Towards Safety and Security-Related Testing of Crisis Management Solutions

Todor Tagarev, Petya Ivanova, Laurent Dubost, Cyril Dangerville

Towards Safety and Security-related Testing of Crisis Management Solutions

Todor Tagarev[1], Petya Ivanova[2], Laurent Dubost[3] and Cyril Dangerville[3]

[1] Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Bl. 2, Sofia 1113, Bulgaria
[2] Procon Ltd., 3, Razluka Str., ap. 20, Sofia 1111, Bulgaria
[3] Thales Communications & Security S.A., 20-22 Grange Dame Rose, 78141 Vélizy, France
tagarev@bas.bg, petya@procon.bg, laurent.dubost@thalesgroup.com, cyril.dangerville@thalesgroup.com

Abstract. A number of research and innovation projects aim to develop and demonstrate the benefits of novel solutions, in the particular case analysed in this paper – in the field of disaster or crisis management. The focus of the assessment of these solutions is on the benefits they bring by increasing the effectiveness and/or the performance of crisis management actors in a controlled environment. As a rule, little attention is given to safety and security considerations related to their intended use beyond trials and demonstrations, in an actual crisis management context. To speed up market uptake and innovation, this paper presents a technology-based classification of existing and potential solutions and a structure of their possible impact on safety and security. On that basis the authors identify pertinent 'technology-impact' combinations, list some relevant norms and standards for each such combination, and provide the outlines of three illustrative test cases. The paper concludes by a discussion on the implementation of the presented approach.

Keywords: Crisis management, Disaster management, Preparedness, Demonstration, Trial, Safety, Security, Test case, Innovation, DRIVER+.

1 Introduction

Modern societies face diverse risks of natural, industrial and human-caused disasters and catastrophes and the related human and economic losses once a disaster occurs [1, 2]. With the growing speed of communication facilitated by modern media, including social networks, citizen's expectations towards public authorities are also on the increase [3, 4]. To respond to these expectations, first responders' organisations, other public authorities and stakeholders need to develop a comprehensive set of capabilities to mitigate risks, prepare for, perform a variety of functions in a crisis, manage the consequences and adapt to climate and other changes [5].

One approach to develop the requisite capabilities is to implement the so-called "capabilities-based planning" [6, 7, 8]. A complementary approach involves the development of novel concepts and experimentation with promising technological and other solutions [9, 10].

The latter approach facilitates innovation and allows to speed up the capability development process [11]. Innovations are not always based on most advanced technologies and necessarily expensive; by accounting for context and building on social science insights, they can provide effective and prompt responses and contribute to disaster risk reduction [12].

The DRIVER+ project—Driving Innovation in Crisis Management for European Resilience—built on the idea of experimentation with crisis management concepts and potential solutions for current and future challenges posed by natural disasters, human-caused emergencies, and terrorist threats. It aimed to facilitate the development and market uptake of innovative solutions with account of the operational needs of crisis management practitioners and through their participation in the organisation of trials and demonstrations and the evaluation of the trialled solutions [13].

Crisis management solutions, developed and/or trialled in the DRIVER+ project aim to fill-in identified crisis management gaps, enhance resilience to disaster risks or increase the effectiveness or the efficiency in performing crisis management operations in a resource-constraint framework. Solution providers, often developing innovative ideas or exploiting emerging technological opportunities, aim to demonstrate new effects or more efficient use of limited crisis management resources in a realistic trial setting. Less attention at this stage has been paid to additional considerations that might influence the wider use of a solution in an actual crisis management context.

The aim of the research presented here was to fill in this gap by providing a framework and a knowledge base for safety and security testing of crisis management solutions. This paper starts with the outline of the methodological approach. Section 3 presents a technology-based classification of existing and potential solutions, followed by the structuring of their possible impact on safety and security in Section 4. On that basis the authors identify pertinent 'technology-impact' combinations, list some relevant norms and standards for each such combination, and provide the outlines of three illustrative test cases. The paper concludes by a discussion on the implementation of the presented approach.

2 Methodological Approach

The study aimed to set the ground for examining safety and security considerations in the use of solutions in a real crisis management environment. It followed the approach outlined on Figure 1.

The task is to assist practitioners and solution providers in defining safety and security related requirements to crisis management solutions of interest and demonstrate how to develop respective test cases. Towards that purpose this section of the report provides:

- a classification scheme used to classify crisis management solutions on the basis of the underlying technology used;
- structure of the safety and security considerations, i.e., the type of negative impact a solution may have;
- identification of couples "technology – type of impact" where one has, or can realistically expect, concerns for the safe and secure use of a crisis management solution;
- identification of applicable norms (standards, directives, regulations, etc.) for each "technology – type of impact" couple;
- design of illustrative test cases.

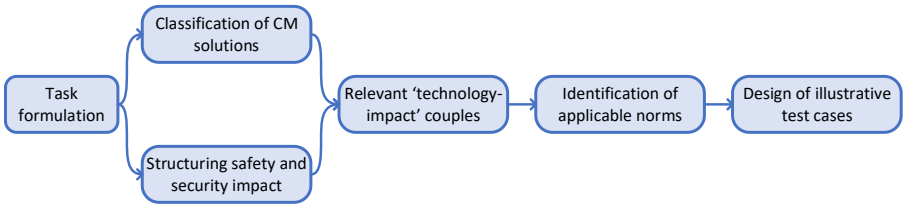

Fig. 1. Safety and security related testing of Crisis Management Solutions: Methodological approach.

