PREDICT

PREparing for the Domino effect in Crisis siTuations.

PROJECT SUMMARY

This project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-607697

PREDICT PROJECT SUMMARY
Coordinator: Kathrin Faber
Editor: Security Division, security@uic.org
Layout and production: Marina Grzanka, graphic designer, marina.grzanka@gmail.com
ISBN: 978-2-7461-2626-8

INTERNATIONAL UNION OF RAILWAYS

This summary is focused on the interests from the UIC-Members and gives them an overview about the main aspects and results from the PREDICT project. Detailed information and further material can be found on the website www.predict-project.eu. Otherwise, you can get directly in contact with the coordinator Dominique SÉRAFIN (dominique.serafin@cea.fr).

DESCRIPTION

"A small cause may have a big effect!" – Decision-makers in crisis situations and Critical Infrastructure (CI) organisations must consider many factors: political, social, legal, cultural, ethical and economic parameters are always to be considered during threat assessments and counter-measures. The increasing complexity of crisis and disasters have mobilized crisis management organisations and motivated the industry and the scientific community to create tools that will be able to help crisis managers to act more quickly and effectively.

The aim of the PREDICT project was to provide a comprehensive solution for dealing with cascading effects in multi-sectoral crisis situations covering aspects of critical infrastructures. The PREDICT integrated Tool Suite (iPDT) consists of a suite of decision support tools (DST) integrating different services facilitating foresight, prediction, communication and eventually decision making in crisis situation. This tool suite is based on improved and innovative methodologies, models and software tools. It aims to increase the awareness and understanding of cascading effects by crisis response organisations, enhance their preparedness and improve their capability to respond in case of cascading failures.

