H2020-DS-2015-1-Project 700581

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

D8.6 - Standardization interim report

General information

Dissemination level	Public
State	Final
Work package	WP8 Project dissemination and commercial strategy
Task	Task 8.1
Delivery date	31/10/2017
Version	1.0

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700581. This document is the property of the ATENA consortium and shall not be distributed or reproduced without the formal approval of the ATENA governing bodies.

Editors

Name	Organisation
M. Aubigny	ITRUST

Authors

Name	Organisation
M. Aubigny	ITRUST

Reviewers

Name	Organisation	Date
Paolo Pucci	FNM	30/10/2017

Executive Summary

According to the project Description of Action [3], one of the objectives of the project is to ensure the connection between the research and development performed during the project and "*the current and emerging standard development in the areas of CI protection and organisations' resilience, such as ISO 27001, ISO 27019, ISA-99, IEC 62443, ISO 22316*" and more generally the relevant standard linked to the main research fields of the project i.e. energy and water network, smart grid, cybersecurity (attack detection and analysis) incident management regarding the Essential Services, modelling and simulation, risk assessment, decision expert system, secured communication protocols. This task, part of the dissemination activity of the project, has the aim to support the consortium to define the tools specifications and to choose the most fitted technology to design the tool according not only to the future end-users' operational needs but also to the international, European, national regulations and standardization expectations.

The present document constitutes a first (and declaredly preliminary) report of the standardization monitoring for the ATENA project. The document identifies first the standard and the standardisation activities useful for the project; secondly proposes a simple management process to ensure that the identified standardization framework is considered during the project progress and that the project provides some input in the identified framework; thirdly gives some information about the work done during M1-M18 to contribute to open source framework and standardization.

Table of Contents

List of figures

List of table

1 Introduction

1.1 Motivation and context

According to the project Description of Action [3], one of the objectives of the project is to ensure the connection between the research and development performed during the project and "*the current and emerging standard development in the areas of CI protection and organisations' resilience, such as ISO 27001, ISO 27019, ISA-99, IEC 62443, ISO 22316*" and more generally the relevant standard linked to the main research fields of the project i.e. energy and water network, smart grid, cybersecurity (attack detection and analysis) incident management regarding the Essential services, modelling and simulation, risk assessment, decision expert system, secured communication protocols. This task, part of the dissemination activity of the project, has the aim to support the consortium to define the tools specifications and to choose the most fitted technology to design the tool according not only to the future end-users' operational needs but also to the international, European, national regulations and standardization expectations. The standardization framework study will also encompass the work performed to contribute to open-source community in the aim to enhance the security and the resilience of targeted services. In M18 and M36, in the dissemination activity framework, the consortium shall report the results of this monitoring and, per regular management process during the plenary meeting, set the corrective actions needed to improve the consortium involvement.

The present document constitutes a first (and declaredly preliminary) report of the standardization monitoring for the ATENA project.

1.2 Objectives and scope

The objectives of the document are:

- To identify the standard and the standardization activities useful for the project;
- To ensure that relevant standard has been considered into the design, development and deployment of the ATENA solution;
- To report the contribution of the consortium to standard and open-source community.

The present document limits its scope to results that are measured in the project period M1-M18.

1.3 Document Structure

The chapters of the document respectively deal with:

- Chapter 2 lists the identified standards and open-sources framework regarding the ATENA project and links this list with the relevant tasks of the project and the involved partners.
- Chapter 3 describes the contribution (if exists) of partners in the creation or improvement process of standards regarding the security of Essential services or relative open-source projects. It includes also a planning of potential contributions in identified standard working groups.

1.4 Glossary

During the writing of the glossary table done by WP2 partners, the consortium arrives to a quite long version of this table. Therefore, for sake of maintenance, manageability and completeness, the reader is invited to refer to the project-level separate glossary document (i.e., “D2.0: ATENA glossary” [1]) that we are also placing on ATENA web-site (www.atena-h20202.eu) for public use.