Each of the enumerated issues is examined in a dedicated section of this paper. The final section outlines the envisioned implementation and future use of this approach to the safety and security related testing of crisis management solutions.

3 Technology-based Classification of Solutions

To categorise crisis management solutions in terms of the underlying technology and in view of their potential impact on safety and security, we analysed three main taxonomies:

- STACCATO security taxonomy [14];
- CRISP Taxonomy of Security Products, Systems and Services [15];
- EDA Technology Taxonomy [16].

and developed a classification scheme with nine main categories:

1. Sensors and navigation systems and networks
passive (Optical, IR, magnetic, acoustic, UW, electrical and electro-chemical sensors, magnetometers and magnetic gradiometers, gravity meters and gravity gradiometers) and active sensors (radar, ladar, lidar, sonars, X-ray, Gamma sensors, Active IR sensors), chemical and biological substances detectors, radiological and nuclear detectors, other sensors.

2. Communications
Radio communications and networks; cable communications and networks; mass emergency notification systems; early warning and alerting systems; targeted emergency

notification systems; secured, wireless broadband systems; rapidly deployable communication system (rescue services mobile communication system); emergency information hotlines.

3. Computer-based systems
data bases and database management systems; decision support systems; training, modelling & simulation systems and environments; …

4. Specialised software applications
Personnel management software; material reserves management software; supply chain management software, information management & dissemination software; privacy and data protection software; electronic tagging systems; volunteers registries and management software, crowd sourcing/ crowd tasking systems.

5. Transportation vehicles and equipment
ground, air, river, and maritime vehicles, ambulances, transportation containers and structures, etc.

6. Remotely controlled systems and autonomous vehicles and systems
Remotely Piloted Vehicles (RPVs) and systems (RPAS), air, ground, surface, sub-surface vehicles.

7. Fire extinguishers and decontamination devices and substances
Fire retardants, decontamination devices and substances for radiation sources, biological materials, chemical sources and poisons; other substances.

8. Specialised disaster management equipment
protective clothing and equipment, (mobile) shelters, Mobile livestock shelters, mobile field hospitals, mobile energy systems and electricity generators, mobile water purification equipment, access control and electronic authentication systems, training ranges, physical obstacles (e.g., to stop flooding), waste management systems, logistics tracking, transportation management systems, other related equipment.

9. Training and personnel services
Education and skills training systems; Psycho-social support systems; Exercises; Manuals; Distance learning (e-Learning, m-Learning); Fatigue and stress observation, analysis and coping system.

4 Types of Potential Safety and Security Impact of CM Solutions

The implementation of crisis management solutions is expected to contribute to reduction of risks and more effective and efficient operations. However, they may have potential undesired side effects on the safety and security of personnel, property, infrastructure and the environment.

International Safety Standards define “safety” as freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment. Standards IEC 61508 and

IEC 61511-1:2016 refer to this also as "functional safety." In the discussion of crisis management solutions, the analysis of security concerns can start from the definition utilised by the International Society of Automation (ISA), i.e., "security" means prevention and protection from illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of motivation (intentional or unintentional) or consequence (result) [17].

Starting from these definitions, and accounting for societal and environmental concerns, this study examines the potential negative impact of crisis management solutions on:

- people, both those involved in crisis management and others who happen to be at or near the crisis scene;
- the equipment and/or the data and information used in crisis management;
- the functioning of critical infrastructures, e.g., energy, transport [18], digital infrastructure and the delivery of essential services, e.g., food, water, financial services [19], etc.
- the environment, i.e., on the animals, the vegetation, air, soil, and water quality.

Respectively, we consider here only direct impact, not taking into account possible cascading effects, e.g., software breech leading to a drone crash and injury of first responders. The reason is that testing will be conducted to assure that a crisis management solution meets the requirements of certain safety and security norms, while potential secondary effects may be studied via more complex models or trial scenarios.

Hence, seven types of negative impact, marked from A to G, are taken into consideration:

- Impact on humans (professional responders and other crisis management personnel, volunteers, service providers, other people in the area of the crisis or its vicinity):

  A. *Physical* (injury, poisoning, blinding, death, …)

  B. *Psychological* impact; impact on the perceptions

  C. Breech of sensitive *personal data*

- Temporary of lasting impact on crisis management materiel, data, and information (equipment, communications, information, …)

  D. Obstructing the use of CM *equipment* (e.g., by physical damage, radio-electronic interference, etc.)

  E. '*CIA*' – impact on the confidentiality, integrity and availability of information (including malicious attempts to manipulate information)

  F. *Impact on critical infrastructures and/or the provision of essential services*

  G. *Environmental impact* (flora, fauna, soil, air, water)

5 Pertinent 'Technology-Impact' Combinations

There are 63 possible combinations among the nine categories of solutions and the seven types of impact (see Table 1 below). Not all combinations are possible, i.e. certain categories of solutions cannot have a particular type of impact (only direct impact is considered here; possible cascading effects are not subject of this study). For example, a software application is highly unlikely to cause physical injury, transportation vehicles and decontamination devices are unlikely to infringe on the confidentiality, integrity and availability of information, etc.