ORGANISATION

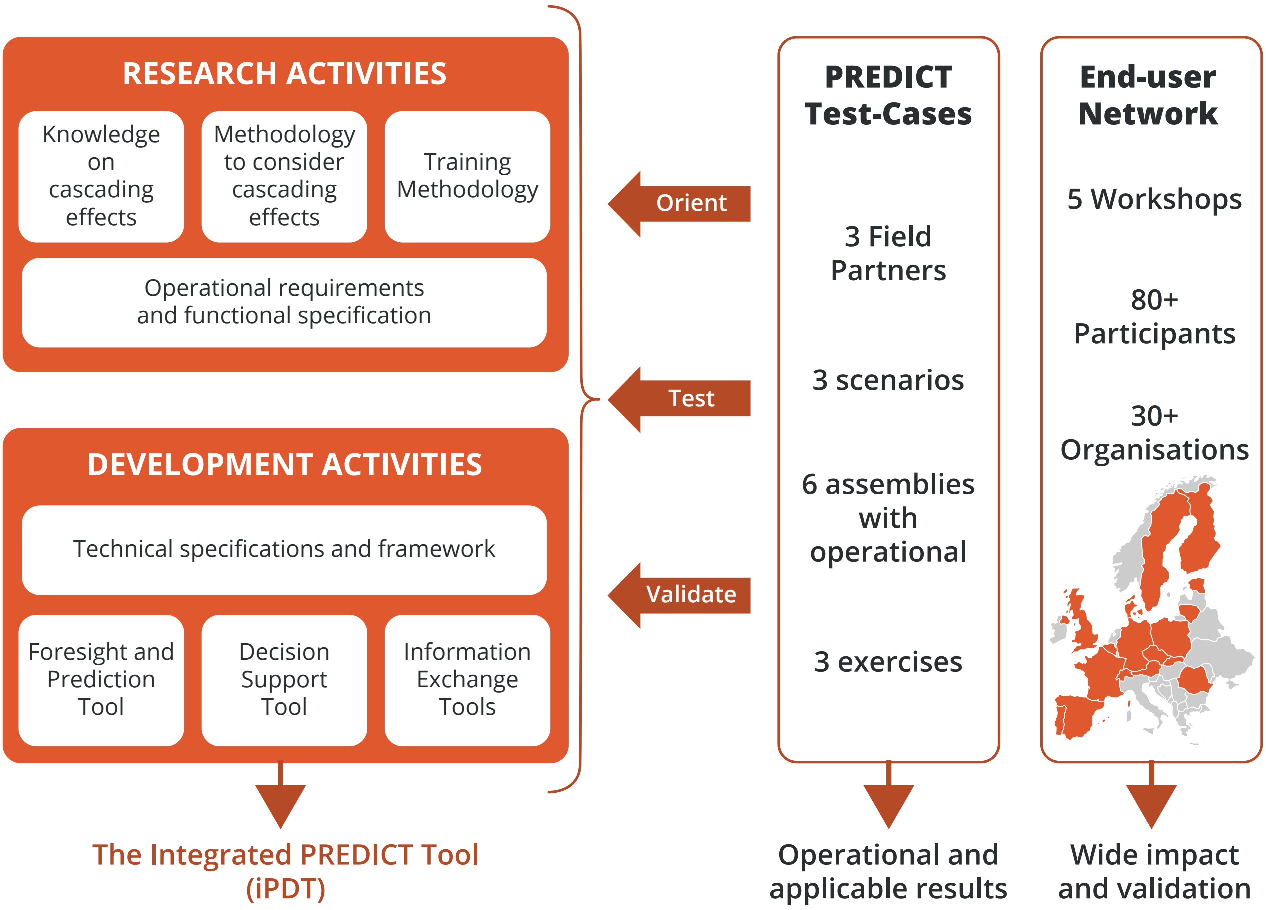


Figure 1: Organisation of the PREDICT project with continuous inputs from end-users

OBJECTIVES

01 Gather and analyse available domain knowledge

02 Develop a common framework

03 Create conceptual and executable models of cascading effects and interdependencies

04 Develop a suite of software tools

05 Validate the solution through running simulations in the framework of three test cases

06 Disseminate project results and build appropriate liaisons among stakeholders

FACTS AND FIGURES

Project Reference
607697

Coordinator
CEA

Starting date
1 April 2014 – 31 March 2017
(36 months)

Total budget
4.635.020,99€

Total EU funding
3.460.192,99€

PARTNERS AND METHODOLOGY

Figure 2: Projects partners

During the project, several activities and measures have enabled to reach the project goals.

KEY RESULTS

The PREDICT incident evolution framework

Which provides a threat quantification methodology allowing for the assessment of cascading effects and the modelling of interdependencies between CIs.

Improved version of tools

SBR (scenario reasoning)
A tool supporting the generation and analysis of most probable set of scenarios

PROCeed (scenario player)
Which enables crisis managers to model and simulate crisis scenarios

Myriad (decision analysis)
A tool supporting decision by risk-based assessment of the current and predicted situation

The Integrated PREDICT Tool Suite (iPDT)

Which successfully combined these tools to provide a solution enabling decision-makers to generate, run and analyse alternative scenarios of a given crisis, identify crucial dependencies between CIs and act with better understanding of the future.