1.5 Acronyms

Acronym or symbol	Description
CD	Committee stage
CI	Critical Infrastructure
CMP	Congestion management procedures
DIS	Draft International Standard
DOTS	Distributed-Denial-of-Service Open Threat Signalling
DoA	Description of Action
DSS	Decision Support System
DTLS	Datagram Transport Layer Security
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSO-G	European Network of Transmission System Operators for Gas
FDIS	Final Draft International Standard
HOST	Homeland Open Security Technology
IACS	Industrial and Automation Control Systems
IADS	Intrusion and Anomaly Detection System
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Inline Intrusion Prevention
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IWA	International Water Association
MMS	Manufacturing Messaging Service
NSM	Network Security Monitoring
PROFINET	Process Field Net
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RTU	Remote Terminal Unit
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SIEM	Security information and event management
SIFT	SANS Investigative Forensic Toolkit
TEE	Trusted Execution Environment
VMS	Vulnerability Management System

2 Relevant monitored frameworks

This chapter is based on the deliverable D2.1 [2] which lists, as much as possible in an exhaustive manner, the relevant standards at both international and European level. In this panel, the consortium has identified which standards would be closely followed and monitored regarding the design, development and test activities of the project. Additionally, the present chapter identifies the open-source projects that are in line with the tools developed within the ATENA project. For each identified framework, the present chapter (1) maps the framework topics with one or more tasks and with the developed ATENA tools and (2) identifies which partner is involved in the relative topic.

2.1 Standards frameworks

The present chapter lists the standards already identified in deliverable D2.1.

2.1.1 ISO framework

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
ISO/IEC 31000	Risk management: general guidance	High	▪ T2.5, T3.5, T6.2 ▪ Risk Analysis Tool Risk models Risk prediction tool	ENEA, MULTITEL, ITRUST, UNIROMA3
ISO/IEC 27005	Risk management applied to information security	High		
ISO/IEC 27002	Good practices in Information Security	Medium	▪ All task ▪ All components	All
ISO/IEC 27019	Good Practices for managing information security for Energy utility industry	Medium		
ISO/IEC 27033	Secure communication	Medium		
ISO/IEC 15408	Evaluation criteria for IT security to ensure a reliable assurance level for IT components	High	▪ T3.4 ▪ Composer	FNM, CRAT
ISO/IEC15446	Protection profile and security target	High		
ISO/IEC 18045	Guidance to apply ISO 15408	High		
ISO/IEC 27035	Incident management	High	▪ T4.2, T5.3, T5.4, ▪ IACS, VMS, Risk Analysis tools	CRAT, ITRUST, UC, UL, UNIROMA3
ISO/IEC 27041	Incident investigative method	High		
ISO/IEC 27042	Guidelines for the analysis and interpretation of digital evidence	Medium	▪ T4.5 ▪ Forensic tool	UC, UL, ITRUST
ISO/IEC 27043	Incident investigation principles and processes	Medium		
ISO/IEC 27044	Guidelines for security information and event management (SIEM)	High	▪ T4.4, T4.5 ▪ SIEM	UC, UL, ITRUST
ISO/IEC 29182	Sensor Network Reference Architecture	Medium	▪ T4.3, T4.5, T5.5, T5.6, T6.2 ▪ IACS, Adaptors	UC, UL, ITRUST, UNIROMA3, CRAT, FNM
ISO/IEC 18033	Encryption algorithm	Low	▪ T3.4, T5.5 ▪ Composer, Protection Software	ITRUST, CRAT, UNIROMA3
ISO/IEC 29192	Lightweight encryption	Low		
ISO/IEC 29147	Vulnerability Disclosure	High	▪ T3.4, T3.5 ▪ VMS	CRAT, ITRUST
ISO/IEC 30111	Vulnerability handling processes	High	▪ T3.4, T3.5, T5.2 ▪ VMS, DSS	CRAT, ITRUST, UNIROMA3
ISO/IEC 30127	Penetration testing methodology	Medium	▪ T4.3, T4.4 ▪ Probes, IACS	ITRUST, UC, UL

ISO/IEC 30104	Physical security requirements	Medium	▪ T3.4 ▪ Composer	FNM, CRAT
ISO/IEC 18043	Selection, deployment and operation of IDS	High	▪ T4.3, T4.4 ▪ IACS	UC, ITRUST, UL
ISO/IEC 27039	Selection, deployment and operation of IDPS	High		
ISO/IEC 27044	Security information and event management	High		
ISO/IEC 30121	Governance of Digital Forensic Risk Framework	High	▪ T4.5 ▪ Forensic tool	UC, UL, ITRUST
ISO/IEC 29151	Code of practice for the protection of personally identifiable information	Medium	▪ T4.3; T6.2 ▪ Probes, Asset management system	ITRUST, FNM
ISO/IEC 29191	Requirements on relatively anonymous unlikable authentication	Medium		
ISO/IEC 29155-1	Information technology project performance benchmarking framework - Part 1: Concepts and definitions	Medium		
ISO/IEC 19770-1	IT asset management – Part 1 Requirements	Medium	▪ All	All

