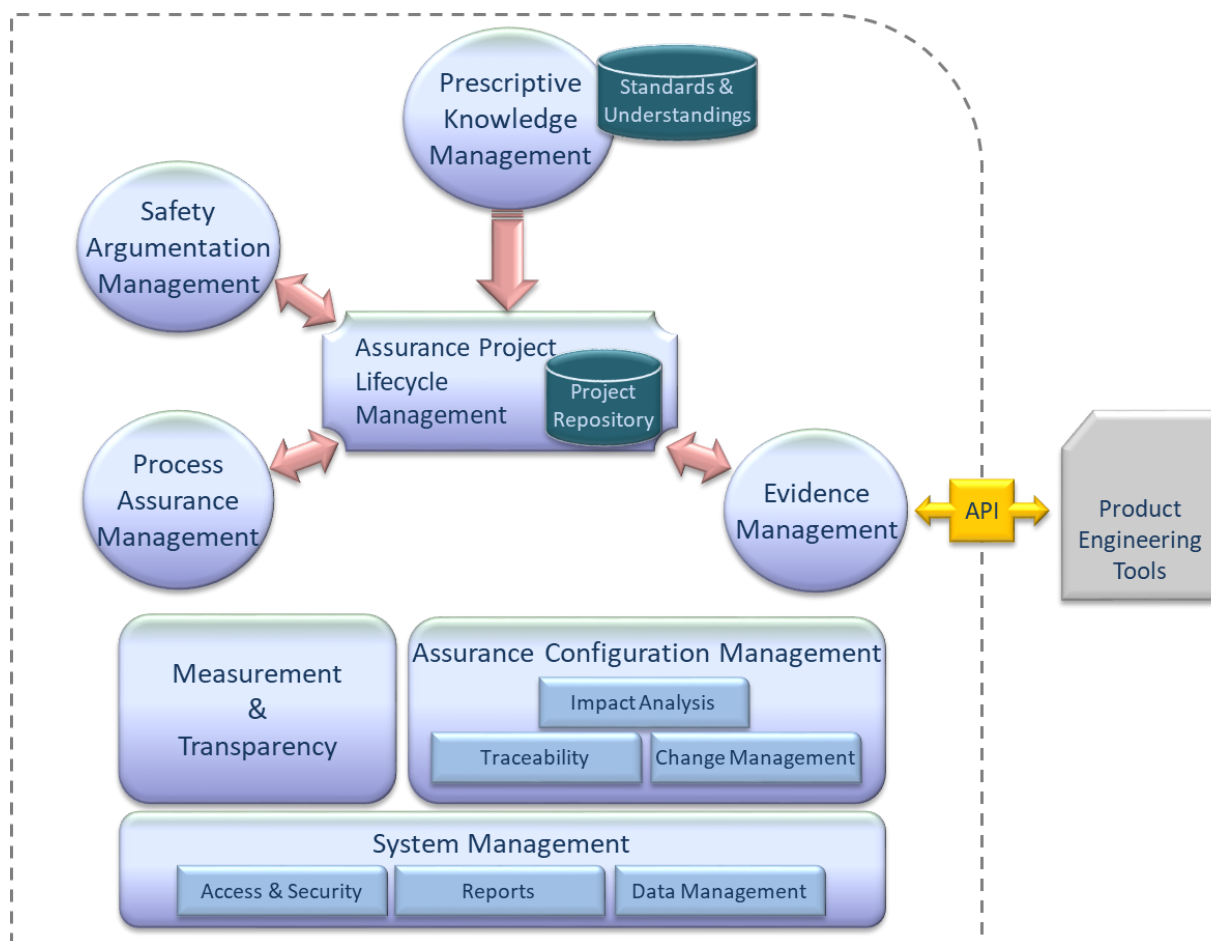


Figure 23: Functional decomposition of OpenCert platform.

The main functional blocks from OpenCert are:

- **Reference Framework Management:** Functionality related to the management of standards information as well as any other information derived from them, such as interpretations about intents, mapping between standards, etc. This functional group maintains a knowledge database about “standards & understandings”. The database is independent of the assurance projects.
- **Assurance Project Lifecycle Management:** This functionality factorizes aspects such as the creation of assurance projects. This module manages a “project repository”, which can be accessed by the other modules.
- **Assurance Case Management:** This group manages argumentation information in a modular fashion. It also includes mechanisms to support compositional safety assurance, and assurance patterns management. It supports the idea of the assurance case as the OMG defined “An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. An Assurance Case is a document that facilitates information exchange between various system stakeholder such as suppliers and acquirers, and between the operator and regulator, where



the knowledge related to the safety and security of the system is communicated in a clear and defendable way”<sup>4</sup>.

- **Evidence Management:** This module manages the full life-cycle of evidences and evidence chains. This includes evidence traceability management. This module is used to store all evidenced used for regulatory accountability purposes.
- **Assurance Reporting:** This functionality is related with the reporting and compliance levers measurement.

## 6.5.2 *Services provided*

### 6.5.2.1 Support platform for R + D + I projects

The OpenCert platform was developed in the context of an R&D project and it has evolved in later R&D projects with a cooperative approach. There is an open source version being maintained inside the umbrella of the Eclipse community with different extensions developed either in collaboration with TECNALIA or by individually or third parties by themselves.

These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use regulation and standards models used in the regulation database are contemplated for using the platform for the aim of financing the projects amortization or maintenance.

### 6.5.2.2 Benchmarking, evaluation and / or certification of products and / or services

The platform can be used to support certain activities done during the development process for certification purposes such as evidence accountability or assurance cases edition and evolution.

### 6.5.2.3 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, security informed safety cases or a specific security standard compliance process. In other words, enabling access to end users, companies offering cybersecurity training or researchers, so they can prepare and provide training.

### 6.5.2.4 Consultancy

The asset may be used as a platform to support activities performed around consultancy services around

- Privacy and GDPR appliance
- Functional safety standards such as ISO 26262, IEC 61508 appliance
- Security management related standards appliance such as IEC 62443

### 6.5.2.5 Support for awareness actions or generation of cybersecurity culture

In the event that public-private partnerships are encouraged, the platform could be used in a public demo showing the different assurance activities perform during the product development process in order to comply with a specific standard or to ensure that threats and or hazards have been managed, creating appealing scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

---

<sup>4</sup> OMG; SACM – Structured Assurance Case Metamodel v2.1, March 2019



### 6.5.3 Current Usage

#### 6.5.3.1 Past Projects

Name (Funds)	Short description
OPENCOS	OPENCOS was a European large scale integrating FP7 project. The project aims to produce the first European-wide open safety certification platform: an Open Platform for Evolutionary Certification Of Safety-critical Systems. The purpose of the platform is to reduce time and cost for (re)certification of safety-critical embedded systems, in particular for the railway, avionics and automotive markets. It was the origin and first release for OpenCert.
SafeAdapt	Safe Adaptive Software for Fully Electric Vehicles. The main idea of SafeAdapt is to develop novel architecture concepts based on adaptation to address the needs of a new E/E architecture for FEVs regarding safety, reliability and cost-efficiency. TECNALIA dealt with assurance issues and ISO 26262 compliance interpretation related to safe adaptation and a novel fail-operational behaviour based on a model-driven development of self-describing components for self-adaptive distributed embedded systems.
SEKUTEK - SEKurtasun TEKnologiak	SEKUTEK objectives were to increase: <ul style="list-style-type: none"> <li>• Availability of installations, manufacturing processes and embedded systems in industrial domains.</li> <li>• Information integrity of the industrial equipment, of the people and the developments and configurations of devices and industrial networks.</li> <li>• Information confidentiality and the protection of the intellectual property.</li> </ul>

#### 6.5.3.2 Live Projects

Name (Funds)	Short description
AMASS	TECNALIA has led the ECSEL Joint Undertaking project AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems). AMASS has created and consolidated the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, and energy. In the project, OpenCert evolved to support the management of information from standards and regulations, the management of assurance projects, architecture-driven assurance, assurance case management, and compliance management. For architecture-driven assurance, OpenCert is linked with the Papyrus [3] and CHES [4] Eclipse projects, and with the EPF project [5] for compliance management.
PDP4E	PDP4E will extend OpenCert towards privacy assurance by leveraging MDE techniques. OpenCert will be used in PDP4E to support assurance related management processes to demonstrate compliance with data protection regulation. The objective is to be able to check the progress of product (software system, Cyber physical system, service) compliance with regulations such as GDPR in a transparent way. At the same time, PDP4E aims at providing



Name (Funds)	Short description
	guidance to product management in order to plan their development to comply with GDPR rules and provide semi-automated actions such as report generations in relation with compliance activities. The goal will be to provide guidance on how to comply with the GDPR and help to check accomplishments.
AQUAS	The AQUAS project (Aggregated Quality Assurance for Systems) investigates the challenges arising from the inter-dependence of safety, security and performance of systems and aims at efficient solutions for the entire product life-cycle within three essential capabilities of the ECSEL JU MASRIA 2016: Design Technologies (DT), Cyber-Physical Systems (CPS), and European Asset Protection (EAP). OpenCert is used in AQUAS to support a common process for developing a co-engineering product lifecycle and the creation of specific assurance cases as a result of the interaction points between the different communities of experts (safety/security/performance).

### 6.5.3.3 Other relevant actions taking place

Live demonstrations to industrial companies.

## 6.5.4 Resources

### 6.5.4.1 Scientific and Technological Team

Dr. Alejandra Ruiz (female) holds a Ph.D. degree in Telecommunications and Computer Engineering, (2015, U. of Deusto), an MSc in Advanced Artificial Intelligence (2012, UNED) and the degree in Telecommunication Engineering (2005, University of Deusto). She joined Tecnalia in 2007 and is a Research Engineer in the Cyber Security and Safety group. She currently leads the area of Modular Assurance and Certification of Safety-critical Systems, with particular focus on automotive, aerospace, railway and medical device industries. She is the main contributor in these areas for European projects such as RECOMP (Reduced Certification Costs for Trusted Multicore Platforms), OPENCROSS (Open Platform for Evolutionary Certification of Safety-critical Systems) SafeAdapt (Safe Adaptive Software for Fully Electric Vehicles) and EMC2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments). Dr. Ruiz has extensive experience on EU projects as project leader and has coordinated the work of large international teams, such as e.g. the AMASS ECSEL project.

Dr. Jabier Martinez (male) joined the cyber-security and safety department of TECNALIA in 2018. His background is on providing methods and tools for achieving systematic reuse covering all the artifacts that conform a system life-cycle. He obtained the title of computer engineering from the University of the Basque Country in 2007 and, after several years of industrial experience, he received his PhD in 2016 from the Luxembourg University (SnT, Interdisciplinary centre for Security and Trust) and Sorbonne University (Lip6, Laboratory of Computer Sciences, Paris 6) with an awarded thesis about mining software artefacts for product line migration and analysis. He co-organizes the Reverse Variability Engineering series of workshops and has authored more than thirty peer-reviewed publications on software reuse, variability management and software product lines.

Mr. Angel López (male) has more than 17 years of experience working on research projects. He was involved in European project OPENCROSS, whose objective is to produce the first European-wide open safety certification platform: an Open Platform for Evolutionary Certification Of Safety-critical Systems. The purpose of the platform is to reduce time and cost for (re)certification of



safety-critical embedded systems, in particular for the railway, avionics and automotive markets. He was also involved in the European project AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems). This project is continuation of OPENCROSS project that will create and consolidate the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, energy. Mr. López is the open source project Lead for OpenCert public version.

#### 6.5.4.2 Technical Equipment

Server Asset	Quantity
IT TECHNOLOGIES	
COMPUTERS	
Hard Disk 50Gb	1
RAM 4GB	1
SOFTWARE LICENSES	
Windows 10 - 64 bits	1
PostgreSQL Database Server 9.3.15 or 9.4.10 version	1

Client Asset	Quantity
IT TECHNOLOGIES	
COMPUTERS	
Dell Pc PRECISION 3530, 16Gb,200Gb	1
SOFTWARE LICENSES	
Windows 10 Pro - 64 bits	1
Java Runtime Environment 1.8	1

#### 6.5.5 Request of use

<b>Ticketing system</b>	Managed by Eclipse and assisted by TECNALIA
<b>Communication Channels</b>	Internet access to the public infrastructure
<b>Time management</b>	Completed labour days, support can be requested to the whole community by email
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	public



### 6.5.5.1 Privacy compliance specialized version

<b>Ticketing system</b>	Managed by TECNALIA TrustTech team
<b>Communication Channels</b>	Either VPN access to infrastructure or inhouse installation
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Commercial

## 6.6 Tecnalia's SABOTAGE

<b>Name of the asset</b>	SABOTAGE
<b>KeyWords</b>	Fault Injection, Simulation, Safety, Model-based Design
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	estibaliz.amparan@tecnalia.com
<b>Location</b>	Parque Tecnológico de Bizkaia

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Early evaluation of the dependability of safety-critical systems.</li> <li>• Validation and Verification of dependable systems.</li> <li>• Testing of the robustness of system architecture.</li> </ul>
<b>Technological Areas of Work</b>	Integrated cybersecurity and safety, fault /attacks injection, Model-based Design, Automotive, Robotics, Avionics

### 6.6.1 Functional Components Description

Model-driven and simulation-based fault injection tool to accomplish an early evaluation dependability evaluation of safety-critical systems. The framework sets up, configures, executes and analyses the simulation results. It includes a fault model library and it is possible to connect to virtual environments such as a virtual vehicle or a robot.

The user, such as the safety engineer, starts configuring the fault injection experiments by creating the fault injection policy or fault list (Where should the faults be injected? What is the most appropriate fault model representing the functional failure modes? How should the faults be triggered within the system? Where should the fault effect be observed?). Then the faulty model is created, and the fault free simulation compared to the faulty ones. This means running, storing, visualizing and computing the obtained simulation traces, while comparing the results versus a pre-established safety requirement or pass/fail criterion.

The Sabotage tool can be used in an early assessment of safety-critical systems. It is a tool based on the Simulation fault injection technique which involves the construction of a simulation model (Simulink) of the system under analysis. Thanks to this simulated system the verification and validation is achieved during early development phases.



## 6.6.2 Services provided

### 6.6.2.1 Support platform for R + D + I projects

The Sabotage tool was developed under two different European projects and it will be used to develop R+D+I project with a cooperative approach.

### 6.6.2.2 Benchmarking, evaluation and / or certification of products and / or services

The Sabotage tool could be used to support benchmarking, evaluation or validation of safety critical systems.

### 6.6.2.3 Training

This tool could be used as a platform for offering and developing several training activities, e.g. cyber-ranges to enable access to end users, companies or researchers.

### 6.6.2.4 Support for awareness actions or generation of Functional Safety culture in different domains

Currently, there are some domains like the automotive or aerospace ones that are widely aware about the importance of testing techniques for the verification and validation of safety. Nevertheless, other domains which are emerging strongly in the last decade such as Robotics are not aware about the safety critical risks, for example, collaborative robots. This is one of the reasons why different testbeds will be developed creating different scenarios to show these weaknesses and how to improve them.

## 6.6.3 Current Usage

### 6.6.3.1 Past Projects

Name (Funds)	Short description
eITUS-RobMoSys ITP	The eITUS project aims at creating a basic experimental infrastructure (models, software and tools) that enables robotic development stakeholders to assure system safety at design time, using analysis and simulation-based techniques. <a href="https://robmosys.eu/e-itus/">https://robmosys.eu/e-itus/</a>

### 6.6.3.2 Live Projects

Name (Funds)	Short description
AMASS	The AMASS project creates and consolidates the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, and energy. <a href="https://www.amass-ecsel.eu/">https://www.amass-ecsel.eu/</a>
AUTOSAR	AUTOSAR project will research and develop functional modules based on the fusion of complex-analysis algorithms and understanding of the environment, to generate a platform which allows the automation of safe and secure heterogeneous vehicles.



### 6.6.3.3 Other relevant actions taking place

Presentation of the “*Design-Time Safety Assessment of Robotic System Usign Fault Injection Simulation in a Model-Driven Approach*” paper in Morse 2019: International Conference on Mechatronics, Robotics, and System Engineering

Live demonstrations to local industrial companies.

## 6.6.4 Resources

### 6.6.4.1 Scientific and Technological Team

Mrs. Estibaliz Amparan Calonge (female) carried out her Degree in Industrial Electronic and Automation Engineering at the University of the Basque Country (EHU/UPV). She is currently studying for a master’s degree specialised on Computational Engineering and Smart Systems at the University of the Basque Country. In 2016 she joined the research group of Safety and Cybersecurity at TECNALIA where she has been researching on Safety critical-embedded systems into different domains as Automotive and Robotics. She focuses on the functional safety from the design to the verification and validation of systems. Currently, she is developing a tool for safety analysis which is based on the methodology of Simulation-based Fault Injection. The simulation-based Fault injection tool allows the evaluation of the robustness of design at early development phases. She worked on different European research projects as AMASS and eITUS. Both projects are focused on the development of new tools and methodologies to reach a high level of safety on critical systems.

Mr. Angel Lopez Carrera (male) is member of Safety and Cybersecurity research group of Tecnalia. He is the technical responsible of WHITEZONE, a Tecnalia’s cybersecurity product that prevents malware presence at the operational zone of an industrial plant or critical infrastructure and restricts the access, to the delimited area designed as operational zone, only to the authorised users carrying safe and identified software. He was involved in the OPENCROSS European project, which was the first European-wide open safety certification platform. The AMASS European project was the continuation of OPENCROSS that created and consolidated the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, energy. In his 17 years of experience he was working in a lot research projects, for example, developing applications for decision making processes, developing agile algorithms for indexation and retrieval of medical images by visual similarity in great data volumes, web and desktop tools for management, an Indoor Location System based on WI-FI signal, as well as working on knowledge extraction applications related to social networks in the Internet.

Mrs. Cristina Martinez Martinez (female) BSc in Computing Engineering from University of Deusto (Bilbao, 1989) and MSc in “Foundations of Advanced Information Technologies” – Imperial College (University of London, 1990). Her working experience in the ICT Division of TECNALIA has focused primarily on the development and management of projects related to the implementation of secure and reliable systems and services in different areas: workflow platforms and document management systems, digital assets management, digital security, advanced user interfaces design and user experience. Responsible of the Privacy and Digital Security Cluster within the AmlGUNE program (ETORTEK 2005-2007, Basque Government). Responsible of the design, development and deployment of a commercial Tool for Document Management, Workflow Design and Workflow Management. Currently she is researcher and project manager of R&D national and international projects related to CPS and Cybersecurity. She has managed Tecnalia’s participation in several EU projects such as: €-Confidential (UE/ ITEA), VITALAS (FP6-IST),



ASSETS (CIP-ICT PSP), SecureSME (FP6-SEC), SecureCHAINS (FP7-Security), AMASS (H2020-ECSEL 2015) and SPARTA (H2020-SU-ICT-2018).

Mr. Daniel Landa (male) obtained his bachelor's in Information Systems Engineering by Deusto University (Bilbao, 2004). Currently he develops his activity as a senior technologist in the Cyber Security & Safety area within the ICT division of Tecnalia. Wide experience in the development of high availability, scalable cloud-applications about mobile payments and geolocation using wearables over Linux systems in Django/Python server environments. He has led the design and development of a multimedia assets manager (MAM) for professional broadcast environments (Media department, Tecnalia). Previously he took part in the development of an ERP over Microsoft's .NET platform in Bangalore (India, Lantek I+D, 2005-09). Formerly he worked, thanks to the Leonardo Da Vinci scholarships program of the Ministry of Science and Innovation of the Government of Spain, in the development of documentary management tools with open source web technologies in the Institute of composite materials of Kaiserslautern (Germany, IVW, 2005).

#### 6.6.4.2 Technical Equipment

Sabotage has been developed on the Eclipse environment (Eclipse Modelling tools Neon 0.3).

##### Requirements

Java SE 1.8

MATLAB/Simulink from 2017b version

##### Tool documentation

Sabotage: A Simulation-Based Fault Injection Tool Framework

<https://www.cyberssbytecnalia.com/node/271>

AMASS D3.3 deliverable, pages 57-62

[https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D3.3\\_Design-of-the-AMASS-tools-and-methods-for-architecture-driven-assurance-%28b%29\\_AMASS\\_Final.pdf](https://www.amass-ecsel.eu/sites/amass.drupal.pulsartecnalia.com/files/documents/D3.3_Design-of-the-AMASS-tools-and-methods-for-architecture-driven-assurance-%28b%29_AMASS_Final.pdf)

#### 6.6.5 Request of use

<b>Ticketing system</b>	Managed by TECNALIA TrustTech team
<b>Communication Channels</b>	By email
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	Non profit



## 6.7 Tecnalia's Smart Grid Facilities

<b>Name of the asset</b>	BDIH Cybersecurity – Cybersecurity for the Smart Grid Laboratory
<b>KeyWords</b>	OT Cybersecurity, Machine Learning, Honeypots
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	ana.ayerbe@tecnalia.com
<b>Location</b>	Parque Científico y Tecnológico de Bizkaia

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Simulate the real communications between the different equipment and systems that conform a Substation and Telecontrol Center.</li> <li>• Penetration testing</li> <li>• Testing the response to cyberattacks</li> <li>• Test the effectiveness of attack detection tools</li> </ul>
<b>Technological Areas of Work</b>	Cybersecurity, Energy, Smart Grid, Ethical Hacking

### 6.7.1 Functional Components Description

The Laboratory of Cybersecurity in the Smart Grid emulates a Software - Hardware real time communications environment of a Primary Distribution Substation, in which the electronic equipment (IEDs) that control and supervise the electrical equipment (switches, transformers ...) have been deployed. It also simulates a Control Center, with basic functionalities, to which the Substation equipment is connected.

The laboratory allows to:

- Simulate the real communications between the different equipment and systems of the control center and the substation.
- Play a set of cyber-attacks through tools for generating penetration tests (ethical hacking).
- Test the response of equipment (RTU, SCU, protection relays ...) and information systems (SCADA, LDAP server ...) from external manufacturers to those attacks.
- Test the effectiveness of attack detection tools developed by external manufacturers.

The two environments (substation and control center) are connected through an Ethernet network established between two routers. This allows the management of external access to the laboratory. Both routers establish a VPN connection.





Figure 24: Facilities of Cybersecurity for the Smart Grid Laboratory.

The laboratory is composed of two environments, the Control Center environment in which a SCADA has been installed that simulates the operation of the electric grid (reduced to a substation), and the Substation environment in which the electronic equipment is installed (SCU and relays of Protection).

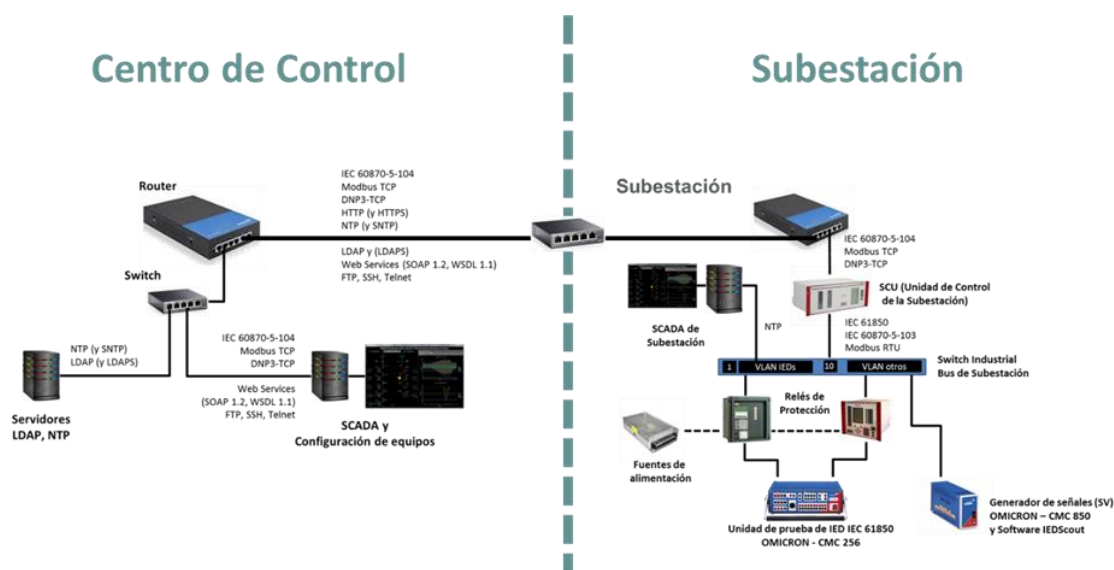


Figure 25: Composition of the Cybersecurity for the Smart Grid Laboratory

Other complementary elements of the laboratory are:

- **SECUREGRID HACKING TOOLBOX**  
SecureGrid Hacking Tool Box (HTB) is a toolbox that allows to configure and perform different penetration tests to electronic devices of an electric substation. SecureGrid HTB is thought to be used by the equipment manufacturers to check the security level of their equipment.
- **WHITEZONE**  
WHITEZONE prevents malware presence at the operational zone of industrial plants, restricting the access to the delimited area designed as operational zone, only to the authorised users carrying safe and identified software. This is a way of securing the industrial zone and improving the update process of the industrial production control (ICS) devices. It offers the following functionalities:



- Ensures that the information that is to be used within the operational zone by means of a USB key is secure, i.e. there is no virus or malware.
- Authenticates users manually or via an NFC card.
- Allows to choose the data that is going to be used in the protected zone and analyzes it to search for any virus or malware or any data not allowed through a multi-virus service in the cloud. If this verification is exceeded, it ejects a key "USB Whitezone ©" where the encrypted and signed data will be copied, to avoid modifications. These USB Whitezone © will be the only valid one within the protected operational zone. In addition, this component sends, in real time, all its activity to the BackEnd software.
- The Software Agent is an element that controls all USB port activity on the computer on which it is installed. If a non-Whitezone © USB device is inserted, it will be ejected immediately, making it impossible to use. If a USB Whitezone © is connected, it verifies that its contents have not been altered. If it has been altered, ejects the USB and otherwise decrypt the information contained so that the data is available. The software agent can communicate, in real time, all its activity to the BackEnd.

## 6.7.2 Services provided

### 6.7.2.1 Support platform for R + D + I projects

This platform will be used to develop R+D+I projects with a cooperative approach. Participants may use their own nodes, both individually or with third parties, in order to carry out other R+D+I projects of a different nature in relevant conditions. These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use models may be contemplated for using the testbed for the aim of financing the projects amortization or maintenance.