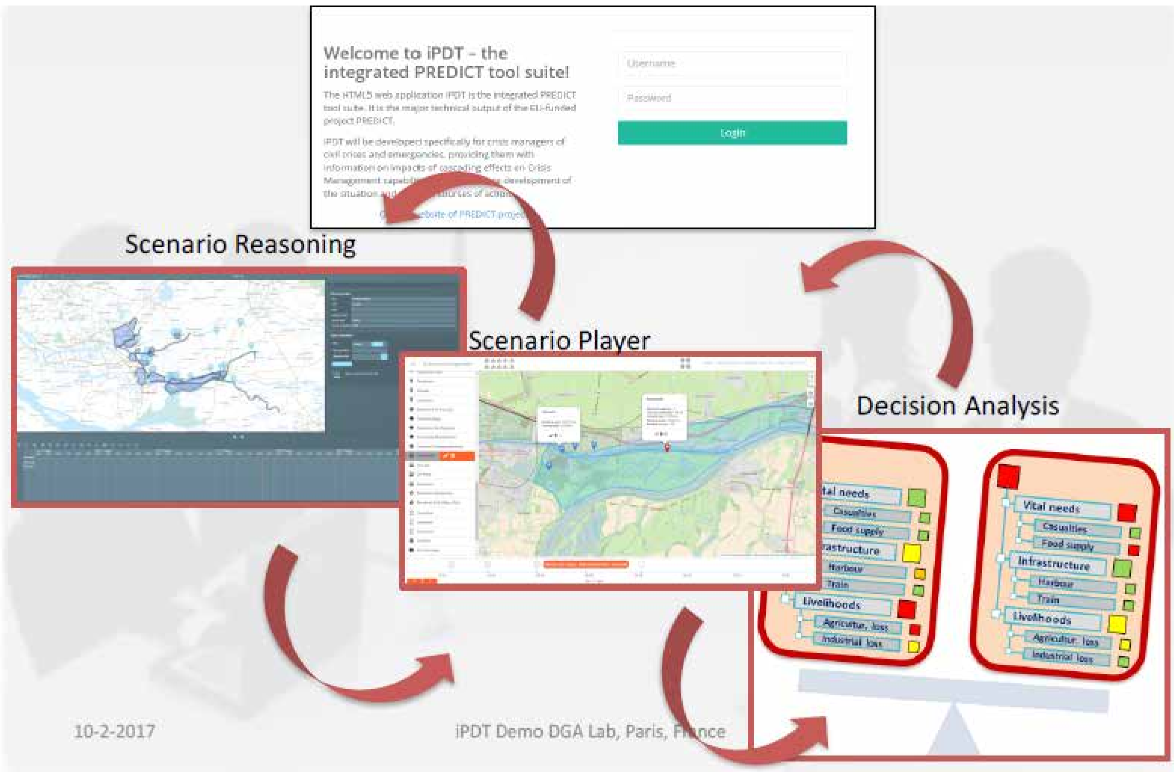


Figure 3: iPDT Components

Furthermore, PREDICT project has delivered a unique set of models and modelling approaches (including objects' classes, attributes, characteristics and dependencies), which proved to be applicable in three different scenarios (Flooding, Railway Incident and Maritime Incident).

SCENARIOS

The table 1 summarized the main aspects from all three cases, the case B – Railway accident is detailed afterwards.

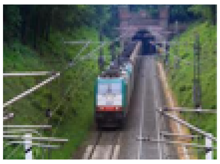
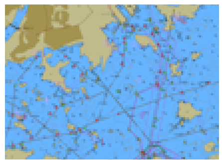
	FLOODING VRZHZ	RAILWAY INCIDENT UIC	MARITIME INCIDENT SYKE
SCENARIO			
TIME DIMENSIONS	Some warning days, potential dyle breach	Instant response to railway incident	Instant response on shipping incident
CHALLENGES	To evacuate or not ■ What kind of preparations ■ What kind of potential cascading effects	■ Railway traffic management ■ Potential impact on neighbouring (x-border) areas and people	■ chemical spill and threat to City ■ Search and Rescue Operations
SETTING	■ Demonstration of iPDT functions ■ Demonstration of use during a ROT-session ■ Evaluation and discussion	■ Functions of the iPDT were presented using a video walkthrough ■ Evaluation and discussion	■ Demonstration of iPDT functions ■ Use of iPDT functions in a training session ■ Evaluation and discussion

Table 1: Summary of PREDICT cases

RAILWAY INCIDENT

The railway emergency case occurs in Germany close to the "Dreilaenderpunkt", where the German, Belgium and Dutch borders meet, on the so called "Montzenroute". A freight train, bound for Belgium, consisting of 2 engines and 26 cars, loaded with hazardous chemicals is approaching the tunnel of Rheinartzkehl (one side in Germany, the other in Belgium). Out of unknown reasons the first engine derails, causing it to crash into the bridge. Due to the high momentum of the following engine and cars these are shoving the first engine diagonally over the rails, destroying the bridge and blocking the track completely. The second engine and most of the following cars are creating a large barrier, completely blocking the tunnel. Minutes later a second cargo train, inbound for Aachen is exiting the tunnel and crashing into the wreckage. The further chain of incidents leads to threaten the town of Aachen with fumes and smoke.

APPRAISAL

iPDT is an integrated system dedicated to crisis managers of civil crises and emergencies. One of the most important results of the project was the incident evolution framework. This framework aimed at relying on a generic methodology for understanding the incident evolution and the response operations that are needed to prevent potential cascading failures. This framework allows identifying the key elements that affect infrastructures and stakeholders during a crisis.

The functions of the iPDT have been carefully assessed against acknowledged training tool requirement. It has the potential to train end-users in awareness, understanding and decision making by visualization the impact of the decisions to the further development of the situation.

Please find below some of the identified benefits and limits of iPDT:

BENEFITS	LIMITS
Adaptability: The iPDT tool is still in an experimental phase (TRL 4 to 5) which means that it can be adapted and modified if necessary to address the needs of the market, companies and integrate new technologies. It is possible to edit an already defined scenario but also to create new scenarios. It depends on the situation the user is willing to train.	**Commercialization:** The IPDT is made of components with a TRL from 4 to 6 (prototype demonstrated in a relevant environment) and needs further development to be available for commercialization.
Usability: The iPDT is user-friendly and it is not difficult learning how to use the tool.	**Holistic:** The iPDT addresses problems with a focus on CIs while issues related to environmental background, societal and human events, crisis communication and social medias are left aside.
Versatility: It is possible to develop different scenarios, to compare many different types of crisis, etc.	**Adjustments:** Configuring the iPDT and including new scenarios, events or phenomena is a matter of expertise, time, and data. The necessary time depends on the complexity of the situation that the user is willing to configure. It also depends on the availability of the data. If it is assumed that the user's organization has already needed data, the issue is to turn this data into expertise. The tool could be bought with a service to deal with that.
Practicability: The iPDT has been developed in close collaboration with end-users and demonstrated during several workshops and demonstrations with these end-users.	**Updates:** Some data can easily be added directly into the Scenario Player. What is more difficult is the interdependencies needed for the decision analysis.
Availability: iPDT is an integrated solution that could be available online and easily available for end-users.	**Investment:** Support, updating and maintenance of the tool may involve several organisations.
Holistic: Similar solutions exists on the private sector but they generally focus on only one type of incident or crisis.	**Interoperability:** The iPDT is interoperable if a bi-directional communication channel can be established with the existing system. Often existing systems offers only outputs which is an obstacle for end-users to adopt new tools.

Table 2: Benefits & Weakness of iPDT

RESULTS – FURTHER ASPECTS

PREDICT considered a lot of interesting aspects to create the iPDT. In the following you will find more general Information, which could also be used in other security contexts.

TERMINOLOGY

To use the same terminology and have the same understanding of them is every time a big issue when people from different companies, units, etc. work together. The PREDICT project aims to get a better understanding of cascading effects in crisis situations. It focuses on cascading effects impacting critical infrastructures. The following definitions have been selected:

- **Cascading failures**: "A cascading failure occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure." (Rinaldi, 2001)
- **Critical Infrastructures**: "Critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (European Council Directive 2008/114/EC).

RISK ASSESSMENT

In classic risk assessments, engineers and experts use the concept availability and/or reliability. The concept of resilience is unusual for classic risk assessment. However, resilience - like availability/reliability - is strongly related to the system's quality of propagating failures amongst its different components/sub-systems and its recovery quality. One can't, then, model and simulate the resilience without treating the (inter)dependency aspects.

System safety & risk analysis focuses on the set of failures leading to the failure of a system, whatever the complexity of the system, in order to: enhance the system resistance to elementary failures, to decrease the occurrence frequency of failures, to decrease the shutdowns intervals and to mitigate the consequences of failures, on the system integrity and its environment. System safety & risk analysis looks at the time interval before and during the system's failure. Crisis management focuses on the interval during and after the system's failure. Still many approaches that have been developed for classic risk analysis can be very useful in M&S of resilience of complex systems.

That is why an important part of dealing with crisis situations is concerned with system safety & risk analysis concepts and methodologies. These topics are widely treated in literature in a very extensive manner. A brief summary of the content of those works is given in what follows. This literature review shows that the techniques of risk analysis and assessment can be classified into three main categories: qualitative, quantitative and hybrid.

Qualitative methods:

The qualitative techniques in risk analysis are based both on analytical estimation processes and on the safety manager-engineer's ability. Qualitative techniques include:

Checklists: Checklist analysis is a systematic evaluation against pre-established criteria in the form of one or more checklists, which are enumerations of questions about operation, organization, maintenance and other areas of installation safety concern.

What-if analysis: What-if analysis is an approach that: (i) uses broad, loosely structured questioning to postulate potential upsets that may result in accidents or system performance problems and (ii) determines what things can go wrong and judges the consequences of those situations occurring.

Safety audits: Safety audits are procedures by which operational safety programs of an installation, a process or a plant are inspected.

Task analysis: Task analysis is a process that analyses how field engineers and technicians perform the tasks in their work environment and how these tasks are refined into subtasks and describes how the operators interact both with the system itself and with other personnel in the system.

The Sequentially Timed Event Plotting (STEP) technique: The STEP technique provides a graphical overview of the timing and sequence of events and actions that contributed to an accident, or in other words, a reconstruction of the harm process by plotting the sequence of events that contributed to the accident.

The Hazard and Operability study (HAZOP) method: The HAZOP method is a formalized method to identify and document hazards through imaginative thinking.

Quantitative methods:

In quantitative techniques, risk may be expressed as a quantity, which can be estimated and described mathematically based on real systems failure data. Quantitative risk analysis is by essence probabilistic, on the overall system level, although it may use deterministic models to describe the failure modes and mechanisms of some components belonging to the system. The most widely used quantitative techniques include:

The proportional risk-assessment (PRAT) technique: The PRAT technique uses a proportional formula for calculating the quantified risk due to hazard.