In Table 1, the cells of such unlikely combinations are marked with grey background colour. The remaining 39 combinations "solution's underlying technology – negative impact on safety and security" are considered pertinent. Respectively, the next section provides standards and other norms for each pertinent combination, followed by provide illustrative test cases for the combinations marked with 'X' in Table 1.

By 'X' in the table are marked "technology-impact" combinations for which this paper presents illustrative test cases.

Table 1. 'Technology-Impact' Combinations.

Potential impact on/	Humans			CM materiel, data, and information		F. Critical infrastructures	G. Environment
Solutions	A. Physical	B. Psychological, perceptions	C. Personal data	D. Materiel	E. CIA of information		
1. Sensors and navigation systems and networks: passive (optical, IR, magnetic, acoustic, UW, electrical and electro-chemical sensors, magnetometers and magnetic gradiometers, gravity meters and gravity gradiometers) and active sensors (radar, ladar, lidar, sonars, X-ray, Gamma sensors, active IR sensors), chemical and biological substances detectors, radiological and nuclear detectors, …							
2. Communications: Radio communications and networks; cable communications and networks; mass emergency notification systems; early warning and alerting systems; targeted emergency notification systems; secured, wireless broadband systems; rapidly deployable							

communication system (rescue services mobile communication system); emergency information hotlines							
3. Computer-based systems: data bases and database management systems; decision support systems; training, modelling & simulation systems and environments; …						X	
4. Specialised software applications: Personnel management software; material reserves management software; supply chain management software, information management and dissemination software; privacy and data protection software; electronic tagging systems; volunteers registries and management software, crowd sourcing/ crowd tasking systems			X		X		
5. Transportation vehicles and equipment: ground, air, river, and maritime vehicles, ambulances, transportation containers and structures, …							
6. Remotely controlled systems and autonomous vehicles and systems: RPVs/RPAS, air, ground, surface, subsurface vehicles							
7. Fire extinguishers and decontamination devices and substances: Fire retardants, decontamination devices and substances for radiation sources, biological materials, chemical sources and poisons							
8. Specialised disaster management equipment: protective clothing and equipment, (mobile) shelters, mobile livestock shelters, mobile field hospitals, mobile energy systems and electricity generators, mobile water purification equipment, access control and electronic authentication systems, training ranges, physical obstacles (e.g., to stop flooding), waste management systems, logistics tracking, transportation management systems …							
9. Training and personnel services: Education and skills training systems; Psycho-social support systems; Exercises; Manuals; Distance learning (e-Learning, m-Learning); Fatigue and stress observation, analysis and coping system							

6 Sample Safety and Security Norms for Pertinent 'Technology-Impact' Combinations

Selected regulations on safety and security of crisis management solutions are presented in Table 2 below.

This table included in this paper is illustrative. The study did not deliver a comprehensive list of norms as well; yet, it intentionally included a broad variety of sources, such as international (ISO) and European standards, national standards, potential standards /under development/, i.e., CEN Workshop Agreements (CWAs), EU Directives, regulations, recommendations and guidelines by UN bodies such as ITU and IAEA, good practices identified by industry associations and non-governmental organisations, etc.

A number of these norms are relevant to more than one "technology-impact" combination. Such norms are listed ones, with the respective remark on applicability.

Of general relevance is how testing fits into the development of a strategic crisis management capability, addressed in CEN/TS 17091:2018 "Crisis management – Guidance for developing a strategic capability."

Table 2. Illustrative set of norms for pertinent 'Technology-Impact' combinations.

Document	Relevance
(1-A) Sensors and navigation systems and networks – Physical impact	
EN ISO 15367-2:2005 (WI=00123043) Lasers and laser-related equipment – Test methods for determination of the shape of a laser beam wavefront - Part 2: Shack-Hartmann sensors (ISO 15367-2:2005).	Power (energy) density distribution, widths and divergence angles of laser beams.
BS EN 50270 Electromagnetic compatibility - Electrical apparatus for the detection and measurement of combustible gases, toxic gases or oxygen	This document applies to apparatus intended for use in variety of settings, including hazardous areas which could contain explosive or potentially explosive atmospheres. It specifies requirements for immunity tests in relation to continuous and transient, conducted and radiated disturbances, including electrostatic discharges, and also for emission tests.
Radiation Protection of the Public and the Environment, IAEA Safety Standards Series No. GSG-8 [applicable to 1-G]	This Safety Guide provides guidance on the implementation of the requirements in the International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, in relation to protection of the public and the environment against radiation risks. It provides generic guidance on the application of the radiation protection principles of justification, of optimization of protection and safety, and of dose limits. The publication covers the protection of the public and the