### 6.7.2.2 Benchmarking, evaluation and / or certification of products and / or services

The testbed may be used to support benchmarking, evaluation or certification of goods and services. For instance, provided that Basque authorities issued a certificate, the evaluation of the products or services could be conducted on the testbed.

### 6.7.2.3 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, cyber-ranges. In other words, enabling access to the testbed to end users, companies offering cybersecurity training or researchers, so they can prepare and provide training or sophisticated simulation environments.

### 6.7.2.4 Support for awareness actions or generation of cybersecurity culture in the Smart Grid

In the event that public-private partnerships are encouraged, the testbed will enable conducting activities in order to support international events, to create scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

## 6.7.3 Current Usage

### 6.7.3.1 Past Projects

Name (Funds)	Short description
SECUREGRID - New cybersecurity and data analytics technologies for electrical substations	The SecureGrid project ( <a href="http://www.clusterenergia.com/securegrid">http://www.clusterenergia.com/securegrid</a> ), deals with the securization of the electrical installations of the high and medium voltage network and of its electronic equipment, the so-called IEDs (Intelligent Electronic Devices), whose characteristics and remote communication capabilities make them critical points of Smart Grids.



### 6.7.3.2 Live Projects

Name (Funds)	Short description
SDN - microgrid reSilient Electrical eNergy SystEm	The SDN-microSENSE project intends to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of EPES as well as the integrity and the confidentiality of communications. In particular, adopting an SDN-based technology, SDN-microSENSE will develop a three-layer security architecture, by deploying and implementing risk assessment processes, self-healing capabilities, large-scale distributed detection and prevention mechanisms, as well as an overlay privacy protection framework. Firstly, the risk assessment framework will identify the risk level of each component of EPES, identifying the possible threats and vulnerabilities. Accordingly, in the context of self-healing, islanding schemes and energy management processes will be deployed, isolating the critical parts of the network in the case of emergency. Furthermore, collaborative intrusion detection tools will be capable of detecting and preventing possible threats and anomalies timely. Finally, the overlay privacy protection framework will focus on the privacy issues, including homomorphic encryption and anonymity processes
SPEAR – Secure Private Smart Grid	Securing smart grids against cyber-attacks is of vital importance for National Security and Public Safety, since the collapse of an energy production utility may cause human lives, millions of euros, denial of a very important and common good such as energy and days or even months of recovering. To this end, the SPEAR proposal aims at a) detecting and responding to cyber-attacks using new technologies and capabilities, b) detecting threat and anomalies timely, c) developing all-in-one security detection solutions, d) leveraging advanced forensics subject to privacy-preserving, e) confronting Advanced Persistent Threat (APT) and targeted attacks in smart grids, f) increasing the resilience of the smart grid innovation, g) alleviating the lack of trust in smart grid operators and h) empowering EU-wide consensus. Within SPEAR, four proof-of-concept Use Cases are planned in order to validate and assess the implemented security and privacy tools.
Research and development in cybersecurity technologies for the deployment of a more secure Electrical Network	The objective of the project is to provide the electrical distribution network with greater logical security (cybersecurity). To do that, it is necessary to: (1) increase the level of security of the components and information systems (SCADA), (2) define a reference architecture and security deployment methodology in the SG, (3) detect cyber-attacks and prevent them from having consequences, and (4) evaluate the level of security of the electrical network itself.

### 6.7.3.3 Other relevant actions taking place

Live demonstrations to local industrial companies
---



## 6.7.4 Resources

### 6.7.4.1 Scientific and Technological Team

<p>Mr. Jose Antonio López (male): Degree in Computer Science by Deusto University (1998). He started his career in systems integration in a Telecommunications company. In 1999, he joined Labein-Tecnalia in its ICT department, developing e-learning applications and SOA/BPM-based systems as project manager. In 2007 he changed to the Energy Department developing DSM, demand forecast and several DSO MV systems. From 2010, he moved to the Electric Vehicle team as project manager, developing infrastructures, management systems and designing a reference architecture for all actors involved in the EV. He also complements his activity with other projects related to the Smartgrids systems specification and design.</p>
<p>Mr. Iñaki Angulo (male): B.Sc. in Computer Science in 1989 from the University of Deusto (Bilbao, Spain). In 1989 he joined LABEIN (since 2011 TECNALIA), taking part in several European Research Projects mainly in the field of intelligent training and assistant systems of industrial operators in the field of electric energy generation (ITSIE, EXTRASS, AMEBICA) and distribution (IMPRESS).</p>
<p>Mr. Santiago de Diego de Diego (male) is a Mathematician and Computer Science Engineer from the University of Granada. He has experience in Pentesting and Security of Information in general and has participated in research projects on Honeypots in collaboration with the Department of ATC of the University of Granada and is currently working in projects related to the cybersecurity in the Smart Grid. In addition, it has the CPHE certification focused on Ethical Hacking and has participated in several national conferences related to programming and computer security.</p>
<p>Mrs. M<sup>a</sup> Carmen Palacios (female) has a Degree in Physics from the UPV/EHU (1989) and more than 20 years of experience working at TECNALIA. Her areas of expertise are Functional Security and Cybersecurity, having been involved in European and National projects in those areas, including SafeAdapt, OPENCROSS, TACIT, FM-biased and MUSA among others.</p>

### 6.7.4.2 Technical Equipment

CONTROL CENTER	<ul style="list-style-type: none"> <li>Router: Allows to establish a VPN connection with the router of the substation.</li> <li>Internal Switch: Connects all computers in the control center.</li> <li>SCADA equipment: It contains the monitoring and control software (SCADA) of the substation. It also allows to modify the configuration of the IEDs from the Control Center.</li> <li>Computer LDAP and NTP servers: This equipment houses the different servers that are accessed from the IEDs of the substation:</li> <li>Server running the services: <ul style="list-style-type: none"> <li>LDAP: Performs management of the control, access (authentication and authorization) of users and information systems to the IEDS.</li> <li>NTP — provides the time synchronization service.</li> </ul> </li> </ul>
SUBSTATION	<ul style="list-style-type: none"> <li>Router: Allows to establish a VPN connection with the router of the control center.</li> <li>Substation Control Unit (SCU): It makes the functions of a remote unit by establishing the communication with the SCADA of the control center through the Telecontrol IEC 60870-5-104 Telecontrol protocol. Other protocols that are accepted are the</li> </ul>



	<p>Modbus TCP and the DNP3-TCP. On the other hand, it also makes the client functions 61850 of the protection relays through the protocol IEC-61850.</p> <ul style="list-style-type: none"> <li>• Industrial Switch: Connects all IEDs by setting up the substation Bus.</li> <li>• Protection relays: Perform the protection functions of the electrical equipment (switches, transformers,...). These relays implement the Protocol IEC-61850, which allows them to receive the electrical signals generated by the team OMICRON</li> <li>• CMC 850, communicate with the SCU, and launch GOOSE between them.</li> <li>• Power supplies: Those relays whose power supply is in continuous (VCC) are equipped with their corresponding power supply.</li> <li>• SCADA equipment. It contains the monitoring and control software (SCADA) of the substation. It also allows to modify the configuration of the IEDs from the Control Center.</li> <li>• OMICRON – CMC 850: Allows to simulate up to 3 Merging units, electrical data acquisition equipment of the substation. This equipment is connected to the TCP/IP protection relays via the substation Bus.</li> <li>• OMICRON – CMC 256: Allows to simulate electrical signals and connect them directly to the protection relays through the digital input and output connections. In addition, it allows to simulate the activity of switches.</li> </ul>
--	--

### 6.7.5 Request of use

<b>Ticketing system</b>	Managed by SPRI (Basque Country Government) through the BDIH Platform (Basque Digital Innovation Hub)
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit

## 6.8 Tecnalia's Industrial Blockchain Facilities

<b>Name of the asset</b>	BDIH Cybersecurity - Industrial Blockchain Laboratory
<b>KeyWords</b>	DLT, Blockchain
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	oscar.lage@tecnalia.com
<b>Location</b>	Parque Científico y Tecnológico de Bizkaia



<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Show the possibilities of Distributed Ledgers Technologies like Blockchain and IOTA in different domains</li> <li>• Implementation of real cases of blockchain applications</li> <li>• Test blockchain cybersecurity and privacy</li> </ul>
<b>Technological Areas of Work</b>	Cybersecurity, DLT, Blockchain, IOTA, Automotive, Energy, Health, Industry in general

### 6.8.1 Functional Components Description

The Blockchain Laboratory has a high capacity to quickly process the large amount of digitized data, obtained today, as a result of industrial processes, as well as the business logic offered by Blockchain that can lead to complex communication mechanisms between multiple Smart Contracts and in which, each of them must process complex entries in a minimum time. For this reason, this laboratory is composed of:

- DELL Servers of Deep Learning with graphic cards
- Dell EMC Unity 350F Flash Storage System
- HSM device



Figure 26: Industrial Blockchain Laboratory.

### 6.8.2 Services provided

#### 6.8.2.1 Support platform for R + D + I projects

This platform will be used to develop R+D+I projects with a cooperative approach. Participants may use their own nodes, both individually or with third parties, in order to carry out other R+D+I projects of a different nature in relevant conditions. These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use models may be contemplated for using the testbed for the aim of financing the projects amortization or maintenance.

#### 6.8.2.2 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, cyber-ranges. In other words, enabling access to the testbed to end users, companies offering cybersecurity training or researchers, so they can prepare and provide training or sophisticated simulation environments.



### 6.8.2.3 Support for awareness actions or generation of cybersecurity culture in DLT

In the event that public-private partnerships are encouraged, the testbed will enable conducting activities in order to support international events, to create scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

## 6.8.3 Current Usage

### 6.8.3.1 Past Projects

None.

### 6.8.3.2 Live Projects

Name (Funds)	Short description
POSEID-ON - Protection and control of Secured Information by means of a privacy enhanced Dashboard	PoSeID-on is aimed at developing a novel Privacy Enhancing Dashboard for personal data protection supporting the pillars of the new EU's General Data Protection Regulation (GDPR) with regards to digital security that will be implemented within a single, integrated tool, adopting blockchain and smart contracts technology. It will provide targeted benefits for final end users by enabling data protection by design and by default.
P_EUSKATE - New interoperability technologies for the collaborative coordination based on Blockchain of industries in the Basque Country	The main objective of the project focuses on the generation of new knowledge based on the use and applicability of the Blockchain technology in industry, and in particular in Advanced Manufacturing and its contexts of production automation, traceability and energy management in such a way that new products, processes or services can be generated that can significantly improve existing ones.
SERVICECHAIN - New Blockchain based technologies for identity management, reliability and trazability of goods and services' transactions	ServiceChain project is structured around the aim of creating business-oriented Blockchain solutions that allow both the consortium companies and their customers to adopt Blockchain technology in their business environments.
BESEIF-BLOCKCHAIN: Secure sales among particulars using Blockchain	Analysis of the applicability of blockchain technology to the platform and business model of BESEIF, identifying the type of transactions that can be registered and carrying out an initial design of the most appropriate solution, in terms of platform and network infrastructure.
L-BLOCKCHAIN_EJIE - Analysis, development and installation of a blockchain solution for the Contractors' Register of the Basque Government	Analysis, development and implementation of a blockchain solution to cover the scenarios linked to the register of Basque Government contractors.



### 6.8.3.3 Other relevant actions taking place

1. Theoretical-practical Blockchain course. The course was composed of several modules for a total of 22 teaching hours:
  - a. Introduction to Blockchain, concepts and use cases: two sessions where Blockchain concepts and architecture will be introduced, as well as differences between different architectures and use cases from different sectors such as industrial sector, energy and health among others.
  - b. Hyperledger Composer Framework: practical module in which attendees can exercise with the Hyperledger Composer framework, as a simple and quick way to start with Blockchain and deploy test networks.
  - c. Hyperledger Fabric platform: practical module in which attendees will learn how to create and deploy Smart Contracts on this platform, as well as good programming practices in the development of Smart Contracts in Hyperledger.
  - d. Ethereum Platform: practical module where attendees will learn how to create and deploy Smart Contracts on this platform, as well as good programming practices will be included in the development of Smart Contracts with Ethereum.
2. Weekly Showroom with companies interested in Blockchain.
3. Technical discussions about companies' needs - several discussions have taken place on demand.

## 6.8.4 Resources

### 6.8.4.1 Scientific and Technological Team

Mr. Oscar Lage (male) is responsible of the Cybesecurity research line within the CyberSecurity & Safety research group. He is an Informatics Engineer from the University of Deusto. Expert in mobility, security and portable technologies, as a security and mobile researcher since 2003, he has taken part in several European and Spanish research projects like IOE-Internet of Energy, CHIRON, nSHIELD, SAFECITY or Smart Urban Spaces, developing innovative Information security technologies based on cryptographic algorithms. His current research interests include Identity & Access Management, Blockchain, Mobile Security and Mobile Payments. He has numerous publications in international conferences (IEEE), and has been part of the Organization of Scientific Congresses. Oscar has participated as an entrepreneur in the creation of several technology-based startups, and in most of them his participation was linked to computer security and cryptography, such as Qing Solutions

Mr. Iván Gutiérrez (male) received his degree in Computer Science Engineering at UPV/EHU. Expert in Cryptography and Cybersecurity, he owns a Master's Degree in Software Engineering and Intelligent Systems.

Mr. Eneko Gómez Ramos (male) is a Telecommunication Engineer, majoring in Telematics, by the University of the Basque Country (UPV/EHU). He works in Tecnalia as R&D Engineer for the Cybersecurity & Safety Group of the IT Competitiveness Area on the ICT (TIC) Division. He is currently researching about Blockchain technologies (Hyperledger Fabric, Ethereum, Quorum) applied to industrial systems and processes. During his experience as CyberSecurity senior researcher, Eneko has taken part in public and private projects related to cryptographic tools, vulnerability analysis, secure architecture designs and security anomaly detection through heuristic techniques. Some of the main CyberSecurity-related technologies Eneko deals with are Blockchain, PKI, IAM platforms, IDS, log analysis and network monitoring, having applied some of these technologies in industrial environments in projects such as WHITEZONE, SOTER or PETROLOC. Moreover, Eneko is an expert software developer that deals frequently with languages such as Java, Python or C++, relational databases (MySQL, PostgreSQL), cloud technologies and interoperability formats (XML, JSON, YAML); using them both in web (Django framework...) and mobile (Android...) developments.



Mr. Borja Urquizu Gomez (male) is an engineer at the Cybersecurity & Safety Group of the IT Competitiveness Business Area belonging to TECNALIA where he is developing projects using Blockchain technologies based on Hyperledger Fabric and Ethereum. Previously he worked in Panda where he took part in the development of a mail management system in cloud (Trustlayer) and in the development of appliance for the perimeter defense (family GateDefender).

Mr. Sergio Anguita Lorenzo (male) is a graduate in computer engineering from the University of Deusto. Initially working in the Department of DeustoTech Computing, S3lab, focused on computer security, currently works as a researcher in the IT competitiveness business area of the ICT division of Tecnalia Research & innovation. During his professional career, he has participated in several projects related to web infrastructures, implementation and securing of solutions NFC (Near Field Communication), analysis of massive data for the detection of anomalies, investigation in the field of mobile cybersecurity, reversing of Android applications for threats and detection of potential risks to the privacy of users. It has high knowledge in technologies such as Android, Java, SQL, NoSQL, Docker, embedded systems and Linux. It is especially focused on Linux systems and embedded systems, dedicating itself to the areas of security, analysis, architecture and programming of the same and is currently part of the research team of Cybersecurity, focusing on the Applicability of Blockchain solutions for industrial systems and processes.

#### 6.8.4.2 Technical Equipment

DEEP LEARNING SERVERS WITH GRAPHICAL CARDS	<p>Two state-of-the-art servers with high computing capacity (DELL PowerEdge R740). Each server is composed of:</p> <ul style="list-style-type: none"> <li>• 24 cores distributed in 2 12-core processors Intel Xeon® Xeon® Gold 6146 (3.2GHz, 12C / 24T, 24M cache, 2UPI, 165W, Turbo, HT) • Chassis with up to 8 SAS / SATA 2.5 "hard drives</li> <li>• 128 GB of RAM in 4 RDIMMs of 32 GB DDR4 to 2666 MHZ • iDrac9 Enterprise with KVM for management</li> <li>• 2 Solid State Hard Drives of 960 GB SSD SATA to 6G, mixed use, 2.5 "</li> <li>• 1 HBA Fiber Channel 16Gb QLogic 2692 dual port</li> <li>• 2 SFP + cards with four 10Gb Intel X710 ports</li> <li>• 6 Fans</li> <li>• 2 redundant 1600 Watt power supplies</li> <li>• 1 NVIDIA Tesla P100 GPU 12GB graphics acceleration card. The graphics cards are NVIDIA PASCAL P100. 2 Switches Dell Networking S4048-ON, 48 ports 10GbE SFP + and 6 ports 40GbE QSFP +. Each switch includes 24 Twinax cables from 1 meter SFP+ to SFP+ to 10Gb</li> </ul>
FLASH STORAGE SOLUTION	<p>DellEMC Unity 350F All-Flash cab, with Intel® Xeon® processor technology, with 16 Gb FC connectivity, Disks: 5 Flash 2.5 "1.92 TB, Total capacity: 5 TB net, Performance: 67500 IOPS The proposed composition allows a growth of more than double the current capacity thanks to the 20 free disk slots (17 TB additional net with disks of 1.92 TB), without the need for expansion trays. The equipment is complemented with 2 Brocade 6505 Switches from 24 ports to 16 Gb FC, 12 of them licensed and active.</p>
HARDWARE SECURITY MODULE	<p>Hardware-based cryptographic device that generates, stores and protects cryptographic keys.</p>



### 6.8.5 Request of use

<b>Ticketing system</b>	Managed by SPRI (Basque Country Government) through the BDIH Platform (Basque Digital Innovation Hub)
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit

## 6.9 Tecnalia's Automotive Cybersecurity Facilities

<b>Name of the asset</b>	BDIH Cybersecurity - Automotive Cybersecurity Laboratory
<b>KeyWords</b>	ECU's cybersecurity, V2V cybersecurity, V2I cybersecurity, Fault Injection
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	maite.alvarez@tecnalia.com
<b>Location</b>	Parque Científico y Tecnológico de Bizkaia

<b>Asset objectives</b>	Development and evaluation of safety and cybersecurity functions in autonomous and connected vehicles
<b>Technological Areas of Work</b>	Cybersecurity, Automotive, Connected and autonomous vehicles

### 6.9.1 Functional Components Description

Fleet of 3 MODEL CARS (VELOX CARS) that allow to evaluate safety (safety) and cybersecurity functions in the early stages of the development of automotive functions. Designed in collaboration with vehicle manufacturers, they represent the real vehicle scaled to 1: 8 0.

These vehicles are composed of sensors like cameras, control units (Electronic Control Unit - ECU) and actuators capable of reproducing the behavior of real vehicles facilitating the road to highly automated driving, passing through more traditional systems such as the control of the engine.





Figure 27: Fleet of 3 Model Cars (Velox Cars).

Fleet of 3 Model Cars (Velox Cars), each of them with the following Hardware and Software configuration:

- **HARDWARE COMPONENTS:** Losi 8IGHT-E: 1/8-Scale 4WD Buggy (Base vehicle body): - Scale: 1:8 - Length: 497 mm - Width: 308 mm - Height: 180 mm - Wheelbase: 323 – 327 mm - Wheel Size: Diameter: 83.5mm, Width: 42mm - Shock Type: 15mm Bore Threaded Composite - Drivetrain: 4WD All-Metal Shaft Driven - Motor: Fuze 1/8 Scale 2500KV Brushless Sensorless Motor - Servo: 9KG Servo, Waterproof, 23T - 2x LiPo battery pack (7.4V, 2 cells, 5000mAh) Sensory: - Ultrasonic sensor (front view) - Camera (front view) - Wheel Encoder Development Boards: - ADAS-ECU (Odroid-XU4 Board) - Development environment for advanced driver-assistance systems and autonomous driving algorithms. - Vehicle-ECU (STM32F4DISCOVERY Board): Manages all motor control (both longitude and lateral) and contains vehicle model for odometry calculation. Additional Circuit Boards: - STM-breakout board. - Power-circuit-board.
- **SOFTWARE COMPONENTS:** ADAS Board: - Preinstalled and Configured Linux - ROS development environment - Custom ROS Packages for basic functionality STM Board: - Control Functionality: lateral control, speed control, trajectory control, Control State Machine, Wheel encoder driver, odometry model AVES Software Diagnose and Configuration Tool. Vehicle-ECU Software Backups and ADAS-ECU Software Backups.

## 6.9.2 Services provided

### 6.9.2.1 Support platform for R + D + I projects

This platform will be used to develop R+D+I projects with a cooperative approach. Participants may use their own nodes, both individually or with third parties, in order to carry out other R+D+I projects of a different nature in relevant conditions. These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use models may be contemplated for using the testbed for the aim of financing the projects amortization or maintenance.

### 6.9.2.2 Benchmarking, evaluation and / or certification of products and / or services

The testbed may be used to support benchmarking, evaluation or certification of goods and services. For instance, provided that Basque authorities issued a certificate, the evaluation of the products or services could be conducted on the testbed.

### 6.9.2.3 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, cyber-ranges. In other words, enabling access to the testbed to end users, companies offering cybersecurity training or researchers, so they can prepare and provide training or sophisticated simulation environments.



#### 6.9.2.4 Support for awareness actions or generation of cybersecurity culture in the Automotive sector

In the event that public-private partnerships are encouraged, the testbed will enable conducting activities in order to support international events, to create scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

### 6.9.3 Current Usage

#### 6.9.3.1 Past Projects

Name (Funds)	Short description
OPENCROSS (Open Platform for Evolutionary Certification of Safety-critical Systems)	Tecnalia led the project and participated in the development of the common certification language and the OPENCROSS platform. OPENCROSS is a European large scale integrating FP7 project dedicated to produce the first European-wide open safety certification platform: an Open Platform for Evolutionary Certification Of Safety-critical Systems for the railway, avionics and automotive markets.
EMC2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments) (Apr 2014 - Jun 2017)	Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments. Its main aim is to establish Multi-Core technology in all Embedded Systems domains handling mixed criticality applications for dynamic adaptability in open systems.
SafeAdapt (Safe Adaptive Software for Fully Electric Vehicles)	FP7-Green Vehicles SafeAdapt (Safe Adaptive Software for Fully Electric Vehicle). The main idea of SafeAdapt is to develop novel architecture concepts based on adaptation to address the needs of a new E/E architecture for FEVs regarding safety, reliability and cost-efficiency. TEC dealt with assurance issues related to safe adaptation and a novel fail-operational behaviours based on a model-driven development of self-describing components for self-adaptive distributed embedded systems.

#### 6.9.3.2 Live Projects

Name (Funds)	Short description
AMASS	AMASS is an ECSEL project that will create and consolidate a de-facto European-wide assurance and certification open tool platform, ecosystem and self-sustainable community spanning the largest CPS vertical markets. This will be achieved by establishing a novel holistic and reuse-oriented approach for architecture-driven assurance, multi-concern assurance, and seamless interoperability between assurance and engineering activities. TECNALIA is the project coordinator.
eITUS (Experimental Infrastructure Towards Ubiquitously Safe Robotic Systems using RobMoSys)	The eITUS project aims at creating a basic experimental infrastructure (models, software and tools) that enables robotic development stakeholders to assure system safety both at design time, using analysis and simulation-based techniques, and at run time, using safety monitoring algorithms eITUS addresses safety validation by fault injection simulations, code generation of runtime monitors and formalisation of safety properties.



### 6.9.3.3 Other relevant actions taking place

Live demonstrations to local industrial companies.

## 6.9.4 Resources

### 6.9.4.1 Scientific and Technological Team

Dr. Jabier Martinez (male) joined the cyber-security and safety department of Tecnalía in 2018. His background is on providing methods and tools for systems modelling, and for achieving systematic reuse covering all the artefacts that conform a system life-cycle. He obtained the title of computer engineering from the University of the Basque Country in 2007 and, after several years of industrial experience, he received his PhD in 2016 from the Luxembourg University (SnT, Interdisciplinary centre for Security and Trust) and Sorbonne University (Lip6, Laboratory of Computer Sciences, Paris 6) with an awarded thesis about mining software artefacts for product line migration and analysis. He participated in several European research projects. He co-organizes the Reverse Variability Engineering series of workshops and has authored more than thirty peer-reviewed publications on modelling, software reuse, variability management and software product lines.

Dr. Alejandra Ruiz (female) holds a Ph.D. degree in Telecommunications and Computer Engineering, (2015, U. of Deusto), an MSc in Advanced Artificial Intelligence (2012, UNED) and the degree in Telecommunication Engineering (2005, University of Deusto). She joined Tecnalía in 2007 and is a Research Engineer in the Cyber Security and Safety group. She currently leads the area of Modular Assurance and Certification of Safety-critical Systems, with particular focus on automotive, aerospace, railway and medical device industries. She is the main contributor in these areas for European projects such as RECOMP (Reduced Certification Costs for Trusted Multicore Platforms), OPENCROSS (Open Platform for Evolutionary Certification of Safety-critical Systems) SafeAdapt (Safe Adaptive Software for Fully Electric Vehicles) and EMC2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments).

Mrs. Estibaliz Amparan Calonge (female) carried out her Degree in Industrial Electronic and Automation Engineering at the University of the Basque Country (EHU/UPV). She is currently studying for a Master's Degree specialised on Computational Engineering and Smart Systems at the University of the Basque Country

### 6.9.4.2 Technical Equipment

#### MODEL CARS SOFTWARE

Fleet of 3 Model Cars (Velox Cars), each of them with the following Hardware and Software configuration:

#### ADAS Board:

- Preinstalled and Configured Linux - ROS development environment
- Custom ROS Packages for basic functionality STM Board
- Control Functionality: lateral control, speed control, trajectory control, Control State Machine, Wheel encoder driver, odometry model AVES Software Diagnose and Configuration Tool.

Vehicle-ECU Software Backups and ADAS-ECU Software Backups.