The decision matrix risk-assessment (DMRA) technique: The DMRA technique is a systematic approach for estimating risks, which consists of measuring and categorizing risks based on an informed judgment of probability, consequence and relative importance (gravity).

Quantitative risk measures of societal risk: The societal risk associated with operation of given complex technical system is evaluated on the basis of a set of the triplet R = {Sk, Fk, Nk}, where Sk is kth accident scenario (usually representing an accident category) defined in the determined modelling process, Fk is the frequency of this scenario (expressed as a probability per time unit), and Nk denotes the consequences of kth scenario, i.e. potential losses (the number of injuries, fatalities or other hazard metrics).

The Quantitative Risk-Assessment (QRA) tool: The QRA tool has been developed for the external safety of industrial plants with a dust explosion hazard. However, the approach can still be applicable for other types of industrial systems.

Quantitative assessment of domino scenarios (QADS): The domino effect is perceived as an accident in which a primary event propagates to nearby equipment, triggering one or more secondary events resulting in overall consequences more severe than those of the primary event. A domino effect is then characterized by: propagation (dynamic) and amplification (of hazards).

The Clinical Risk and Error Analysis (CREA) method: The CREA method is a methodological approach to quantitative risk analysis, consisting of several steps based on techniques which are well established in industry that have been adapted for the medical domain.

The Predictive, Epistemic Approach (PEA) method: The PEA method is based on the so-called predictive, epistemic approach to risk assessment. It provides formal means for combining hard data and subjective information. It allows predicting the abnormal (accident-related) states of a given system with the help of mathematical models that quantify epistemic (state-of-knowledge) uncertainties in characteristics of the actions.

The weighted risk analysis (WRA): In order to balance safety measures with aspects, such as environmental, quality, and economical aspects, a weighted risk analysis is used. The weighted risk analysis is a tool comparing different risks, such as investments, economic loss and the loss of human lives, in one dimension (e.g. money), since both investments and economic loss are expressed solely in money.

Hybrid Methods:

The hybrid techniques present a great complexity due to their ad-hoc character that prevents a wide spreading. This group includes:

Human Error Analysis Techniques (HEAT) or Human Factor Event Analysis (HFEA): Human errors have become widely recognized as a major cause of serious accidents/incidents in a wide range of industries. A major drawback comes from the lack of: appropriate data and appropriate models describing human behaviour in normal and in crisis situations.

Fault-tree analysis (FTA): FTA is a deductive technique that focusses on one particular accident event and provides a method for determining causes of that event. It is of a great use for calculating non-dynamic failure models (degradation, ageing, interdependencies).

The Event Tree Analysis (ETA) technique: Event tree analysis is a technique that uses decision trees to logically develop visual models of the possible outcomes of an initiating event.

The Method Risk Based Maintenance (RBM): The RBM method is a comprehensive hybrid (quantitative/qualitative) technique for risk based maintenance that can be applied to all types of assets irrespective of their characteristics.

THREAT TAXONOMY

In total, this taxonomy (Luiijf & Klaver, 2006) contains over 140 natural threats, 145 human-induced threats and over 40 dependency threats to CIs. Table 3 shows a high-level summary of natural and human-induced threats. In the complete taxonomy, the threats are classified to several sublevels, branching to more detailed categorisation of various threats.

NATURAL THREATS	
GEOLOGICAL	Earthquake, landslide, volcanic activity, subsidence, erosion
AIR	High wind speed, absence of wind, high air temperature, low air temperature, high air humidity, low air humidity
PRECIPITATION	Snow, hail, rain, fog
WATER	High water levels, low water levels, high flow rates, low flow rates, high water temperature, low water temperature
SPACE	Meteorite impact, comet shock wave / collision
RADIATION	Electro-magnetic storm, earth-magnetic change, natural nuclear radiation, sun radiation bursts, cosmic high-energy particles
FIRE	Heat, smoke, toxic gases
BIOLOGICAL	Vegetation threats, bacterial threats, viral threats, animal threats, prion threats, fungal threats

HUMAN-INDUCED THREATS	
ECOLOGICAL	Soil contamination, air contamination, water contamination, troposphere contamination
ECONOMICAL	Diminishing stature, sale barriers, instable banking / economy, organisational problems, legal problems, disruption of conditional goods or services (dependency)
SOCIETAL	Civil disorder / riots, insurrections, political crises, strike / labour unrest, mass migration
PERSONAL	Lapse of attention, incompetence / training, missing or wrong information/ communication, organisational structure, criminal intent, epidemic illness
TECHNICAL / TECHNOLOGICAL	Force, fire, chemical, electro-magnetic, hardware, ICT

Table 3: High-level summary of taxonomy of natural and human-induced threats (Luiijf & Klaver, 2006)

MARKET ANALYSIS – DECISION SUPPORT SYSTEMS

The key aspect of Decision Support Systems (DSS) is that they provide information which are used in the decision-making process; the emphasis is not on the quantity of information, but rather on the quality.

