Ensuring acceptable levels of infrastructure related risks due to natural hazards with emphasis on conducting stress tests

Bryan T. Adey[1], Jürgen Hackl[1], Juan Carlos Lam[1], Pieter van Gelder[2], Peter Prak[3], Noel van Erp[2], Magnus Heitzler[4], Ionut Iosifescu[4], Lorenz Hurni[4]

[1]ETH Zurich, Institute of Construction and Infrastructure Management, Switzerland

[2]TU Delft, Safety and Security Group and PSCT, The Netherlands

[3]PSJ, The Netherlands

[4]ETH Zurich, Institute of Cartography and Geoinformation, Switzerland

Abstract: In this paper, a process to ensure that infrastructure is managed so that levels of infrastructure related risk due to natural hazards are acceptable, is presented. This is the proposed within Work Package 4 of the European Research Project “Novel indicators for identifying critical infrastructure at risk from natural hazards (INFRARISK)”. It consists of three main tasks, 1) *initiate*, 2) *conduct stress tests*, i.e. determine if there are acceptable levels of infrastructure related risk due to natural hazards, and, 3) *construct intervention program*, i.e., determine the risk reducing interventions to be executed to reduce the risk to acceptable levels. The process is described making appropriate references to four principles of systems engineering, a) follow a basic structured process for solving problems, b) work in phases, c) work from a high level to a low level of abstraction, and d) think in multiple possibilities. Emphasis is given on the second of the three main tasks: *conduct stress tests*. The process can be used for a wide range of natural hazards, infrastructure networks and at many different levels of abstraction. It can be used with and without computer support, and can take into consideration both simple and complex system representations.

1 Introduction

The main goal of infrastructure managers is to ensure that infrastructure provides an adequate level of service. This involves determining when and where to execute interventions on the infrastructure in a way that strikes an optimal balance between the costs and benefits incurred when no interventions are being executed and the costs and benefits incurred when interventions are being executed. These interventions include interventions to reduce the risks of inadequate levels of service due to natural hazards. Determining these interventions, which together constitute an intervention program, requires three main tasks, 1) *initiate*, 2) *conduct stress tests*[1], i.e., determine if there are acceptable levels of infrastructure related risk due to natural hazards, and 3) *construct intervention program*, i.e., determine the risk reducing interventions to be executed to reduce the risk to acceptable levels[2].

In this paper, the basic process proposed in Work Package 4 to do this within the European Research Project “Novel indicators for identifying critical infrastructure at risk from natural hazards (INFRARISK)”, with references to other work being done within the project is presented. It is an extension of the work presented in Adey et al., 2009, Adey et al., 2010, Adey et al., 2014 and Hackl et al., 2015. The process is complementary to many of the recent developments in the assessment of infrastructure related risk, e.g. Moini, 2015; Buritica Cortes et al., 2015; Dehgani et al., 2015;

[1] In general, there are two types of stress tests. The first type of stress test is a set of scenarios to determine whether the infrastructure related risks due to natural hazards are acceptable. The second type of stress test is the set of tests to be performed on part of a system to better analyse / model it in the process. Both are used in the process. To avoid confusion in this paper, the first type is referred to as a stress test, and the second is referred to as a test. A review of different types of stress tests can be found in [Avdeeva et al., 2014].

[2] An acceptable level of risk is one where the infrastructure manager is not required to execute interventions to reduce risk.

Nourzad, et al., 2015, to name a few. The big difference at this work is done from the perspective of an infrastructure manager who must decide one whether or not the level of infrastructure related risk is acceptable, and is interested in spending the least amount of effort possible to determine this. In other words, the focus is on the process.