	environment in all exposure situations, including in emergency.
(1-B) Sensors and navigation systems and networks – Psychological impact, impact on perceptions	
ISO 27048:2011 Radiation protection — Dose assessment for the monitoring of workers for internal radiation exposure	This standard specifies the minimum requirements for the evaluation of data from the monitoring of those occupationally exposed to the risk of internal contamination by radioactive substances. It presents procedures and assumptions for the standardised interpretation of monitoring data, in order to achieve acceptable levels of reliability. Among others, it addresses assumptions for the selection of dose-critical parameter values; criteria for determining the significance of monitoring results; their interpretation; uncertainties arising from sampling, measurement techniques and working conditions; interpretation of multiple data arising from different measurement methods at different times, handling data below the decision threshold, rogue data.
(1-G) Sensors and navigation systems and networks – Environmental impact	
Guide for the Selection of Explosives Detection and Blast Mitigation Equipment for Emergency First Responders Preparedness Directorate Office of Grants and Training, Guide 105–07, US Department of Homeland Security, February 2008 [applicable to 1-A, 8-A, 8-D, 8-F]	The Guide presents a broad spectrum of sensing technologies and techniques, with their advantages and disadvantages, of visual detection and blast mitigation equipment, as well as methods and results of the evaluation of concrete products.
(2-A) Communications – Physical impact	
Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications (Geneva: ITU-T – Telecommunication Standardization Bureau, 2015). – 206 pp. [applicable to groups 2, 3 and 4]	This manual provides a broad introduction to the ICT security work of the ITU, with key areas and a discussion of the basic requirements for the protection of ICT applications, services and information, security architectures and management. An 8-page annex provides a list of relevant ITU recommendations and standards.
Directive 2013/35/EU of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) and repealing Directive 2004/40/EC	This Directive lays down minimum requirements for the protection of workers from risks to their health and safety arising, or likely to arise, from exposure to electromagnetic fields during their work. It covers all known direct biophysical effects and indirect effects caused by electromagnetic fields and provides exposure limit values (ELVs)

	with scientifically well-established links between short-term direct biophysical effects and exposure to electromagnetic fields.
(2-B) Communications – Psychological Impact, impact on Perceptions	
ISO 22322:2015: Societal security — Emergency management — Guidelines for public warning [applicable to 2-A, 2-F, 2-G]	This International Standard provides guidelines for developing, managing, and implementing public warning before, during, and after incidents.
(2-E) Communications – CIA of Information	
ETSI/TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites	The Technical Specifications provide guidance on selection of cryptographic suites with particular emphasis on interoperability. The present document is based on the specified agreed cryptographic mechanisms of the SOG-IS Crypto Evaluation Scheme [15]. The SOG-IS Crypto WG is in charge of providing requirements and evaluation procedures related to cryptographic aspects of Common Criteria security evaluations of IT products.
(2-F) Communications – Critical infrastructures	
ITU-T K.87 (06/2016) Guide for the application of electromagnetic security requirements – Overview [applicable to 2-A and 2-E, 3-E and 3-F]	This document outlines electromagnetic security risks of telecommunication equipment and illustrates how to assess and prevent those risks, in order to manage information security management systems (ISMS) in accordance with Recommendation ITU-T X.1051. Major electromagnetic security risks addressed in this Recommendation are as follows: natural electromagnetic (EM) threats (e.g., lightning); unintentional interference (i.e., electromagnetic interference, EMI); intentional interference (i.e., intentional electromagnetic interference, IEMI); deliberate EM attacks; information leakage from EM emanation (i.e., electromagnetic security, EMSEC); and mitigation methods against electromagnetic security threats.
(2-G) Communications – Environmental impact	
Maximum Exposure Levels to Radiofrequency Fields —3 kHz to 300 GHz, Radiation Protection Series Publication No. 3 (Australian Radiation Protection and Nuclear Safety Agency, 2002). [applicable to 2-A]	This Standard specifies fundamental limits … that correlate most closely with the established biological effects for which protection is required. Therefore, a set of indicative levels called ‘reference levels’ have been provided as an alternative means for determining compliance. … This rationale

	does provide a broad overview of the scientific and philosophical considerations that lead to the derivation of the exposure limits.
Physicians for Safe Technology, Environment and Wildlife Effects, https://mdsafetech.org/environmental-and-wildlife-effects/	A compilation of norms and studies of the harmful effects of radio, microwave communication and magnetic fields on wildlife and the environment.
(3-B) Computer-based systems – Psychological Impact, impact on Perceptions	
Eva Flaspöler et al., The human machine interface as an emerging risk (European Agency for Safety and Health at Work, 2010). [applicable to 4B]	The documents review the literature allowing to foresee multi-factorial risks (e.g. due to combined effects of poor ergonomic design, poor work organisation, mental and emotional demands); complexity of new technologies, new work processes and human-machine interface (HMI) leading to increased mental and emotional strain; poor ergonomic design of non-office visual display unit workplaces; and poor design of HMI (excessively complex or requiring high forces for operation).
(3-C) Computer-based systems – Personal Data	
ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	This standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
(3-E) Computer-based systems – CIA of Information	
ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security	The standard establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation of security properties of IT products. Parts 2 and 3 defines operations for tailoring functional and assurance components.
(3-F) Computer-based systems – Critical infrastructures	
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	This Directive lays down measures with a view to achieving a high common level of security of network and information systems … To that end, this Directive lays down obligations … ; …; establishes security and notification requirements for operators of essential services and for digital service providers; …
(4-B) Specialised software applications – Psychological Impact, impact on Perceptions	
Eva Flaspöler et al., The human machine interface as an emerging risk (European Agency for Safety and Health at Work, 2010).	The documents review the literature allowing to foresee multi-factorial risks (e.g. due