Table 1: ISO Framework

2.1.2 ISA framework

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
ISA/IEC 62443-2-1	Requirements for an ISMS in the industrial automation and control systems environment and guidance to apply the requirements.	High	▪ T3.3, T3.4, T4.3, T4.4, T4.5 ▪ IACS, Simulation model	UC, UL, ITRUST, ENEA, MULTITEL, UNIROMA3
ISA/IEC 62443-2-2	Requirements to securely operate IACS	High		
ISA/IEC 62443-3-3	Detailed technical control system requirements especially the control system capability security levels	High		

Table 2: ISA Framework

2.1.3 IEC framework

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
IEC 60870-5	SCADA system to RTU data communications	High	▪ T3.3, T3.4, T4.3, T4.4, T4.5 ▪ IACS, Simulation model	UC, UL, ITRUST, ENEA, MULTITEL, UNIROMA3
IEC 60870-6	Communication between controls centres and also for communication between SCADA systems and other engineering systems within controls centres	High		
IEC 62351-3	Security for profiles including TCP/IP.	High		
IEC 62351-4	Security for profiles including MMS (Manufacturing Messaging Service) and similar payloads	High		
IEC 62351-5	Security for IEC 60870-5/6	High		
IEC 62351-14	Cyber Security event Logging	High		

Table 3: IEC Framework

2.1.4 IETF framework

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
OTrP	protocol to install, update, and delete applications and to manage security configuration in a Trusted Execution Environment (TEE)	High	▪ T3.3, T3.4, T4.3, T4.4, T4.5, T5.3, T5.4 ▪ IACS, Composer, Orchestrator	CRAT, UNIROMA3, UL, UC, ITRUST, FNM
DTLS	Datagram Transport Layer Security (DTLS) allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery	High		
TLS	Security over internet	High		
DOTS	Distributed-Denial-of-Service Open Threat Signalling (DOTS) Architecture	High		

Table 4: IETF Framework

2.1.5 ENTSO-E and ENTSO-G framework

2.1.5.1 ENTSO-E document for electricity sector

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
FG-2012-E-009	Framework Guidelines on Electricity Balancing	Low	Indirect (information). The technical document provided by ENTSOE drives the overall operations of electrical grid at European level and could induce useless complexity for the project. The targeted audience of these guidelines are the operators.	CREOS LU
FG-2011-E-003	Framework Guidelines on Electricity System Operation	Low		
FG-2011-E-002	Framework Guidelines on Capacity Allocation and Congestion Management for Electricity	Low		
FG-2011-E-001	Framework Guidelines On Electricity Grid Connections	Low		
NA	Emergency and Restoration Code	Low		
NA	System operation	Low		
NA	Network Code on Operational Security	Low		
NA	Manual of Procedure for the ENTSO-E Central Information Transparency platform	Low		

Table 5: ENTSO-E document for electricity sector

2.1.5.2 ENTSO-G document for gas sector

Ref.	Description/Title	Relevance	Impact on ATENA tasks and developed modules	Involved partners
NA	Security of Supply regulation	Low	Indirect (information). The technical document provided by ENTSOG drives the overall operations of gas distribution at European level. The targeted audience these guidelines are the operators.	CREOS LU
NA	EU-wide assessment of potential disruption scenarios	Low		
Guidelines on CMP	Congestion management procedures (CMP) are applied at interconnection points to facilitate the efficient use and maximisation of capacities in the networks.	Low		

NC on Interoperability and Data Exchange Rules	Operational, technical, communication and business rules are a prerequisite for a proper interoperability of transmission systems	Low		