The process is described making appropriate references to four principles of systems engineering, a) follow a basic structured process for solving problems, of which determining optimal risk reducing intervention programs is one, b) work in phases, c) work from a high level to a low level of abstraction, and d) think in possibilities. The process is composed of the three main tasks listed above. Emphasis is given on the second, i.e. *conduct stress tests*, for which the sub-tasks are 2.1) *define stress test*, 2.2*) determine approach*, 2.3) *define system representation*, 2.4) *estimate risk*, 2.5) *evaluate risk*, and 2.6) *determine parts of system to be analysed in more detail*. The first and third main tasks are subjects for future work. The process can be used for a wide range of natural hazards, infrastructure networks and at a wide range of details. It can be used with and without computer support, where an example of the latter will be supported in the INFRARISK project through the development of decision support software [Meachem et al., 2014]. It can also take into consideration both simple and complex system representations. As the INFRARISK project is not yet finished, the final process may have small variations to the one presented here.

This paper is structured as follows. Section 2 contains a description of the principles of system engineered used. Section 3 contains a description of the process. Section 4 contains an explanation of the sub-tasks within the *conduct stress test* task. Section 5 contains a discussion and the conclusions.

2 Principles

The four principles of systems engineering used to develop the process are presented in this section. They are a) follow a basic structured process to solve problems, of which determining optimal risk reducing intervention programs is one, b) work in phases, c) work from a high level to a low level of abstraction, and d) think in possibilities.

2.1 Follow a basic structured process to solve problems

The principle that you should follow a basic structured process to solve problems helps to ensure that you do not miss important tasks, you do not move too fast to a (sub-optimal) solution and you find the optimal solution to your problem. The process is illustrated in Figure 1, and the work in each of the tasks is summarised in Table 1. Please note that this process can be highly iterative, where at any point in the process one can return to an earlier phase if deemed necessary. The feedback loops are not shown for ease of reading.

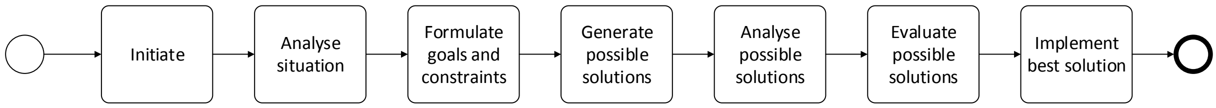


Figure 1. Illustration of the basic structured process to solve problems

Table 1. Work to be done in the problem solving process

Task	Goals	Work description
Initiate	To form general ideas of how the problem solving process should be formulated	Run through each of the tasks in the entire process in a short time frame.
Analyse situation	To clearly identify the problem	Gather all required information and consolidate this information into a clear description of the problem
Formulate goals and constraints	To formulate the goals and constraints to be used in searching for the optimal solution	Determine the things to achieve as far as possible, as well as the things that are not acceptable.
Generate possible solutions	To generate a list of possible solutions at an appropriate level of abstraction	Determine multiple technically possible solutions at an appropriate level of abstraction without detailed consideration of how well your goals will be achieved or whether or not the constraints will be met.
Analyse possible solutions	To determine the optimal solution in a narrow sense	Verify that each possible solution fulfils the constraints and assess how far each solutions achieves your goals using only the specific variables to be analysed.
Evaluate possible solutions	To evaluate the possible solutions in a wider sense	Evaluate the possible solutions taking results of the analysis with a wider perspective than used in the analysis, including rechecking the values used in the analysis and re-questioning all assumptions in the process.
Implement best solution	To make a decision and implement it	Decide which solution should be used, and implement it.

2.2 Work in phases

The principle that you should work in phases helps to ensure that you do not waste time and effort on doing unnecessary activities. Structuring work in phases gives people the opportunity to come together at appropriate points of time in the process to voice their opinions and make decisions. By doing so all people can agree on how to move forward so that no one later in the process can object to the decisions made earlier in the process, or they can at least do so in a formalised way. An example of the commonly used design and construct process divided into phases at two levels of abstraction is given in Figure 2.