[applicable to 3B]	to combined effects of poor ergonomic design, poor work organisation, mental and emotional demands); complexity of new technologies, new work processes and human-machine interface (HMI) leading to increased mental and emotional strain; poor ergonomic design of non-office visual display unit workplaces; and poor design of HMI (excessively complex or requiring high forces for operation).
(4-C) Specialised software applications – Personal Data	
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), *Official Journal* L 119, 4 May 2016	Defines principles relating to and lawfulness, and conditions of processing of personal data
(4-E) Specialised software applications – CIA of Information	
ISO/IEC 27002:2013 "Information technology -- Security techniques -- Code of practice for information security controls" [applicable to 3-C, 3-E, 3-F, 4-F, 9-E]	The standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment.
(4-F) Specialised software applications – Critical infrastructures	
NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations", revision 4, April 2014 [applicable to 3-C, 3-E, 3-F, 4-F, 9-E]	The document provides a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber and other threats.
(5-A) Transport vehicles and equipment – Physical Impact	
CEN/TR 1459-6:2015 (WI=00150078) Rough-terrain trucks - Safety requirements and verification	Explains the risk assessment methodology followed to determine the Performance Level required, for specific safety related parts of control system (SRP/CS) of rough-terrain variable-reach trucks. Part 6 examines the application of EN ISO 13849-1 to slewing and non-slewing variable-reach rough-terrain trucks.
(5-D) Transport vehicles and equipment – Materiel	
ISO 19116:2019 Geographic information — Positioning services	This document specifies the data structure and content of an interface that permits

[applicable to 5-A, 5-F, 6-A, 6-D, 6-F]	communication between position-providing device(s) and position-using device(s) enabling the position-using device(s) to obtain and unambiguously interpret position information and determine, based on a measure of the degree of reliability, whether the resulting position information meets the requirements of the intended use.
(5-G) Transport vehicles and equipment – Environmental impact	
Directive 2008/68/EC of the European Parliament and of the Council of 24 September 2008 on the inland transport of dangerous goods [applicable to 5-A and 5-D]	The Directive applies to the transport of dangerous goods by road, by rail or by inland waterway within or between Member States, including the activities of loading and unloading, the transfer to or from another mode of transport and the stops necessitated by the circumstances of the transport.
(6-A) Remotely controlled systems and autonomous vehicles and systems – Physical Impact	
Ludovic Apvrille et al., Autonomous Drones for Disasters Management: Safety and Security Verifications, AT-RASC 2015	The paper presents a tool (SysML-Sec/TTool) that can be used for formally verifying the safety and security of an autonomous drone mission and flight, based on an architecture developed within drone4u project.
(6-D) Remotely controlled systems and autonomous vehicles and systems – Materiel	
CWA 17357:2019 Urban search and rescue (USaR) robotic platform technical and procedural interoperability – Guide [applicable to 6-A]	This CWA provides recommendations to enable interoperability between USaR robotic platforms and the equipment, sensors and tools that are attached to them; principles for enabling USaR robotic platforms to operate in all ground search environments.
(6-F) Remotely controlled systems and autonomous vehicles and systems – Critical infrastructures	
CEN - PREN 16803-2 Space – Use of GNSS-based positioning for road Intelligent Transport Systems (ITS) – Part 2: Assessment of basic performances of GNSS-based positioning terminals [applicable to 6-A and 6-D]	This document proposes testing procedures to assess the basic performance of any GNSS-based positioning terminal for a given use case described by an operational scenario. These tests address the basic performance features Availability, Continuity, Accuracy and Integrity of the Position, Velocity and Time (PVT) information.
(7-A) Fire extinguishers and decontamination devices and substances – Physical Impact	
EN 3-10:2009 Portable fire extinguishers. Provisions for evaluating the conformity of a portable fire extinguisher to EN 3-7 (characteristics, performance requirements and test methods)	European standard EN 3 specifies requirements for portable fire extinguishers. Compliance with the standard is legally required in the EU.

