# CEN

# WORKSHOP

# AGREEMENT

# CWA 17356

December 2018

**ICS** 13.310; 35.240.01

English version

# Interoperability of security systems for the surveillance of widezones

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

# Contents

Page

## European foreword

CWA 17356:2018 was developed in accordance with CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – The way to rapid agreement" and with the relevant provisions of CEN/CENELEC internal Regulations – Part 2. It was agreed in a Workshop on 2018-11-07 by representatives of interested parties, approved and supported by CEN following a public call for participation made on 2017-12-11. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The CEN Workshop offers a platform whereby stakeholders can discuss and resolve standardization issues by consensus and validation in an open process.

The main activity of a CEN Workshop is the development and publication of a CEN Workshop Agreement (CWA). The CWA is a voluntary standard applicable internationally and does not have the force of regulation. A CWA can be an initial step in the development of a European standard.

The development of CWA 17356 *Interoperability of security systems for the surveillance of widezones* has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no.607292 ZONeSEC.

The secretariat was held by the British National Standards Body, BSI. A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. These are listed below:

- AQUASERV SA
- Attikes Diadromes SA
- Carlos III University of Madrid (UC3M)
- DESFA SA
- European Commission Directorate-General for Migration and Home Affairs Fundacion Tekniker
- Gap Analysis SA
- Silixa
- Telesto Technologies
- The Centre for Security Studies (KEMEA)
- The Extended Virtual Fencing Thematic Group, EU Reference Network for Critical Infrastructure Protection (ERNCIP) programme
- The Institute of Communication and Computer Systems (ICCS)

Along with the following individuals:

- Dr Dimitris Drakoulis, Chair

Those CEN-CENELEC Technical committees supporting technical consensus are as follows:

- CEN/TC 391 Societal and citizen security
- CLC/TC 79 Alarm systems

The formal process followed by the Workshop in the development of the CEN Workshop Agreement has been endorsed by the National Members of CEN, but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of the CEN Workshop Agreement or possible conflict with standards or legislation. This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its members.

The final review/endorsement round for this CWA was started in October 2018 and was successfully closed in November 2018. The final text of this CWA was submitted to CEN for publication in November 2018.

This CEN Workshop Agreement is publically available as a reference document from the National Members of the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

It is possible that some elements of CWA 17356 may be subject to patent rights. The CEN-CENELEC policy on patent rights is set out in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patents (and other statutory intellectual property rights based on inventions)". CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

# Introduction

Critical infrastructure (CI), such as highways, energy lines or pipelines, might extend over large areas covering wide geographic zones (widezones). There is clearly a need to provide proper security for such infrastructure against illicit actions and against incidents that might escalate to crises. Damages, intentional or not, to critical points (functions, equipment and controls) can compromise the integrity of the involved CI installations and the security of energy and resource supply, with adverse socio-economic effects to citizens, customers and the environment. Developing 24/7 surveillance systems for the security of widezones is of major strategic relevance to European economies, industries, authorities and citizens.

Systems involved in the surveillance of large areas are highly complex, employing different types of technology and equipment, and frequently coming from different manufacturers. The combined use of a number of surveillance systems is a challenging task due to the differences in the way that data and services are structured, stored, used and communicated. To work effectively, the systems have to be efficient as well as robust and resilient, while also providing sufficient accuracy to detect illicit activity patterns.

An opportunity thus exists for the development of guidelines to allow diverse systems used in the surveillance of widezones and large area security to interoperate with each other, as well as with legacy systems, providing a best-of-breed approach to the aforementioned challenges.

This document constitutes a CEN Workshop Agreement (CWA) that represents a consensus among the participants of the Workshop and provides a proactive approach towards identifying a guide on the interoperability of surveillance systems used for the protection of widezone CI). Particularly, it provides specific information on technical content where this is deemed to be necessary for the application of the CWA (e.g. type of information exchange, architecture guidelines, etc.) and it contains guidance on the approach taken (e.g. operational needs, security requirements, etc.) and explanation content on any new concepts that the CWA is based on (e.g. interoperability, sensing units, etc.).

The CWA has been initiated within the context of the FP7 ZONeSEC project (Grant No. 607292). ZONeSEC aims to address the needs of widezone surveillance by defining a new European-wide framework that extends beyond a sole technical proposition.

# 1 Scope

This CWA will provide guidance on aspects of the information exchange requirements between entities in widezone surveillance systems used in critical infrastructures. These entities can comprise human actors and system components. In particular, the CWA focuses on the services, data and metadata that need to be exchanged.

Given the distributed nature of widezone surveillance systems, the CWA gives guidance and offers guidelines on the architecture in order to address any processing and communication performance limitations. The CWA introduces the concepts of security capillaries and clusters that can enhance the overall system's performance, interoperability, scalability and ease of deployment and use.

The CWA covers the security requirements regarding the interaction of physical and cyber-threats in a widezone surveillance system, both in terms of data communication and storage, as well as the protection of the sensing units themselves. The CWA also covers representation of the surveillance information to the different stakeholders, although the emphasis is not on human computer interaction (HCI).

The CWA offers recommendations on the type of information exchanged, the use of data models for exchanging sensor observations, the use of metadata models for describing the measurement process, the means to validate the conformance of information exchanged to the models selected. It provides references to industry standard protocols which describe implementation aspects like the OGC's Sensor Web Enablement (SWE) industry standards for sensor data representation and discovery. However, it does not cover implementation details of the exact communication protocols, data models, data structures used, or specific schemas for the description of message interfaces, the syntax of the exchange or the file formatting required for the exchange. The CWA also does not cover simulation and training processes for security personnel.

The CWA is for use by organizations responsible for designing, configuring, operating and maintaining wide area security systems. It is also of use to those organizations manufacturing components for the surveillance market that will interoperate with modern or/and legacy surveillance platforms.

The CWA is also of interest in the procurement of surveillance systems that combine best-of-breed technological solutions from several vendors. It is also of interest to risk assessment analysts and to public authorities involved in dealing with the protection of widezones.

# 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/DIS 19156:2010, *Geographic information — Observations and measurements*

OpenGIS® Encoding Standard SWE Common Data Model, v2.0, OGC document 08-094r1

# 3 Terms, definitions, abbreviations and acronyms

## 3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.