Table 6: ENTSO-E document for gas sector

2.1.6 Water Sector

Ref.	Description/Title	Relevance for ATENA	Impact on ATENA tasks and developed modules	Involved partners
Lisbon Charter	The Lisbon Charter is an international framework of good practice for public policy and regulation in drinking water supply, sanitation and wastewater management services.	Low	This information is either high level information with no direct impact on the project, or addressed only to the operators. The impact should be only indirect to avoid a too large gap between these requirements and the ATENA monitoring tools' aim.	SWDE
AWWA G430-14	Security Practices for Operation and Management: minimum requirements for a protective security program for a water, or wastewater, or reuse utility.	Low		
AWWA J100-10 (R13)	Risk and Resilience Management of Water and Wastewater Systems (RAMCAP): standard encompassing an all-hazards risk and resilience management process for use specifically by water and wastewater utilities.	Low		
AWWA M19	Emergency Planning for Water Utilities, Fourth Edition: presents techniques for developing contingency plans for a variety of emergencies from natural disasters to human-caused.	Low		
Dir. 2001/7/EC	The Bathing Waters Directive	Medium	These directives will not directly impact the project but as they are mandatory requirements for operational activities of the operator, the ATENA tools (model, detection, risk assessment, simulation) should consider the requirement to prioritise the functionalities developed.	SWDE
Dir. 91/271/EEC (21/05/1991)	The Urban Waste Water Treatment Directive concerning discharges of municipal and some industrial waste water;	Low		
Dir. 98/83/EC (3/11/1988)	The Drinking Water Directive on the quality of water intended for human consumption	Low		
Dir. 200/60/EC (23/10/2000)	The Water Framework Directive concerning water resources management. (Integrated river basin management)	Medium		

Table 7: Water sector

2.2 Open-source projects

As there are many open-source projects, the following table is not able to describe the exhaustive overview of the open-sources, but identifies the main tools and documents under open-source licence, which should be considered during the design, the development and the testing of the ATENA tools.

Ref.	Relevance	Relevance for ATENA	Considered in module of ATENA tools	Involved partners
Generic Tools				
Kali Linux	Penetration testing and forensic platform	Medium	IACS	UC, UL, ITRUST
BackBox Linux	Network and systems analysis toolkit.	Medium	IACS	UC, UL, ITRUST
Penetration tools (including network analyser)				
Metasploit Framework + Armitage GUI	Modular and extensible tool suite for cybersecurity penetration testing	Medium	IACS	UC, UL, ITRUST
Wireshark	Network traffic analyser and forensic	High	IACS, validation	UC, UL, ITRUST
nmap	Network discovery and security auditing	High	IACS	UC, UL, ITRUST
Vega	web security scanner and web security testing platform	Low	IACS	UC, UL, ITRUST
inSSIder	Wi-Fi network discovery tool	Low	SmartHome IDS	ITRUST
Floodlight	Network controller	High	Composer	CRAT
NodeRed	Flow controller	High	Composer IACS	CRAT, UC
Forensic tools				
SANS Investigative Forensic Toolkit (SIFT) Workstation	Forensic software bundle	Medium	IACS/SIEM	UC, UL, ITRUST
Maltego	Data mining tools used in forensic to analyse large database	Medium	IACS/SIEM	UC, UL, ITRUST
IDS/IDPS and protection systems				
Suricata	Real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing.	High	Multi-antivirus probes	ITRUST
Kismet	802.11 wireless network detector, sniffer, and intrusion detection system	Low	IACS	UC, UL, ITRUST
Tripwire ®	A security and data integrity tool useful for monitoring and alerting on specific file change(s) on a range of systems	Low	IACS	UC, UL, ITRUST
Munin	Monitor the performance of your computers, networks, SANs, applications, weather measurements	Low	IACS	UC, UL, ITRUST
OSSEC	IPS	High	IACS	UC
OS Hardening				
AppArmor	Proactive protection of the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behaviour	Medium	Composer	CRAT
Methodology or security guidance				
NSA Security configuration	Open source document to implement security good practices	Medium	ATENA Development	ALL
CIS Security Benchmarks	Set of open sources documents to set up securely systems and applications	Medium	ATENA Development	ALL
ICS tools				
AEGIS Fuzzer	Commercial fuzzing framework with open source version. The tools can identify the robustness and security issues in communication (support several protocols especially Modbus)	Medium	IACS, Composer	UC, CRAT
IEC server	Simulation software of telecontrol message based on IEC 60870-5 protocol	Medium	Validation	UC, UL, ITRUST, IEC,