(7-D) Fire extinguishers and decontamination devices and substances – Materiel	
Phillip Carson and Clive Mumford, Hazardous Chemicals Handbook, Second edition (Oxford: Butterworth Heinemann, 2002). – 619 pp. [applicable to the whole group 7]	The Handbook presents a variety of hazardous chemicals, including radioactive chemicals, safety by design principles, operating procedures, transport, impact on the environment, monitoring and protection. It includes selected topics of testing and evaluation.
(7-F) Fire extinguishers and decontamination devices and substances – Critical infrastructures	
CEN/TS 16595:2013 CBRN – Vulnerability Assessment and Protection of People at Risk [applicable also to 7-A, 7-D, 7, 7-G]	This Technical Specification is based on an all-hazards approach, with a specific focus on terrorism and other security related risks. Looking at the combination of threats, vulnerabilities and values to be protected, threats may be terrorist attacks with chemical, explosive and biological agents, or nuclear waste materials, or with conventional means on CBRN plants, causing a similar devastating effect on a potentially large scale. It can serve to guide the development of safety and security test cases.
(8-A) Specialised disaster management equipment – Physical Impact	
Group of standards ISO 13.340 Protective equipment	The group includes standards for protective equipment in general, protective clothing, head protective equipment (helmets, eye-protectors, hearing protectors, ear muffs, teeth protectors and hoods), respiratory protective devices, hand and arm, leg and foot protection, etc.
(8-C) Specialised disaster management equipment – Personal data	
CEN/TR 16670:2014 Information technology – RFID (Radio-Frequency IDentification) threat and vulnerability analysis See also CEN/TR 16674:2014 – Analysis of privacy impact assessment methodologies relevant to RFID	This Technical Report consider the threats, vulnerabilities and mitigation methods associated with specific characteristics of RFID technology in a system. In particular the document should be a tool used by RFID system integrators, to improve security aspects using a privacy by design approach.
(8-D) Specialised disaster management equipment – Materiel	
ISO/IEC 29197:2015 Information technology — Evaluation methodology for environmental influence in biometric system performance	This standard elaborates fundamental requirements for planning and execution of environmental performance evaluations for biometric systems based on scenario and operational test methodologies, respective specifications, baseline performance and procedures for carrying out the overall evaluation.
(8-E) Specialised disaster management equipment – CIA of Information	

CEN/TS 15291:2006 Identification card system – Guidance on design for accessible card-activated devices [applicable to 8-A, 8-D and 8-F]	This document provides guidance for the design and location of card-activated devices and the immediate environment, to facilitate access for the widest possible range of users (all/most members of the community), subject to conditions of adequate privacy and security.
(8-F) Specialised disaster management equipment – Critical infrastructures	
CWA 17260:2018 Guidelines on evaluation systems and schemes for physical security products [applicable to 8-A and 8-D]	This CWA provides guidelines on how to design certification systems and schemes for physical security products and presents a framework in which these systems and schemes can be upheld. Physical security products include products which provide protection of people, property and infrastructure from acts of malicious intent, such as physical attacks.
(8-G) Specialised disaster management equipment – Environmental impact	
Group of ISO standards 13.030.30 Special wastes, including radioactive wastes, hospital wastes, carcasses, electrical, electronic equipment and other hazardous wastes	See ISO/DIS 16640 Monitoring radioactive gases in effluents from facilities producing positron emitting radionuclides and radiopharmaceuticals; ISO/DIS 22450 Elements recycling –Communication formats for providing recycling information on rare earth elements in industrial waste and end of life products; etc.
(9-A) Training and personnel services – Physical Impact	
ISO 22398:2013 – Societal security — Guidelines for exercises.	This International Standard describes the elements of a generic approach to planning, conducting and improving exercise programmes and projects. It introduces the "exercise safety officer" position for a person tasked with ensuring that any actions during the exercise are performed safely.
(9-B) Training and personnel services – Psychological Impact, impact on Perceptions	
IASC Guidelines on Mental Health and Psychosocial Support in Emergency Settings (Geneva: Inter-Agency Standing Committee, 2007 & 2008).	The Guidelines present good practice in planning, establishing and coordinating a set of minimum multi-sectoral responses to protect and improve people's mental health and psychosocial well-being in the midst of an emergency. The 2008 edition provides a Checklist for Field Use.

7 Illustrative Test Cases

This section outlines three illustrative test cases for testing safety and security of crisis management solutions that have participated in one or more of the DRIVER+ project trials:

- The Social Media Analysis Platform, trailed in Trial France
- The CrisisSuite solution, trailed in Trials France and The Netherlands, and in the Final Demo
- The Test-bed infrastructure with the Common Information Space, and its embedded security features.

The role and the guidelines for preparing test cases are described in DRIVER+ deliverable D934.21 – Solution Testing Procedure, March 2019 [20].

Test Case 1 "Personal Data Protection in the Social Media Analysis Platform"

The Social Media Analysis Platform is presented in the DRIVER+ Portfolio of Solutions at https://pos.driver-project.eu/en/PoS/solutions/62.

This test case illustrates the couple 4-C, i.e., the potential negative impact of specialised software applications on personal data.

General norms: Regulation (EU) 2016/679

Specific norms: OASIS / Common Alerting Protocol Version 1.2

During Trial 2 of the DRIVR+ project, the Social Media Analysis Platform (SMAP) solution was identified as requiring a GDRP analysis. The solution collects and exploits Social Media post which are considered as "personal data." The analysis which was conducted with the support of Thales Legal Department is reproduced in the Annex 2 of D942.22 Report on the application of solutions in the Trial 2. In short, this analysis concluded that due to the fact that the purpose of the collection and processing of these personal data was clearly aiming at improving Social Resilience, and thus was in the interest of the persons, they were legitimate, and consequently authorized. Yet, due to the specific nature of the data, some restrictions regarding the access to the data needed to be limited (through authentication of a single user) and their retention over time also. In addition to these measures, the anonymisation of the pseudos (which often contain names in clear) was recommended and implemented. This analysis is a good basis to foresee the requirements which could derive for such a Social Media Analysis Platform if it were to become an operational system.