Since mid-1960, DSS have transformed from automated systems for simplifying calculations into highly sophisticated arrangements combining hardware, software and human intelligence.

Theory developments evolved in the 70's with also the implementation of financial planning systems and spreadsheet-based DSS. In the 1980's, the Group DSS appeared. Together with data warehouses, executive information systems (EIS), OLAP and the business intelligence industry, the DSS market flourished in the early 1990's.

Today, the DSS market is almost exclusively web-based. Computerized decision support tools and software are expanding with new technologies like Internet of Things and Artificial Intelligence to create new applications and functionalities. These recent and on-going developments show that concepts and technologies are still evolving in this field as well as the potential to be exploited for DSS. The success and increasing use of DSSs in different sectors demonstrate the value of Information Technology to support decision making.

Due to this growing demand, Decision Support Systems (DSS) are numerous on today's security market. They are extensively applied in flood prevention and environmental disaster management1. They are used in pollution control, in water resources management and rationing, in flood control and forecasting, in agriculture for pest control, in forestry, in the prevention of epidemic diseases, etc.

DSS are mostly found in the private sector market. In general, industry builds the systems and devices used to prevent a crisis and help decision makers build a case to predict cascading effects to public entities.

The European industry has firms that specialize on DSS solutions mainly in the United Kingdom, the Nordic states like Sweden, Germany and France. For example, one of the most successful enterprises on DSS tools is Crisis Commander2, a Swedish company that owns a cloud-based software that specializes in crises and incident management. The tool has already been used by over 250 organizations and 40 countries. The company's software has been useful on major disasters like the cyclone in Myanmar in 2008, the hurricane Katrina and the London Subway Bombing. More recently, the software was used to help local authorities in Iceland to deal with a volcano eruption.

The international private sector mostly consists of the United States' market although Canada, Australia, Israel and China also possess a part of this market. The international private sector DSS market is more present on the large-scale disasters than the European one. Although there is a clear superiority on that aspect, Europe compensates with awareness on the subject and technological expertise.

[1] http://cdn.intechopen.com/pdfs-wm/6878.pdf

[2] http://www.crisiscommander.com/crisis-management-system/

TRAINING

Using a simulation tool for training allows manipulating specific aspects of the training. However, a training tool involves more than simulation. The major extension is the learning context of a training. For a simulation environment to be effective for training, it needs to have the following features (Pikaar and Buiel, 2008):

The task to be trained needs to be simulated realistically enough to actually make the transfer of the training. This requires a validated model of the system, process or task for which the training tool is designed.

The goal of the simulation is to reach pre-defined learning objectives, these will determine functions that are simulated within the training tool and the fidelity of the simulation.

The simulation must be used to evoke a learning process, in order to reach the learning objective, decisions must be made and actions must be undertaken by the trainee.

The simulation must confront the trainees with the consequences of their decisions and actions.

During the training the attitudes, knowledge and behaviour of the trainee needs to be monitored, influenced, assessed, analysed and eventually be provided with feedback. The simulation environment needs to support this.

When more than one system for simulation is used during the training, consistency over multiple systems is necessary.

To enhance preparedness, CI-operators, emergency managers and public authorities (on multiple levels) need to be trained in:

- creating awareness about failing CI,
- understanding of cascading scenarios and their impact on society,
- making decisions how to manage cascading effects and their impact on society and
- communicating with stakeholders about effects and measures to mitigate these effects.

It should also be acknowledged that for simulation to fulfil training needs, there is always a need for an instructor who guides the learning process and the after-action review. By use of simulation alone these needs can never be met (Sabel-Pikaar & Bloem, 2003).

Event Based Approach to Training (EBAT) is a systematic approach to develop a training and is characterized by introducing specific events in exercises. The events are targeted to evoke the behaviour that contributes to the knowledge and skill acquisition as described in the learning objectives.