				UNIROMA3
QTester104	Software implementing the IEC 60870-5-104 protocol and allowing to poll and view data from substation system (RTU/Concentrator) and to send command.	Medium	Validation	UC, UL, ITRUST, IEC, UNIROMA3
IEDScout	Simulation platform of IEC 61850 protocol.	Medium	Validation	UC, UL, ITRUST, IEC, UNIROMA3
ModbusPAL	Simulation tools of Modbus protocol	Medium	Validation	UC, UL, ITRUST, IEC, UNIROMA3
SMOD	Modbus Penetration Testing framework.	Medium	Validation	UC, UL, ITRUST, IEC, UNIROMA3
ProFuzz	Simple PROFINET fuzzer engine	Medium	Validation	UC, UL, ITRUST, IEC, UNIROMA3
S7comm	Open source Wireshark plugin for Siemens S7	Medium	IACS, Validation	UC, UL, ITRUST, IEC, UNIROMA3
Killerbee	IEEE 802.15.4 Zigbee Security Research toolkit	Medium	SmartHome IDS	ITRUST
AFL	Security oriented fuzzer	Medium	IACS	UC, UL, ITRUST, IEC, UNIROMA3

Table 8: Open-source projects

Additional information on open security tools is available in the US Department Homeland project titled HOST (Homeland Open Security Technology) and the last version of this list is included in the Appendix A of this document.

3 Standard follow-up

3.1 Management process regarding the standardisation

The following process shows how the consortium manages the compliance of the ATENA results with the identified standards. This management process is also used to identify the several improvements produced by the ATENA results and that could be proposed to Standard Organisations through the intercession of a Consortium contact point.

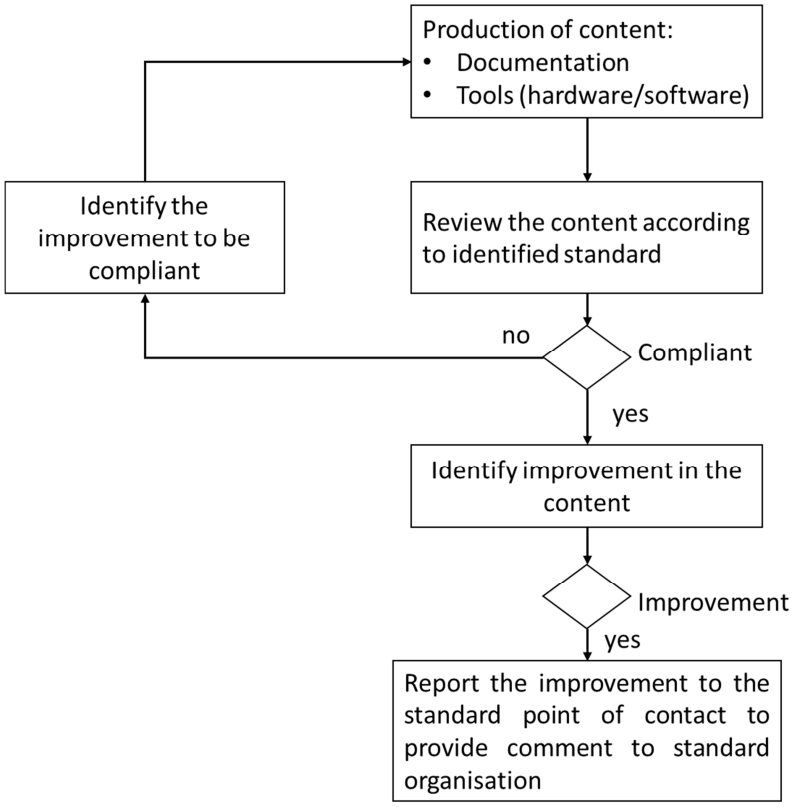

Figure 1: Management process of standard compliance and standard improvement

3.2 List of standard working documents

Ref.	Title	Status	Follow by	As
ISO/IEC 15408-1	Evaluation criteria for IT security-Part 1: Introduction and general model	Vote on 1st Working Draft issued	ITRUST	ISO expert for Luxembourg
ISO/IEC 15408-2	Evaluation criteria for IT security-Part 2: Security Functional Component			
ISO/IEC 15408-3	Evaluation criteria for IT security-Part 3: security assurance component			
ISO/IEC 15408-4	Evaluation criteria for IT security-Part 4: Framework for the specification of evaluation methods and activities			
ISO/IEC 15408-5	Evaluation criteria for IT security-Part 5: Pre-defined packages of security requirements			
ISO/IEC 21878	Security guidelines for design and	Comment	ITRUST	ISO expert for

