
**Draft Project plan for the CEN
Workshop on "Improvement of
information processing in crisis
management of critical
infrastructures for computer
assisted data gathering, display
and reporting"**

**Requests to participate in the Workshop
and/or comments on the project plan are
to be submitted by 2022-03-26 to
sofernandez@une.org¹**

Recipients of this project plan are kindly requested to name all patent rights known to them to be relevant to the Workshop and to make available all supporting documents.

Madrid, 2021-12-27 (Version 1)

¹ Applications for participating in the Workshop and comments on the project plan that are not received by the deadline do not need to be taken into consideration. Once constituted, the Workshop will decide whether or not to consider the comments received in good time.

Contents

1	Status of the project plan	4
2	Workshop proposer and Workshop participants	4
2.1	Workshop proposer	4
2.2	Other potential participants.....	6
2.3	Participants at the kick-off meeting.....	6
3	Workshop objectives and scope.....	8
3.1	Background.....	8
3.2	Scope	8
3.3	Related activities	9
4	Workshop programme	10
4.1	General	10
4.2	Workshop schedule	10
5	Resource planning	12
6	Workshop structure and rules of cooperation	12
6.1	Participation in the Workshop.....	12
6.2	Workshop responsibilities.....	12
6.3	Decision making process	13
7	Dissemination and participation strategy	14
8	Contacts	16

Summary

There are many gaps in standardization for crisis management, and more specifically for critical infrastructures (CI). This workshop deals with three of the gaps identified in this field, which are:

1. Semantic Layer Definition for electronic data provision
2. Evaluation of the suitability of existing standards for crisis management in CIs
3. Incident situational reporting for Critical Infrastructures

CWA 17356 '*Interoperability of security systems for the surveillance of widezones*' from project ZONESEC already provided an initial study on data interoperability and operational needs that can be reused for gaps 1) and 2) and for that reason the workshop will produce a CWA that will complement CWA 17356. As such, that new CWA will be focused on Semantic layer definition and suitability of OASIS EDXL-CAP + OASIS EDXL-SitRep standards for crisis management in Critical Infrastructures.

Also, in the framework of this CEN workshop another CWA will be produced aiming to close gap 3) mentioned above. Currently, no formal standard exists on the minimum information that must be exchanged, in the case of an incident to a Critical Infrastructure, from the critical infrastructure to a command and control centre or to another Critical interconnected Infrastructure. The most relevant type of information that is standardized is the EDXL-SitRep standard. This CWA will focus on the content that has to be exchanged and examples of information forms will also be provided as templates.

The two (draft) CWAs will be evaluated through Table Top Exercises (TTXs) and a Full Scale Exercise (FSX) that will be carried out during the period of discussions of the workshop in the [STRATEGY Project](#), from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883520.

1 Status of the project plan

Draft project plan for public commenting (Version 1.0).

This draft project plan is intended to inform the public of a new Workshop. Any interested party can take part in this Workshop and/or comment on this draft project plan. Please send any requests to participate or comments by e-mail to sofernandez@une.org.

All those who have applied for participation or have commented on the project plan by the deadline will be invited to the kick-off meeting of the Workshop on 2022-04-06.

2 Workshop proposer and Workshop participants

2.1 Workshop proposer

The CEN Workshop is proposed by [STRATEGY Project](#) (*Facilitating EU pre-standardization process through streamlining and validating interoperability in systems and procedures involved in the crisis management cycle*) Project consortium. This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883520.

The proposers of the CEN Workshop are specifically ATOS and KEMEA, which are respectively proposers for CWA 1 and CWA 2 with the objectives and scopes explained in clause 3.

