




PANOPTIS

Development of a Decision Support System for increasing the Resilience of Road Infrastructure based on combined use of terrestrial and airborne sensors and advanced modelling tools- Grant Agreement Number: 769129

D 8.8: Report on Standards and Liaison Activities with relevant Organisations-V1

Work package	WP8: General Dissemination, Creation of PANOPTIS Identity and Standardization Activities
Activity	Task 8.6
Deliverable	D8.2 (D8.7.1) Reports on Standards and Liaison activities with relevant organisations – V1
Authors	ADS
Status	Final (F)
Version	1.0
Dissemination Level	Public (PU)
Document date	31/10/2020
Delivery due date	31/03/2020
Delivery date	07/12/2020
Delivery date after EC revision	
Internal Reviewers	D.Vamvatsikos
External Reviewers	
	This project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under grant agreement no769129.

Document Control Sheet

Version history table			
Version	Date	Modification reason	Modifier
0.1	30/10/2020	<i>First version of the deliverable</i>	ADS
1.0	07/12/2020	<i>Submitted after reviewers comments</i>	ADS

Legal Disclaimer

This document reflects only the views of the author(s). Neither the Innovation and Networks Executive Agency (INEA) nor the European Commission is in any way responsible for any use that may be made of the information it contains. 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 above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. © 2018 by PANOPTIS Consortium.

Contents

EXECUTIVE SUMMARY	4
1 STANDARDS	5
1.1 STANDARDS FOR MULTI-HAZARDS MODELLING, VULNERABILITY AND IMPACT ASSESSMENT OF THE RI	5
1.2 STANDARDS FOR SYSTEM DESIGN	6
1.2.1 <i>Middleware (Cloud Infrastructure)</i>	6
1.3 STANDARDS FOR SENSORS	8
1.3.1 <i>In situ sensors</i>	8
1.3.2 <i>UAVs</i>	8
1.3.3 <i>Satellites</i>	8
1.4 STANDARDS ON DISPLAY – GIS LAYERS	8
2 LIAISON ACTIVITIES WITH RELEVANT ORGANISATIONS	8

Executive Summary

The first part of this document presents the first findings and recommendations on the standards that could/should be used for the development of the system. These standards can be procedural/operational (description of Road Infrastructures, of events, of defects, of vulnerabilities, standardized cross-border events), system standards (structure of information systems. Design standards) or technical standards (sensor interfaces, development of modules, HMI rules).

The second part of the document presents the organisations envisaged to push the pre-standards, the norms and recommendations.

1 Standards

1.1 Standards for Multi-Hazards Modelling, Vulnerability and Impact Assessment of the RI

Due to the innovative nature of multi-hazard fragility & vulnerability assessment, which mainly confines it to the academic realm, there is no definitive standard to fully guide the process of fragility assessment. Still, in various stages of our work in WP4, we have employed a number of standards and guidelines WP4 that deal with single hazards.

Eurocodes: The Eurocodes are the ten European standards (EN; harmonized technical rules) specifying how structural design should be conducted within the European Union (EU).

1. EN1990 (2005). *Eurocode 0: Basis of structural design*. Comité Européen de Normalisation, Brussels, Belgium.
2. EN1991 (2002). *Eurocode 1: Actions on structures*. Comité Européen de Normalisation, Brussels, Belgium.
3. EN1992 (2005). *Eurocode 2: Design of concrete structures*. Comité Européen de Normalisation, Brussels, Belgium.
4. EN1993 (2005). *Eurocode 3: Design of steel structures*. Comité Européen de Normalisation, Brussels, Belgium.
5. EN 1997 (2004). *Eurocode 7: Geotechnical design*. Comité Européen de Normalisation, Brussels, Belgium.
6. EN 1998 (2004). *Eurocode 8: Design of structures for earthquake resistance*. Comité Européen de Normalisation, Brussels, Belgium.

Standards on materials:

1. EN 206-1: Concrete – Part 1: Specification, performance, production and conformity,
2. EN 10027: Designation systems for steel.
3. Concrete, hardened: Accelerated chloride penetration (NT BUILD 443),
4. Concrete, mortar and cement-based repair materials: Chloride migration coefficient from non-steady-state migration experiments (NT BUILD 492),
5. XP P18-462, Test on hardened concrete - Accelerated chloride ion migration test in non-stationary regime - Determination of the apparent diffusion coefficient of chloride ions (Essai sur béton durci - Essai accéléré de migration des ions chlorure en régime non-stationnaire - Détermination du coefficient de diffusion apparent des ions chlorure).

Guidelines for fragility assessment:

1. FEMA P-58 (2018): *Seismic Performance Assessment of Buildings (2nd Edition)*, Federal Emergency Management Agency, Washington, D.C.
2. D'Ayala D., Meslem A., Vamvatsikos D., Porter K., Rossetto T. (2015). *Guidelines for Analytical Vulnerability Assessment of Low/Mid-Rise Buildings*. GEM Technical Report 2014-12. Global Earthquake Model Foundation, Pavia, Italy. DOI 10.13117/GEM.VULN-MOD.TR2014.12
3. Porter K., Farokhnia K., Vamvatsikos D. and Cho I.H. (2014). *Guidelines for component-based analytical vulnerability assessment of buildings and nonstructural elements*. GEM Technical

Report 2014-13. Global Earthquake Model Foundation, Pavia, Italy. DOI: 10.13117/GEM.VULN-MOD.TR2014.13.