	implementation of virtualized servers	period ended. Vote on Committee draft issued		Luxembourg
ISO/IEC 29147	Vulnerability disclosure	DIS ballot	ITRUST	ISO expert for Luxembourg
ISO/IEC 30111	Vulnerability handling processes	CD Ballot	ITRUST	ISO expert for Luxembourg
ISA/IEC 62443-2-3	Description of IACS patch management requirements.	Under development	To be identify in the next project's period..	ISA expert
ISA/IEC 62443-3-2	Security Levels for Zones and Conduits	Under development		
ISA/IEC 62443-4-1	Product Development Requirements	Under development		
ISA/IEC 62443-4-2	Technical Security Requirements for IACS Components	Under development		
ENTSOE documentation	European network of transmission system operators for electricity		CREOS LU	Energy Provider
ENTSOG documentation	European network of transmission system operators for gas		CREOS LU	Energy Provider
IWA doc	International Water Association		SWDE	Water provider

Table 9: List of standard working documents

3.3 Contribution from partners

3.3.1.1 Standard contribution

During the first period of the project, ITRUST has contributed to the standardisation work as expert member of the ILNAS standardisation group for the ISO/JTC1/SC27 working group (Information security) and TC262 working group (Risk management). More specifically ITRUST has participated to the vote of the working document and has provided comments via the Luxembourg representative (part of ILNAS) for the following documents:

ID	Document	Title	Working group	Date of comment
2	ISO 27019 1st CD	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	ISO/JTC1/SC27	05/2016
4	ISO 27009	Sector-specific application of ISO/IEC 27001 -- Requirements Comment on the defected report	ISO/JTC1/SC27	10/2016
1	CD3-31010	Risk management -- Risk assessment techniques	TC 262	04/2017
3	ISO 270189-FDIS	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	ISO/JTC1/SC27	07/2017
5	ISO 27003-DIS	Information security management systems -- Guidance	ISO/JTC1/SC27	09/2017

Table 10: Standard contribution

3.3.1.2 Open source contribution

As of now, the open source contributions of partners are mainly focused on two open source projects:

1. The first one is the Floodlight Open SDN [4], which support the development of an "*enterprise-class, Apache-licensed, Java-based OpenFlow Controller*". Figure 2 shows how a Floodlight application is actually deployed. This tool will be useful to deploy the Controller module used to manage devices security policies and to secure the targeted network. The main functionalities of the tool are the following:
   a. Control of virtual or physical broad-range switches;
   b. It is based on OpenFlow and supports both OpenFlow and no-OpenFlow networks;
   c. Multithreaded from the ground up;
   d. Support for OpenStack [5] cloud orchestration platform.