Person or organisation	Short description and interest in the subject
<p>Darío Ruiz López ATOS Calle de Albarracín, 25 28037 Madrid, Spain dario.ruiz@atos.net +34 91 038 9924 https://atos.net/en/</p>	<p>Darío Ruiz (male) is a Bachelor in Computer Science from the Universidad Politécnica de Madrid. He has worked in application development since 1997 and collaborated in research projects since 2008. Among other relevant activities, he has worked in several projects for electricity operator, led the development of the Command & Control Centre of research project TOXI-triage and a Control Centre for CBRNe research project COSMIC.</p> <p>Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and a major provider of Big Data, Cybersecurity, High Performance Computing and Digital Workplace, Among other things, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. ATOS is also the official IT provider for the Olympic Games.</p> <p>The Homeland and Security Defence Sector within the Atos unit of Research & Innovation coordinates the R&I activities in the security sector, based on experience gained with clients that include national and regional security bodies, intelligence agencies and international bodies (such as the UN, NATO and the EU). HSD Sector has performed essential security and crisis management projects for many years (e.g., COSMIC, Toxi-triage, DRIVER+, ZONeSEC, PACT, VALUESEC, CIRAS, FORCE, RECOBIA, FOCUS, VIRTUOSO, etc.) aiming to close the gaps between technology, IT and the security related needs of the society.</p>
<p>Georgios Sakkas Center for Security Studies (KEMEA) Ministry of Citizen Protection P. Kanellopoulou 4 101 77 Athens, Greece g.sakkas@kemea-research.gr Tel: +30 2107481630 Mob: +30 6978229551 http://www.kemea.gr/en</p>	<p>Georgios Sakkas (male) is a Geologist with a MSc in Geophysics – Seismology and a PhD degree in Seismology. The past 3 years works as a Research Associate at the Centre for Security Studies (KEMEA) – Ministry of Citizen Protection actively engaged in research projects dealing with natural hazards, civil protection, critical infrastructures and crisis management. His expertise and research interests cover the domains of seismic hazard and engineering seismology, ground motion prediction equations modelling, seismic risk, landslide risk, citizen awareness, civil protection, crisis management, resilience and mitigation against multi-risk assessment approaches, GIS, HTML, Matlab, Python, and standardisation related to crisis management. He has 33 scientific publications in peer reviewed journals and international conferences.</p> <p>KEMEA is established in 2005 (L. 3387/2005, Art. 4 L.3938/2011) as the research organization of the Hellenic Ministry of Citizen Protection. It operates as National think tank on security (cyber and physical) and civil protection policies. Its role focuses on the provision of technical and scientific consulting and training services to the first responder organizations</p>

	<p>under the Ministry's auspices. More specifically, its activities comprise theoretical and applied research on security and civil protection, support of emergency organizations and crisis management authorities with R&D activity and development of technological tools customised to their needs, consultation of strategies and policies.</p> <p>In addition, pursuant to the provisions of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and by a Presidential Decree of 2011 (Nr. 39 of 6.5.2011) KEMEA is the nationally designated European Critical Infrastructure Protection (ECIP) Contact Point, responsible to coordinate ECIP issues domestically, as well as with other Member States and the European Commission.</p> <p>Moreover, in close cooperation with the first responder agencies, KEMEA provides training, being involved in planning and coordination of operational exercises and field demonstrations of new systems and technologies. KEMEA by its networking and training activities aims to bring together national LEAs, First Responders, Civil Protection stakeholders, Critical Infrastructure operators and other involved parties in the disaster management cycle and society's security and resilience, to enable them to collaborate, to exchange experiences and built synergies.</p>
--	---

2.2 Other potential participants

These CWAs will be developed in a Workshop (temporary body) that is open to any interested party. The participation of other experts would be helpful and is desired. It is recommended that:

- Representatives of civil protection authorities (national and local level)
- Representatives of command and control centres
- Representatives of the OASIS Consortium committees on Emergency Management
- Representatives of first responders' organizations acting as end users of the information provided in the crisis management
- Scientists in the area of crisis management
- Participants in related CEN and ISO Technical Bodies
- Participants in consortia (such as the OGC®) and international associations generating related standards
- Participants in related Research Projects
- Representatives of DG ECHO
- Security and safety officers of critical infrastructure operators

take part in the development of these CWAs.

2.3 Participants at the kick-off meeting

The following persons or organisations already signed up to the kick-off meeting prior to the publication of the draft project plan.

