TECHNICAL REPORT

ISO/TR 22312

Societal security — Technological capabilities

Sécurité sociétale — Capacités technologiques

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 22312:2011
https://standards.iteh.ai/catalog/standards/sist/7d6ba0b4-c3d8-4bf8-bde0-
98f575e62f48/iso-tr-22312-2011

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TR 22312:2011
https://standards.iteh.ai/catalog/standards/sist/7d6ba0b4-c3d8-4bf8-bde0-
98f575e62f48/iso-tr-22312-2011

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 22312 was prepared by Technical Committee ISO/TC 223, *Societal Security*.

Introduction

In ISO/TC 223's business plan version 1 from 2006-11-24, the scope of ISO/TC 223 is defined as international standardization in the area of societal security, aimed at increasing crisis and continuity management and capabilities through technical, human, organization, operational, and management approaches as well as operational functionality and interoperability, as well as awareness amongst all interested parties and stakeholders.

ISO/TC 223 will work towards international standardization that provides protection from and response to risks of unintentionally, intentionally, and naturally caused crises and disasters that disrupt and have consequences on societal functions. The committee will use an all-hazards perspective covering the phases of emergency and crisis management before, during, and after a societal security incident.

ISO/TC 223 will address and supplement issues not currently addressed by other technical committees or international bodies with which ISO has formal agreements.

From this scope, it is clear that ISO/TC 223 has set its goals to develop International Standards in the area of societal security that will relate to crisis and continuity management from a number of different angles, among them the following:

— the cause of the crisis; the cause of the crisis relates to intentional (i.e. crime or terror), unintentional, i.e. accidents caused by persons, and natural;

— the phase of the crisis; the phase of the crisis is defined as before, during and after;

— the elements of the management of the crisis; these elements include technical, human, organizational, operational and management.

In addition, the scope of ISO/TC 223 is unique from a typical technical committee in that ISO/TC 223 has taken a holistic approach to the International Standards to be developed and the emphasis is on developing deliverables that will contribute to improving the resilience of society. The work is not to be focused on a specific type of International Standard, i.e. a management system, terms, a specification, or to be focused on a specific technological field or capability, but in regards to the contribution the International Standard has to the resilience of society with the condition that the subject of the International Standard is not currently being addressed by other technical committees or international bodies with whom ISO has formal agreements.

To achieve its goals, ISO/TC 223 has established, at the beginning of its activities, three working groups to develop a framework document, vocabulary and an incident management framework which was called command and control, coordination and cooperation. In addition to these three WGs, the TC established a task group which focused on setting a base for the development of relevant management system standards. This task group evolved and became a fourth WG which focused on developing management system International Standards for societal security related events, i.e. emergency management, crisis management, business continuity management. ISO/TC 223 did not focus on technical capabilities and the needs for technical International Standards until the establishment of the Ad-hoc group on societal security technological capabilities was created.

The need for including the development of technically oriented International Standards in the field of societal security in the scope of ISO/TC 223 was voiced and advocated by Israel from the stage when the first draft of the business plan was prepared. The logic was that the deliverables of ISO/TC 223 should give a complete solution for security and equipment and, therefore, security systems are a vital piece of the equation.

Based on this, in its 2008 spring plenary meeting held in Seoul, ISO/TC 223 passed a resolution to form the Ad-hoc group (AHG1) to conduct a six-month study in which the key societal security technological domains will be identified and recommendations made to the TC on how to deal with them.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Societal security — Technological capabilities

1   Scope

The purpose of this Technical Report is to document the knowledge accumulated in the six-month study period conducted by ISO/TC 223/Ad-hoc group 1 (AHG1), in which AHG1 examined the different existing available technologies which would be relevant to standardize within the field of societal security.

The terms of reference of the AHG1 are as follows:

— identify the "key technical domains" that are important for the work of the committee;

— recommend how the committee should deal with identified "key technical domains".

2   Existing international security standardization work

2.1   General

The AHG1 was formed and was comprised by a convenor and experts from within the P-members of ISO/TC 223. The first stage was to identify work being done by recognized Standards Development Organizations (SDOs) that can contribute to the mission of the AHG1. The activities that were identified are outlined in 2.2 to 2.5.