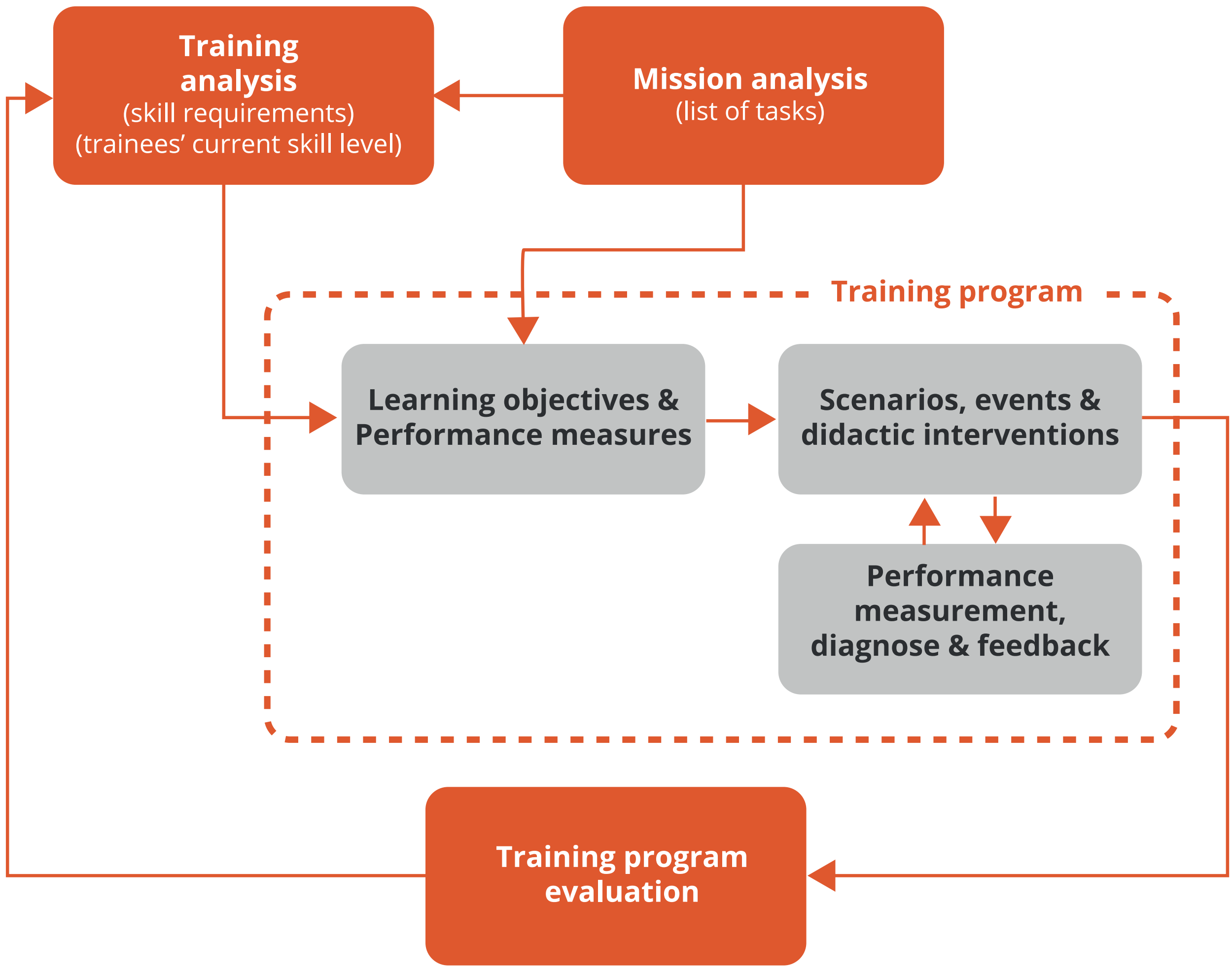


Figure 4: Event Based Approach to Training (inspired by Fowlkes et al. 1998)

In the exercise development process, there are four steps supported by four templates, each concerning a different detail level, together leading to the specification of an appropriate scenario for training:

STEP 1

Scope, goals and constraints

The purpose of this step is to define the scope of the exercise. Primary Questions are:

- What is your overarching training objective (e.g. create awareness of failing critical infrastructure and its impact on society)?
- What is your target audience (e.g. operational team, policy team)?
- Specify the key players in the training team (e.g. operational team: team leader; operational commander(s); liaison officer(s); communication officer; information manager)
- What are the constraints of the training?
  - » type of crisis as requested by the organisation to be trained (e.g. does it need to be a flooding scenario; an international scenario)
  - » the available resources for training (e.g. time, staff, equipment)

This step produces an explicit framework for the following steps.