Person	Organisation
Workshop proposer (CWA1): Darío Ruiz López	ATOS (Spain)
Workshop proposer (CWA 2): Georgios Sakkas	Ministry of Citizen Protection-Center for Security Studies (KEMEA) (Greece)
Danai Kazantzidou-Firtinidou	Ministry of Citizen Protection-Center for Security Studies (KEMEA) (Greece)
Ioannis Tsaloukidis	
Wilson Antunes	Unidade Militar Laboratorial de Defesa Biológica e Química do Exército Português (UMLDBQ) (Portugal)
Júlio Gouveiva-Carvalho	
Luís Miguel Carvalho	
Marcello Marzoli	Ministero dell'Interno (CNVVF) (Italy)
Giovanni Fresu	
Natascia Erriu.	
Nikos Stefanou	Hellenic Police (HP) (Greece)
Konstantinos Vlamidis	
Tor Olav Grøtan	SINTEF (Norway)
Knut Øien	
Leonidas Perlepes	Satways Ltd (Greece)
Dimitris Diagourtas	
Antonis Kostaridis	
Jan Steiz	Technical University of Applied Sciences Wildau , (Germany)
Aquiles Remón	ATOS (Spain)
Workshop secretariat: Sonia Fernández	Workshop secretariat: UNE (Spain)

(After the Kick off Meeting, a list of attendees and WS participants will be included in Annex A).

3 Workshop objectives and scope

3.1 Background

Each EU country has unique processes and procedures for crisis management and disaster response. In the case of cross-border crises, these different approaches may cause confusion or conflict among first responders and civil protection bodies. Developing a common language and standardising procedures and interfaces across the EU is thus essential for facilitating cross-border collaboration, thereby helping to protect assets and save lives.

The EU-funded research project [STRATEGY](#) has systematically identified and prioritised gaps in standardisation in crisis and disaster management and has compared them to the needs of end users and to available opportunities across a broad spectrum of disaster management activities. All standardisation items to be developed in the course of the STRATEGY project will be fully tested and validated in tabletop exercises (TTXs) and in one full-scale exercise (FSX).

Following the [Directive 2008/114](#) for the identification and protection of critical infrastructures and the more recent updated Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities ([COM/2020/829](#)) “*member states shall ensure that critical entities notify without undue delay the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt their operations.*” Within this framework the competent national authority shall operate an information or coordination centre that will collect data from all operators characterised as critical entities in a coherent, secure and timely manner. Moreover, the ‘national point of contact’ (identified by the competent authority) that will operate as liaison with other Member States and the European Commission, needs to notify other States upon incidents that may affect their critical entities. Consequently, it is important that all national authorities implement common information exchange protocols with standardised fields to be reported for better timely understanding and effective cross-border response when applicable. According to [2020/829 Directive proposal](#), “*notifications shall include any available information necessary to enable the competent authority to understand the nature, cause and possible consequences of the incident, including so as to determine any cross-border impact of the incident*” and a set of given parameters should be also included so that the recipient coordinating body will be able to determine the significance of the disruption at national, cross-border or European level.

Although there are already several standards and protocols for the transmission of data and its reporting in a crisis, they currently have the following lacks:

- There are already standards for representing the content of a message from the sensors and even its meaning, but there is currently no standard for defining the possible values for those meanings, including in the context of critical infrastructures. This makes it impossible to create generic sensors and generic software modules that exploit the data from the sensors, because the modules will need to have internal knowledge on how the sensors represent the meaning of their values sensed.
- Though there are already OASIS EDXL standards for defining the information to send when reporting an alert and for the reports to be generated from the information contained in the system, it is necessary to evaluate the suitability of those standards for covering the full crisis cycle of collecting automatically information about the crisis and producing automatically situational reports from the information collected in the system.
- Though OASIS EDXL-SitRep defines a mechanism to create situational reports with a wide variety of possible fields, it does not define what are the situational reports to be generated during a crisis, and even less for a crisis involving critical infrastructures or for the contents they are meant to include.
- Currently, in case of an incident, there is no standardised type and content of information, as a minimum requirement, that must be exchanged between a critical infrastructure and a command and control centre or between interconnected infrastructures. A standardised description with specific fields of incidents dedicated to critical infrastructures would help to support the response to the incident and the restoration of services.