2.2   ANSI-Homeland Security Standards Panel (HSSP)

A number of workshops were organized to explore different elements related to homeland security while focusing on gaps and the contribution standards can have on the awareness and preparedness of society to meet security challenges. The workshops that were studied by the AHG1 included the Standardization Related to Biological and Chemical Threat Agents workshop, the Biometrics Standardization workshop, the Emergency Communications workshop, the Standardization for Enterprise Power Security and Continuity workshop, the Training Program Standardization for First Response to Weapons of Mass Destruction (WMD) Events workshop, the Perimeter Security workshop and the Transit Security Standardization workshop.

2.3   CEN BT/WG 161 Protection of the Citizen

At the request of the EU, CEN has established a strategic group to explore the different aspects of the security of the European public and determined where standardization can make a contribution. This group formed a number of expert groups whose report served as material and information for the AHG1. The reports used by the AHG1 include Critical Infrastructure – Buildings and Civil Engineering Works mini business; Chemical, Biological, Radiological and Nuclear (CBRN) business plan; Critical Infrastructure-Energy Supply final report; Supply chain final report; Integrated Border Management report; Water supply security mini business program; Emergency Services business plan; and the Defense against Terror (DAT) business plan.

2.4   ISO/IEC/ITU-T/SAG-S

ISO's Technical Management Board (TMB) established an Advisory Group on Security (AGS) to conduct a review of existing ISO deliverables related to the field of security, assess the needs of all relevant stakeholders for international security standards, assess relevant standards developed by other organizations

that may support international needs for security standards, and recommend actions to be taken by the ISO Council and/or ISO/TMB on subjects within the field of security that may benefit from the development of International Standards and that ISO would have the capability to provide. The final report was used by the AHG1.

2.5 Asian-Pacific Economic Cooperation (APEC) and Standards Australia initiative

Standards Australia and APEC initiated a survey whose results will be used to promote a better standards infrastructure for security Critical Infrastructure and Support Systems. The rational and background documents were used by the AHG1.

In addition to the above documentation, there are SDO's developing standards related to security at the national level such as SII and there are different industries with security related products that are exploring the possibility to promote the use of this type of equipment by identifying and setting standards for necessary capabilities that can be satisfied by using technologies.

3 Work being done in other technical committees within ISO, IEC and ITU-T

3.1 General

ISO/TC 223 will address and supplement issues not currently addressed by other technical committees or international bodies with which ISO has formal agreements. ISO/TC 223 will not initiate standards' projects that fall within the scope of existing TCs, whether ISO, IEC or ITU-T. The need for standards in the security domain has been noted by ISO, IEC and ITU-T and activities have been initiated. The outstanding initiatives are as follows.

3.2 ISO

ISO has formed an advisory group on security which was given the task to evaluate the gaps in security standardization and make recommendations to the TMB. Among the recommendations was the need to form a Strategic Advisory Group for Security (SAG-S). The report also lists the ISO/TCs that are involved in security. This list was revised by the ISO/IEC/ITU/SAG-S. The list of the ISO/TCs involved in security as stated in the AGS with the additional list as discussed in the SAG-S meeting is given in Annex A.

3.3 IEC

IEC submitted a report to the SAG-S in January 2008 showing the security activities in the IEC. The areas stated are alarm systems and access control. It should be noted that IEC/TC 79, Alarm Systems, is involved in security-related work which consists of the preparation of standards for detection, alarm and monitoring systems for protection of persons and property, and for elements used in these systems.

3.4 ITU-T

ITU-T has been running a security standardization program for several years. The areas in which ITU-T is focusing are tele-biometrics, security management, mobility security, cyber-security, home-networking security, NGN security, countering spam and emergency telecommunications.

4 AHG1 study methodology

4.1 General

Since this effort is the first step in introducing technical International Standards into the work of ISO/TC 223, the main objective is to locate key technical domains that contain products and technologies which are clearly candidates for standardization processes within ISO/TC 223. The International Standards which will be identified will have market relevance and be of interest to defined parties, including industry, regulators and

end users. Based on this, the technical International Standards to be in the focus of the AHG1 will have the attributes outlined in 4.2.

4.2 The key technical area's attributes

— The topic of the International Standard is not covered by any other International Standards' committee within ISO or other standards' organization such as the IEC or ITU-T.