For encoding multi-hazard vulnerability modules in JSON / GeoJSON format we employed the following standards:

1. Butler, H., Daly, M., Doyle, A., Gillies, S., Hagen, S., & Schaub, T. (2018). RFC 7946: The GeoJSON Format. Internet Engineering Task Force.
2. Bray, T. (2017). RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format. Internet Engineering Task Force.

Business continuity:

1. ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements,
2. ISO 22316:2017, Security and resilience — Organizational resilience — Principles and attributes.

1.2 Standards for system design

1.2.1 Middleware (Cloud Infrastructure)

Standardisation is a strong enabler for the interoperability and portability, which are important to avoiding vendor lock-in, whether at the technical, service delivery or business level, providing broader choice and greater clarity. In this direction in PANOPTIS context, open standards can protect the users and are one of the most important means used to bring new cloud technologies to the market.

Category	Standard	Description
Portability	ISO/IEC 17203:2011 Information technology — Open Virtualization Format (OVF) specification	It specifies an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines
	OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC	It enhances the portability of cloud applications and services providing a machine-readable language to describe the relationships between components, requirements, and capabilities.
Interoperability	Open Cloud Computing Interface (OCCI) specification from Open Grid Forum	OCCI is a Protocol and API with a strong focus on integration, portability and interoperability.
	Cloud Infrastructure Management Interface (CIMI) from the Distributed Management Task Force (DMTF)	It standardises interactions between cloud environments to achieve interoperable cloud infrastructure management between service providers and their consumers and developers.
	Cloud Data Management Interface (CDMI) from The Storage Networking Industry	It defines the functional interface that applications will use to create, retrieve, update and delete data elements from the

PANOPTIS

	Association (SNIA)	Cloud.
	Cloud Application Management Protocol (CAMP) by the OASIS	It is a PaaS management interface intended to provide a common basis for developing multi-cloud management tools as well as offering cloud providers and consumers a REST-based approach to application management.
	ISO/IEC 17788, Cloud computing – Overview and vocabulary	It provides definitions of common cloud computing terms, including those for cloud service categories such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
	ISO/IEC 17789, Cloud computing – Reference architecture	It contains diagrams and descriptions of how the various aspects of cloud computing relate to one another.
Security	ISO / IEC 27018 Code of practice for data protection controls for public cloud computing services - ISO	It establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
	NIST 800-53 Rev.4 Security Controls - NIST	It provides a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls.
	NIST Security Reference Architecture	It lays out a risk-based approach of establishing responsibilities for implementing necessary security controls throughout the cloud life cycle.s
	Cloud Controls Matrix (CCM) - Cloud Security Alliance	It provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.
	Open Certification Framework (OCF) - Cloud Security Alliance	It allows for the global, accredited, trusted certification of cloud providers.
	Cloud Trust Protocol (CTP) - Cloud Security Alliance	It provides the mechanism by which cloud service consumers (also known as “cloud users” or “cloud service owners”) ask for and receive information about the elements of transparency as applied to cloud service providers.
	CloudAudit - Cloud Security Alliance	It provides a common interface and namespace that allows enterprises who are interested in streamlining their audit processes (cloud or otherwise) and cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology.

	Privacy Level Agreement - Cloud Security Alliance	It defines baselines for compliance with data protection legislation and best practices by defining a standard format for Privacy Level Agreements (PLAs) and standards.
	EuroCloud Star Audit (ESCA) – EuroCloud	It provides an accountable quality rating of Cloud Services.
	Data Security Framework - Open Data Center Alliance	It defines requirements associated with increasing data security in the cloud and documents the necessary data security controls.

1.3 Standards for sensors

1.3.1 In situ sensors

The weather stations installed in the project are bought of the shelf and respect the same interface standards than the legacy weather stations already installed by ACCIONA and Egnatia Odos.

The cameras are those already installed in the respective CCTVs.

All the other in situ sensors (accelerometers essentially) are also off-the-shelf with standards interfaces (digital interface SPI 32).

1.3.2 UAVs

The most important standard used in the project is the NATO standard STANAG 4586. It defines the architecture principles and the interfaces that need to be respected to integrate The Unmanned Air System (UAS) in a larger surveillance system.

1.3.3 Satellites

The first developments of PANOPTIS for road monitoring are based on the exploitation of Pleiades constellation tools. The first objective is to use these satellites images as the map underlying the situation picture.

1.4 Standards on display – GIS layers

There is no single standard to display the situation picture or the COP. The GIS are vendor dependant and enable creation of specific symbol systems for each customer. The objective of PANOPTIS is to propose a first standardisation of these symbols at European level by gathering a minimal interoperability set.

2 Liaison activities with relevant organisations

As described in the DOA, ADS have access to ETSI (European Telecommunications Standardization Institute) in different standards as TETRA for PMR, EMTEL for Emergency Telecommunications, ERM EMC and Radio spectrum matters, RRS for reconfigurable Radio Systems. ADS is also involved in the CEN (European Norms Center) in Brussels in different working groups as BT161 Protection and Security of the citizen, BT125 Standardization for Defense procurement. Also outside EU, ADS is involved as member or chair in ISO TC233 for emergency management, ITU TDR Telecommunications Disaster Relief and US standardization as TIA Telecommunication Industry Association APCO and IEEE 802.16 group.