3.2 Scope

The planned CEN Workshop is aimed to develop two CEN Workshop Agreements (CWAs).

Draft title CWA 1- *Semantic layer definition and suitability of EDXL-CAP+EDXL-SitRep standards for crisis management in Critical Infrastructures*

This CWA will have two objectives:

- Provide a formal definition of the concepts to be reported during a crisis. These concepts will correspond to the meaning of the fields / parts that comprise the messages transmitted during a crisis. Those messages include data coming from sensors but also other intelligent software modules, which will act as virtual sensors. As the possible concepts are potentially unlimited, this list of concepts is initially foreseen to be based on the measure units already defined in ISO standards (ISO/IEC 80000 series) and on chemical compounds sensed defined accordingly to IUPAC nomenclature recommendations.

This formal definition will fill the last gap in the definition of a format for data transmission, which is the last obstacle to link generic components that provide data with software modules that exploit them, potentially providing additional information. In practice, this will enable that Command & Control Centres will be able to add new generic sensors that will be automatically recognized by the system without any additional support from the software vendors.

This definition is meant to be used by sensor and software providers and should be demanded by the crisis operators, but not necessarily used directly by them.

CWA-1 will also complement the information for the operational needs and data interoperability (clause 4 and subclause 6.4 respectively) in CEN/CLC ZONeSEC CWA 17356:2018.

- Evaluate/assess the suitability of the standard OASIS EDXL-CAP for collecting automatically the information of a crisis and the standard OASIS EDXL-SitRep for the generation of situation reports from the information collected in the system and their automatic delivery to the strategic command. This evaluation will be built on the analysis and end-users' feedback of the TTXs and FSX carried out within the STRATEGY Project and considering the operational needs already included in CEN/CLC ZONeSEC CWA 17356:2018 as evaluation criteria.

Thus, the result of this evaluation in CWA 1 is aimed mainly to be used by crisis operators.

Draft title CWA 2- *Emergency management – Incident situational reporting for Critical Infrastructures*

This CWA 2 will define the information exchanged and a common template of reporting incidents of certain significance that affect Critical Infrastructures, as well as their impact to their service provision, health and society. The report with its standardised form may be used by Critical Infrastructure operators for incident notification of the command and control centre of competent authorities and control centres of interconnected infrastructures.

The standardised form will identify the type of information to be included and will determine necessary parameters to be reported, together with a qualitative description of their values. The resulting situational reports will be human readable and can be used to form the reference reporting tool between emergency centres, competent authorities for critical infrastructure protection and infrastructures control centres.

This CWA 2 aims to be used by Critical Infrastructure and security liaison officers of infrastructures operators in the critical infrastructure authorities, by command and control centres, emergency response organizations and by software providers.

3.3 Related activities

The subjects of the planned CWAs are not at present the subject of a standard. However, there are committees, standards and/or other technical specifications that deal with related subjects and thus need to be taken into account - and involved, where necessary - during this Workshop.

The Workshop is open to experts willing to contribute. The following CEN and ISO Technical Bodies are invited to appoint experts/representatives to take an active part in the CEN Workshop deliberations:

- CEN/TC 391 Societal and Citizen Security
- CEN/TC 439 Private Security Services /WG 1 Critical Infrastructure Protection
- CEN/CLC WS ZONeSEC CWA 17356:2018 Interoperability of security systems for surveillance of widezones"
- CEN-CENELEC Sector Forum on Security (SF-SEC)
- ISO/TC 292 Security and resilience

Also, OASIS-Management Emergency TC and OGC® have been addressed by the WS Proposers to participate in the Workshop.