MODEL CARS HARDWARE	<p>Losi 8IGHT-E: 1/8-Scale 4WD Buggy (Base vehicle body): - Scale: 1:8 - Length: 497 mm - Width: 308 mm - Height: 180 mm - Wheelbase: 323 – 327 mm - Wheel Size: Diameter: 83.5mm, Width: 42mm - Shock Type: 15mm Bore Threaded Composite - Drivetrain: 4WD All-Metal Shaft Driven - Motor: Fuze 1/8 Scale 2500KV Brushless Sensorless Motor - Servo: 9KG Servo, Waterproof, 23T - 2x LiPo battery pack (7.4V, 2 cells, 5000mAh) Sensory: - Ultrasonic sensor (front view) - Camera (front view) - Wheel Encoder Development Boards: - ADAS-ECU (Odroid-XU4 Board) - Development environment for advanced driver-assistance systems and autonomous driving algorithms. - Vehicle-ECU (STM32F4DISCOVERY Board): Manages all motor control (both longitude and lateral) and contains vehicle model for odometry calculation. Additional Circuit Boards: - STM-breakout board. - Power-circuit-board.</p>
---------------------	--

### 6.9.5 Request of use

<b>Ticketing system</b>	Managed by SPRI (Basque Country Government) through the BDIH Platform (Basque Digital Innovation Hub)
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit

## 6.10 Tecnalía's Cyber-Ranges Facilities

<b>Name of the asset</b>	BDIH Cybersecurity - Cyber-Ranges Facilities
<b>KeyWords</b>	Cyber-range
<b>Organization</b>	TECNALIA
<b>Point of contact</b>	Daniel.landa@tecnalia.com
<b>Location</b>	Parque Tecnológico de Álava

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Cyber Ranges Showroom</li> <li>• Cyber Ranges R&amp;D projects</li> <li>• Test and experimentation in Cyber Ranges technologies and cybersecurity technologies for the detection, answer, resilience and recover.</li> <li>• Definition and implementation of Cyber Ranges scenarios in collaboration with the other cybersecurity nodes of the DIH</li> <li>• Training at individual and group levels about cyber defences, cyber-attack and forense analysis for the Public Administration</li> </ul>
<b>Technological Areas of Work</b>	Cybersecurity IT-OT, multisector



### 6.10.1 Functional Components Description

A cyber-range is a virtual environment that is used for the training of personnel and for the research and development of cybersecurity technology. The cyber-range includes tools that help strengthen the stability, security and performance of IT / OT systems.

From the physical point of view, there is a room to host a Security Operations Center (SOC), which is the one that controls the cyber-range, and a second room that is where training and training exercises takes place. The SOC has software for monitoring, supervising and preventing IPS, IDS and SIEMS for the supervision of cyber-exercises and cyber-ranges.

On the other hand, the second room includes work stations for the people that will take part in the exercises (students or researchers), screens and video walls with information on the system, as well as the physical equipment needed to replicate the different scenarios of the IT / OT network for the cyber-ranges.

Concerning training, the cyber range allows to perform exercises of the type Capture The Flag (CTF) or Red-VS-Blue type. A CTF is a cybernetic challenge based of about four people that compete to attack servers and, if they manage to control, get points. In the case of Red-VS-Blue exercises, two teams are created, one that attacks a system and the other that defends it. The configuration of the exercise room is therefore flexible, so that it can be configured for one type of exercise as well as for the other.



Figure 28: Cyber-Ranges Facilities in Tecnalia.

### 6.10.2 Services provided

#### 6.10.2.1 Support platform for R + D + I projects

This platform will be used to develop R+D+I projects with a cooperative approach. Participants may use their own nodes, both individually or with third parties, in order to carry out other R+D+I projects of a different nature in relevant conditions. These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use models may be contemplated for using the testbed for the aim of financing the projects amortization or maintenance.

The facilities allow for the testing and experimentation in Cyber Ranges technologies and cybersecurity technologies for the detection, answer, resilience and recover.



### 6.10.2.2 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, cyber-ranges on the other industrial cybersecurity nodes of the BDIH. In other words, enabling access to the testbed to end users, companies offering cybersecurity training or researchers, so they can prepare and provide training or sophisticated simulation environments.

Training at individual and group levels about cyber defences, cyber-attack and forensic analysis for the Public Administration.

### 6.10.2.3 Support for awareness actions or generation of cybersecurity culture

In the event that public-private partnerships are encouraged, the testbed will enable conducting activities in order to support international events, to create scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

## 6.10.3 Current Usage

### 6.10.3.1 Past Projects

None.

### 6.10.3.2 Live Projects

Name (Funds)	Short description
SENDAI	Implementing cyberrange technology and putting it into practice within the laboratories of the BDIH Cybersecurity Node.
SPARTA	Incorporating the cyber range to SPARTA cyber range facilities.

### 6.10.3.3 Other relevant actions taking place

<p>Live demonstration to local industrial companies.</p> <p>Initial cyberranges of the type “Capture the Flag” with cybersecurity students.</p>
---

## 6.10.4 Resources

### 6.10.4.1 Scientific and Technological Team

<p>Mr. Daniel Landa (male): Information Systems Engineer by Deusto University. Currently he develops his activity as a senior technologist in the Cyber Security &amp; Safety Group within the ICT division of Tecnalia where he is currently in charge of the Cybers Ranges facilities in Tecnalia. Wide experience in the development of high availability, scalable cloud-applications about mobile payments and geolocation using wearables over Linux systems in Django/Python server environments. He has led the design and development of a multimedia assets manager (MAM) for professional broadcast environments (Media department, Tecnalia). Previously he took part in the development of an ERP over Microsoft's .NET platform in Bangalore (India, Lantek I+D, 2005-09). Formerly he worked, thanks to the Leonardo Da Vinci scholarships program of the Ministry of Science and Innovation of the Government of Spain, in the development of documentary management tools with open source web technologies in the Institute of composite materials of Kaiserslautern (Germany, IVW, 2005).</p>
<p>Mr. Iván Gutiérrez (male): received his degree in Computer Science Engineering at UPV/EHU. Expert in Cryptography and Cybersecurity, he owns a Master's Degree in Software Engineering and Intelligent Systems. After working on neural network sets, ontological driven expert systems and automated image processing, he has grown as a software engineer developing technical skills</p>



at cybersecurity and software design. As a member of Tecnia, Iván has been working on R&D projects related to PKI, IDM/IAM, chip based cryptography, contactless technologies and mobile devices. Nowadays he applies his knowledge on security to Blockchain technologies for the team that coordinates the Blockchain Innovation Center by Tecnia. Iván has gained new technical skills through cooperation with organizations such as Enterprise Ethereum Alliance, Hyperledger Corporate Membership and Alastria. With the aim of technology knowledge-sharing, Iván is actively contributing to its dissemination through specialized learning programs and congresses about Blockchain, Cybersecurity and Cryptography.

#### 6.10.4.2 Technical Equipment

SECURITY OPERATIONS CENTER	<p>It is composed by the equipment from which the Cyber-range is controlled. It has monitoring, supervision and prevention software for IPS, IDS and SIEM attacks.</p> <p>It is composed by: - FortiSIEM FSM-2000F: SIEM-specific hardware with perpetual licensing for monitoring 100 devices and 1,000 events per second. – 3 workstations with Dell equipment, model Optiplex 3050 Mini Tower XCTO, with Dell 22 “monitors, with the following features each workstation: * Intel Core i5-6400 processor, 4Cores 2.7 GHz * DVD +/-RW * 4GB (1x4GB) 2400MHz DDR4 * hard drive 3.5 “500GB 7200rpm SATA * extra 1GB AMD Radeon R5 430 graphics card (DP/VGA) * USB keyboard Dell KB-522 * Dell MS116 USB Optical Mouse * O.S. Español Windows 10 Pro (64bits) * 2 monitors Dell 22 “S2218H-54, 6cm (21.5 “) Black.</p>
CYBER RANGE MASTER ROOM	<p>The Cyber Range Master room is the place where Cyber Ranges are held. It allows to carry out Cyber Ranges in which up to a maximum of 10 people can participate. Each participant has a Workstation with a double screen to carry out the Cyber Range. The Cyber Range is monitored on a wall screen consisting of 10 screens of 55 “model Dell 55 Conference Room. It also has equipment to create the Cyber Ranges scenarios as: -2 3D printers with different technology: FDM FlashForge Dreamer Printer and SLA Wanhao duplicator 7 printer - Virtual Reality Equipment (VR)/Augmented Reality (AR) composed by: * Alienware Area-51 with Monitor * Virtual reality glasses brand OCULUS * Virtual reality glasses brand HTC Live The Cyber Range supports the use of different software for the execution of Cyber Ranges.</p>

#### 6.10.5 Request of use

<b>Ticketing system</b>	Managed by SPRI (Basque Country Government) through the BDIH Platform (Basque Digital Innovation Hub)
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit



## 6.11 INOV's BP-IDS

<b>Name of the asset</b>	BP-IDS
<b>KeyWords</b>	Intrusion detection, Incident detection, business processes
<b>Organization</b>	INOV
<b>Point of contact</b>	<a href="mailto:nelson.escravana@inov.pt">nelson.escravana@inov.pt</a>
<b>Location</b>	Rua Alves Redol, 9 1000-029 Lisboa PORTUGAL

<b>Asset objectives</b>	BP-IDS allows monitoring how business processes (e.g. control processes) are executed based on the traces they leave on the systems and networks involved in the execution of the processes. BP-IDS can monitor the process execution for deviations against a specification, detecting intrusions, incidents and other violations of the specification.
<b>Technological Areas of Work</b>	Cybersecurity, OT, ICS, SCADA

### 6.11.1 Functional Components Description

The BP-IDS is a monitoring solution that aims at the detection of incidents on technology enabled infrastructures. It operates by collecting traces from multiple sensors scattered on the monitored infrastructure that indicate execution of activities in business processes, and reconstructs in real time the business process executed based on those traces. The reconstructed processes are then validated by comparing them with their specification and business rules. Whenever the executed process deviates from the specification, the activity is marked as a possible incident and the infrastructure administrator is notified in real-time by BP-IDS with the causes of that anomaly (traces, affected processes, etc.). Thus, offering broad protection against: cybersecurity incidents (such as, intrusions or forgery of equipment behaviour); and operational security incidents (like, equipment and network failure, human error, or natural disasters).

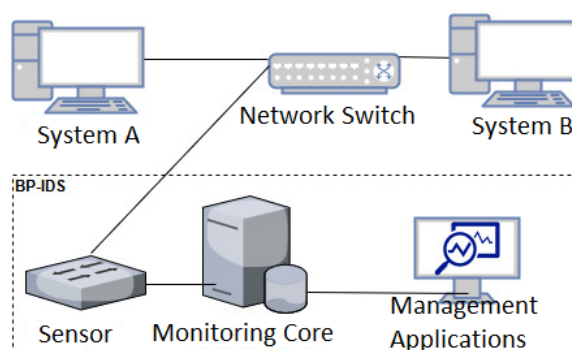


Figure 29: Example of a BP-IDS deployment.

The deployment example of Figure 29 is relative to an infrastructure comprised by two systems (A and B) network connected using a network switch. In this example BP-IDS is composed by: its



essential components (sensor and monitoring core); and its additional management applications (the administration and monitoring Interfaces).

As illustrated in Figure 29, in its essence, BP-IDS is architected as a distributed system composed by: the monitoring components, that gather business process traces and analyse them according to the specification; and the management applications, that allow system administrators to interact with the monitoring components to setup the components and obtain the monitoring results.

## Monitoring Components

The monitoring components are comprised by: a monitoring core, that analyses the business process traces according to the specification and business rules; and sensors, that discover and send to the monitoring core all the traces of activities traces found on infrastructures data resources, based on identification patterns that dictate how activities of business processes are extracted from the data. BP-IDS provides two types of sensors: network-based sensors, that extract traces by inspecting network traffic; or host-based sensors that extracts them based on the logs stored in the infrastructure's systems.

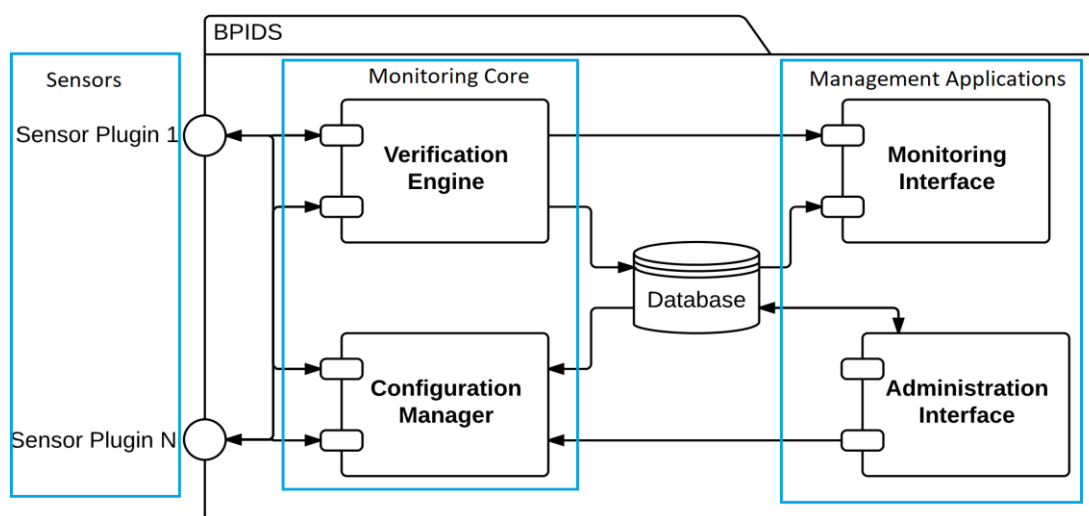


Figure 30: Software architecture of the several modules that comprise the BP-IDS system.

As depicted in Figure 5 the monitoring components are implemented by several software modules.

The monitoring core is composed by two software modules: Verification Engine and Configuration Manager. Verification Engine is the module responsible for conducting the analysis of the traces captured by the sensors, using the business specifications of the organization. It is also the Verification Engine's responsibility to report the incidents found during the analysis and export the incident details (implemented by its inner component Event Output Engine that performs such exportation). The Configuration Manager module, on the other hand, is responsible for automatically configuring the several sensors when BP-IDS system is launched, based on the network topology of the monitored environment and identification patterns that dictate how the business process traces are identified.

Each sensor is composed by a network/host-based COTS sensor and its corresponding Sensor Plugin software module. The Sensor Plugin serves as an interface between the monitoring core and the actual sensor. It receives the information from the Configuration Manager, and sets up the sensor for capturing data. Whenever data is captured by the sensor, the Sensor plugin receives the data captured and converts it into business process traces, which are then sent to the monitoring core's Verification Engine.



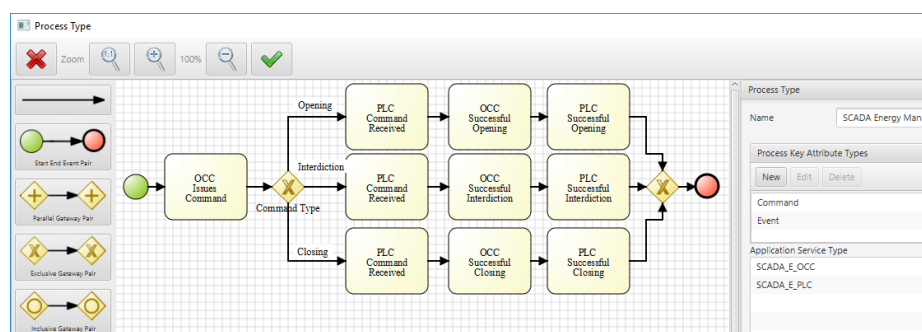


Figure 31: Setting up the monitoring core analysis module with business information using the Administration application.

## Management applications

The management applications are interfaces that allow the system administrators to interact with BP-IDS, and are composed by the administration and monitor interfaces.

The administration application allows the administrators to provide all the necessary information to setup the monitoring core: the business specification used by the Verification Engine during the analysis (Figure 31); and the infrastructure network topology used by the Configuration Manager to configure the sensors (Figure 32).

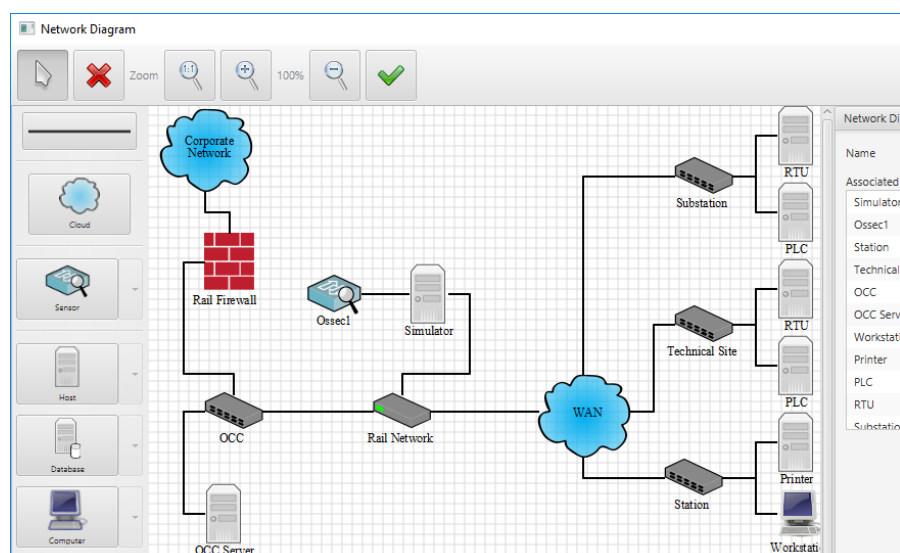


Figure 32: Configuration Manager

The Monitoring Interface, on the other hand, allows the administrators to conduct forensic investigations based on the results obtained from BP-IDS monitoring core analysis. As depicted in Figure 8, this interface allows administrators to view the several incidents reported by BP-IDS, and pinpoint the business traces non-compliant with the specification.



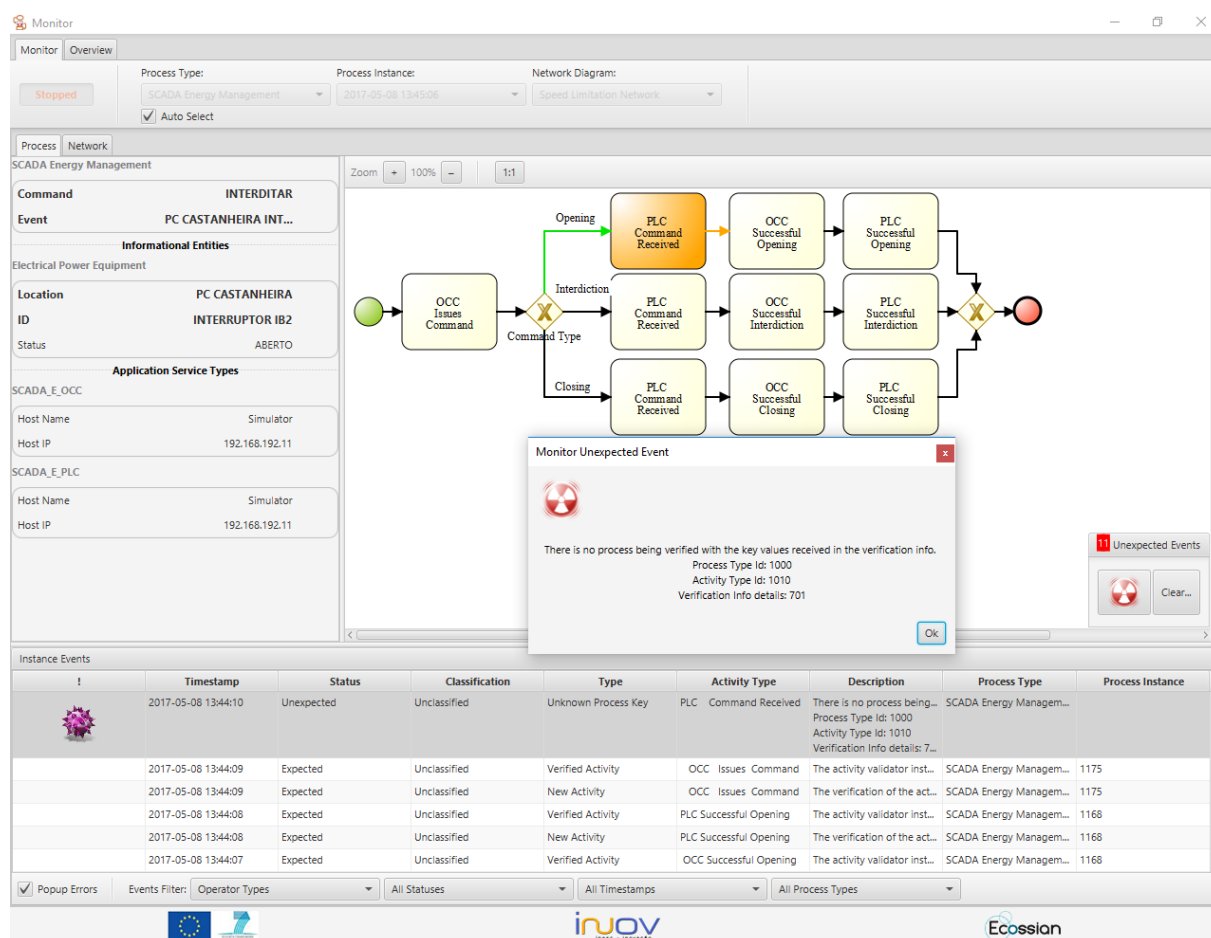


Figure 33: Forensic analysis of an incident reported by BP-IDS using the Monitoring Interface.

### 6.11.2 Services provided

INOV hosts BP-IDS, providing partners access to the platform in order for them to test the process monitoring approach with their own datasets of Industrial Control Systems (or even other type of systems) and process specification. Remote access to the Administration and Monitoring interface is available.

### 6.11.3 Current Usage

#### 6.11.3.1 Past Projects

Name (Funds)	Short description
FP7 SECUR-ED	SECUR-ED “Secured Urban Transportation – European Demonstration”, <a href="http://www.secured.eu">www.secured.eu</a> , was a demonstration project with an objective to provide a set of tools to improve urban transport security. The list of participants included all major stakeholders from Europe. SECUR-ED was one of the most representative forums in which European transportation operators, authorities, academia and industry openly discussed cyber security in public transportation systems. BP-IDS was first tested on this project on railway systems from Thales.



Name (Funds)	Short description
FP7 ECOSSIAN	Improved detection and management of sophisticated cyber attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities. Critical infrastructures operate specific types of systems, such as industrial control systems. ECOSSIAN addresses industrial control system forensics within the scope of incident management and information sharing. Within ECOSSIAN BP-IDS was tested on different railways systems and in networks of gas distribution.

### 6.11.3.2 Live Projects

Name (Funds)	Short description
COMPACT	Empowering Local Public Administration, entities which are traditionally dependent on central authorities for their security to take control of their own cyber security. Within COMPACT BP-IDS was adapted to monitor database based systems, and processes for compliance with the GDPR.
SATIE	SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in the airports, while guaranteeing the protection of critical systems, sensitive data and passengers. In SATIE BP-IDS is being adapted for monitoring ICS present in the airport, namely the Baggage Handling System.

### 6.11.3.3 Other relevant actions taking place

Demonstrations of the platform to industrial partners.
--

### 6.11.4 Resources

#### 6.11.4.1 Scientific and Technological Team

<p><b>Nelson Escravana</b> (male) – has a degree in Computer Science Engineering from IST and Management post graduation from ISEG, Technical University of Lisbon, Portugal. He has over 15 years of experience and is currently the head of the Communications &amp; Cybersecurity Units at INOV, where he coordinates more than 20 researchers. He actively participates in research, development and integration projects — as a technical leader and manager in the fields of penetration testing, technological developments for detection, forensic auditing, mobile authentication, as well as a leading security auditor. During the past 15 years he has participated in 10 EU funded research projects and more than 13 National funded research &amp; innovation projects.</p> <p>From 2011 to 2014, he was the responsible for the Cybersecurity activity of SECUR-ED and is currently involved in several European R&amp;D cybersecurity related projects, such as, ASGAR, DOGANA, COMPACT, ECOSSIAN, etc.. He has participated in multiple projects and studies for the Portuguese Government, ESA and NATO. In 2011, he was responsible for the creation of the INESC group shared service centre, which he manages, and which includes the group's CSIRT. He is also responsible for the annual participation of INESC group in National cyber-defence exercises held by the Portuguese Army and is member of the Board of Directors (statutory body) at INOV.</p>
---



Bernardo Pacheco (male) has a degree in electronics and computer science from IST. He has over 15 years of professional experience, being part as a project manager and developer of several research, development and integration projects in the fields of social engineering vulnerability assessment, intrusion detection, mobile applications and voice technologies. He has participated in several EU and national funded projects and he was responsible for the development of attack simulation tools and trials execution in the FP7 DOGANA, and other cybersecurity related activities in projects such as FP7 ECOSSIAN, H2020 SPARTA, H2020 EUNOMIA, H2020 SATIE, H2020 ASGARD. Currently is a project manager in Communications & Cybersecurity Units at INOV, assuming also the position of DPO in INOV.

Filipe Apolinário (male) computer science expert and doctoral student in the Cybersecurity Unit of INOV – INESC INOVAÇÃO. He received his B.Sc and M.Sc. in Computer Science from the Instituto Superior Técnico (IST) – University of Lisbon with focus on distributed systems and cybersecurity. Throughout his work career Filipe has worked in cyber security and computer science engineer for consultation companies (Novabase and Aubay) and for research institutes (INESC-ID and INOV) where he participated in European funded projects: SAFECLOUD (cloud security researcher working at INESC-ID); ECOSSIAN, COMPACT, SATIE and SPARTA projects (as critical infrastructure security researcher and software developer working at INOV- INESC INOVAÇÃO). His current research interests include intrusion detection systems, Industrial control systems and critical infrastructure protection.

#### 6.11.4.2 Technical Equipment

The system is hosted in INOV's 99atacentre.

#### 6.11.5 Request of use

<b>Ticketing system</b>	Email supported by TRAC software.
<b>Communication Channels</b>	email
<b>Time management</b>	Access available during business hours.
<b>Granularity</b>	Booking should be done in terms of weeks, and will be subject to the availability of resources.
<b>Type of access (public, free, comm)</b>	Free access for Consortium Partners for non-commercial usage. For commercial usage, license fees apply.