— The technology or product subjected to being standardized is technically mature.

— The International Standard will focus on the function/performance (capabilities) requirements and not on procurement specification or product standardization.

— The International Standard will have market and global relevance.

— There are stakeholders with a specific interest in developing the International Standard (i.e. industry, academia, government and end users).

4.3 Method

4.3.1 General

The AHG1 was commissioned to identify the key technical domains that are applicable to societal security. In order to analyze the field of security, the AHG1 used a security model commonly used by the different SDOs in their pursuit of gaps to be filled by International Standards. See Figure 1.
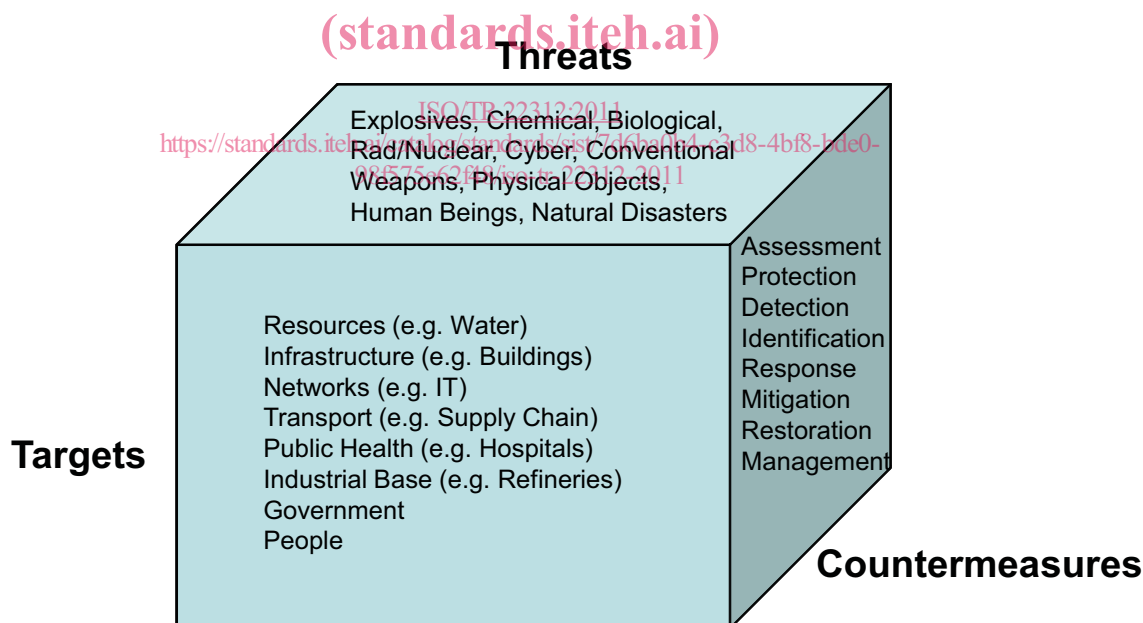

Figure 1 — Three-dimensional security gaps model

The model is based on defining three dimensions: targets, threats and phases of an incident; in the ISO/TMB/AGS the third dimension is called "countermeasures". The AHG1 added an additional dimension, the 4th dimension: basic security capabilities. The AHG1 compiled an exhaustive list for all four dimensions - drawing the roadmap. Based on this list, the AHG1 identified the technological capabilities. The AHG1 achieved this by the following steps outlined in 4.3.2 and 4.3.3.

4.3.2 Data collection

Much security standards gap analysis work has been done within standards development organizations. These documents and reports have been used by the AHG1 where relevant and used for compiling a list of the elements of the four dimensions mentioned above. The recommendations made in these documents has also been considered by the AHG1 when drafting recommendations for ISO/TC 223. The following is a partial list of sources and publications:

⎯ ISO/TMB/AGS, final report;

⎯ ANSI/HSSP, final reports from the workshops;

⎯ CEN/BT/WG 161, final business plans from nine expert groups and additional relevant documents;

⎯ Standards Australia, Critical infrastructure security standards survey;

⎯ APEC, Critical Infrastructure and Support Systems Standardization Project.