4 Workshop programme

4.1 General

The kick-off meeting is planned to take place on 2022-04-06 via Microsoft TEAMS (online). Due to the travel restrictions and Covid-19 circumstances, all meetings are intended to be made online. If a physical meeting is convened, the possibility of online participation will be granted, if possible.

A draft for public commenting will be published for 60 days.

Several Workshop meetings via web conference will be held, during which the content of the CWA(s) will be presented, discussed, and approved. The meetings will be convened considering the technical discussions and comments received by the participants to the draft CWAs together with the implications of the STRATEGY TTXs feedback.

The CWAs will be drawn up in English (language of meetings, minutes, etc.). The CWAs will be written and published in English.

4.2 Workshop schedule

The two work items (CWAs) with the scope specified in subclause 3.2, are expected to be developed following the same timescale. Table 1 (below) with the preliminary Workshop schedule is then applicable for both CWAs.

The estimated duration of this Workshop is 14 months. During the Workshop lifetime, several online meetings and a public commenting 60 days stage are foreseen.

Table 1: Workshop schedule (preliminary)

CEN/CENELEC Workshop	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21
Calendar month	dic-21	jan-22	feb-22	mar-22	apr-22	may-22	jun-22	jul-22	aug-22	sep-22	oct-22	nov-22	dec-22	jan-23	feb-23	mar-23	apr-23	may-23	jun-23	jul-23	aug-22
Initiation																					
1. Proposal form submission and TC response																					
2. Project plan development																					
3. Open commenting period on draft project plan (mandatory)																					
Operation																					
4. Kick-off meeting																					
5. CWA(s) development																					
6. Open commenting period on draft CWA(s) (optional)																					
7. CWA(s) finalised and approved by Workshop participants																					
Publication																					
8. CWA(s) publication																					
<u>Dissemination (see 7)</u>																					
Milestones																					

- K** Kick-off (online meeting)
- TTX** STRATEGY Tabletop Exercises
- FSX** STRATEGY Full Scale Exercise
- A** Adoption of CWA
- P** Publication of CWA
- D** Online distribution of CWA

5 Resource planning

Costs of the CEN/CENELEC Workshop

The management cost of the CEN Workshop will be covered by resources from the STRATEGY (Facilitating EU pre-Standardisation process Through streamlining and vAlidating inTeroperability in systems and procEdures involved in the crisis management cYcle) Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883520.

The copyright of the final CEN Workshop Agreement will be at CEN/CENELEC.

The final document will include the following paragraph: "Results incorporated in this CEN/CENELEC Workshop Agreement received funding from the European Union's HORIZON 2020 research and innovation program under grant agreement number 883520 (STRATEGY)".

The foreseen CWAs will be freely downloadable from the CEN/CENELEC Website.

Participation and registration fee

Both registration and participation at the CEN Workshop described here are free of charge. Due to the travel restrictions and Covid-19 circumstances, all meetings are intended to be made online. If a physical meeting is convened, the possibility of online participation will be granted, if possible.

Each participant has to bear his/her own costs for travel, accommodation, and subsistence in case of physical attendance.

6 Workshop structure and rules of cooperation

6.1 Participation in the Workshop

The Workshop will be constituted during the course of the kick-off meeting. By approving this project plan, the interested parties declare their willingness to participate in the Workshop and will be formally named as Workshop participants, with the associated rights and duties. Participants at the kick-off meeting who do not approve the project plan are not given the status of a Workshop participant and are thus excluded from further decisions made during the kick-off meeting and from any other decisions regarding the Workshop.

As a rule, the request to participate in the Workshop is closed once it is constituted. The current Workshop participants shall decide whether any additional members will be accepted or not.

Any new participant in the Workshop at a later date is decided on by the participants making up the Workshop at that time. It is particularly important to consider these aspects:

- a. expansion would be conducive to shortening the duration of the Workshop or to avoiding or averting an impending delay in the planned duration of the Workshop;
- b. the expansion would not result in the Workshop taking longer to complete;
- c. the new Workshop participant would not address any new or complementary issues beyond the scope defined and approved in the project plan;
- d. the new Workshop participant would bring complementary expertise into the Workshop in order to incorporate the latest scientific findings and state-of-the-art knowledge;
- e. the new Workshop participant would actively participate in the drafting of the manuscript by submitting concrete, not abstract, proposals and contributions; and
- f. the new Workshop participant would ensure wider application on the CWA.