#### 6.12 CESNET's Nemea

<b>Name of the asset</b>	Nemea
<b>KeyWords</b>	Flow traffic analysis, network monitoring
<b>Organization</b>	CESNET
<b>Point of contact</b>	<a href="mailto:cejkat@cesnet.cz">cejkat@cesnet.cz</a>
<b>Location</b>	Zikova 1903/4, 160 00 Praha 6 CZECH REPUBLIC

<b>Asset objectives</b>	The NEMEA (Network Measurements Analysis) aims to create a framework which allows an
-------------------------	--



	assembly of a system for automated real-time analysis of data gathered by network monitoring processes.
<b>Technological Areas of Work</b>	Telecom

### 6.12.1 Functional Components Description

Nemea system consists of separate building blocks called modules which are interconnected by interfaces. A module is a separate system process receiving a stream of data on its input interface(s), processing it, and sending another stream of data through module's output interfaces(s). There are modules for data acquisition (e.g. receiving NetFlow/IPFIX records), preprocessing, detection of various types of malicious traffic or anomalies (network attacks, link failure...), postprocessing of detection results, logging and reporting.

### 6.12.2 Services provided

The NEMEA Framework implements the communication layer, flexible format called UniRec and other common tasks. As such when installed it detects network security events in flow data.

### 6.12.3 Current Usage

Nemea is deployed in CESNET backbone network infrastructure, SWITCH, Casablanca.

#### 6.12.3.1 Past Projects

None.

#### 6.12.3.2 Live Projects

Name (Funds)	Short description
SmartADS	Project of Technology Agency of the Czech Republic. Its goal is to embed application monitoring, Machine Learning and reputation scoring.

#### 6.12.3.3 Other relevant actions taking place

None.

### 6.12.4 Resources

#### 6.12.4.1 Scientific and Technological Team

Tomáš Čejka
Karel Hynek

#### 6.12.4.2 Technical Equipment

Nemea can be installed on physical servers as well as in virtual environment. The resources dedicated to Nemea influence its throughput.

Network monitoring	CESNET network backbone
--------------------	-------------------------



### 6.12.5 Request of use

<b>Ticketing system</b>	NO
<b>Communication Channels</b>	Email
<b>Time management</b>	Working hours
<b>Granularity</b>	Whole system
<b>Type of access (public, free, comm)</b>	Open source

## 6.13 CESNET's IPFIXcol

<b>Name of the asset</b>	IPFIXcol
<b>KeyWords</b>	Flow record collector
<b>Organization</b>	CESNET
<b>Point of contact</b>	hutak@cesnet.cz
<b>Location</b>	Zikova 1903/4, 160 00 Praha 6 CZECH REPUBLIC

<b>Asset objectives</b>	Collect, process and store IPFIX and NetFlow data.
<b>Technological Areas of Work</b>	Telecom

### 6.13.1 Functional Components Description

IPFIXcol framework is a set of:

- IPFIXcol - collector for capturing IPFIX NetFlow data
- input, intermediate and storage plugins for collector
- tools for data processing etc.

### 6.13.2 Services provided

IPFIXcol is a flexible IPFIX flow data collector designed to be easily extensible by plugins. It loads input, intermediate and output plugins on startup. Each input plugin runs in a different process. IPFIXcol corresponds to RFC7011

### 6.13.3 Current Usage

IPFIXcol is deployed in CESNET backbone network infrastructure, SWITCH, Casablanca.

#### 6.13.3.1 Past Projects

<b>Name (Funds)</b>	<b>Short description</b>
SecurityCloud	Project of Technology Agency of the Czech Republic. Its goal was to build distributed flow collector.

#### 6.13.3.2 Live Projects

None.



### 6.13.3.3 Other relevant actions taking place

None.

### 6.13.4 Resources

#### 6.13.4.1 Scientific and Technological Team

Lukáš Huták
Michal Sedlák

#### 6.13.4.2 Technical Equipment

Individual packages of the IPFIXcol framework can be installed from Fedora copr repository

Network monitoring
--------------------

### 6.13.5 Request of use

<b>Ticketing system</b>	NO
<b>Communication Channels</b>	Email
<b>Time management</b>	Working hours
<b>Granularity</b>	Whole
<b>Type of access (public, free, comm)</b>	Open source

## 6.14 CESNET's Warden

<b>Name of the asset</b>	Warden
<b>KeyWords</b>	Network security, event sharing, platform
<b>Organization</b>	CESNET
<b>Point of contact</b>	ph@cesnet.cz
<b>Location</b>	Zikova 1903/4, 160 00 Praha 6 CZECH REPUBLIC

<b>Asset objectives</b>	System for efficient sharing information about detected events (threats). The WARDEN system enables CERTS/CSIRT teams (and security teams in general) to share and make use of information on detected anomalies in network and services operation generated by different systems – IDS, honeypots, network probes, traffic logs, etc. – easily and efficiently.
<b>Technological Areas of Work</b>	Telecom



### 6.14.1 Functional Components Description

The architecture of the WARDEN system is that of the client – server type. The Warden system consists of a server, receiving clients and sending clients. The server, on request of receiving clients, distributes new (previously undistributed) events fed to the server by sending clients.

Each entity/network that wishes to feed data into the WARDEN system should have a so called sending client. Each entity/network that wishes to receive data from the WARDEN system should have a so called receiving client. The server (the centre) ensures the data reception and storage as well as the interface for the access to data stored. Data which the clients send into the centre will be referred to as events. Events are sent by the clients after authentication; the access to the centre is also authenticated. X.509 is used for the authentication.

### 6.14.2 Services provided

None.

### 6.14.3 Current Usage

The Warden system is currently developed and deployed mainly to satisfy the needs of the national research and education network CESNET2 administered by the CESNET association for its members and other entities involved. In the future, we plan to develop the Warden project as open. Until then, non-members of CESNET2 wishing to participate in the project can participate only based on ad-hoc agreements.

#### 6.14.3.1 Past Projects

Name (Funds)	Short description
SABU	Project of Ministry of Interior to enhance Warden with connectors to selected data sources, enriching capabilities per IP address and prediction of future events.

#### 6.14.3.2 Live Projects

Name (Funds)	Short description
CTI	Project of Ministry of Interior to apply Warden in national infrastructure to collect network security events, passiveDNS and blacklists relevant for the Czech Republic.

#### 6.14.3.3 Other relevant actions taking place

None.

### 6.14.4 Resources

Warden runs on a server with following configuration:

Warden	Dell PowerEdge R410	2x Intel Xeon L5640 (2.26GHz, 6C, 12M Cache, 5.86 GT/s QPI, 60W TDP, Turbo, HT)	32 GB RAM, DDR3-1066MHz	540 GB RAID5 HDD (3x 300GB, 15k RPM, 3.5" SAS; PERC H700A RAID Controller)	2 port Broadcom NetXtreme II BCM5716 1000Base-T (C0) PCI Express
--------	---------------------	---	-------------------------	--	--



#### 6.14.4.1 Scientific and Technological Team

Pavel Kácha
Jan Mach
Daniel Studený

#### 6.14.4.2 Technical Equipment

Alert sharing
---------------

#### 6.14.5 Request of use

<b>Ticketing system</b>	NO
<b>Communication Channels</b>	Email
<b>Time management</b>	Working hours
<b>Granularity</b>	Joining Warden community
<b>Type of access (public, free, comm)</b>	Open source

### 6.15 CESNET's NERD

<b>Name of the asset</b>	NERD
<b>KeyWords</b>	Network entity reputation database
<b>Organization</b>	CESNET
<b>Point of contact</b>	bartos@cesnet.cz
<b>Location</b>	Zikova 1903/4, 160 00 Praha 6 CZECH REPUBLIC

<b>Asset objectives</b>	NERD aims to build an extensive reputation database of known sources of cyber threats. That is, a list of known malicious IP addresses or other network entities (e.g. ASNs or domain names) together with all security-relevant information about each of them.
<b>Technological Areas of Work</b>	Telecom

#### 6.15.1 Functional Components Description

First, there are several databases. The main one, called entity database, stores all the entity records. There is also a separate database to store original data from primary sources (events, alerts). These may be actually multiple databases, since different technologies may be suitable for different types of data. At last, there is an instance of a fast in-memory key-value database (Redis), that serves for



storage of various, often temporary or fast changing, data that need to be accessed globally by different components. It also serves for various logging and caching purposes.

The main input of the system is represented by a set of primary data receivers. They receive messages, alerts, or entity lists from the primary data sources and put tasks (called update requests) to a global queue to create or update records of related entities. The tasks are processed by the core of the system – a set of workers. They apply the requested updates on given entity records. Also, the workers fetch data from external (secondary) sources and compute other attributes. This functionality is handled by plug-in modules, so it is easy to add, change or remove secondary data sources or computed attributes.

The workers may run in any number of instances in parallel, which makes the system easily scalable. Tasks are distributed to workers according to a hash of the entity identifier (a task always involves processing of a single entity record only), so the same record is always handled by the same worker. This helps to avoid a need for record locking and other concurrency issues. If the processing core or a plug-in needs to store a global state information, it is stored outside the workers, usually in the Redis database. Most of the plug-ins fetches data from external sources. Depending on the type and availability of the data, three methods of data acquisition are used: (i) the data are queried directly from their original sources by the plug-in module (for example, whois data are got this way); (ii) there is a special microservice or a cache to provide easier or more efficient access to the data (an example Services provided From a user's point of view, the Network Entity Reputation Database (NERD) system is an online portal where the user can search any IP address, domain name or another network identifier (an entity) and get all security related information known about it list of all alerts that reported it as a source of some malicious activity, whether it is listed on some blacklists or other databases, related information from DNS, whois, geolocation, or data from internet wide scanning services. It is also possible to search for entities that match various criteria and sort them by various attributes or by a score summarizing the associated threat level. There is also a REST API for easy integration of the data into any other security or threat intelligence system. Behind the web portal and the API, which servers to access the data, there is a complex, modular system to acquire and process data from various sources, store them to the database and periodically update them.

## 6.15.2 Current Usage

### 6.15.2.1 Past Projects

None.

### 6.15.2.2 Live Projects

Name (Funds)	Short description
CTI	Project of Ministry of Interior to apply Warden in national infrastructure to collect network security events, passiveDNS and blacklists relevant for the Czech Republic.
GEANT	In the scope of GEANT the reputation scoring is evaluated.

### 6.15.2.3 Other relevant actions taking place

None.

## 6.15.3 Resources

### 6.15.3.1 Scientific and Technological Team

Václav Bartoš
Pavel Eis



### 6.15.3.2 Technical Equipment

NERD runs on a server with following configuration:

NERD	Virtual server Wmware	8x vCPU (Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz)	32 GB RAM	132 GB
------	-----------------------	--	-----------	--------

### 6.15.4 Request of use

<b>Ticketing system</b>	NO
<b>Communication Channels</b>	Email
<b>Time management</b>	Working hours
<b>Granularity</b>	Limited public access, private access for CSIRT teams
<b>Type of access (public, free, comm)</b>	Open source

## 6.16 LIST's Node in Infrachain Blockchain

<b>Name of the asset</b>	Node in Infrachain Blockchain
<b>KeyWords</b>	Blockchain, smart contract
<b>Organization</b>	LIST
<b>Point of contact</b>	Thierry.grandjean@list.lu
<b>Location</b>	Esch / Belval

<b>Asset objectives</b>	Allow Infrachain members to test Blockchain applications
<b>Technological Areas of Work</b>	Blockchain

### 6.16.1 Functional Components Description

Ubuntu 16.04 server Virtual Machine hosted by a cloud provider.

### 6.16.2 Services provided

This server is registered on the Infrachain test infrastructure via a Rancher console. It is dedicated to be used by Infrachain members to deploy and test their Blockchain based applications on a distributed infrastructure

### 6.16.3 Current Usage

#### 6.16.3.1 Past Projects

<b>Name (Funds)</b>	<b>Short description</b>
Test environment	No productive usage. Pure testing for Infrachain members.



### 6.16.3.2 Live Projects

None.

### 6.16.3.3 Other relevant actions taking place

None.

### 6.16.4 Resources

#### 6.16.4.1 Scientific and Technological Team

Jonathan Lamont
Thierry Grandjean
Uwe Roth

#### 6.16.4.2 Technical Equipment

Virtual Machine Ubuntu 16.04 Server	2 CPU – 2GB RAM – 50 GB HDD
-------------------------------------	-----------------------------

### 6.16.5 Request of use

<b>Ticketing system</b>	None
<b>Communication Channels</b>	E-mail
<b>Time management</b>	
<b>Granularity</b>	
<b>Type of access (public, free, comm)</b>	Infrachain Members only

## 6.17 UKON's Visual Computing Center for Cyber Security

<b>Name of the asset</b>	Visual Computing Center for Cyber Security
<b>KeyWords</b>	Powerwall, Control Room, Machine Learning Infrastructure
<b>Organization</b>	University of Konstanz (UKON)
<b>Point of contact</b>	support@dbvis.inf.uni-konstanz.de
<b>Location</b>	Universitaetsstrasse 10 78464 Konstanz Germany



Asset objectives	<p>Large-Scale Visual Analyses of Security of Information</p> <p>Monitoring room for the implementation and analysis of user-centered interfaces</p> <p>Machine learning infrastructure</p>
Technological Areas of Work	<p>Visual Analytics</p> <p>Cyber Security</p> <p>Machine Learning</p> <p>User-Centered Monitoring</p>

### 6.17.1 Functional Components Description

The infrastructure provided by the University of Konstanz consists of several components which together enable the visual analysis of cyber security information. The individual components allow to efficiently analyze data using the machine learning infrastructure and afterward visualize it on either the Powerwall or in the Control Room setup. The interactive infrastructure aims to involve the user in the analysis process of security relevant information to semi-automatically generate and verify knowledge. The individual components and their interfaces are described in detail in the following sections. The visual computing center for cyber security consists of the following components:

- **Powerwall:** The Powerwall consists of a small cluster computer connected to the 5x2.1m<sup>2</sup> Powerwall with 11 megapixels, which was updated in 2016 for stereo projection and improved resolution. Through its wall-sized display, it is capable of displaying large-scale visualizations and animations of large datasets allowing for the development and evaluation of new modes of data analysis.
- **Control Room:** The Control Room features a combination of three 4k displays and an HD-resolution capacitive touch table for data visualization and interaction technology research. The combination of high-resolution screens with a touch-table allows the design of state-of-the-art and application-specific interaction techniques.
- **Machine Learning Infrastructure:** The Visual Computing Center for Cyber Security features a GPU-Cluster which consists of five NVIDIA Tesla P100 HPC graphic cards. Until now, these are among the fastest GPUs for high-performance computing. The compute-cluster is primarily used for the analysis of large and high-dimensional datasets with data mining techniques, including state-of-the-art neural networks.

### 6.17.2 Services provided

#### 6.17.2.1 Research and Innovation

The Visual Computing Center for Cyber Security may be used for the research and development of innovative technologies in research projects. These projects should be mainly conducted by researchers in the domains Visual Analytics (VA) and Human-Computer Interaction (HCI) and may be focused on Cyber Security.

#### 6.17.2.2 Teaching and Training Activities

Individual components of the Visual Computing Center for Cyber Security can be used as assets in teaching activity. For instance, the Powerwall can be used in the teaching and presentation of visualization techniques requiring a high-resolution screen.



### 6.17.3 Current Usage

#### 6.17.3.1 Past Projects

Name (Funds)	Short description
VIS-SENSE (EU)	The VISSENSE (Visual Analytic Representation of Large Datasets for Enhancing Network Security) project enabled researchers from the visual analytics domain to research and implement demonstrators for the network security domain. In close collaboration with domain experts and companies, several novel visualization and interaction techniques were developed to cope with risk factors, damages, or critical network failures during network operations.
VASA (BMBF)	The VASA (Visual Analytics for Security Applications) project was a research project targeting at the research and development of visual analytics techniques for security applications. For smart grid environments, interactive visualization techniques have been developed that help the involved companies to perceive the network status, cope with failures and deal with damages in the power network.
VALCRI (EU)	The purpose of VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis) is to foster sense-making in criminal intelligence by means of visual analytics. This project combines advanced data analysis techniques with interactive visualizations for an effective visual analytic solution that take into account geo-spatial, temporal, and content dimension of crime-related data. It enables intelligence analysts to explore the data, find new links, and generate new knowledge using interactive visual interfaces.
FLORIDA (BMBF)	The overarching goal of the joint project FLORIDA is to implement legally compliant tools for law enforcement agencies that will increase their effectiveness in analysing mass video data and speed up investigative work. A range of new methods for the analysis of video data will be developed in close cooperation with end users. These include geo-spatial crime scene reconstruction, interactive exploration of extracted information (Visual Analytics), prioritisation of video data, generic object search and audio analysis. Combining these methods will greatly reduce the amount of data to be analysed by investigators, thus increasing focus on relevant events, and supporting decision making.

#### 6.17.3.2 Live Projects

Name (Funds)	Short description
SPARTA (EU)	Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.



Name (Funds)	Short description
SmartDataLake (EU)	SmartDataLake aims at designing, developing as well as evaluating novel approaches, techniques and tools for extreme-scale analytics over Big Data Lakes.
PRIMAGE (EU)	This project proposes an open cloud-based platform to support decision making in the clinical management of two pediatric cancers, Neuroblastoma, the most frequent solid cancer of early childhood, and the Diffuse Intrinsic Pontine Glioma the leading cause of brain tumour-related death in children.
VICTORIA (EU)	VICTORIA will develop a set of robust and accurate video analytics modalities, selected for their relevance in legal investigations. To be able to reach analytics robustness at TRL-6, VICTORIA will create the yet missing video data of crime/terrorist scenes that are required for development and test purposes. VICTORIA will design an innovative Video Analysis Platform (VAP), optimised for performance through parallel processing of these analytics and use of big data processing technologies. To further accelerate the processing of the video material, VICTORIA will explore novel workflows relying on advanced exploitation of video meta-data (data about objects/events/events identified by the analytics within the videos). The combination of these features is expected to accelerate typical video investigations tasks by a factor of 15-100, depending on the specific use case.
ASGRAD (EU)	ASGARD aims to contribute to LEA Technological Autonomy, by building a sustainable, long-lasting community for law enforcement agencies (LEAs) and the R&D industry. This community will develop, maintain and evolve a best-of-class tool set for the extraction, fusion, exchange and analysis of Big Data, including cyber-offense data for forensic investigation.
IN2DREAMS (EU)	IN2DREAMS will address these challenges through two distinct workstreams: focusing on the management of energy-related data and, focusing on the management of asset-related data. IN2DREAMS will develop and demonstrate a modular cloud-based open data management platform facilitating ubiquitous support of both energy and asset services.

### 6.17.3.3 Other relevant actions taking place

Visual Computing Center for Cyber Security is actively used in teaching activities.

## 6.17.4 Resources

### 6.17.4.1 Scientific and Technological Team

**Prof. Dr. Daniel Keim** (male) is the head of Chair of Data Analysis and Visualization (DBVIS) at the University of Konstanz. He received his diploma (equivalent to a MSc degree) in Computer Science from the University of Dortmund in 1990 and his Ph.D. in Computer Science from the



University of Munich in 1994. Subsequently, he was assistant professor in that department prior to becoming associate professor at the Computer Science department of the Martin-Luther-University Halle. He has been working at AT&T Shannon Research Labs, Florham Park, NJ, USA as a Senior researcher. Prof. Keim is well known for his work in the area of visual analytics, information visualization and data mining and was awarded the IEEE VGTC 2011 Visualization Technical Achievement Award. He is in the program committees of major conferences, publishes extensively and regularly gives keynote talks and tutorials at major venues such as IEEE InfoVis, IEEE VAST, ACM SIGMOD, ACM VLDB, and ACM SIGKDD.

**Eren Cakmak** (male) is a research associate and doctoral student in the Data Analysis and Visualization Group. He received his M.Sc. in Computer Science from the University of Konstanz with a focus on visual computing, which includes data analysis, visualization, and visual analytics techniques. His current research interests are data analysis, visualization, and the development of visual analytics techniques in the domain of dynamic network analysis.

**Frederik Dennig** (male) is a research associate and doctoral student in the Data Analysis and Visualization Group. He received his M.Sc. in Computer Science from the University of Konstanz with a focus on visual computing, which includes data analysis, visualization, and visual analytics techniques. His current research interests are data analysis, visualization, and the development of visual analytics techniques in the domain of pattern detection and similarity search.

**Matthew Sharinghousen** (male) is part of the technical support of the Data Analysis and Visualization Group. He received his M.Sc. in Computer Science from the University of Konstanz with a focus on visual computing, which includes data analysis, visualization, and visual analytics techniques.

#### 6.17.4.2 Technical Equipment

Assets	Quantity
Powerwall	
Display	
Powerwall Display Size: 5m x 2.1m Resolution: 5224px x 2160px Optical Output: 12,000 Lumen	1
Projectors	
Galaxy 4k-12 projectors Luminous system: D-ILA system Pixel pitch: 6.8 millimicrons Picture prime: 4,096 dots X 2,400 dots	2



Assets	Quantity
Projection lens: 1.22 time electromotive zoom Projection distance: Approx. 2.5m - 12m Optical Output: 3,5000 Lumen Illuminant Lamp: 825W Xenon Lamp Contrast Ratio: 10,000:1	
Workstation for running the Powerwall	
Intel Xeon E5-2687W0 3.1 GHz	2 x 8 core
Samsung M393B2G70BH0-CK0 16 GB DDR4	8x
NVIDIA Quadro M6000	1
Samsung 850 Pro 512GB SSD	1
Workstation for running the Powerwall with 3D	
Intel Xeon E5-2687W0 3.1 GHz	2 x 8 core
Samsung M393B2G70BH0-CK0 16 GB DDR4	8x
NVIDIA Quadro M6000	1
Samsung 850 Pro 512GB SSD	1
Streaming-Server	
Intel Core i7-5930K	1 x 6 cores
Kingston HyperX DDR4 2133 C14 8 GB RAM	8 x 8GB
NVIDIA GeForce GTX 960	1
Samsung 850 Pro 512GB SSD	1



Assets	Quantity
Samsung 850 Pro 2TB SSD	2
Control Room	
Displays	
Samsung Digital Signane QH65H Resolution: 3840x2160 (4k UHD) Contrast: 6000:1 Diagonal Size: 65" Type: LED	1
Eyevis EYE-LCD-6000-QHD-LD Resolution: 3840x2160 (4k UHD) Contrast: 5000:1 Diagonal Size: 60" Type: LED	2
Workstation for controlling the Displays	
Intel(R) Xeon(R) CPU X5690 3.47GHz	1 x 6 cores
Kingston 9965433-034.A00LF 12 GB DDR3 RAM	3
NVIDIA Quadro K5000	3
Samsung SSD 830 120 GB	1
Seagate Constellation ES.3 ST2000NM0011 2TB HDD	2
Touch-Displays	
3M Multi-Touch Display C4667PW Resolution: 1920 x 1080 (FullHD) Display Colors: 1.07 billion Contrast Ration: 4000:1 LCD Technology: SPVA Number of Touch Points: 60 points with palm rejection	1



Assets	Quantity
Touch Point Speed: <12 milliseconds Input Type: Finger, thin glove Touch Communication: USB Operating System Support: Win 8/7/Vista/XP, Linux, Mac	
Machine Learning Infrastructure	
GPU Server 1 with Multi-User Environment	
Intel(R) Xeon(R) CPU E5-2637 v4 @ 3.50GHz	2 x 4 cores
Kingston 9965604-001.D00G 16GB DDR4 RAM	6
NVIDIA Quadro M6000 GPU	2
10 GB/s Intel Ethernet Controller 10G X550T	1
Samsung SSD 850 EVO 250GB	2
SEAGATE ST2000NM0034 HDD 2TB	2
GPU Server 2 with Multi-User Environment	
Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz	2 x 10 cores
Samsung M393A2G40EB2-CTD 16GB DDR4 RAM	8
NVIDIA Tesla P100 GPU	5
10 GB/s Intel Ethernet Controller 10-Gigabit X540-AT2	1
Samsung SSD 850 500 GB	2
Western Digital WDC WD10JPLX-00M HDD 1TB	6



### 6.17.5 Request of use

Ticketing system	Managed by the support team of the DBVIS (Data Analysis and Visualization) Team
Communication Channels	On-site and partially VPN access
Time management	Labour days between 9:00-16:00
Granularity	Access to subsystems can be provided
Type of access (public, free, comm)	Non profit

## 6.18UBO's IT-Security Awareness Pentesting Framework

Name of the asset	IT-Security Awareness Pentesting Framework
KeyWords	Employee awareness assessment, Intrusion Detection, Phishing
Organization	UBO
Point of contact	sykosch@cs.uni-bonn.de
Location	Regina-Pacis-Weg 3 D-53113 Bonn GERMANY

Asset objectives	Allows the control of success if IT security awareness interventions, e.g. new classes, online trainings, etc.
Technological Areas of Work	Enterprise IT environments, Critical infrastructures

### 6.18.1 Functional Components Description

The tool consists of two parts: The software framework and a collection of recipes. The software framework is composed of all services necessary to deploy arbitrary artefacts to user's interaction area during a companies' day-to-day business. The recipes define the actual test scenario, e.g. the gestalt of the artefact and interpretable reactions to capture.

### 6.18.2 Services provided

The tools may be used to measure the impact of TI security awareness interventions, e.g. classes, e-learning platforms, awareness campaigns, or rollouts of new programs, to user behaviour and therefore their IT security awareness.



### 6.18.3 Current Usage

#### 6.18.3.1 Past Projects

Name (Funds)	Short description
ITS.APT (German Federal Ministry of Education and Research)	The goal of the project was the design and implementation of a tool that allows to measure employee's IT security awareness. The solution is validated by conduction of a field study within the environment of a critical infrastructure across 259 individuals.

#### 6.18.3.2 Live Projects

Name (Funds)	Short description
SPARTA (EU)	The framework will be revised, and crucial improvements will be made.

#### 6.18.3.3 Other relevant actions taking place

None.