4.3.3 Analysis

The AHG1 compiled four lists, a list for each dimension. The AHG1 first compiled the lists of threats, targets and phases of an incident to focus the group, and then a list of technologies and technological capabilities to form the 4th dimension. Finally, the list of capabilities was examined and considered to be relevant based on the following parameters:

⎯ the capability of improving societal resilience;

⎯ the relevance of the work being done by ISO/TC 223;

⎯ the maturity of the market to supply products that meet the required capabilities;

⎯ the interest of the members of the AHG1 and other stakeholders in promoting the standardization of the capability in question.

To compile these lists, four teams were formed to address each of the lists.

5   Raw results

The list of threats is given in Figure 2, the list of targets is given in Figure 3 and the list of phases is given in Figure 4. Based on these three lists, a list of technologies, capabilities, equipment and technology was derived, as shown in Figure 5. This list was organized to form the list of technological capabilities to be presented to ISO/TC 223.

The conclusions of the AHG1 are actually the categories (first level nodes) in the list of capabilities as shown in Figure 5, i.e. surveillance, detection technologies. The additional nodes are a list of examples of specific systems or capabilities that are inclusive of the category and should be considered as examples that can clarify the scope of the recommend key technological field.
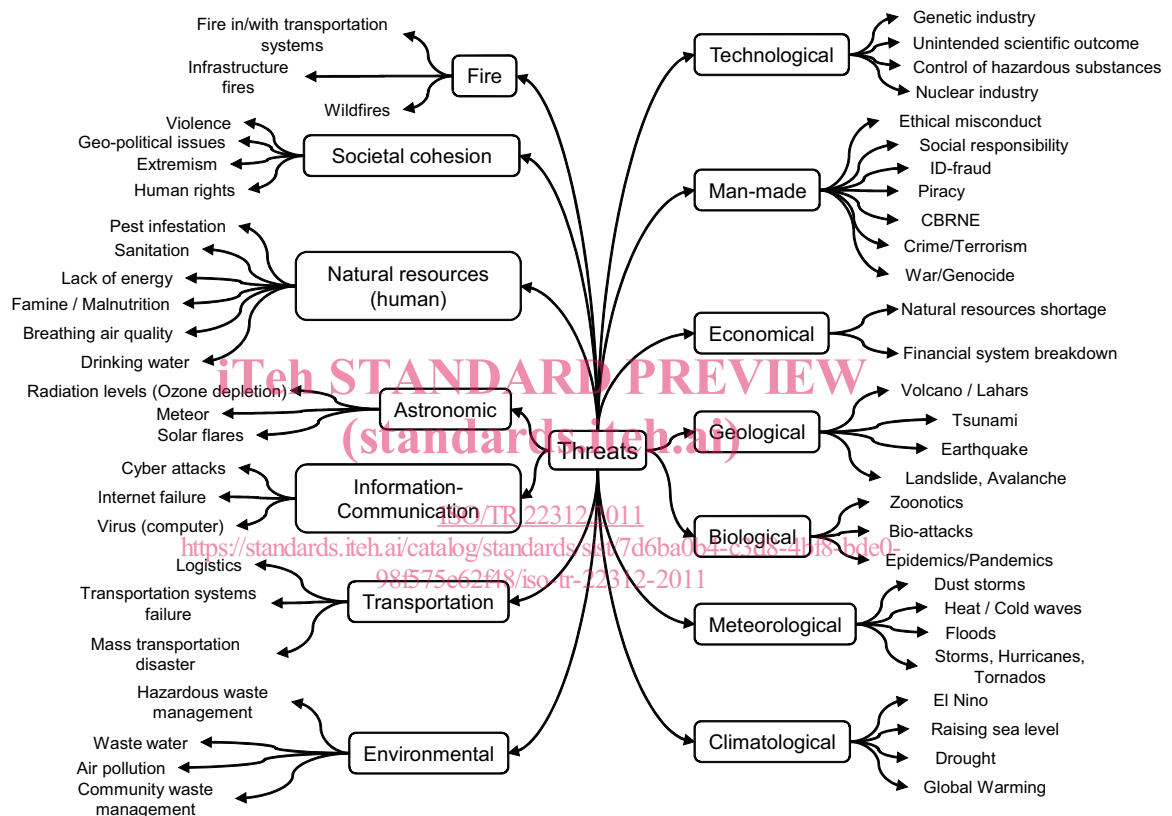
Figure 2 — List of threats