All Workshop participants who voted for the publication of the CWA(s) or their drafts will be named as authors in the European Foreword, including the organisations which they represent. All Workshop participants who voted against the publication of the CWAs, or who have abstained, will not be named in the European Foreword.

6.2 Workshop responsibilities

The Workshop Chair is responsible for content management and any decision-making and voting procedures. The Workshop Chair is supported by the Workshop Vice-Chair and the responsible Workshop secretariat, whereby the Workshop secretariat will always remain neutral regarding the content of the CWA(s). Furthermore, the Workshop secretariat shall ensure that CEN-CENELEC's rules of procedure, rules of presentation, and the principles

governing the publication of CWA(s) have been observed. Should a Workshop Chair no longer be able to carry out her/his duties, the Workshop secretariat shall initiate the election of a new Workshop Chair. The list below covers the main tasks of the Workshop Chair. It is not intended to be exhaustive.

- Content related contact point for the Workshop
- Presides at Workshop meetings
- Ensures that the development of the CWA respects the principles and content of the adopted project plan
- Manages the consensus building process, decides when the Workshop participants have reached agreement on the final CWA, on the basis of the comments received
- Ensures due information exchange with the Workshop secretariat
- Represents the Workshop and its results to exterior
- Detect potential security issues in the distributed documents and consulting with the STRATEGY Security Advisory Board decide on the nature of the sensitive information to eliminate (or not) from the documents before distribution.

The Workshop secretariat, provided by a CEN/CENELEC national member, is responsible for organising and leading the kick-off meeting, in consultation with the Workshop proposer. Further Workshop meetings and/or web conferences shall be organised by the Workshop secretariat in consultation with the Workshop Chair. The list below covers the main tasks of the Workshop secretariat. It is not intended to be exhaustive.