### 6.18.4 Resources

#### 6.18.4.1 Scientific and Technological Team

<p><b>Prof. Dr. Michael Meier</b> (male) is full professor for IT-Security in the computer science department at University of Bonn and head of the Cyber Security Department at Fraunhofer FKIE. His research interests include most aspects of applied computer security, with an emphasis on attack and malware analysis as well as detection. From 1993 to 1998 Michael Meier studied computer science and earned his PhD in 2006 for his work on Intrusion Detection at Brandenburg University of Technology Cottbus. From 2006 he worked as Senior Researcher with the Information Systems and Security working group of the Technical University Dortmund before he became Professor in Bonn in 2012. Michael Meier is founder member and chair of the special interest group on Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society and co-chairs the steering committee of the international conference on Detection of Intrusion &amp; Malware and Vulnerability Assessment (DIMVA). He is executive board member of the German Association for Data Protection and Data Security (GDD).</p>
<p><b>Arnold Sykosch, MSc.</b> (male) is an experienced researcher in the fields of Threat Intelligence and IT security awareness measurement. He achieved the degree Master of Science in Computer Science the Heinrich-Heine-University in Duesseldorf, Germany in 2012. Since then he is employed as a researcher at the IT-Security department of the University of Bonn and the Cyber Security department at the Fraunhofer FKIE.</p>

#### 6.18.4.2 Technical Equipment

There is no special technical equipment needed to work with the framework, as that was one of its design goals. However, the repository is connected to a full CI pipeline, implementing a full Dev(Sec)Ops approach. This ensures the software is always in a known state.



### 6.18.5 Request of use

<b>Ticketing system</b>	Issue tracker in the in-house Gitlab-Server
<b>Communication Channels</b>	Chat, Issue tracker, email
<b>Time management</b>	-
<b>Granularity</b>	Only the framework may be available
<b>Type of access (public, free, comm)</b>	Recipes Commercial, Framework open source

## 6.19 TUM's Malware Zoo

<b>Name of the asset</b>	Malware Zoo
<b>KeyWords</b>	Large-Scale Malware Analysis
<b>Organization</b>	TUM
<b>Point of contact</b>	<a href="mailto:alex@sec.in.tum.de">alex@sec.in.tum.de</a> (Admin)
<b>Location</b>	Boltzmannstraße 3 85748 Garching (near Munich) Germany

<b>Asset objectives</b>	- execution of static and dynamic malware analysis - statistical and machine learning operations for malware classification and clustering
<b>Technological Areas of Work</b>	- Cybersecurity - Big Data Analytics - AI systems

### 6.19.1 Functional Components Description

Malware Zoo has services for static and dynamic analysis of malwares. It has Holmes-Totem Planner, Holmes-Storage, Holmes-Gateway, Holmes-Analytics and Holmes-Totem-Dynamic.

**Holmes-Totem Planner:** The Holmes-Totem Planner is responsible for turning data into information by performing feature extraction against submitted objects. When tasked, Holmes-Totem schedules the execution of its services which are capable of performing static and dynamic analysis as well as gather data from third parties. The Holmes-Totem Investigation Planner is optimized for executing extraction services that complete in a few seconds, i.e. static analysis and 3<sup>rd</sup> party queries. When dealing with services that take longer to complete, we recommend pairing the Holmes-Totem Planner with Holmes-Totem-Dynamic.

**Holmes-Storage:** Holmes-Storage is responsible for managing the interaction of Holmes Processing with the database backends. At its core, Holmes-Storage organizes the information contained in Holmes Processing and provides a RESTful and AMQP interface for accessing the data. Additionally, Holmes-Storage provides an abstraction layer between the specific database types. This allows a Holmes Processing system to change database types and combine different databases together for optimization.

**Holmes-Gateway:** Holmes-Gateway orchestrates the submission of objects and tasks to HolmesProcessing. Foremost, this greatly simplifies the tasking and enables the ability to automatically route tasks to Holmes-Totem and Holmes-Totem-Dynamic at a Service level. In addition, Holmes-Gateway provides validation and authentication. Finally, Holmes-Gateway



provides the technical foundation for collaboration between organizations. Holmes-Gateway is meant to prevent a user from directly connecting to Holmes-Storage or RabbitMQ. Instead tasking-requests and object upload pass through Holmes-Gateway, which performs validity checking, enforces ACL, and forwards the requests.

**Holmes-Analytics:** The goal of this project is to implement a semi-generic interface that enables Holmes Processing to manage the execution of advanced statistical and machine learning analysis operations.

**Holmes-Totem-Dynamic:** Just like Holmes-Totem the “Dynamic” Planner is responsible for turning data into information by performing feature extraction against submitted objects. When tasked, Holmes-Totem-Dynamic schedules the execution of its services which are focused on dynamic and other long or indefinite running analysis tasks.

### 6.19.2 Services provided

- Analysis result for malware
- Static and dynamic analysis for submitted samples or hashes
- Having services like Yara, Cuckoo, Objdump, Gadgets, Rich Header

### 6.19.3 Current Usage

#### 6.19.3.1 Past Projects

Name (Funds)	Short description
IUNO (BMBF)	<p>For Germany as a leading industrial location, the networking of production is a key opportunity for the future. German companies and institutions, however, are increasingly confronted with highly professional cyber-attacks. In addition to the classic threats such as viruses or Trojans, novel attacks on industrial control systems are threatening networked industrial plants.</p> <p>For effective protection, it is not enough to adopt the established security concepts. Unlike in IT, for example, you cannot simply switch off production systems in the event of damage, even in planned maintenance windows. In process control and factory automation, systems need to be available around the clock and operate stably. The aim of the National Reference Project for IT Security in Industry 4.0 is to protect networked industrial facilities effectively against cyber-attacks and espionage. Fourteen companies in the German industry are working together with seven research institutes and universities to minimize attack points for hackers.</p>
ForSEC (StMWFK)	<p>As part of the ForSEC project, new concepts and methods for the development of secure, customizable security architectures for embedded mobile devices are being researched and prototypically implemented in a concrete architecture. To this end, a holistic approach will be examined, which includes secure hardware modules, system security and anomaly detection. Preventive security concepts should be combined with reactive measures to control data flows and prevent damage from loss or manipulation of data.</p>
SIBASE (BMBF)	<p>The aim of the SIBASE project to develop solutions for secure embedded systems is to develop a modular system of standardized, interlocking security components for embedded systems in hardware and software in order to ensure long-term security. For this purpose,</p>



Name (Funds)	Short description
	<p>security requirements for embedded systems are analysed and suitable concepts for securing the systems are developed. Based on the results, standardized software components for secure embedded systems are developed and concepts for the unambiguous identification of hardware components are researched.</p> <p>At the Chair of Security in Computer Science, a tool for analysing and analysing security requirements at the software architecture and design level based on the Unified Modeling Language (UML / OCL) is created. To parse security properties of C / C++ software at the implementation level (source code), symbolic execution is used. A tool is being developed to automatically detect vulnerabilities that could be abused for remote exploits or privilege escalation exploits. The focus is on errors in information flow, memory access (buffer overflow, etc.), and number formats (integer overflow, etc.).</p>

### 6.19.3.2 Live Projects

Name (Funds)	Short description
SPARTA (EU)	The SPARTA consortium assembles a balanced set of 44 actors from 14 EU Member States at the intersection of scientific excellence, technological innovation, and social sciences in cybersecurity.

### 6.19.3.3 Other relevant actions taking place

None.

## 6.19.4 Resources

### 6.19.4.1 Scientific and Technological Team

<p><b>Prof. Dr. Claudi Eckert</b> (female) is director of the department “Security in Computer Science” at the Technical University of Munich and head of the Fraunhofer AISEC (Fraunhofer Research Institution for Applied and Integrated Security). After graduating from the University of Bonn she received her PhD in 1993 and qualified as a professor in 1999 at the Technical University of Munich. The focus of her research and teaching activities is on the areas of operating systems, middleware, communication networks, information security, and Anomaly Detection. In 2008 she founded the Center for Advanced Security Research Darmstadt (CASED), where she was deputy director until 2010. Eckert is vice-president of the Society for Computer Science (GI) and a member of several scientific advisory boards.</p>
<p><b>Mohammad Reza Norouzian</b> (male) is a PhD candidate at the Technical University of Munich. His research areas are in Anomaly Detection and Intrusion Detection Systems (IDS). He explores detection of cyber-attacks specifically in the area of Industrial Control Systems with the help of Machine Learning. In addition to his research, he offers and supervises practical courses, seminars, and lectures to university students within the area of anomaly detection and IDS.</p>
<p><b>Sergej Proskurin</b> (male) is a PhD candidate at the Technical University of Munich. His research areas cover a wide range of low level and IT security related topics focusing, in the first place, at dynamic malware analysis through virtual machine introspection. In particular, he explores modern cross-architectural hardware features that enable stealthy analysis of guest VMs. His secondary objectives involve hypervisor/OS design and security, rootkits, reverse engineering, and trusted computing. In addition to his research, he contributes to the open source Xen Project hypervisor</p>



and offer and supervise practical courses, seminars, and lectures to university students within the area of rootkit programming, reverse engineering, and operating systems.

#### 6.19.4.2 Technical Equipment

##### Malware Zoo Specification

Asset	Quantity
Openstack	
Computer Server	1
2x AMD EPYC 7501 512 GB RAM 1x 250 GB SSD 10 GBit Ethernet (2x RJ45)	
Storage Server	1
AMD Ryzen 5 1600 64 GB RAM 8x 10TB Raid 6 10 GBit Ethernet (2x RJ45)	
Cassandra	
DB Server	6
AMD Ryzen 7 1700 2x 2048 GB Samsung SSD 32GB RAM 10 GBit Ethernet (2x RJ45)	
S3	
Storage Server	4
AMD Ryzen 5 1600 2x 6TB 32GB RAM 10 GBit Ethernet (2x RJ45)	



### 6.19.5 Request of use

<b>Ticketing system</b>	Supported by Admin
<b>Communication Channels</b>	On-site or remote
<b>Time management</b>	9:00 – 16:00
<b>Granularity</b>	Access to the subsystems can be provided
<b>Type of access (public, free, comm)</b>	Non profit

## 6.20 LEO's Cyber Threat Intelligence Services

<b>Name of the asset</b>	Cyber Threat Intelligence Services
<b>KeyWords</b>	Vulnerability detection, attack detection, monitoring, Darknet, real-time analysis, Fraud detection
<b>Organization</b>	LEO
<b>Point of contact</b>	antonio.berardi@leonardocompany.com
<b>Location</b>	Via Enrico Mattei, 21, 66100 Chieti ITALY

<b>Asset objectives</b>	-
<b>Technological Areas of Work</b>	Critical Infrastructures, Government, Large Corporations at national and international levels

### 6.20.1 Functional Components Description

Leonardo's Threat Intelligence Services include three sets of functionalities that can be selected according to customer's context and requirements.

Each set is configurable into single services designed to operate in specific application scenarios, in cloud or on premises, depending on the operating context:

- **Cyber Threat Intelligence:** detects new vulnerabilities, cyber-attacks being prepared and information illegally stolen from companies and organisations posted on the Internet, through the continuous monitoring of web and darknet sources and the realtime analysis of huge amounts of data searching for possible clues.
- **Social and Security Threat Intelligence:** acquires, analyses and correlates information on open sources in order to offer a complete overview of the online sentiment related to socio political events. This contributes to improve the awareness of imminent potential threats against the customers' assets.
- **Fraud Detection Threat Intelligence:** prevents internet frauds relevant to phishing campaigns, domain hijacking and theft of digital identities through the continuous monitoring of web and darknet sources aimed at identifying attackers and improving the customers' ability to protect themselves against internet frauds.

### 6.20.2 Services provided

The customer can choose, according to the specific sector and its peculiar needs and requirements, to install a Leonardo Threat Intelligence system on premises and to include, in addition to the design & build of the solution, also on site ongoing support provided by Leonardo (on premises model).



Selecting the full-outsourcing model, the customer can decide to use a subset of services with pre-configured functions based on specific application scenarios of interest and receive automatic reports that can be used without the support of analysts.

Customers can also decide to implement the system at their premises and simultaneously make use of Leonardo's infrastructure only for those services that require high computing capacity without facing additional costs (hybrid model).

Leonardo's Threat Intelligence on-premises model is better suited to the needs of Law Enforcement and Intelligence Agencies for counter terrorism activities and for the support of investigation and crime preventing activities.

On the contrary, hybrid or remote models, best meet protection and cyber resilience needs of critical infrastructures and multi-national strategic enterprises with international networks.

### 6.20.3 Current Usage

#### 6.20.3.1 Past Projects

None.

#### 6.20.3.2 Live Projects

Name (Funds)	Short description
TIS	Monitoring and analysis of large amounts of open source data, deep and dark web, aimed at detecting cyber attacks being prepared and information illegally stolen and published on the web.
SICOTE	Investigation support system for Italian Military Police

#### 6.20.3.3 Other relevant actions taking place

None.

### 6.20.4 Resources

#### 6.20.4.1 Scientific and Technological Team

**Antoni Berardi** (male) He is Head of the pre-sales engineering and delivery unit for Open Source Intelligence services (OSINT). From 2010 to 2012 he was head of the offer engineering unit. In this role, he managed complex proposals addressing challenging cyber security requirements. An example is the sign of the cybersecurity components of the "Process Control System for the Threat of Locks for the Personal Control" (CADA system for the networks of the Personal Control). From 2005 to 2010 he was technical director of offer engineering unit playing the role of technical lead for many complex projects.

**Andrea Mecella:** achieved a University Degree in the University of Pisa, Department of Computer Science. Till 2012 he worked in Cyber Security Business Area in SELEX covering project management, planning and decision support aspects in Big Data Analysis projects related to the Cyber Security field.. has been involved in FP7 projects since 2013; he participated in SAWSOC (Situation AWARE Security Operations Center) project coordinating the development activities; he is participating in GAMMA (Global ATM security management) project giving his experience in the system architecture, coordinating the development activities and the demo exercises.



#### 6.20.4.2 Technical Equipment

<b>HPC:</b> 500 TFlops High performance computing resources elaborating 500,000 bln operations every second
HPC, ISO27001 perimeter, 24x7 operation, Cloud Infrastructure

#### 6.20.5 Request of use

<b>Ticketing system</b>	-
<b>Communication Channels</b>	-
<b>Time management</b>	-
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	-

### 6.21 LEO's Intelligence Enabled Next Gen SOC

<b>Name of the asset</b>	Intelligence Enabled Next Gen SOC
<b>KeyWords</b>	Security operation center, dynamic risk assessment
<b>Organization</b>	LEO
<b>Point of contact</b>	nino.fasciani@leonardocompany.com
<b>Location</b>	Via Enrico Mattei, 21, 66100 Chieti ITALY

<b>Asset objectives</b>	-
<b>Technological Areas of Work</b>	Critical infrastructures, government, large Corporations at national and international levels

#### 6.21.1 Functional Components Description

Leonardo's **Next Generation Security Operation Center (NextGen SOC)** provides a significant range of **Managed Security Services** to large and critical organization.

Currently, the security services portfolio is composed of a full range of service in the phases of **Prediction, Prevention, Proaction** and **Reaction**.

The predictive capabilities of Leonardo's NextGen SOC are significantly enhanced by the Leonardo's Threat Intelligence solutions with services proactively targeting the detection of cyber threats, the management of vulnerabilities and the response to security incidents.

Leonardo's Threat Intelligence Solutions include systems and services based on the monitoring and analysis of large amounts of open source data, deep and dark web, aimed at detecting cyber attacks being prepared and information illegally stolen and published on the web. The solution also provides a comprehensive overview on brand or event sentiment, and the prevention of cyber frauds carried out through the Internet

Since the human factor is essential, even though edge technologies such as artificial intelligence are used to enhance research and highlight deductions, new links and information, Leonardo's analysts team operates through the Intelligence Operation Center supported by next generation SOC's.



The system processes information and data through an end-to-end flow ranging from the collection of open sources information (OSINT), to the building of a knowledge base to carry out analysis and reasoning.

Both artificial intelligence techniques and a big data analytics engine are used for the purpose.

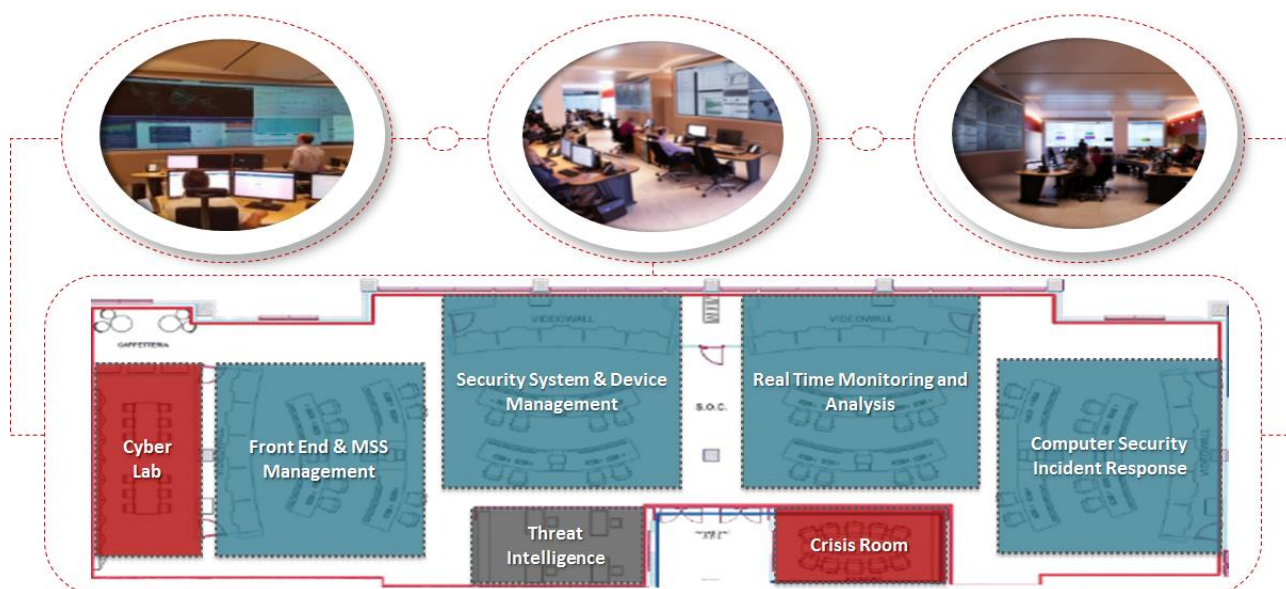


Figure 34: Leonardo's NexGen SOC overview.

### 6.21.2 Services provided

- Predictive → Identify the threat before it can become a problem for customer security (IOC)
- Preventive → Identify the customer security problem before it can become a security incident (RTSM \_ SDM)
- **Proactive** → Identify the security incident and activate all necessary processes (RTSM – SSM)
- Reactive → Reacts to the security incident by performing all necessary actions (CSIRT)

The SOC Service Lines are shown in the following picture:



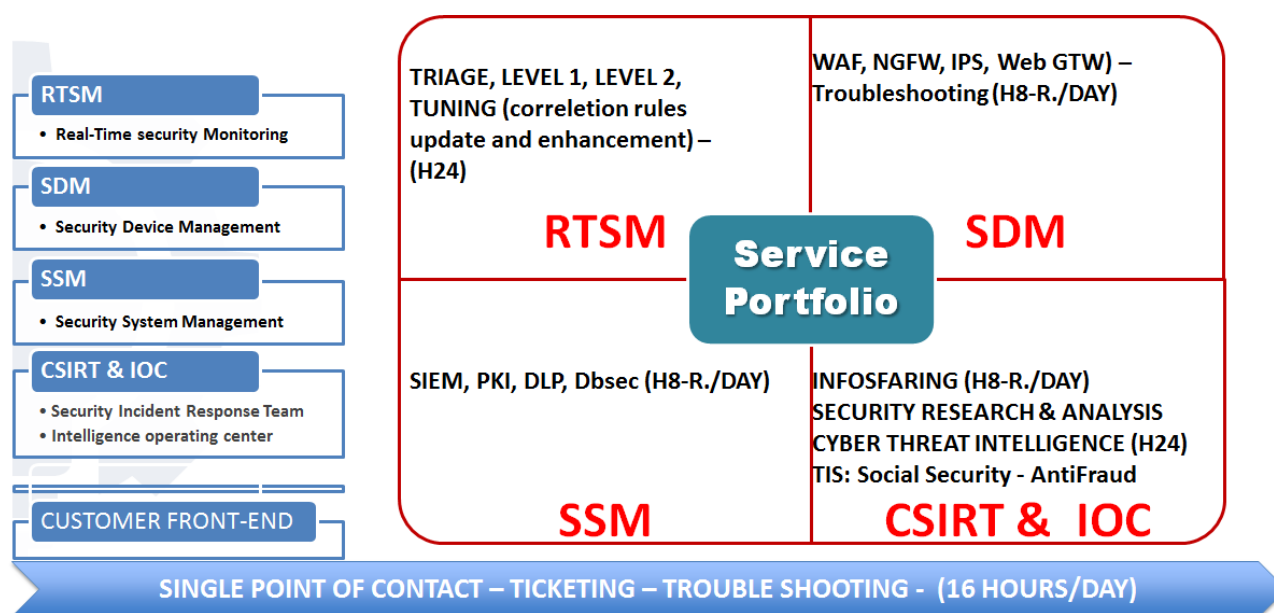


Figure 35: Leonardo's NexGen SOC Service Lines.

### 6.21.3 Current Usage

#### 6.21.3.1 Main Customers

Customer
Fincantieri (Shipbuilding)
Acea (Utilities)
Public Administration (S-RIPA project)
Enav (backup of internal ENAV SOC)

#### 6.21.3.2 Other relevant actions taking place

None.

### 6.21.4 Resources

#### 6.21.4.1 Scientific and Technological Team

30 SOC operators
------------------

#### 6.21.4.2 Technical Equipment

<b>HPC:</b> 500 TFlops High performance computing resources elaborating 500,000 bln operations every second, ,
Cloud Infrastructure



### 6.21.5 Request of use

<b>Ticketing system</b>	-
<b>Communication Channels</b>	Secure internet connection
<b>Time management</b>	Remote service (H24x7x365) Customer premises (H8x5) Extra-Time Remote SOC support :
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	private

### 6.22 LEO's Security Evaluation Facility

<b>Name of the asset</b>	Security Evaluation Facility
<b>KeyWords</b>	Security evaluation, civil and military
<b>Organization</b>	LEO
<b>Point of contact</b>	andrea.morgagni@leonardocompany.com
<b>Location</b>	Via Laurentina 760 00143 Rome ITALY

<b>Asset objectives</b>	-
<b>Technological Areas of Work</b>	Critical infrastructures, manufacturers

#### 6.22.1 Functional Components Description

The Leonardo Security Evaluation Facility (LVS) is operational since 2017 following the incorporation into Leonardo of the pre-existing Consorzio RES LVS (active since 1997), in response to the ICT market growing needs in the framework of security processing and maintenance of electronic data.

Consorzio RES operates in accordance with the international standards ISO/IEC IS-15408 (Common Criteria) and ISO/IEC 27001 (ex BS 7799)

LVS, qualified by the Information Security Certification Body (Organismo di Certificazione della Sicurezza Informatica – OCSI), the meets following requirements:

- Ability to guarantee impartiality, independence, confidentiality and objectivity that regulate the evaluation process
- Availability of premises and assets to carry out the security evaluation in the field of Information Technology
- Ability to monitor the compliance with security and quality measures foreseen for the security evaluation process
- Availability of skilled personnel on the evaluation criteria and in general on IT security issues. This personnel is qualified by the Security Certification Body to conduct evaluation and assistance activities for the purposes of security evaluation process





Figure 36: Leonardo's LVS activities.

## 6.22.2 Services provided

LVS operates as:

- Security Evaluation Facility qualified by OCSI
- Global Consultant in the physical, organizational and ICT security
- ICT consultant for military security certifications (consistently with the national certification schemes).

The LVS also carries out training and consultancy activities to support the customer in addressing the processes of evaluation and certification. In particular, it deals with:

- definition of the security documentation during the preparation phase of the evaluation;
- analysis of the ST/ToE/PP (Protection Profile) to verify if it is evaluable
- training on general security issues in the information technology environment and, in particular, on evaluation techniques

To guarantee impartiality, independence, confidentiality and objectivity in the evaluation process, LVS consultants that provide assistance to a supplier or customer for the evaluation of a ToE or part of it, cannot participate as evaluator in the same process. LVS is able to offer a complete security assessment, not limited to the evaluation process, including security risk assessment, security requirements definition and their formalization in the ST and the definition of the whole documentation necessary to face the evaluation process.

## 6.22.3 Current Usage

### 6.22.3.1 Past Projects

None.

### 6.22.3.2 Live Projects

Name (Funds)	Short description
nShield	HSM device for nCypher company (evaluation process)
Finx O.S.	Operating System for MBDA (consulting)



### 6.22.3.3 Other relevant actions taking place

None.

### 6.22.4 Resources

#### 6.22.4.1 Scientific and Technological Team

**Andrea Morgagni** is the Head of Cyber Resilience and SCADA Security Consulting and responsible of three laboratories (Red Team Laboratory, SCADA Security Laboratory, Consorzio RES Evaluation Facility in Leonardo).

**Amedeo Amormino** is Leonardo technical expert on Risk Assessment (Risk Analysis and management), Certification support according to Standard ITSEC, Information Security Management System - ISMS (Standard ISO 27001 compliant) design and implementation. He is a Certified Common Criteria (ISO 15408) evaluator certified by OCSI.

#### 6.22.4.2 Technical Equipment

Laboratory, ISO27001 perimeter, specialized SW, "Design for Certification Methodology"

### 6.22.5 Request of use

<b>Ticketing system</b>	-
<b>Communication Channels</b>	-
<b>Time management</b>	-
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	-

## 6.23 CNR's CyberSecurity Osservatorio

<b>Name of the asset</b>	CyberSecurity Osservatorio
<b>KeyWords</b>	Cyber threats, risk assessment, malware detection, CVE, CWE, cyber security, spam analysis, security reports
<b>Organization</b>	CNR
<b>Point of contact</b>	info@cybersecurityosservatorio.it press@cybersecurityosservatorio.it
<b>Location</b>	Via Giuseppe Moruzzi, 1 56124 Pisa ITALY

<b>Asset objectives</b>	Improve security over the internet by raising awareness in small/medium sized enterprises, professionals and citizens on cybersecurity topics.
<b>Technological Areas of Work</b>	It, multisector



## 6.23.1 Functional Components Description

### 6.23.1.1 The Web portal (www.cybersecurityosservatory.it)

The Cyber Security Osservatorio of the CNR Institute of Informatics and Telematics (IIT-CNR) was created with the aim of informing and raising awareness in small and medium-sized enterprises, professionals and the public on the importance of information security.