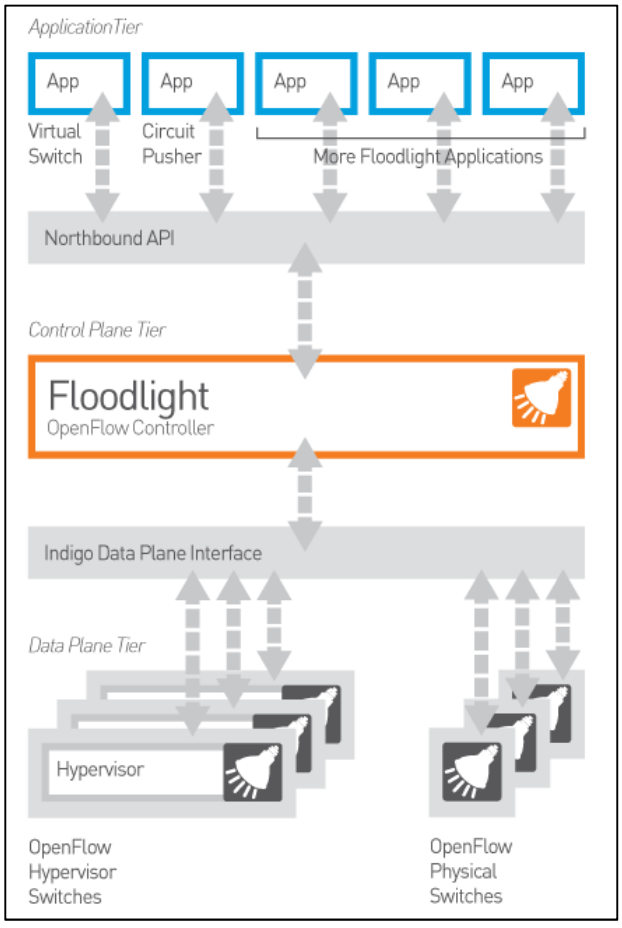

Figure 2: Floodlight Project

2. The second one is the open source project Node-RED [6]. This project, as described on its website, provides "*a programming tool for wiring together hardware devices, APIs and online services*". In the ATENA project, it is used to support the Orchestrator module functionalities.

4 References

[1] ATENA Consortium, “D2.0: ATENA Glossary,” 2016. Online: https://www.atena-h2020.eu/wp-content/uploads/ATENA/Publishable%20material/D2.0/Version%201.1%20revised%20201706300/D2.0%20ATENA%20Glossary%20v1.1.pdf

[2] ATENA Consortium, “D2.1: State of the Art,” 2016, publicly available in https://www.atena-h2020.eu

[3] ATENA Consortium, “Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures (ATENA) – Grant Agreement no. 700581,” *Horiz. 2020 Call H2020-DS-2015-1 Top. DS-03-2015 Type action IA*, 2016.

[4] Floodlight project website - http://www.projectfloodlight.org/floodlight/

[5] OpenStack website - https://www.openstack.org/

[6] Node-RED website - https://nodered.org/

Appendix A: Open security tools

Here we report the HOST list of software:

CATEGORY	APPLICATION(S)
Administration	CFengine, Expect, Process Hacker, Webmin
Anti-spyware	Nixory
Antivirus	ClamAV, ClamWin, Moon Secure Antivirus, Simple Machine Protect
Application Languages & Development Environments	BASH, Clang, Coccinelle, Cygwin, DDD, Eclipse, Emacs, GCC, GDB, Gedit, Java, phpHtmlLib, Python, Qlue, Ruby, Vi, VIM
Browser Add On	Password Maker, Web of Trust
Business Continuity	AMANDA, Areca Backup, Partimage
Cloud Computing	ABIQUO, Cloudstack, Eucalyptus, Juju, Nimbula, Open Nebula, OpenStack
Configuration Management	CFengine, Puppet, Salt
Content Management	Chef, Drupal, Joomla, Juju, Wordpress
Data Backup & Archival	Bacula, Open Nebula, PeaZip, Unison
Database	MariaDB, MySQL, NetDB, Percona, PostgreSQL, SQLite
Data Removal Directory	BleachBit, Darik's Boot and Nuke, Eraser, Wipe
Disk Email	OpenLDAP
Email Protection & Anti- Spam	BleachBit, DBAN, Gparted, Midnight Commander, Parted, Partimage
Email Services	amavisd-new, ASSP, JAMES Mail, Mozilla Thunderbird, Postfix, Spam Assassin, SquirrelMail, VPOP Email, Zarafa, Zimbra
Encryption	amavisd-new, ASSP, Postgrey, Spam Assassin JAMES Mail, Postfix, SquirrelMail, Zimbra
Enterprise Applications	AxCrypt, Crypt, Cryptacular, GNU Privacy Guard, John the Ripper, Mac GNU Privacy Guard, NeoCrypt, Network Security Services (NSS), OpenSSL, TrueCrypt
File Transfer	Open Atrium, Open Source Corporate Management Information Systems (OSCMIS), WorldVistA
Filtering	CyberDuck, FileZilla, Fugu, Samba, vsftpd, WinSCP DansGuardian, IP Tables, Java EE PDF uXSS Filter, Web Scarab
Firewall	Devil Linux, Endian Firewall Community, ferm, Firestarter, Firewall Builder, IP Cop, m0n0wall, ModSecurity, NetCop UTM, Open WAF, pfSense, Sentry Firewall, Shorewall, Smoothwall, Turtle Firewall, Untangle, Vuurmuur, Vyatta, Zentyal
Forensics	BackTrack, LibHTP, Maltego, Mobius Forensics Toolkit, mod_sslhaf, ODESSA, tcpdump, tcpindex, The Sleuth Kit/Autopsy Browser, WinDump, WinPcap, Wireshark
Geographic Information Systems (GIS)	Falcon View, Open Streetmap, Opticks, PGGIS
Host Based IPS (HIPS)	AFICK (Another File Integrity Checker), Open Source Tripwire, OSSEC
ID Authentication Methods	WiKID
Information Technology Infrastructure	Dradis, OpenCPI
Intrusion Detection & Monitoring	ackack, Kismet, Munin, Open Source Tripwire, OpenVAS, Process Hacker, Suricata, Thicknet, Zabbix
Intrusion Detection & Prevention Systems (IDS/IPS)	Fail2Ban, IronBee, OSSEC, QuIDScor, Snort, Suricata
Monitoring Systems	Cacti, ICINGA, Nagios, NetDB, OpenNMS, PandoraFMS, Zabbix, Zenoss
Network	ackack, AFTR, BIND, BIND 10, Bird, BSD Router, ISC DHCP, Munin, Netcat, NetDB, Nmap, Quagga, Samba, Squid
Network Communications Protection	OpenSSH, OpenSSL, Squid
Operating System (OS)	Android, Arch Linux, BackTrack, CentOS, ClearOS, Cygwin, Debian Linux, Devil Linux, Endian Firewall Community, Fedora, FreeBSD, Gentoo, IP Cop, Knoppix, Kubuntu, Lightweight Portable Security (DoD Linux Distro), m0n0wall, Mandriva Linux, NetBSD, NetCop UTM, OpenBSD, openSUSE, Openwall GNU/Linux (OWL), Red Hat Enterprise Linux, Samuri WTF, Sentry Firewall, Slackware, Smoothwall, SUSE Enterprise, Ubuntu, Untangle, Zentyal
OS Hardening	AppArmor, Bastille Unix, Gentoo Hardened Profile, SE Linux