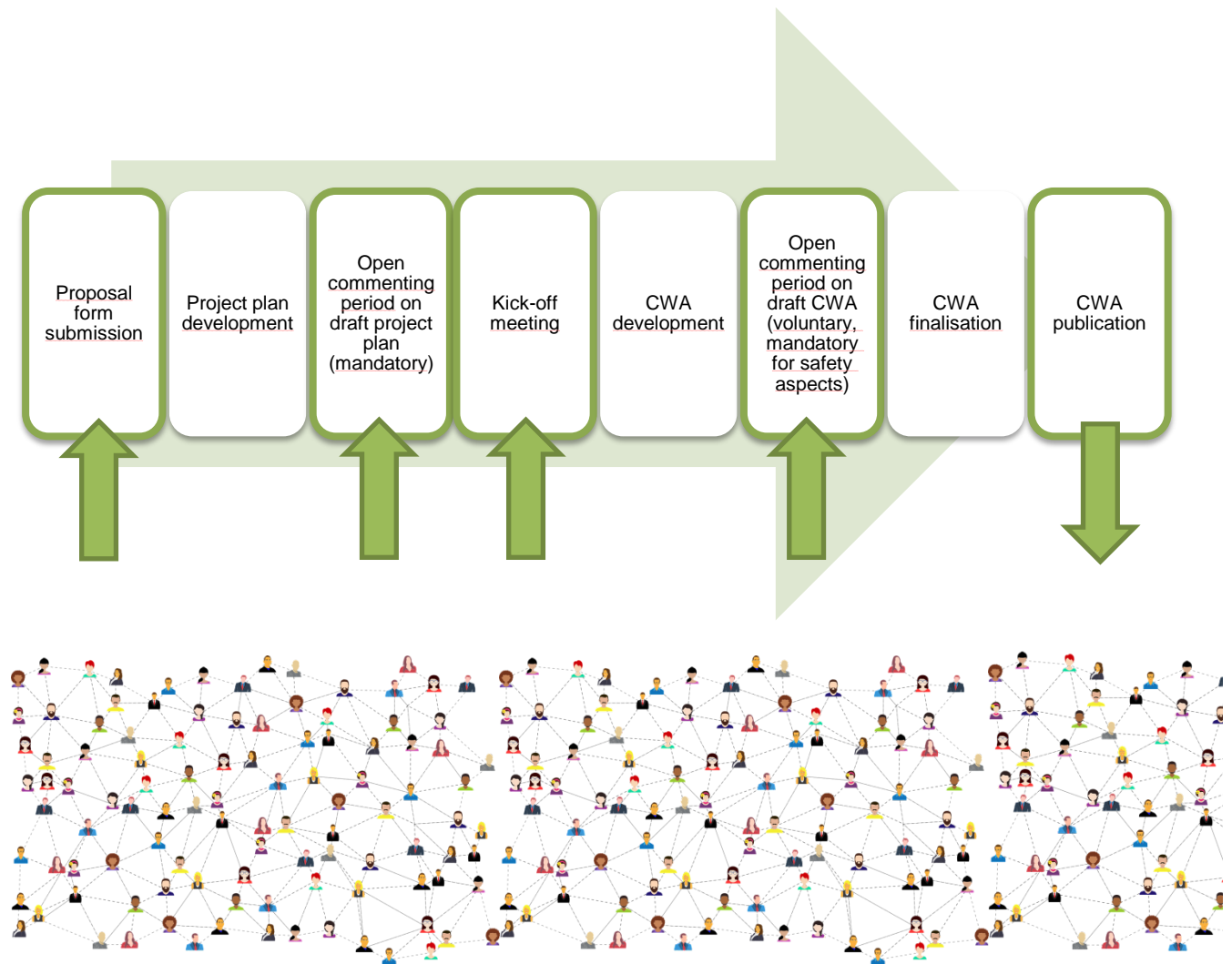
- Administrative and organisational contact point for the Workshop
- Ensures that the development of the CWAs respects the principles and content of the adopted project plan and of the requirements of the CEN-CENELEC Guide 29
- Formally registers Workshop participants and maintains record of participating organisations and individuals
- Offers infrastructure and manage documents and their distribution through an electronic platform (CEN Documents)
- Prepares agenda and distribute information on meetings and meeting minutes as well as follow-up actions of the Workshop
- Initiates and manage CWAs approval process upon decision by the Workshop Chair
- Interface with CEN-CENELEC Management Centre (CCMC) and Workshop Chair regarding strategic directions, problems arising, and external relationships
- Advises on CEN-CENELEC rules and bring any major problems encountered (if any) in the development of the CWA to the attention of CEN-CENELEC Management Centre (CCMC)
- Administrates the connection with relevant CEN or CENELEC/TCs

6.3 Decision making process

Each Workshop participant is entitled to vote and has one vote. If an organisation sends several experts to the Workshop, that organisation has only one vote, regardless of how many Workshop participants it sends. Transferring voting rights to other Workshop participants is not permitted. During voting procedures, decisions are passed by simple majority; abstentions do not count.

If Workshop participants cannot be present in the meetings when the CWAs or their draft are adopted, an alternative means of including them in the voting procedure shall be used.

7 Dissemination and participation strategy



Proposal form submission

The Workshop proposal will be disseminated to the following relevant stakeholders and bodies for consultation:

- CEN/TC 391 Societal and Citizen Security
- CEN/TC 439 Private Security Services /WG 1 Critical Infrastructure Protection
- CEN/CLC WS ZONeSEC CWA 17356:2018
- CEN-CENELEC Sector Forum on Security (SF-SEC)
- ISO/TC 292 Security and resilience/WG 3 Emergency Management
- ISO/TC 292 Security and resilience/ WG 9 *Crisis management*
- OASIS TC Emergency Management

In addition to the CCMC website, the project plan and the date of the kick-off meeting will be advertised on STRATEGY and partners websites to raise awareness and will be shared by European Commission dissemination tools (e.g., CERIS), where possible together with the dissemination to other R&I Projects thematically relevant. Moreover, the announcement of CCMC website will be posted in STRATEGY social media as well as in partners social media to reach as many interested parties as possible to raise awareness.