Identifying levels of vulnerability, threat characteristics, studying, refining and implementing techniques and methodologies of network, systems and information security in order to increase the reliability and resilience of the systems are just some of the activities of the Cyber Security Laboratory that contains within it the skills and projects that embrace the various areas of research on the topic.

The observatory makes available to all interested parties the skills and the result of the Laboratory activities through the publication of constantly updated information, documents and services useful for knowing, understanding and reacting to cyber security threats.

### 6.23.1.2 Data collection & storage system

The Cybersecurity Osservatorio collects and gathers heterogeneous data related to cybersecurity topics. These data are updated daily and they grow as time passes. It hosts different databases exploited by various services offered by the website. Among these data sources, it stores databases of CVEs, CWEs, Exploits, Malwares, Spam emails, and tweets which contain cybersecurity keywords.

#### Statistics

This OCS section has been realized to provide statistics on data stored in our database.

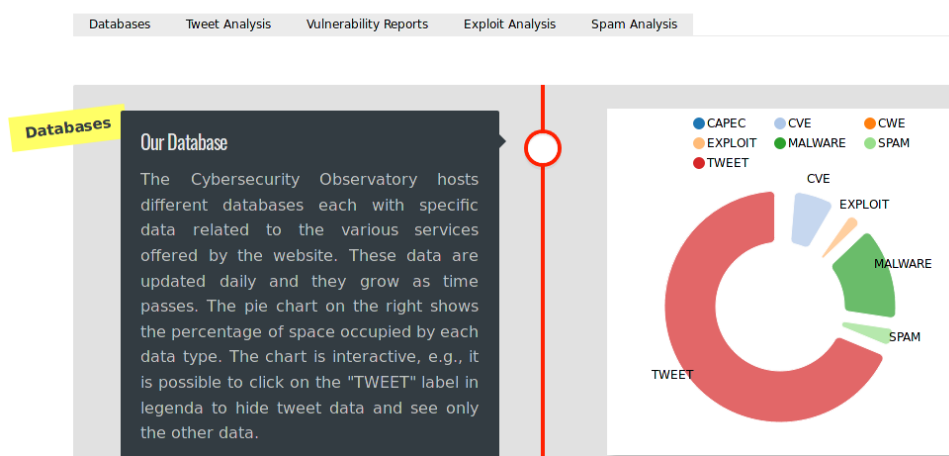


Figure 37: Data collection and storage system.

## 6.23.2 Services provided

### 6.23.2.1 Threat detection tools

The cybersecurity Osservatorio provides a set of tools for security analysis of different sources. Namely, a spam email detector, a ransomware classifier, and a network logs analyser.

The spam email service analyses a set of email file in .eml format to identify the unsolicited ones (SPAM). Furthermore, it divides the spam email in different spam classes.

The ransomware detector service identifies typical ransomware behaviours such as file cipherring. This service is able to identify also malware whose signature is not available yet.

The network logs analyser scans a DNS request log (CEF format) and detects if there are domain names which can be generated by a Domain Generating Algorithm (DGA). These domains are



exploited by malware to register new domain names aimed at avoiding the dependency between the malware and a static domain or IP address, which would be easily blocked.

#### Spam Analysis

This service analyzes sets of email files in eml format to identify the unsolicited ones (SPAM). Moreover, the service divides the spam email in the following classes:

- Advertisement: Unsolicited advertisement e-mails, designed to advertise a product without the recipient's consent to receive advertisement e-mails.
- Portal: Malicious e-mails that redirect the reader toward a set of intermediate steps to an advertisement portal web page. These pages advertise several products from different categories, making difficult to identify who is behind the spam email.
- Malware: The email carries a malicious attachment (malware), aimed at infecting the recipient device.
- Phishing: The email attempts to convince the recipient to reveal the credentials for one or more services that he accesses (bank, social network, etc.).
- Confidential Trick: Fraud email aimed at pushing the recipient in paying money to the attacker.

Figure 38: Threat detection tools

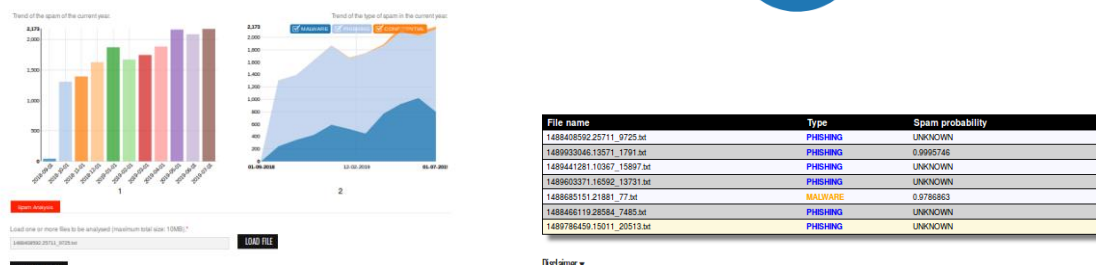


Figure 38: Threat detection tools

### 6.23.2.2 Social media analysis

The cybersecurity social media analysis services, as well as offering tools for the visualization of aggregation statistics related to cybersecurity tweets, offer analysis tools for the verification of the counterfeit phenomena in social media. The Fake Follower Detection system on Twitter, is integrated into the Cybersecurity Osservatorio as a service that allows to detect the percentage of “Fake Followers” of a particular Twitter user.

### 6.23.2.3 Cyber risk analysis

The cyber risk analysis tool provides a simple and quick tool for cyber risk self-assessment. The tool requires two types of input: information about security measures and information about key assets of the enterprise. When all inputs are provided, the tool estimates the expected annual losses for every relevant threat and a total one. The targets for this service are small/medium companies, it provides them an overview on how much they are complying with security policies.

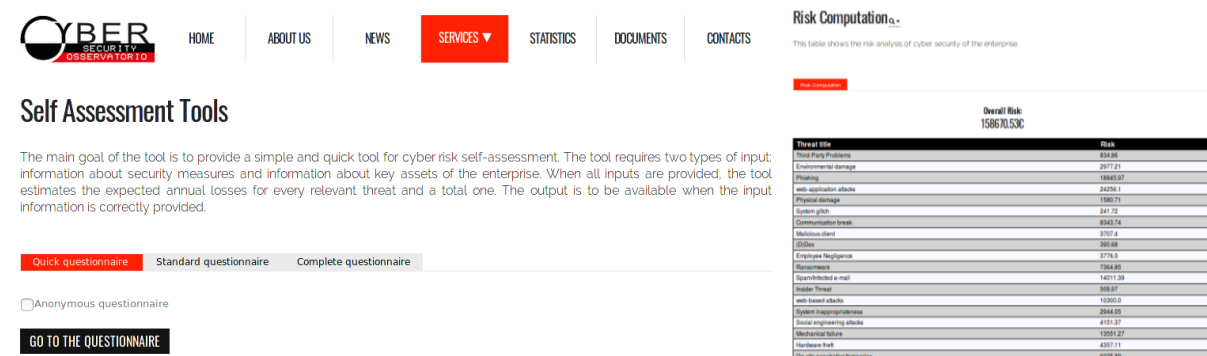


Figure 39: Cyber risk analysis.

### 6.23.2.4 Cybersecurity terminology representation

The cybersecurity Osservatorio, provides services aims at offering a term representation of the Cybersecurity domain knowledge through (i) the creation of a controlled vocabulary, the thesaurus, that contains the terms belonging to the cybersecurity and a series of semantic relationships that exist between the them and (ii) An ontology representation of the knowledge domain which explains the semantic relations existing between the various concepts.



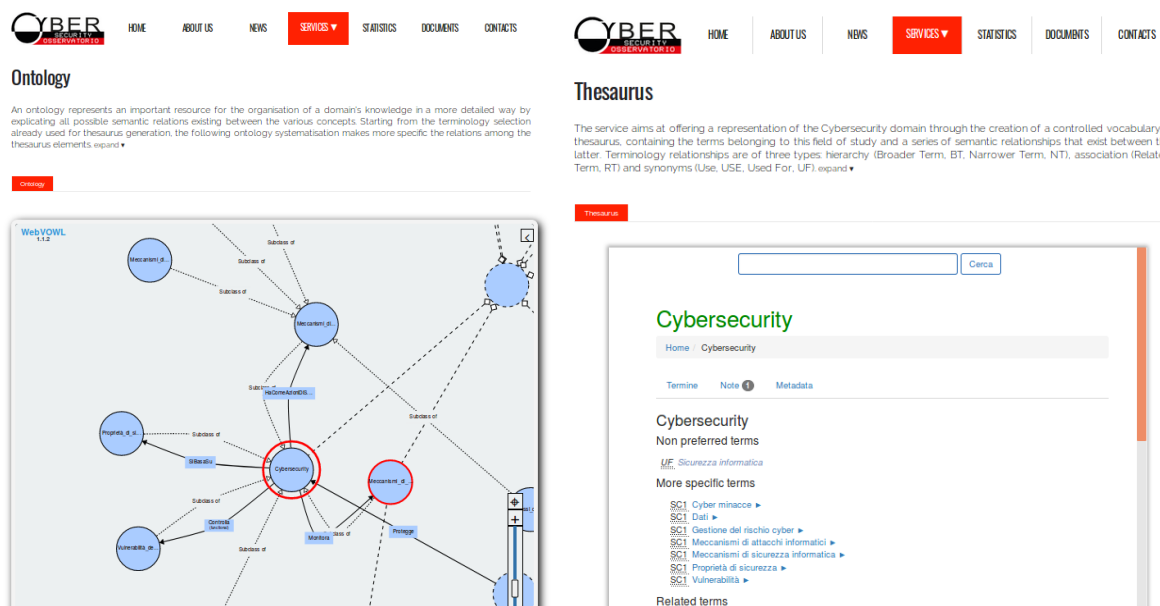


Figure 40: Cybersecurity terminology representation.

### 6.23.2.5 Threat visualization

The threat visualization services, provide an interactive representation of the most important cyber threats as spam email and network attacks. A 3D representation of the network traffic related to attacks on a honeypot located in Pisa is showed. It presents on the map each attack path from the source to the target honeypot and the attack category detected. As well as the attack map, a spam email attack map is provided. It shows the spam email traffic representation, highlighting on the map the source, the destination of the attack and the type of the spam provided by a spam email clustering system.

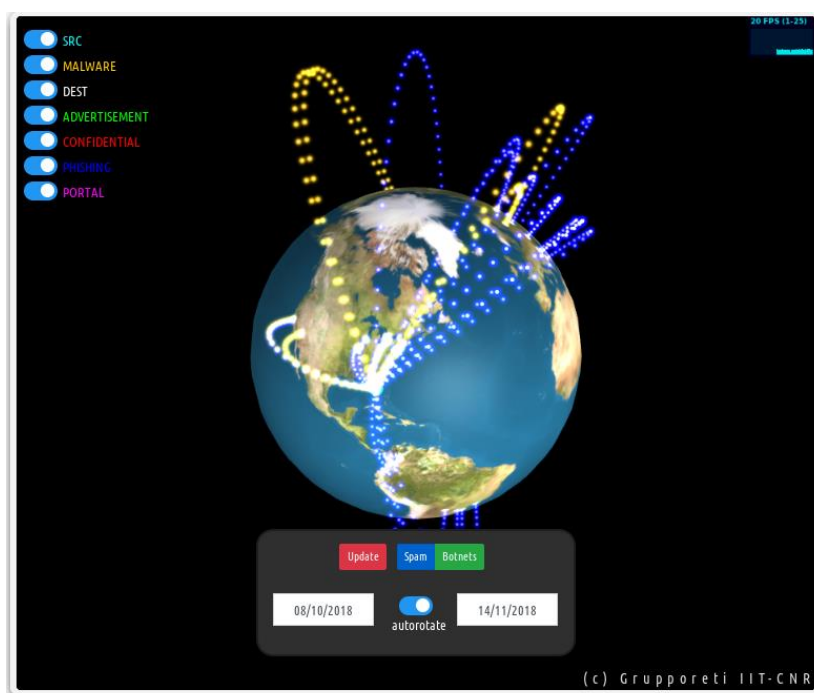


Figure 41: 3D representation of attacks.



### 6.23.2.6 Vulnerability analysis

The vulnerability and exploit service, collecting daily public domain information related to vulnerabilities, exploits, attack pattern and mitigations, performs a data analysis to find a correlation between the information collected. The service offers a visualization tool, which, as well as, showing a general description of the vulnerabilities, offers a global view on these latter providing the hardware and software platforms implicated, the “attack pattern”, the existent possible exploits used on the specific vulnerability and the existent mitigations to address the attacks.

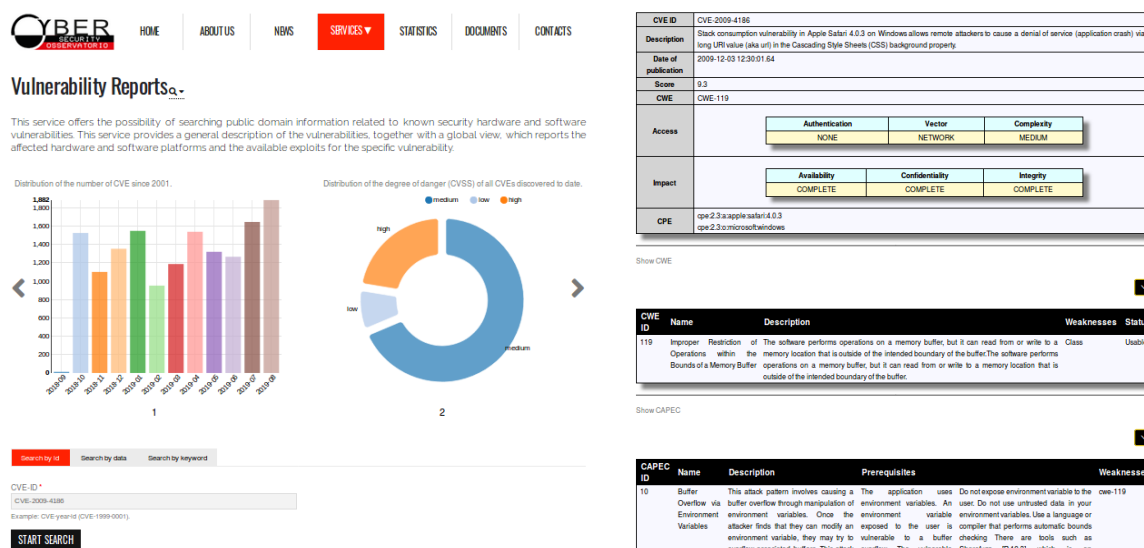


Figure 42: Vulnerability reports.

### 6.23.3 Current Usage

The main resource is the website, which gathers all the available services and projects and make them public to companies, professionals, and internet users. There are not any past projects removed and unavailable anymore, and all the live projects were listed in the services paragraph 1.37.2 above.

#### 6.23.3.1 Past Projects

Name (Funds)	Short description
H2020 NeCS – European Network for Cyber Security (2015-2019)	The European Network for Cyber Security develops technologies for cyber threat management.
H2020 C3ISP – Collaborative and Confidential Information Sharing and Analytic for Cyber Protection	C3ISP project is devoted to create an infrastructure for cyber treat management in a collaborative manner. Some of the technologies developed in C3ISP appears in the observatory.

#### 6.23.3.2 Live Projects

Name (Funds)	Short description
CNR Cyber Security Lab	The CNR runs the observatory as part of its Cyber Security Lab



### 6.23.3.3 Other relevant actions taking place

- Presentation during the Cyber Security Day 2018, 12 Oct. Pisa
- Proposal to become The Tuscany Cyber Security Observatory

### 6.23.4 Resources

#### 6.23.4.1 Scientific and Technological Team

**Dr. Gianpiero Costantino (male)** (M.Sc. 2007, Ph.D. 2011) is a Researcher at the Italian National Research Council (CNR). He has been working for the Security group within the Institute of Informatics and Telematics located in Pisa. From November 2007 to March 2011 he was a Ph.D. student at University of Catania and he conducted his research on Trust, Reputation and Power-Saving within Mobile Ad hoc networks. From 2011 to August 2015 he was a Post-Doc Researcher and his research focused on Security and Privacy aspects within Opportunist Networks, Internet of Things, Social Networking, Fog Computing. Currently, Dr. Costantino is involved in the C3ISP --- H2020 Projects ---, he worked for the following project: Coco Cloud, NESSOS ---FP7 --- HC@WORKS-2, HC@WORKS, Trust in the Cloud --- EIT Digital ---, Securing Smart Airport --- ENISA ---, and his research covers privacy aspects on the Cloud using cryptographic techniques, and Trust solutions for automotive.

**Giacomo Giorgi (male)** graduated in Computer Engineering at the University of Pisa in 2016 with a graduation thesis on the implementation of a deep learning network for person re-identification in a surveillance environment. He has been working at the IIT – CNR institute since 2017 as assistant research fellow and is currently taking a PhD in Information Engineering at the University of Pisa, on the topic “behavioural continuous authentication using AI techniques”. He participated to the “EIT Digital on Trusted Cloud IoT” and the “Collaborative and Confidential Information Sharing and Analysis for Cyber Protection” European projects. His research topics are focused on Machine learning, continuous authentication and text and video analysis for security applications.

**Giacomo Iadarola (male)** obtained the Bachelor degree in Computer Science at the University of Pisa in July 2016 and the Double Master's degree in “Security and Privacy”, awarded by the University of Darmstadt (Germany) and the University of Twente (The Netherlands), in October 2018. He started working at the CNR in Pisa as assistant research fellow in January 2019. In July 2019, he got accepted at the PhD course of Computer Science at the University of Pisa. His research is focused on the field of Software Analysis, Malware detection in Mobile environment and Adversarial Machine Learning.

#### 6.23.4.2 Technical Equipment

None.

### 6.23.5 Request of use

<b>Ticketing system</b>	Managed by CNR
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	09.00-18.00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, comm)</b>	Non profit



## 6.24 JR's CTTC

<b>Name of the asset</b>	JR CTTC – Cyber Test and Training Centre
<b>KeyWords</b>	Data collection, data analysis, IoT security, intrusion detection, APT
<b>Organization</b>	JR DIGITAL
<b>Point of contact</b>	<a href="mailto:branka.stojanovic@joanneum.at">branka.stojanovic@joanneum.at</a>
<b>Location</b>	JOANNEUM RESEARCH DIGITAL Steyrergasse 17 8010 Graz AUSTRIA

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Cybersecurity R&amp;D&amp;I projects</li> <li>• Data collection and analysis</li> <li>• Test and experimentation</li> <li>• Training and consultancy</li> </ul>
<b>Technological Areas of Work</b>	<ul style="list-style-type: none"> <li>• Cyber-security</li> <li>• IoT Technology</li> <li>• Machine Learning</li> <li>• Big Data Analytics</li> </ul>

### 6.24.1 Functional Components Description

Due to the rapidly increasing complexity of networked systems, checking for the vulnerability or resilience of such systems requires not only the relatively expensive development of powerful, partially automated detection, analysis, and defense methods, but also the existence of dedicated laboratory environments consisting of hardware and software components allow simulation and virtualization of systems to be tested outside the production environment.



Figure 43: Initial setup of JR Cyber Test and Training Centre.



The Joanneum Research CTTC (Cyber Test and Training Centre), is as a lab environment, designed to be used in different projects in cyber security and defence field, to help in better concepts understanding, and providing testing environment and data.

The Joanneum Research CTTC setup is an on-going project consisting of several stages. As a hardware and test setup, new components and gadgets can be added without much effort, in order to test these components and to be able to examine vulnerabilities. These components include:

- Stage1: IoT Cyber range environment
  - IoT environment (Smart Home)
  - Industry 4.0 environment
  - Connected Car environment
- Stage 2: Penetration and hacker gadgets
  - Software defined radio
  - IoT device detection tools
- Stage 3: APT red-teaming environment
  - Fully-capable modular network environment including physical and virtual network components
  - APT red-teaming tools and infrastructure
  - Data recording and analysis infrastructure

The current status of CTTC is Stage 1 – finished, Stage 2 – setup in progress, Stage 3 – concept is finished.

### **6.24.2 Services provided**

#### **Support platform for R + D + I projects**

JR CTTC should allow to easily capture and analyse the traffic of different infrastructures – smart home and industrial IoT environments, and campus network environment. It can be used to capture and parse different protocols to validate the effectiveness of IDS systems and formal methods, to capture real traffic from a campus network infrastructure in order to train artificial neural networks, etc.

#### **Isolated environment**

In order to enable the cyber security analysis with different tests (security, penetration) of both external and internal software, the software can be isolated and deployed in the CTTC. The secure environment enables isolated analysis, whether it is a web application, a native application or malware. This includes:

- Penetration Testing
- Security Testing
- Blackbox Testing
- Whitebox Testing
- OWASP Top 10
- Reverse Engineering
- Malwareanalysis

#### **Data collection and analysis**

CTTC will enable researchers to set up isolated network environment, perform red-teaming and collect data for further analysis.

#### **Training**

CTTC may be used as a platform for offering and developing a wide-range of training activities related to PenTesting, IoT and IT network infrastructure protection and anomaly detection.

#### **Consultancy**

CTTC may be used as a platform to support consultancy services.



### 6.24.3 Current Usage

#### 6.24.3.1 Past Projects

None.

#### 6.24.3.2 Live Projects

Name (Funds)	Short description
SPARTA (H2020)	The SPARTA consortium assembles a balanced set of 44 actors from 14 EU Member States at the intersection of scientific excellence, technological innovation, and social sciences in cybersecurity.
IoT4CPS (National)	On this BMVIT and FFG funded project, JR is involved in developing secure IoT-based applications for autonomous vehicles and Industry 4.0.
SecFIT (National)	JR coordinates this BMVIT funded project for developing security by design and security at runtime based on AI for IoT devices.
Critical-Chains (H2020)	Accountability model based blockchain and IoT-enabled XaaS applications
RESOLVD (H2020)	Security requirements specification and security modelling for cyber-physical systems in critical infrastructures
STORY (H2020)	Security requirements and models for ICT systems supporting critical infrastructure

#### 6.24.3.3 Other relevant actions taking place

CTTC is widely used in internal projects of JR.
---

### 6.24.4 Resources

#### 6.24.4.1 Scientific and Technological Team

<p><b>Christian Derler</b> (male) is head of competence group for Cyber Security and Defence and member of the management team of the Institute DIGITAL at JOANNEUM RESEARCH. Having been a business development manager for several years he possesses distinct domain knowledge in security research with its application areas energy systems, defence, manufacturing and transport. He represents the Institute in a number of special interest groups among them the European Cyber Security Organisation (ECSO), the EARTO security and defence research group, the Cyber Security Platform Austria, and the Public Safety Communication Europe Forum (PSCE). He graduated in Information Technology from the University of Technology, Graz in 1995. Since then he managed numerous national and international projects, complemented by consulting activities within the scope of the company's technology transfer mission.</p>
<p><b>Heribert Vallant</b> (male) is a key researcher in the field of cyber security and defence. He graduated in information technology at the Graz University of Technology in 1997. He has been the local manager of various research projects in the information security domain, both national and in the EU context. He was project manager in the Austrian national KIRAS project CriPa (Crime Predictive Analytics). His activities range from designing concepts for IT solutions to</p>



implementation and testing. He is a Certified Tester according to the International Software Testing Qualifications Board (ISTQB®).

**Dr. Ralph Ankele** (male) is a researcher of the Competence Group Cyber Security and Defence that is part of DIGITAL – Institute for Information and Communication Technologies at JOANNEUM RESEARCH. He earned his PhD in Information Security in 2019 from Royal Holloway University of London, UK. Moreover, Ralph holds an MSc and BSc in Computer Science from Graz University of Technology, Austria. Ralph has worked as a security researcher at many international universities and companies and has co-authored 10+ publications that have been accepted at international conferences and journals. His research interests include cryptography, cyber security, penetration testing, secure software development and machine learning.

**Dr. Branka Stojanović** (female) is a senior researcher of the Competence Group Cyber Security and Defence at DIGITAL – Institute for Information and Communications Technologies at JOANNEUM RESEARCH. She graduated in Telecommunication Engineering and obtained doctoral degree (PhD) in Electrical Engineering and Computer Science, from the School of Electrical Engineering, University of Belgrade, Serbia. She is CISSP certified. Her field of research activities covers signal processing algorithms, network security, forensics, biometrics and machine learning. The most recent focus of her research interest is the application of machine learning technologies for cyber security problems in security at runtime and security by design applications.

**Kai Nahrgang** (male) is a Researcher with the competence group cyber security and defense at the DIGITAL – Institute of Information and Communication Technologies at JOANNEUM RESEARCH. He has professional experience in the fields of software development, platform engineering and cloud computing. He received his master's degree in the field of "IT & Mobile Security" at the FH Joanneum - University of applied sciences.