Test Case 2 "Providing confidentiality, integrity and availability of information in CrisisSuite"

The CrisisSuite solution is presented in the DRIVER+ Portfolio of Solutions at https://pos.driver-project.eu/en/PoS/solutions/179.

This test case illustrates the couple 4-E, i.e., the potential negative impact of using specialised software applications to exchange information among units participating in a crisis management operation on its confidentiality, integrity and availability.

General norms: The ISO 27000 family of standards

The CrisisSuite solution. CrisisSuite was trailed three times during DRIVER+ - in two trials and the Final Demonstration. The example which is the most meaningful with regards to the requirements concerning safety and security is the one of the Final Demonstration. In that demonstration, information was shared thanks to CrisisSuite which is deployed at three levels, from EUCPM modules (the tactical level), then at EUCPT level (the operational coordination level), and ERCC, the strategic coordination at European level. The security problems which were faced during the final demonstration related to the right to know (confidentiality) of information: ERCC does not want modules to be able to read the information they share with EUCPT.

During the DRIVER+ Final Demonstration, Warsaw, November 2019, this requirement was implemented by creating two 'crises' in CrisisSuite. This implementation was a work around which actually was satisfying for the table top Trial, but would require other types of implementation if the solution was to be operationally deployed at ERCC, EUCPT and Modules.

Test Case 3 "Security of digital infrastructure in the Common Information Space"

The Test-bed infrastructure is presented in detail in the deliverables from Work Package 923 of the DRIVER+ project.

This test case illustrates the couple 3-E, i.e., the potential negative impact of computer-based systems on critical infrastructures; in this case – on the digital infrastructure of a crisis management operation. Although the illustration relates to trial settings, the approach can be of value in testing actual digital infrastructure.

General norms: The ISO 27000 family of standards

Specific norms: SSL/TLS security protocol

The Common Information Space (CIS) is a software module of the Test-bed infrastructure which enables the exchange of information between Solutions in DRIVER+ Trials. This CIS can be made available on-line which facilitates on-line testing of solutions, or the use of the on-line Test-bed during a Trial. Making such a software available on-line makes it vulnerable to potential cyber intentional attacks or non-intentional interference. A solution that would either by mistake or malicious intention connect to an instance of the CIS during a Trial could disturb the whole trial by sending unintended messages for example. For this reason, it is very important to fully master what solution is able to connect to the CIS and when. In DRIVER+ this level of security was introduced by distributing security certificates which enforced a strong authentication mechanism on the CIS by encrypted security codes: each solution (of each organization) is issued a security certificate by a Certificate Authority of the Test-bed, and the CIS broker requires every connecting solution to authenticate with such certificate (SSL/TLS protocol). This guarantees that the solutions connecting to the CIS are indeed properly identified and authorized to do so.

Besides, the use of SSL/TLS security protocol on the CIS broker also guarantees the confidentiality and integrity of the messages exchanged within the CIS, i.e. it prevents an unauthorized user to intercept, alter, replace or replay messages maliciously. The next security requirement addressed in DRIVER+ is topic-based access control. Indeed,

depending on the sensitivity or criticality of certain CIS topics, only one or more specific solutions should be authorized to publish or read data from these topics. The previous paragraph gives a relevant example where ERCC is exchanging information with EUCPT, which could be done in a specific CIS topic, but does not want the EUCPM modules to read this information. To address this requirement, DRIVER+ provides an access control plugin for the CIS broker that allows to enforce a fine-grained access control policy (defined via the Test-bed's Admin Tool) that consists of rules such as: permit solution X to READ/WRITE from/to topic Y (and deny such rights by default). Although this feature has not been used yet in a Trial, it is available in the Test-bed software repository and tested by the Test-bed infrastructure staff.

In the perspective of an operational use of the CIS, other security measures would be required in order to reduce its vulnerability to potential cyberattacks: the use of one single port to connect to the internet, or the use of a proxy to hide the actual IP addresses of the CIS servers from the outside.

The full securing of the CIS would also depend on the actual physical and logical infrastructure on which the servers would be deployed: the presence of a DMZ zone, firewalls, etc., which can only be examined when all these constraints are known.

8 Conclusions

Assuring safety and security of new crisis management solutions depends on the way practitioners' organisations define their requirements. Solution providers or third parties are expected to warrant that these requirements are met. It is possible also to jointly design and conduct tests to verify the extent to which requirements are met.

The study presented in this paper goes beyond the framework for preparing trials, demonstrations, experiments or tests of innovative crisis management solutions. It is intended to support the process of the uptake of solutions by presenting a framework for dealing with safety and security concerns in the use of crisis management solutions in actual crisis context, which would be of use to both crisis management practitioners and solution providers.

While this framework is comprehensive, the list of normative documents delivered in the study and illustrated above is subject to continuous review, updates and amendment. This also applies to illustrative test cases. An increasing number of test cases and results will contribute to the body of knowledge on the safe and secure use of solutions in actual crisis management context.