STRATEGY Advisory Board and the End User Advisory Board will be contacted by STRATEGY Coordination for dissemination of the draft project plan.

Interested parties are requested to contribute either through commenting of the project plan (short term) or through Workshop participation (long term).

Open commenting period on draft CWAs

The draft CWAs will be disseminated to the following relevant stakeholders and bodies for commenting:

- CEN/TC 391 Societal and Citizen Security
- CEN/TC 439 Private Security Services /WG 1 Critical Infrastructure Protection
- CEN/CLC WS ZONeSEC CWA 17356:2018
- CEN-CENELEC Sector Forum on Security (SF-SEC)
- ISO/TC 292 Security and resilience/WG 3 Emergency Management
- ISO/TC 292 Security and resilience/ WG 9 *Crisis management*
- OASIS TC Emergency Management

In addition to the CCMC website, the draft CWAs will be advertised on STRATEGY and partners websites to raise awareness and will be shared by European Commission dissemination tools (e.g., CERIS), where possible together with the dissemination to other R&I Projects thematically relevant. Moreover, the announcement of CCMC website will be posted in STRATEGY social media as well as in the partners social media to reach as many interested parties as possible. Interested parties are requested to contribute through commenting of the draft CWAs (short term).

STRATEGY Advisory Board and the End User Advisory Board will be contacted by STRATEGY Coordination for dissemination of the draft CWAs for comments during the open commenting period.

CWAs publication

The final CWAs will be free downloadable from CEN/CENELEC website and will be disseminated to the following relevant stakeholders and bodies:

- CEN/TC 391 Societal and Citizen Security
- CEN/TC 439 Private Security Services /WG 1 Critical Infrastructure Protection
- CEN/CLC WS ZONeSEC CWA 17356:2018
- CEN-CENELEC Sector Forum on Security (SF-SEC)
- ISO/TC 292 Security and resilience/WG 3 Emergency Management
- ISO/TC 292 Security and resilience/WG 9 *Crisis management*
- OASIS TC Emergency Management

STRATEGY Advisory Board and the End User Advisory Board will be contacted by STRATEGY Coordination for dissemination of the free downloadable CWAs.

In addition to the CCMC website, the final CWAs will be advertised on:

- website of STRATEGY
- website of UNE
- social media:
 - o LinkedIn
 - o Twitter

8 Contacts

- Workshop Chair (and CWA 1 proposer):

Darío Ruiz López
ATOS
Calle de Albarracín, 25
28037 Madrid, Spain
dario.ruiz@atos.net
Tel:+34 91 038 9924
<https://atos.net/en/>

- Workshop Vice-Chair (and CWA 2 proposer):

Georgios Sakkas
Center for Security Studies (KEMEA)
Ministry of Citizen Protection
P. Kanellopoulou 4
101 77 Athens, Greece
g.sakkas@kemea-research.gr
Tel: +30 2107481630
Mob: +30 6978229551
<http://www.kemea.gr/en>

- Workshop Secretariat:

Sonia Fernández González
UNE
C/Génova, 6
28004-Madrid, Spain
sofernandez@une.org
Tel:+34 91 456 46 38
<https://www.en.une.org/>

- Christina Thorngreen
CEN/CENELEC Management Centre (CCMC)
Rue de la Science 23
B - 1040 Brussels, Belgium
cthorngreen@cencenelec.eu
Tel: +32 2 550 09 10
<https://www.cencenelec.eu/Pages/default.aspx>

Annex A - Registered Workshop participants²

The following persons or organisations have registered as Workshop participants at the kick-off meeting and will actively participate in the development of the CWA.

Person	Organisation
Workshop Chair	Workshop Chair
Workshop Vice-Chair	Workshop Vice-Chair
Workshop secretariat	Workshop secretariat

² To be completed after the WS Kick of Meeting.