#### 6.24.4.2 Technical Equipment

IoT Cyber Range	<p>Setups for Smart Home use cases</p> <p>Setups for Connected Car use cases</p> <p>IoT devices (Smart Lightbulbs, IoT Gateways, Sensors, ...)</p> <p>Raspberry Pi's (15 * Model 3B+, 3 * Model 4)</p> <p>Raspberry Pi Extension Kits (4G/3G/2G/GSM/GPRS/GNSS, Z-Wave, Zigbee, LowaWan, CAN)</p>
Penetration and hacker gadgets	<p>In order to perform/train penetration testing, the CTTC is equipped with various network devices (switches/router/IoT devices) to be able to create certain use cases.</p> <p>The training is performed using Kali Linux with the extension of JR developed tools for IoT devices detection in network. Furthermore, Software Defined Radio (SDR) gadgets like the HackRF One are used to create and test more advanced attack scenarios on IoT devices and protocols.</p>
APT red-teaming environment	APT red-teaming environment includes complete HW/SW infrastructure, and separate internet access:



	<ul style="list-style-type: none"> <li>• network environment with internet access</li> <li>• networking equipment (routers, switches)</li> <li>• workstations (physical and virtual)</li> <li>• user-behaviour simulator</li> <li>• APT red-teaming tools</li> <li>• data recording and analysis tools</li> </ul>
--	---

### 6.24.5 Request of use

<b>Ticketing system</b>	Managed by the JR support team
<b>Communication Channels</b>	On-site
<b>Time management</b>	Labour days of the JR support team between 9:00-16:00
<b>Granularity</b>	Access to subsystems can be provided
<b>Type of access (public, free, comm)</b>	Non profit (NDA and/or acknowledgement required)

## 6.25 VICOM's Secure Industry 4.0

<b>Name of the asset</b>	BDIH Cybersecurity - Secure Industry 4.0
<b>KeyWords</b>	ISA95, IEC-62264, ISA99, IEC-62443
<b>Organization</b>	Vicomtech
<b>Point of contact</b>	rorduna@vicomtech.org
<b>Location</b>	Mikeletegi Pasealekua, 57 20009 San Sebastian, Gipuzkoa SPAIN

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Monitoring of equipment and processes, and implementation in the productive processes</li> <li>• Systems and models of predictive and proactive maintenance of productive systems</li> <li>• Machines/equipment and flexible, intelligent and connected tooling</li> </ul>
<b>Technological Areas of Work</b>	<ul style="list-style-type: none"> <li>• Cybersecurity</li> <li>• Smart and Connected Machines</li> <li>• Big Data Analytics</li> <li>• Flexible Robotics</li> </ul>

### 6.25.1 Functional Components Description

#### 6.25.1.1 Intelligent production line

It is intended to deploy several small production lines that include the necessary machines and devices to simulate real production factories. This line would have several stations, including both the manufacturing and verification stages. The components of this line would communicate with the MES and the product to perform the action that corresponds according to the needs of the client. The components will communicate following the OPC-UA protocol.



The production line includes hardware, software and communication elements. The following are also included:

- MES software which controls the production process at a high level, indicating what has to be produced. It is contemplated using it with an Open Source MES as well as the possibility of incorporating a commercial MES from the surrounding environment in order to validate potential cases that may occur in companies. It is a Software element that must be integrated in a PC within the perimeter of the OT network.
- ERP Software system that allows centralizing the corporate management, including the production planning, cost control, raw material inventories and traceability.

#### 6.25.1.2 Cybersecurity subsystem

- **Gatherer logs agents:** These are lightweight software elements installed in various points of the IT and OT networks in order to collect information on the operational, communication or security applications launched in them. In principle, the use of Open Source Agents is considered since the commercial is not necessary.
- **Intrusion detection and prevention systems (IDS / IPS):** Software elements that allow the detection of unusual traffic patterns by setting standards, blocking them or generating alarms. Additionally, the use of Host IDS (HIDS) will be evaluated, which allows monitoring the status of a specific host and detecting threats within it.
- **SIEM System** is a software system for the collection, centralization and correlation of the information and events collected in the different logs by the agents. This allows the real-time analysis of information in order to launch alerts or detect threats. Both Open Source and commercial solutions will be contemplated.
- **Industrial firewall** is a Hardware Firewall focused on the specific needs of production environments, in which traditional networks (IT) coexist with those of production (OT). It is a specific Security Hardware. This element will also allow the monitoring of the OT network's traffic internally and its interconnection with the OT network.
- **Firewall IT:** This firewall focuses on the general needs of an organization to protect from threats originated through Internet access. It is a commercial product to ensure an analogous environment to that of any company. It is a specific security hardware which will also allow to monitor the traffic entering and leaving the internet.

#### 6.25.1.3 Platform of Historization and Analytics

The generated data will be stored complying with the necessary security measures (encryption, anonymization, transformation...). This data will be processed in a cloud-like platform, thus avoiding the installation and maintenance of IT infrastructure in the plant.

### 6.25.2 Services provided

#### 6.25.2.1 Support platform for R + D + I projects

This platform will be used to develop R+D+I projects with a cooperative approach. Participants may use their own nodes, both individually or with third parties, in order to carry out other R+D+I projects of a different nature in relevant conditions. These projects should be mainly conducted by researchers and in a one-off case private projects may be developed. In the latter case, pay-per-use models may be contemplated for using the testbed for the aim of financing the projects amortization or maintenance.

#### 6.25.2.2 Benchmarking, evaluation and/or certification of products and/or services

The testbed may be used to support benchmarking, evaluation or certification of goods and services. For instance, provided that Basque authorities issued a certificate, the evaluation of the products or services could be conducted on the testbed.

#### 6.25.2.3 Training

The asset may be used as a platform for offering and developing a wide-range of training activities, as for instance, cyber-ranges. In other words, enabling access to the testbed to end users,



companies offering cybersecurity training or researchers, so they can prepare and provide training or sophisticated simulation environments.

#### 6.25.2.4 Support for awareness actions or generation of cybersecurity culture

In the event that public-private partnerships are encouraged, the testbed will enable conducting activities in order to support international events, to create scenarios for attracting talent or to promote the local companies as leaders in industrial cybersecurity.

### 6.25.3 Usage

#### 6.25.3.1 Past Projects

Name (Funds)	Short description
SEKUTEK (SP-GV)	Development of cybersecure components for their integration in the industrial ecosystem.
MINERO (Indus.)	Development of the MINERO-METABOX tool through machine learning and collective intelligence technologies, with the intention of improving security against new and unknown cybersecurity attacks for clients.

#### 6.25.3.2 Live Projects

Name (Funds)	Short description
TITANIUM (H2020)	TITANIUM will develop novel methods and technical solutions for investigating and mitigating illegitimate activities (relating to either crime or terrorism) involving virtual currencies and/or underground market transactions.
SPARTA (H2020)	Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.
CYBERPREST (SP-GV)	Pattern detection and countermeasures in industrial cybersecurity.
SUCESO (Indus.)	Five analysis use-cases of a platform for treating BigData focused on cybersecurity: smartcities, IoT, deception, industry 4.0, cybersecurity industry.
TRAZAK (Indus.)	Pattern analysis, anomalies and specialized visualization.
iPOWER40 (Indus.)	Pattern analysis, anomalies and specialized visualization.

#### 6.25.3.3 Other relevant actions taking place

Live demonstrations to local industrial companies.
--

### 6.25.4 Resources

#### 6.25.4.1 Scientific and Technological Team



**Dr Raul Orduna** (male) obtained his degree in Computer Engineering at the Faculty of Informatics of San Sebastian by the University of the Basque Country (UPV/EHU) and a Ph. D. degree in Computer Science and Artificial Intelligence at the School of Industrial and Telecommunications Engineering (ETSIIT) of the Public University of Navarre (UPNA). In 2001, he started working at S21sec in several departments: Auditory, Consultancy, Learning and Research & Development. In 2005 he joined the Strategic Office of Panda Security and later, in 2006, he started working in Tracasa as Cybersecurity Project Leader and few years later as Chief Innovation Officer. He is currently the Cybersecurity Director in Vicomtech. He has taken part or led projects related to ethical hacking, forensic analysis, malware analysis, access control and cryptography.

**Jon Egaña** (male) received his Bachelor and Master degree in Telecommunications Engineering from the University of the Basque Country (UPV/EHU). Currently he works in Vicomtech developing R&D projects in the field of cybersecurity and data analytics. He has been involved in the European project CogNet where he presented his master's degree's thesis and he has also been involved in other cybersecurity projects with local enterprises.

**Francesco Zola** (male) is graduated in IT Engineering and Telecommunications (2012) in the University of Cassino and Southern Lazio, Italy, and obtained a master's degree in Computer Science in 2015 in the same university. He has worked as a researcher in the department of Information and Electrical Engineering in the University of Cassino and Southern Lazio, in projects such as: developing the telemetry of an electric kart, a firmware for embedded systems, and management solutions regarding the cloud, storing and virtualization.

**Dr. Ines Goicoechea** (female) is a researcher in the Cybersecurity area at Vicomtech since 2019. She completed her PhD in Electrical, Electronic and Automatic Engineering in July 2019, focusing on presentation attacks in biometric fingerprint recognition. In 2014, she obtained a Master's degree in Electronic Systems and Applications at the Universidad Carlos III de Madrid, where she also graduated in Industrial Electronic Engineering and Automation in 2013. In addition, she is a member of the ISO/IEC JTC1 SC37 and CEN/TC 224 WG18 standardization subcommittees on biometric recognition, where she actively participates and is (co-)editor of two international standards (presentation attacks on mobile devices and user interaction with biometrics).

#### 6.25.4.2 Technical Equipment

Computing Asset	Quantity
IT TECHNOLOGIES	
SERVERS & STORAGE	
CELVIN NAS QR1006 8x6 TB NA	2
RX2540 M4 server with storage	2
PGRA CP NVIDIA Tesla M10	2
COMPUTERS	
Dell Pc OptiPlex 3040 SF,i3-4160,4Gb,500Gb,DRW,W10,1 year, DVD±RW	4
Dell Memory 4GB Certified Memory Module - 1RX16 UDIMM 2400Mhz	4



Computing Asset	Quantity
Dell Warranty for Optiplex 3xxx (1 year/s NBD to 5 year/s NBD)	4
Dell Monitor Professional P2417H, 23, 8", 3 years.	4
Monitor Warranty Extension 5 years	4
SOFTWARE LICENSES (3 YEARS)	
WINSVR 2016 STD 16Core ROK	5
WINSVR 2016 STD AddLic 4Core ROK	5
Veeam Backup Essentials Standard 2 socket bundle for VMware	1
2 additional years of Basic maintenance prepaid for Veeam Backup Essentials Standard 2 socket bundle for VMware	1
VMware vSphere 6 Essentials Kit for 3 hosts (Max 2 processors per host)	1
Subscription only for VMware vSphere 6 Essentials Kit for 3 years	1
SQLSvrStd 2017 SNGL OLP NL Academic	1
SQLCAL 2017 SNGL OLP NL Acdmc UsrCAL	10
AlianVault Solution (3 years license)	1
OT TECHNOLOGIES	
PRODUCTION FACILITIES	
Fabrik-Simulation 24V FISCHERTECHNIK	1
SAI8031: IPC-201C Mix station for analog variable control: pressure, level, temperature and flow	1
INDUSTRIAL CONTROL SYSTEM	
PLC SIEMENS, with HMI, tp900 8"	1
PLC BECKHOFF, Basic CPU module CX2040, input/output module	1
PLC Phoenix Contact, CPU AXIOLINE 1050, SD card, Modbus module, Backnet module	1
eWON distributed periphery	1
Relyum SPPS Plan Platform	3
SOFTWARE LICENSES	
MS Windows Embedded Standard 7 P 64 bit (BeckHoff PLC)	1
TwinCAT 3 runtime (BeckHoff PLC)	1



Computing Asset	Quantity
OPC server	1
LAB VIEW SIMULATION PLAN (3 year license)	1
Plant Simulation Siemens 3 years, Academic Version	1
ODOO (ERP and MES)	1

Networking Assets	Quantity
IT TECHNOLOGIES	
RACK & UPS	
APC Smart-UPS SRT 6000VA RM 230V (Warranty: 3 years)	1
NetShelter SV 42U 800mm Wide x 1060mm Deep Enclosure with Sides Black	1
Rack PDU, Basic, 1U, 16A, 208/230V, (12) C13	2
SWITCHES	
CISCO SYSTEMS Nexus 3524x - 24 10G Ports	1
CISCO SYSTEMS N2K/3K 400W AC Power Supply -Std airflow (Port side exhaust)	1
CISCO SYSTEMS Nexus 3524 Layer 3 LAN Enterprise License	1
CISCO SYSTEMS 10GBASE-SR SFP Module	6
CISCO SYSTEMS 1000BASE-SX SFP transceiver module - MMF - 850nm - DOM	6
CISCO SYSTEMS SG300-28 28-port Gigabit Managed Switch	2
CISCO SYSTEMS Gigabit Ethernet SX Mini-GBIC SFP Transceiver	4
FIREWALLS	
FIREWALL PaloAlto PA-820; all modules license. (support for 3 years).	1
FIREWALL PaloAlto PA-220 Basic (support for 3 years)	2
Fortigate 101E Basic (support for 3 years)	1
CheckPoint 750 Basic (support for 3 years)	1
OT TECHNOLOGIES	
RACK & UPS	



Rack unit	2
SWITCHES	
Industrial Switch Siemens RX1400	1
FIREWALLS	
Fortigate 90D Ruggedized Basic (support for 3 years)	1

### 6.25.5 Request of use

<b>Ticketing system</b>	Managed by SPRI (Basque Country Government) through the BDIH Platform (Basque Digital Innovation Hub)
<b>Communication Channels</b>	VPN access to infrastructure
<b>Time management</b>	Completed labour days, support in CET from 8:00 to 14:00
<b>Granularity</b>	One or more subnetworks can be dedicated
<b>Type of access (public, free, non profit, comm)</b>	Non profit



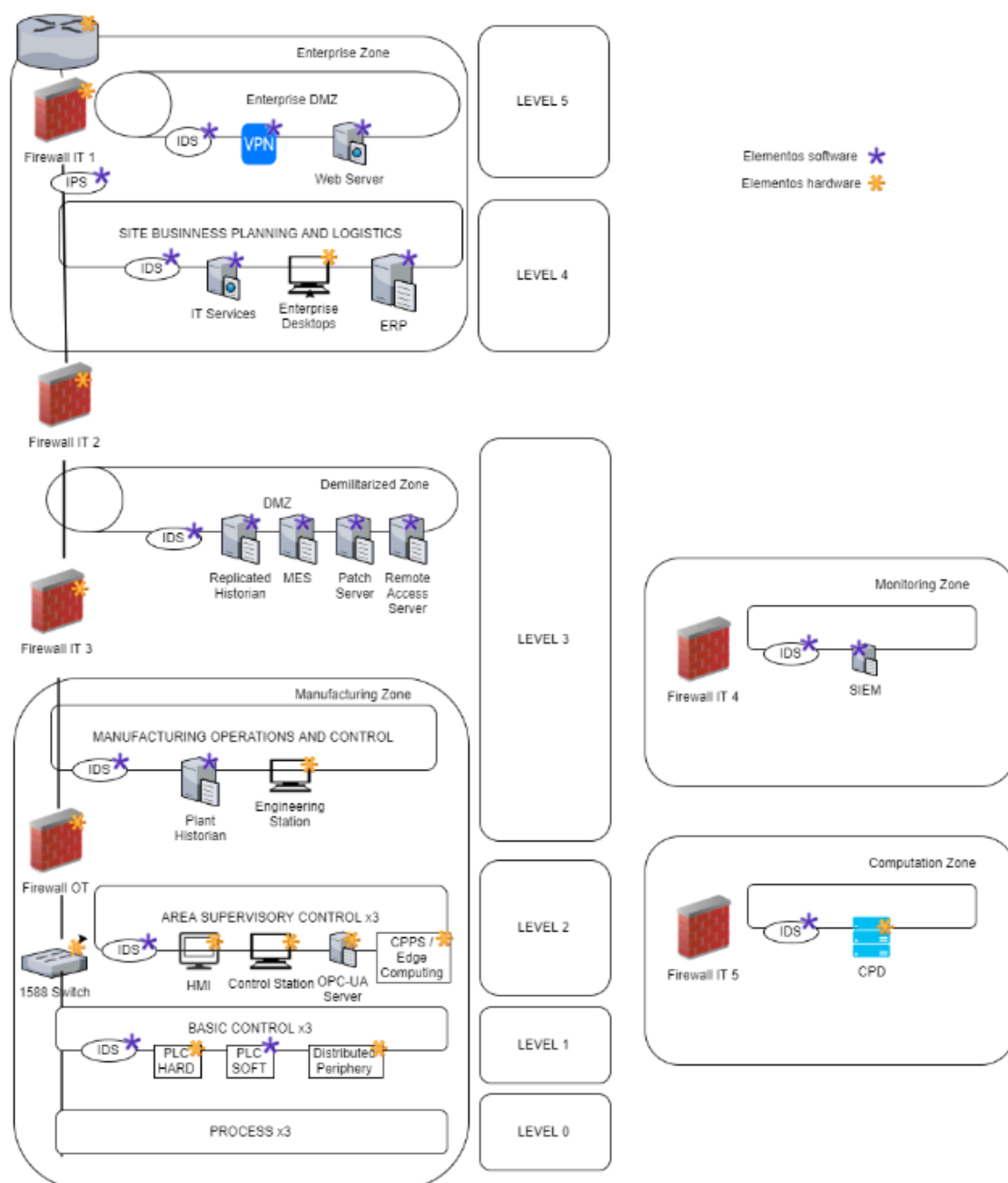


Figure 44: Network topology of VICOM's Secure Industry 4.0.

## 6.26 fortiss' AutoFOCUS3

<b>Name of the asset</b>	AutoFOCUS3
<b>KeyWords</b>	Mode-Based Engineering Tool, Safety and Security, Embedded Systems
<b>Organization</b>	fortiss GmbH
<b>Point of contact</b>	nigam@fortiss.org
<b>Location</b>	Munich, Germany



<b>Asset objectives</b>	Development of Model-Based Engineering methods for Safety and Security Integration
<b>Technological Areas of Work</b>	Embedded Systems, Safety Cases, Security Analysis

### 6.26.1 Functional Components Description

AutoFOCUS3 is a model-based tool and research platform for safety-critical embedded systems. It builds on a generic Eclipse-based tooling framework, is open source (Apache 2.0 license), and is released biannually for the Windows, Linux, and macOS 64-bit platforms.

AutoFOCUS3 supports the design, development and validation of safety-critical embedded systems in many development phases, including architecture design, implementation, hardware/software integration, and safety argumentation based on formal models from the following viewpoints:

- Requirements
- Logical architecture and behaviour
- Technical (hardware and software) architecture
- Deployment (software/hardware mapping, scheduling)
- Safety argumentation
- Security Analysis

Advanced features enable to explore design and implementation alternatives (e.g., safety patterns, task allocation, partition/compartiment architectures) based on state-of-the art formal methods and solvers (e.g., **Z3 solver**), and to validate early designs by means of functional simulation and co-simulation (via FMI). The automatic artefact synthesis capabilities of the tool enable rapid development (e.g., code and configuration generation, scheduling synthesis). Modular assurance cases encoded in the goal-structuring notation (GSN) enable users to document the dependability of a system by bringing in information about its environment and the development context. They provide a structured argument that establishes a systematic relationship between a dependability goal and its evidence (e.g., validation artefact). Finally, AutoFOCUS3 also supports security analysis by using models, such as Attack Defense Trees, including semantic annotations to these models to carry out quantitative risk analysis.

### 6.26.2 Services provided

#### 6.26.2.1 Support platform for R + D + I projects

AutoFOCUS3 is an advanced research prototype that has been used in a number of industrial projects, providing solutions that have been adopted by our industrial partners. It is also subject of intensive research where new features are being tested.

#### 6.26.2.2 Benchmarking, evaluation and/or certification of products and/or services

The models, techniques developed have been applied to large-scale examples, which could in principle be used as benchmarks for other model-based engineering tools.

#### 6.26.2.3 Training

AutoFOCUS3 has been used regularly for both academic and industrial training programs. For example, as can be depicted in <https://www.youtube.com/user/af3fortiss>, it has been used in a regular semester course at TUM. fortiss also offers a training program for industrial partners.

#### 6.26.2.4 Support for awareness actions or generation of safety and security culture for embedded system development

Currently, industries, such as automotive, avionics and industry 4.0, have increasing concerns with respect to the security threats that can affect their safety-critical embedded systems. This has



increased their interest for model-based engineering approaches as they can handle the level of complexity of these systems and are already widely adopted in these industries.

### 6.26.3 Current Usage

#### 6.26.3.1 Past Projects

Name (Funds)	Short description
ASSET-2	In this project, fortiss is working on methods and tools to reduce the costs of the overall development process. In particular we focus on re-usability of certification efforts (from requirements to tests), automatic test case generation, collaborative (multi-user) development and security aspects.
ARAMIS	<p>The ongoing revolution in the mobility domains (automotive, railways and avionic) that enables for the realization of greater safety, comfort, of improved transport efficiency and energy savings. Building up such systems will contain new technologies that are even more efficient. These future control units must perform more functions simultaneously.</p> <p>Advanced features in the mobility domains require this high-performance computing technologies for complex processing or increased networking, as current technologies used in control devices runs up against its performance limit. Therefore, ARAMIS enables the use of these powerful multi-core platforms inside the mobility domains.</p>
BaSys 4.0	<p>The economy stands at the threshold to the fourth industrial revolution. In order to cope with the economic challenges in Germany, the digitalization within the production domain aims at the ability of companies to successfully tackle instability of markets, new global competitors, increasing product variety as well as personalized products down to a lot size of 1.</p> <p>Manufacturing plants that can cope with these challenges and are able to produce such small lot sizes efficiently and cost effectively can only be realized with seriously increased changeability. The required significant reduction of cost for changes requires novel system architectures that focus on the flexibility of production plants. The production of small lot sizes may not always be efficiently controlled in a centralized way. Therefore, decentralized control approaches are required that can quickly be adapted to new products and new product properties. Suitable production resources need to be discovered, evaluated and chosen quickly. This requires an unprecedented level of seamless crosslinking not found in state of the art production plants. While current plants are interconnected within an assembly line or a production site, future plants need to be connected across sites and companies to be able to implement approaches like changeable just-in-time production. Likewise there must not be gaps in networking technology, in production control code, or in exchange of information.</p> <p>In the BaSys4.0 project we and our partners develop an open platform for production plants of the fourth generation. In the project, existing technologies are coupled and integrated to enable the implementation of Industry 4.0 applications. To this end, the project develops a virtual middleware that allows to provide and to couple the required services. This AUTOSAR for Industry 4.0 takes existing technologies to come</p>



Name (Funds)	Short description
	up with required standards, exchange formats, basic services and interfaces that support efficient interconnection and conversion of production plants. The planned base system will be realized as a complete prototype, which can be flexibly extended by the supplying industry.

### 6.26.3.2 Live Projects

Name (Funds)	Short description
IDEA	The methods and modular toolkits will be tailored to the needs (approval aspects) of the aerospace industry, consistent with Flighpath 2050, and will be designed to support the entire development process for fault-tolerant, safety-critical embedded systems. This will be achieved through a wide spectrum of participating companies, including system manufacturers/OEM, suppliers/TIER1, service providers, technology suppliers, universities and research institutes. Participating companies can utilize the methods and modular toolkits with their own specific development process.
RISE	In the RISE project, researchers are examining low-redundancy system architectures for distributed real-time systems with a high degree of safety as an alternative to conventional, multichannel redundancy solutions that are unsuitable for cost-sensitive markets such as vehicle manufacturing.

### 6.26.3.3 Other relevant actions taking place

Live demonstrations to local industrial companies and a regular semester course.
--

## 6.26.4 Resources

### 6.26.4.1 Scientific and Technological Team

<p><b>Dr. Vivek Nigam (FOR)</b>, is the lead of the Safety and Security Research Group at FOR. He obtained his PhD in 2009 from the École Polytechnique (France), held a post-doctoral position from 2009-2010 at the University of Pennsylvania (USA), was awarded the prestigious Alexander von Humboldt award researching from 2010 – 2012, at the Ludwig-Maximilians-University (Germany), and is since 2012 an associated professor at the Federal University of Paraíba (Brazil), on leave since 2017. He has more than 65 peer-reviewed publications and more than 800 citations from topics ranging from structural proof theory, computer security, programming languages, model-based security development, and formal methods. He has experience with a number of national and European projects.</p>
--

### 6.26.4.2 Technical Equipment

- AutoFOCUS3 has been developed on the Eclipse environment.

<b>Requirements</b>
---------------------



Java SE 1.11
<b>Tool documentation</b>
AutoFOCUS3 <a href="https://www.fortiss.org/en/publications/software/autofocus-3">https://www.fortiss.org/en/publications/software/autofocus-3</a>

### 6.26.5 Request of use

<b>Ticketing system</b>	No
<b>Communication Channels</b>	e-mail, forums
<b>Time management</b>	Working hours
<b>Granularity</b>	Developer and user modes of access
<b>Type of access (public, free, comm)</b>	Non profit

## 6.27 UniLU's TSOPEN

<b>Name of the asset</b>	TSOPEN
<b>KeyWords</b>	Logic bomb detection, Android Security
<b>Organization</b>	UNILU
<b>Point of contact</b>	jacques.klein@uni.lu
<b>Location</b>	University of Luxembourg

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>Android malware detection.</li> <li>Identify logic bomb in Android applications.</li> </ul>
<b>Technological Areas of Work</b>	Mobile Security, Android Security, Software Analysis.

### 6.27.1 Functional Components Description

Logic bombs are mechanisms used by malicious apps to evade detection techniques. Typically, an attacker uses logic bomb to trigger the malicious code only under certain chosen circumstances (e.g. only at a given date) to avoid being detected by the analysis. The goal of TSOpen is to detect such logic bombs. The approach used to perform the detection is fully static and combine multiple techniques such as symbolic execution, path predicate reconstruction, path predicate minimization, and inter-procedural control-dependency analysis. In a first version, TSOpen will focus on detecting triggers related to time, location and SMS.



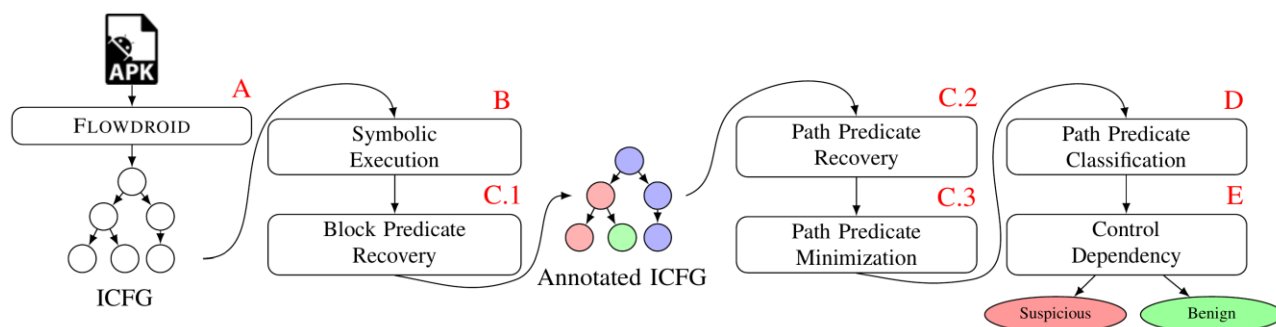


Figure 45: Overview of TSOOpen

TSOpen is developed over Flowdroid, which provides a useful model of the Android Framework on which one can easily apply algorithms. Figure 3.16 provides an overview of the tool. First, an inter-procedural control flow graph from Flowdroid is retrieved on which TSOOpen applies a symbolic execution in order to retrieve the semantic of objects of interest. Then simple predicates are retrieved during the block predicate recovery to annotate the ICFG. The annotated ICFG is then used to retrieve the full path predicate of every instructions. A predicate minimization algorithm is then applied in order to rule out false dependencies. Afterwards, a first decision is taken during the predicate classification step to get suspicious predicates. Finally, a control dependency step is applied in order to take the decision regarding the suspiciousness of the potential logic bomb under study.