Password Management	KeePass Password Safe, KeePassX, Passkool, Password Maker, Password Safe
Penetration Testing & Vulnerability Assessment	Airoscript-NG, Angry IP Scanner, Auto Scan, BackTrack, batchyDNS, Cacti, Deblaze, Deface, Graudit, inSSIDer, JBoss Autopwn Script, JBroFuzz, JSP Tester, KisMAC, Kismet, Lynis, Metasploit, Nmap, Ophcrack, Peach Fuzzing Platform, QuIDScor, SQL Map, tcpindex, Vega, W3AF, Wireshark
Problem Management	BugZilla, Request Tracker
Program Analysis	AntiSamy, Apparat, Avalanche, BLAST: Berkeley Lazy Abstraction Software Verification Tool, Blind Elephant, Checkstyle, ClamWin, CppCheck, CQUAL, CSRF Guard, Dmalloc, DynInst, FindBugs, Flawfinder, Frama-C, Gendarme, JavaSnoop, Jchord, JSP Tester, LibHTP, Moon Secure Antivirus, Moose, Orizon, Pixy, PMD Copy/Paste Detector, ROSE, RTL-Check, Scrubbr, Simple Machine Protect, Smatch, Sonar, Soot, Sparse, Splint, Squale, Stanse, StyleCop, Valgrind, Yasca
Remote Access Methods Clients	NoMachine, OpenSSH, OpenSSL, PuTTY, PuTTY CAC, TightVNC
Revision Control	CVS, Fossil, git, Mercurial, Subversion
Security Planning Tools	Metasploit, spt (Simple Phishing Toolkit), WebGoat
Storage Tools	DRDB, OCFS 2, Openfiler, Orange FS, Sheepdog, Swift
Virtualization	Cygwin, KeepAlived, KVM, OpenStack Compute, OVM, Packetyzer, VirtualBox, Xen
Visualization	ParaView
VPN	Cacti, OpenVPN
Vulnerability Patch Management	Lynis, Nikto2, OpenVAS, Rogue Scanner
Web Accessibility	Chromium, Konqueror, Mozilla Firefox
Web Server Software	Apache, Apache Tomcat, Drupal, Enterprise Security API, Jboss Autopwn Script, JBoss Enterprise Application Platform, Lucene, mod_sslhaf, NGINX, Nikto2, Open Atrium, Plone, WebFSD, Zimbra, Zope
Web Services	AW Stats, Classic ASP Security Image Generator (CAPTCHA), Django, Joomla, MediaWiki, PIWIK, Plone