Acknowledgement

The research leading to these results was performed by the Centre for Security and Defence Management, Institute of ICT, Bulgarian Academy of Sciences and Thales Communications & Security, France, as part of the DRIVER+ project and has received funding from the European Union's Seventh Framework Programme under grant agreement no. 607798.

References

1. Shi, P.: Hazards, Disasters, and Risks. In: Disaster Risk Science, pp. 1-48. IHDP/Future Earth-Integrated Risk Governance Project Series. Springer, Singapore. https://doi.org/10.1007/978-981-13-6689-5_1.
2. Stäubli, A., Nussbaumer, S.U., Allen, S., Huggel, C., Wymann von Dach, S. Diverse natural hazards – high human and economic losses. In: Wymann von Dach, S., Bachmann, F., Alcán-tara-Ayala, I., Fuchs, S., Keiler, M., Mishra, A., Sötz, E. (eds.) Safer lives and livelihoods in mountains: making the Sendai Framework for Disaster Risk Reduction work for sustainable mountain development, pp. 14-19. Centre for Development and Environment, University of Bern, Bern (2017).
3. Chamlee-Wright, E., Storr, V.H.: Expectations of government's response to disaster. Public Choice 144(1/2), 253–274 (2010). https://doi.org/10.1007/s11127-009-9516-x.
4. Jong, W., Dückers, M.L.A.: The Perspective of the Affected: What People Confronted with Disasters Expect from Government Officials and Public Leaders. Risk, Hazards & Crisis in Public Policy 10(1), 14-31 (2019). https://doi.org/10.1002/rhc3.12150.
5. Tagarev, T., Ratchev, V.: A Taxonomy of Crisis Management Functions. Sustainability 12(12), 5147 (2020). https://doi.org/10.3390/su12125147.
6. Caudle, S.: Homeland Security Capabilities-Based Planning: Lessons from the Defense Community. Homeland Security Affairs 1, Article 2 (2005). https://www.hsaj.org/articles/178.
7. Keim, M.E.: An innovative approach to capability-based emergency operations planning. Disaster Health, 1(1), 54-62 (2013), https://doi.org/10.4161/dish.23480.
8. Bradley, D.J.: Applying the THIRA to Special Events: A Framework for Capabilities-Based Planning Adoption in Local Governments. Thesis, Naval Postgraduate School, Monterey, CA, (2018), https://www.hsaj.org/articles/14939.
9. Nikolov, O.: Distributed Training, CAX and Experimentation in support of Crisis Management. Information & Security: An International Journal 27(2), 138-146 (2011). http://dx.doi.org/10.11610/isij.2713.
10. Nikolov, O., Tomov, N., Nikolova, I.: M&S Support for Crisis and Disaster Management Processes and Climate Change Implications. In: Murayama, Y., Velev, D., Zlateva, P., Gonza-lez, J.J. (eds.) Information Technology in Disaster Risk Reduction. ITDRR 2016. IFIP Ad-vances in Information and Communication Technology, vol 501, 240-253. Springer, Cham. https://doi.org/10.1007/978-3-319-68486-4_19.
11. Angevine, R.G.: Time to Revive Joint Concept Development and Experimentation. War on the Rocks, 23 January 2020, https://warontherocks.com/2020/01/time-to-revive-joint-concept-development-and-experimentation, las accessed 2020/10/26.
12. Izumi, T., Shaw, R., Ishiwatari, M., Djalante, R., Komino, T.: 30 innovations for disaster risk reduction. IRIDeS, Keio University, the University of Tokyo, UNU-IAS, CWS Japan, Japan (2019).
13. What is DRIVER+? https://www.driver-project.eu/driver-project/, last accessed 2020/10/24.
14. AeroSpace and Defence Industries Association of Europe: STACCATO Final Taxonomy, Deliverable 1.2.2, STACCATO (Stakeholders Platform for Supply chain Mapping, Market condition Analysis and Technologies Opportunities) project (2007).
15. Sveinsdottir, T., et al.: Taxonomy of Security Products, Systems and Services, Deliverable 1.2, CRISP (Project title: Evaluation and Certification Schemes for Security Products) project (2014).

16. European Defence Agency: EDA Technology Taxonomy Overview (n.d.), https://www.eda.europa.eu/docs/default-source/procurement/eda-technology-taxonomy.pdf, last accessed 2020/10/26.
17. Duran, L.: Safety and Security – Preventing cybersecurity attacks in safety systems. Hazardex (2015), http://www.hazardexonthenet.net/article/105606/Safety-and-Security-Preventing-cybersecurity-attacks-in-safety-systems.aspx, last accessed 2020/10/26.
18. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal L 345 (2008), 75–82, http://data.europa.eu/eli/dir/2008/114/oj.
19. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal L 194 (2016), pp. 1–30, http://data.europa.eu/eli/dir/2016/1148/oj.
20. Laurent Dubost et al.: Solution testing procedure. DRIVER+ Deliverable D934.21, https://www.driver-project.eu/wp-content/uploads/2018/08/DRIVERPLUS_D934.21_Solution-testing-procedure.pdf, last accessed 2020/10/26.