## 6.27.2 Services provided

### 6.27.2.1 Support platform for R + D + I projects

TSOpen tool has been developed under an internal project at The University of Luxembourg. It is to be used in order to detect so-called logic bombs in potential new Android Malware. If precision is proven to be effective, the tool could be leveraged on Android applications before entering a store.

### 6.27.2.2 Benchmarking, evaluation and / or certification of products and / or services

It has been evaluated on several hundred of thousands applications.

### 6.27.2.3 Training

The approaches used for building this tool could be used as a support for training to Android Applications Static Analysis methods.

### 6.27.2.4 Support for awareness actions or generation of Functional Safety culture in different domains

Currently, Anti-Malware companies have increasing concerns with respect to the growing number of new malware and new malicious techniques used in Applications. Security threats are ubiquitous in nowadays mobiles. Therefore, new approaches could be leveraged in order to appease those threats.

## 6.27.3 Current Usage

### 6.27.3.1 Past Projects

Name (Funds)	Short description
Andromap (FNR)	Recent research works try to propose different kind of security analyses on Android applications. However, proposed analyses solutions consider an Android application alone. This is not sufficient. Indeed, even if a permission-based architecture (as the one of Android) ensures that an application A can only access the resources for which A has the permission, the specificities of Android make



Name (Funds)	Short description
	<p>communication between applications (and the components constituting an application) possible through elements called Intents. Consequently, on Android, several applications can collude to leak sensitive information. For instance, an application can get the user's location and send it to another application which then leaks the sensitive information to an untrusted third party.</p> <p>The first expected outcome of AndroMap is a detailed map of Android application components and the links that exist between them. The map can be used to detect problems such as privacy leaks and click fraud, or to determine interesting properties such as long or otherwise interesting communication paths, or paths with loops, hinting at potential for a Morris-worm or denial-of- service attacks. A direct application is to use the map to warn the user when she is about to install an app that would yield suspicious links in the user's "device map".</p> <p>The second expected outcome of AndroMap is to go beyond simply warning the user by providing a tool which allows the correction of the identified security flaws. The main research difficulty is to modify the code of an android application without altering the nominal functionalities of the application.</p>

### 6.27.3.2 Live Projects

Name (Funds)	Short description
Characterize (FNR)	<p>The current momentum of Android has attracted the interest of malicious app writers who are contributing with an increasingly high number of malware distributed through official and alternative markets. A malicious app is typically designed and advertised as providing specific user-desired functionalities, and yet is implemented to behave in a way that contradicts with the user interests. The palette of techniques used by malware goes from simple use of sensitive API methods (such as sendSMS) to more sophisticated exploitation of new vulnerabilities (such as data residue attacks after uninstallation of popular apps). Malware writers can further leverage evasion techniques to harden the job of security analysts by challenging static analysis approaches through the use of reflection, native code and string encryption, or by limiting the efficiency of dynamic analysis techniques through the non-execution of malicious behavior in an emulated environment.</p> <p>Nonetheless, reports from Antivirus vendors and studies in the literature regularly highlight the predominance of a set of malware families within which samples are categorized based on the runtime behavior of app code (i.e., the malware activation process as well as the actions and data used by the malicious payloads).</p> <p>In CHARACTERIZE, we build on this key assumption that malicious behavior types are, to some extent, instantiated by similar code patterns in the variety of malware samples. The first challenge is then, for each family, to identify recurring samples of malicious pieces of code to infer the common patterns or the common features in order to "characterize" them. The second challenge is to leverage these patterns or features to detect Android Malware. To that end,</p>



Name (Funds)	Short description
	CHARACTERIZE envisages to explore two parallel directions: (1) Explainable Per-Family Machine Learning Malware Detection; (2) Pattern Matching Based Malware Detection.

### 6.27.3.3 Other relevant actions taking place

Paper submitted.
------------------

## 6.27.4 Resources

### 6.27.4.1 Scientific and Technological Team

Prof. Jacques Klein, is the lead of the TruX team at the University of Luxembourg since January 2020. He obtained his PhD in 2006 from the University of Rennes (France). He held a Research Scientist position at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg from 2010 to 2015. Since July 2015, he has been working in the same entity as a Senior Research Scientist, then as a Chief Scientist. He is also a member of the University Council of the University of Luxembourg as representative of the Interdisciplinary Centers Professors. His has more than 130 publications and more than 6800 citations in the field of Software Engineering and Software Security.
Prof. Tegawende Bissyande, is the co-lead of the TruX team at the University of Luxembourg since January 2020. He obtained his PhD in 2013 at the University of Bordeaux (France). He held a position of Senior research scientist in the SerVal team at the University of Luxembourg. He has more than 120 publications and more than 2700 citations in the field of Software engineering, Software Debugging and Software Security.
Jordan Samhi, is a Doctoral Researcher of the TruX team at the University of Luxembourg. He received his Master's degree in Computer and Information Systems Security from the University of Lorraine (France), in 2019. His research interests are in the security aspects of software engineering, with a particular focus on malware and vulnerability detection. He is under the supervision of Prof. Jacques Klein.

### 6.27.4.2 Technical Equipment

TSOpen has been developed on the Eclipse environment with the use of state-of-the-art Frameworks.

Requirements
Java SE 1.8 as it relies on the Soot Framework.
Applications to analyse.
A Terminal.
Tool documentation
Not published yet.



### 6.27.5 Request of use

<b>Ticketing system</b>	None.
<b>Communication Channels</b>	By email and Issue Tracker.
<b>Time management</b>	Labour days between 9 am and 16pm (CET).
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	Non-profit.

## 6.28 UniLU's SafeCommit

<b>Name of the asset</b>	SafeCommit
<b>KeyWords</b>	Vulnerability Detection Tool For DevOps Communities
<b>Organization</b>	UNILU
<b>Point of contact</b>	jacques.klein@uni.lu
<b>Location</b>	University of Luxembourg

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>Detection of commits introducing vulnerabilities</li> <li>Detection of commits fixing vulnerabilities</li> </ul>
<b>Technological Areas of Work</b>	Vulnerability detection, machine learning.

### 6.28.1 Functional Components Description

The goal of this tool is twofold:

First, detection of patches which fix software vulnerabilities. To that end, both code and textual features will be engineered and assessed. These features will be then used by machine learning algorithms designed and selected to cope with unbalanced datasets.

Second, detection of patches which introduce software vulnerabilities. Like mentioned previously, code and textual features will be investigated, but it is highly probable that the features are different. The proposed tool aims at being integrated into real-world software maintenance and usage workflows. The objective is to carry out a live study in order to collect practitioner feedback for iteratively improving the tuning of the research output, towards an effective technology transfer.

### 6.28.2 Services provided

#### 6.28.2.1 Support platform for R + D + I projects

SafeCommit tool has been developed under an internal project at The University of Luxembourg. It is to be used in order to detect commits introducing vulnerabilities and commit fixing vulnerabilities.

#### 6.28.2.2 Benchmarking, evaluation and / or certification of products and / or services

None yet.

#### 6.28.2.3 Training

The approaches used for building this tool could be used as a support for training to automated vulnerability detection and machine learning.



#### 6.28.2.4 Support for awareness actions or generation of Functional Safety culture in different domains

Currently, developers tend to prioritize an early date for a software and not the correct building of the software. Hence, the introduction of vulnerabilities is more likely due to time constraints and poor code quality. This tool could lower the number of vulnerabilities introduced by leveraging it before committing new code.

### 6.28.3 Current Usage

#### 6.28.3.1 Past Projects

Name (Funds)	Short description
Andromap (FNR)	<p>Recent research works try to propose different kind of security analyses on Android applications. However, proposed analyses solutions consider an Android application alone. This is not sufficient. Indeed, even if a permission-based architecture (as the one of Android) ensures that an application A can only access the resources for which A has the permission, the specificities of Android make communication between applications (and the components constituting an application) possible through elements called Intents. Consequently, on Android, several applications can collude to leak sensitive information. For instance, an application can get the user's location and send it to another application, which then leaks the sensitive information to an untrusted third party.</p> <p>The first expected outcome of AndroMap is a detailed map of Android application components and the links that exist between them. The map can be used to detect problems such as privacy leaks and click fraud, or to determine interesting properties such as long or otherwise interesting communication paths, or paths with loops, hinting at potential for a Morris-worm or denial-of- service attacks. A direct application is to use the map to warn the user when she is about to install an app that would yield suspicious links in the user's "device map".</p> <p>The second expected outcome of AndroMap is to go beyond simply warning the user by providing a tool which allows the correction of the identified security flaws. The main research difficulty is to modify the code of an android application without altering the nominal functionalities of the application.</p>

#### 6.28.3.2 Live Projects

Name (Funds)	Short description
Characterize (FNR)	<p>The current momentum of Android has attracted the interest of malicious app writers who are contributing with an increasingly high number of malware distributed through official and alternative markets. A malicious app is typically designed and advertised as providing specific user-desired functionalities, and yet is implemented to behave in a way that contradicts with the user interests. The palette of techniques used by malware goes from simple use of sensitive API methods (such as sendSMS) to more sophisticated exploitation of new vulnerabilities (such as data residue attacks after uninstallation of popular apps). Malware writers can further leverage evasion techniques to harden the job of security analysts by challenging static</p>



Name (Funds)	Short description
	<p>analysis approaches through the use of reflection, native code and string encryption, or by limiting the efficiency of dynamic analysis techniques through the non-execution of malicious behavior in an emulated environment.</p> <p>Nonetheless, reports from Antivirus vendors and studies in the literature regularly highlight the predominance of a set of malware families within which samples are categorized based on the runtime behavior of app code (i.e., the malware activation process as well as the actions and data used by the malicious payloads).</p> <p>In CHARACTERIZE, we build on this key assumption that malicious behavior types are, to some extent, instantiated by similar code patterns in the variety of malware samples. The first challenge is then, for each family, to identify recurring samples of malicious pieces of code to infer the common patterns or the common features in order to “characterize” them. The second challenge is to leverage these patterns or features to detect Android Malware. To that end, CHARACTERIZE envisages to explore two parallel directions: (1) Explainable Per-Family Machine Learning Malware Detection; (2) Pattern Matching Based Malware Detection.</p>

### 6.28.3.3 Other relevant actions taking place

Paper in progress.
--------------------

## 6.28.4 Resources

### 6.28.4.1 Scientific and Technological Team

<p>Prof. Jacques Klein, is the lead of the TruX team at the University of Luxembourg since January 2020. He obtained his PhD in 2006 from the University of Rennes (France). He held a Research Scientist position at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg from 2010 to 2015. Since July 2015, he has been working in the same entity as a Senior Research Scientist, then as a Chief Scientist. He is also a member of the University Council of the University of Luxembourg as representative of the Interdisciplinary Centers Professors. His has more than 130 publications and more than 6800 citations in the field of Software Engineering and Software Security.</p>
<p>Prof. Tegawende Bissyande, is the co-lead of the TruX team at the University of Luxembourg since January 2020. He obtained his PhD in 2013 at the University of Bordeaux (France). He held a position of Senior research scientist in the SerVal team at the University of Luxembourg. He has more than 120 publications and more than 2700 citations in the field of Software engineering, Software Debugging and Software Security.</p>
<p>Timothée RIOM, is a Doctoral Researcher who received his Master’s degree in Microelectronics and Computer Science from the Ecole des Mines de Saint-Etienne (France), in 2016. Timothée joined the Security, Design and Validation group, SerVal, headed by Prof. Yves Le Traon. He will be working on characterization of android malwares and the development of tools to enhance the latter, under the supervision of Dr. Jacques KLEIN.</p>



Jordan Samhi, is a Doctoral Researcher of the TruX team at the University of Luxembourg. He received his Master's degree in Computer and Information Systems Security from the University of Lorraine (France), in 2019. His research interests are in the security aspects of software engineering, with a particular focus on malware and vulnerability detection. He is under the supervision of Prof. Jacques Klein.

#### 6.28.4.2 Technical Equipment

Requirements
Dataset of commits.
A Terminal.
Tool documentation
Not published yet.

#### 6.28.5 Request of use

<b>Ticketing system</b>	None.
<b>Communication Channels</b>	By email and Issue Tracker.
<b>Time management</b>	Labour days between 9 am and 16pm (CET).
<b>Granularity</b>	-
<b>Type of access (public, free, comm)</b>	Non-profit.

### 6.29 CETIC VaCSInE

<b>Name of the asset</b>	VaCSInE
<b>KeyWords</b>	Adaptive continuous security orchestration, heterogeneous hardware, edge, fog, NFV, SFC, TOSCA
<b>Organization</b>	CETIC
<b>Point of contact</b>	<a href="mailto:info@cetic.be">info@cetic.be</a>
<b>Location</b>	Avenue Jean Mermoz 28, 6041 Charleroi BELGIUM

<b>Asset objectives</b>	Ensure security of systems based on policies, continuous monitoring, and assessing security (certification) requirements in Cloud-Edge-IoT network environments
<b>Technological Areas of Work</b>	Edge/Fog/Cloud



### 6.29.1 Functional Components Description

The VaCSInE tool provides adaptive continuous security orchestration in edge/fog and cloud infrastructures. It relies on Service Function Chaining (SFC) and continuous monitoring to provide dynamic reconfiguration of the infrastructure.

CETIC built an edge simulator infrastructure to study edge computing challenges such as resilience, scalability, security, ... The simulator consists of a dozen of single board computers with various architectures (x86, ARMv7, ...), Arduino boards, various sensors and actuators (leds, fans, temperature, ...). The simulator leverages Kubernetes for its Container as a Service layer and KubeEdge for the edge infrastructure aspects.



Figure 46: CETIC portable edge simulator

### 6.29.2 Services provided

CETIC can provide access to the edge simulator testbed.

### 6.29.3 Current Usage

#### 6.29.3.1 Past Projects

Name (Funds)	Short description
BEACON	Enabling Federated Cloud Networking - Horizon 2020

#### 6.29.3.2 Live Projects

Name (Funds)	Short description
IDEES	Future Internet to develop businesses, economy and society
Quality 4.0	Transparent product quality supervision in the age of Industry 4.0

#### 6.29.3.3 Other relevant actions taking place

The security orchestration tool is in active development, the edge simulator has been built and tested with Kubernetes/KubeEdge.



## 6.29.4 Resources

### 6.29.4.1 Scientific and Technological Team

**Sebastien Dupont** is expert research engineer at CETIC, a Belgian ICT applied research center. His research interest cover areas of model based distributed systems such as Cloud/Edge/Fog computing and resilience.

**Philippe Massonet** is scientific coordinator at CETIC, a Belgian ICT applied research center. His research interest cover the areas of software, service and security engineering, as well as distributed systems such as Grids and service oriented infrastructures.

### 6.29.4.2 Technical Equipment

HW: x86, Arduino, ARM

SW: VaCSInE, KubeEdge, Kubernetes

## 6.29.5 Request of use

<b>Ticketing system</b>	<a href="https://github.com/cetic/vacsine/issues">https://github.com/cetic/vacsine/issues</a>
<b>Communication Channels</b>	Issue tracker, email
<b>Time management</b>	Labour days between 9:00-16:00
<b>Granularity</b>	Access to subsystems can be provided
<b>Type of access (public, free, comm)</b>	Free

## 6.30 CINI's APPROVER

<b>Name of the asset</b>	Approver
<b>KeyWords</b>	Mobile Security, Mobile Application Risk Assessment, Vulnerability Analysis, SAST, DAST
<b>Organization</b>	CINI (spin-off Talos)
<b>Point of contact</b>	info@talos-sec.com
<b>Location</b>	Talos srls Via Magliotto 2 17100 – Savona (IT)

<b>Asset objectives</b>	<ul style="list-style-type: none"> <li>• Security risk assessment of mobile apps</li> <li>• Automated security analysis of mobile apps</li> <li>• Mobile vulnerability detection</li> <li>• Security risk report</li> </ul>
<b>Technological Areas of Work</b>	Android Security, Mobile Security, Mobile Risk Assessment, Vulnerability Analysis



### 6.30.1 Functional Components Description

At high-level, Approver is composed of a set of modules for both Static Analysis (SAST) and dynamic analysis (DAST). Each module, developed as a microservice using Docker technology, enables a different security analysis and is managed by an orchestration layer. Besides, each module exposes a set of RESTful APIs.

The modules for SAST (Figure 47) are in charge of analyzing the application package according to its content. Examples of implemented SAST analysis include vulnerability analysis, permission analysis, and string analysis. Instead, the DAST modules aim to install the application package in a testing environment and evaluate the security of the application during the execution. Examples of DAST analysis include network analysis, API monitoring, and filesystem monitoring.

Finally, Approver provides a web front-end that allows to i) view the detailed results of each application analyzed, ii) download all the artifacts produced during the analysis, and iii) download a security report which contains all the identified issues.

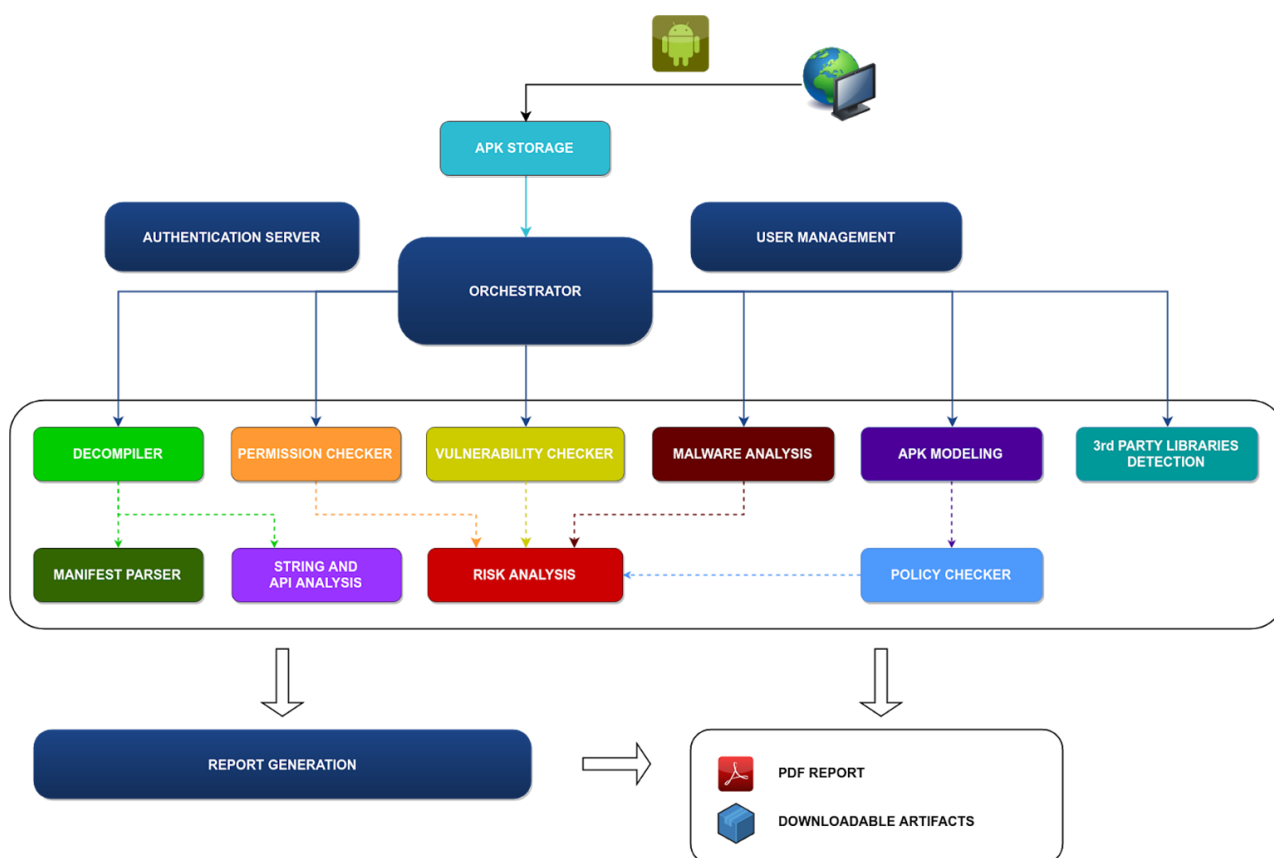


Figure 47: Approver SAST Architecture

### 6.30.2 Services provided

#### 6.30.2.1 Automated Security Risk Assessment of Mobile Applications

Approver provides a web interface to allow users to upload and automatically evaluate the security risks of mobile applications. Approver is a solution available both on-premise and SaaS.

### 6.30.3 Current Usage

#### 6.30.3.1 Past Projects

None.



### 6.30.3.2 Live Projects

Name (Funds)	Short description
SPARTA	Approver is used in Task 5.1 for the security evaluation of mobile applications in the eGov uses case and in Task 5.3 for the security risk assessment of mobile apps during the CI/CD use cases.

### 6.30.3.3 Other relevant actions taking place

Approver is available commercially and provided by company Talos, a spin-off of the University of Genova (Italy) and member of the CINI consortium.

### 6.30.4 Resources

#### 6.30.4.1 Scientific and Technological Team

<p><b>Alessandro Armando</b> Alessandro Armando is professor at the <a href="#">University of Genova</a>, where he received his Laurea degree in Electronic Engineering in 1988 and his Ph.D in Electronic and Computer Engineering in 1994. His appointments include a postdoctoral research position at the University of Edinburgh (1994-1995) and one as visiting researcher at INRIA-Lorraine in Nancy (1998-1999).</p> <p>He has been co-founder and director of the <a href="#">Artificial Intelligence Laboratory (AI-Lab)</a> at <a href="#">DIST</a> (2003-2011), of the <a href="#">Security and Trust Research Unit</a> at the <a href="#">Center for Information Technologies</a> of <a href="#">Bruno Kessler Foundation</a> in Trento (2010-2016), and of the Computer Security Laboratory (CSec) at <a href="#">DIBRIS</a>. He is co-founder of the <a href="#">Talos</a>, a spin-off of DIBRIS focused on Cybersecurity.</p> <p>He has been founder and director (Presidente del Comitato di Gestione) of the <a href="#">Master Universitario di II Livello on "Cyber Security and Data Protection"</a> of the University of Genova for the academic years 2014/2015 and 2016/2017.</p> <p>He has contributed to the discovery of <a href="#">a vulnerability on the SAML-based Single Sign-On for Google Apps</a>, <a href="#">an authentication flaw in emerging SSO protocols (namely SAML SSO v2.0 and OpenID)</a>, and <a href="#">a vulnerability that leads to a Denial of Service attack on all Android devices</a>.</p> <p>His focus is on developing cutting-edge automated reasoning techniques and on using them to build a new generation of push-button software verification and debugging tools supporting the development of complex, large-scale, distributed IT applications.</p>
<p><b>Alessio Merlo</b> received his Ph.D. in Computer Science from University of Genova (Italy) where he worked on performance and access control issues related to Grid Computing. He is currently assistant professor at the Informatics, Bioengineering, Robotics and System Engineering Department (DIBRIS) of the University of Genova and a member of the Computer Security Laboratory (CSEC Lab). His research interests are focused on performance and security issues related to Web and distributed systems (Grid, Cloud). He is currently working on security issues related to Android platform.</p>
<p><b>Gabriele Costa</b> is assistant professor at the SysMA Group. He received his Laurea degree in Computer Science in 2007 and his Ph.D in Computer Science in 2011. He was a member of the cybersecurity group of the Istituto di informatica e Telematica of the CNR. His appointments include a period as visiting researcher at ETH Zurich in 2016-2017.</p> <p>He has been co-founder of the Computer Security Laboratory (CSec) at DIBRIS. He is co-founder and CRO of the Talos, a spin-off of DIBRIS focused on Cybersecurity.</p> <p>His focus is on studying and applying formal methods for the automatic verification and testing of mobile and modular systems. These systems include those based on mobile software, web services, cloud and fog computing as well as the critical infrastructures and supply chains.</p>



**Luca Verderame** is a post-doc research fellow at the Computer Security Laboratory (CSEC Lab) of the University of Genoa (Italy), and the CEO and Co-founder of Talos, a cybersecurity startup and university spin-off.

In 2016, Luca obtained his Ph.D. in Electronic, Information, Robotics and Telecommunication Engineering at the University of Genoa. During his master thesis in 2012, Luca found a severe security vulnerability in the Android operating system and worked with the Android Security Team to develop a patch.

His current research interests mainly cover information security applied, in particular, to mobile and IoT environments, as witnessed by his research publications in the field.

Luca professional activities in the field of cybersecurity include collaborations with international companies and organizations, like Poste Italiane, Deloitte Risk Advisory and NATO Communications and Information Agency.

#### 6.30.4.2 Technical Equipment

##### Hardware Requirements

n.3 servers with the following characteristics each:

RAM: 16 GB

CPU: 8 cores with nested virtualization support

STORAGE: 50 GB

INTERNET CONNECTION

##### Software Requirements

Ubuntu 16 or later

Docker 18.09 or later (<https://docs.docker.com/install/>)

docker-compose (<https://docs.docker.com/compose/install/>)

VirtualBox 5.2.x ([https://www.virtualbox.org/wiki/Download\\_Old\\_Builds\\_5\\_2](https://www.virtualbox.org/wiki/Download_Old_Builds_5_2))

#### 6.30.5 Request of use

<b>Ticketing system</b>	<a href="mailto:support@talos-sec.com">support@talos-sec.com</a>
<b>Communication Channels</b>	Email
<b>Time management</b>	Labour days between 9:00-18:00
<b>Granularity</b>	Access to subsystems can be provided
<b>Type of access (public, free, comm)</b>	Commercial