STEP 2

Task analysis

The purpose of this step is to clarify the essential tasks that need to be practiced during the exercises. Which tasks will be the most important during an emergency or crisis depends on the nature of a crisis (e.g. flooding; terrorist attack) and the objectives of managing the crisis (e.g. evacuation; negotiating). When developing an exercise, the selected learning objectives should be represented in the tasks that are most important for that kind of crisis and the selected target group of the training, and as such these should be practiced during the exercise. A task analysis will clarify the essential tasks and is thus needed to focus the development of the exercise. In many situations, a lot of documentation on functions of personnel and responsibility of the teams is already available and may be of use here as a starting point. Furthermore, it should be noted that this information is fully or largely reusable for new exercises for the same target audience. The task-analysis table consists of seven columns:

- Role: The functional role of a particular player in the team (e.g. operational leader, leader of the fire fighters, representative of an energy company, information manager)
- Main Task: The higher-level tasks / responsibilities of the person’s role (generally consisting of multiple elementary subtasks)
- Subtask: The concrete tasks a person has to perform in order to accomplish the main task
- Input: The knowledge, information and resources needed to perform the task
- Complicating factors: Specify the conditions under which the tasks need to be performed adequately (e.g. under time pressure, when lacking information; at night)
- Output: The result of subtask performance
- Failure consequences: The effects that occur when a subtask is not performed adequately

This step produces a lot of information. It makes the tasks and subtasks of all involved roles explicit. In order to focus the exercise to be developed, it is advised to select a few of the most important tasks for further elaboration in Step 3 and further.

STEP 3

Specifying Training conditions

The purpose of this step is to specify the requirements that will ensure that a training successfully enables trainees to learn the subtasks identified in Step 2. The Training-Specification table consists of five columns:

- Subtask: The selected subtask(s) of Step 2
- The concrete learning objectives: What is learned when performing the subtask adequately
- Learning conditions: what is needed to create the circumstance in the exercise to achieve learning
- Complicating factors: Specify the conditions under which the tasks need to be learned. Conditions that can complicate the learning. For example, time pressure, incomplete information, conflicts of interest between participants.
- Required response: The behaviour associated with adequate task performance

This step produces the elements that are needed to design the (series of) scenarios that should bring about the concrete learning objectives specified here.

STEP 4

Scenario scripts

The purpose of this step is to develop a manual for the response cell (= staff playing key role players) and evaluators / observers to manage, steer and observe the exercise and thus create the intended circumstances that will enable the trainees to learn the concrete learning objectives. The Scenario-script table consists of five columns:

- Time: The moment in the exercise that an event has to occur
- Event: The event designed to trigger the intended activity of the trainee
- Information sources: The information sources available to, or obtainable by the trainee, related to the intended activity
- Considerations of trainee: The consideration(s) that the trainee needs to take into account in the activity
- Behavioural output: The behaviour that demonstrates that the intended activity has been performed

This step will lead to the design and execution of exercises that will enable learning the specified objectives.

Using some sort of structure to develop exercises and training is not new. The explicit match of learning objectives to scenario events and support tools is often not included in these structures and remain an implicit process.

LESSONS LEARNT & OUTLOOK

The increasing complexity of crisis and disasters have mobilized crisis management organisations and motivated the industry and the scientific community to create tools that will be able to help crisis managers to act more quickly and effectively.

The history of DSS covers a relatively brief span of years and the concepts and technologies are still evolving. Throughout the last decade, many advancements have been made in the DSS sector and the crisis management field. The progresses of science and technology will lead this sector to furthermore applications and utilities for future end-users. In the future, and with the newest technologies help, it is envisaged[3] that DSS will have a larger number of applications that will use data at an interim stage and where end-users won't have to constantly update the tool because the software will do it automatically. This will allow end-users to concentrate on the variables and the resulted different possible scenarios during a crisis.

The results of PREDICT and lessons learnt during the project shows that there are still room for collaboration between crisis management practitioners and the R&D community to help end-users better understand their operational needs about cascading effect mitigation and decision support tools, and to better understand how technology could contribute to meeting these needs. In this perspective, the PREDICT project has reached some interesting achievements and opened perspectives for the future.

[3] https://www.managementstudyguide.com/gaining-competitive-advantage-with-decision-support-systems.htm

PREparing for the Domino effect in Crisis siTuations.

PROJECT SUMMARY

www.predict-project.eu
www.cascadingeffects.eu

"The PREDICT project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013). The contents of this document and the view expressed in the publication are the sole responsibility of the author and under no circumstances can be regarded as reflecting the position of the European Union."