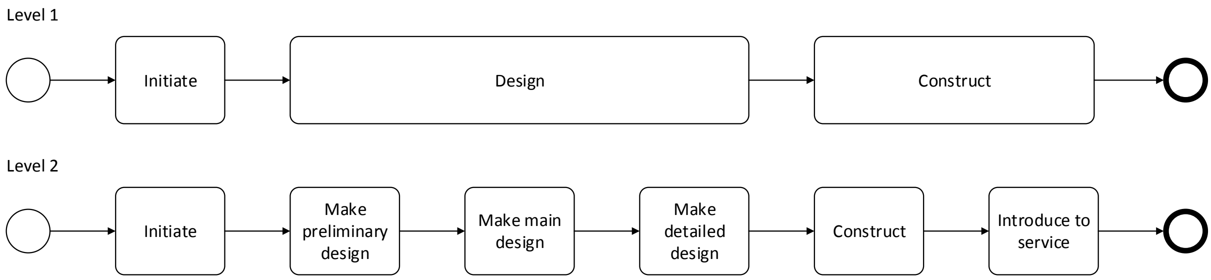
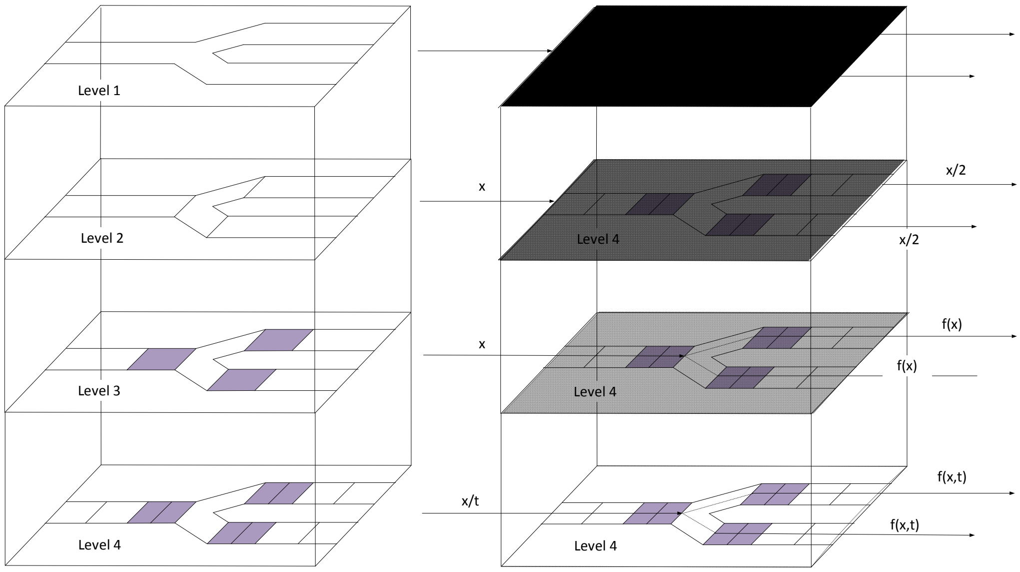


Figure 2. Illustration of the division of work divided into phases

It is important to note that the number or types of phases are of no particular importance, although it is generally useful to have them associated with the work to be done in each phase.

2.3 Work from a high level to a low level of abstraction

The principle that you should work from a high level of abstraction to a low level abstraction helps you ensure that the "big" general things are right before you spend time and effort working on "small" detailed things. Perhaps you have noticed in the previous section that the *design* task of the process in level 1 (Figure 2) was divided into *make preliminary design*, *make main design*, and *make detailed design* tasks. Here, one can imagine in the *make preliminary design* task that something is designed relatively approximately, in the *make main design* task, in more detail, and in the *make detailed design* task, to a level at which all information exists so that the object can be constructed. In other words, work is begun at a high level of abstraction and progresses to a low level of abstraction. This helps to ensure that time is not spent working on detailed things that might be a complete waste of time, when more general things have not been definitively decided. Basically, with this principle you are trying to get things right in general before you work out the details. Examples of how this principle can be understood, making use of the generic static and dynamic systems shown in Figure 3 are given in the next two sections.



Static perspective Dynamic perspective

Figure 3. Levels of abstraction of a generic system

As a civil engineer, when looking at the system from a static perspective, you can imagine here that you would like to ensure where a road (level 1) is going to be built before a lot of time is spent on estimating the capacity of the road sections to be included in the network (level 2) or even clearer, before a lot of time is spent on estimating the strength of the bearings (level 4) to be included in the bridge (level 3) that is to span a river that a road section of the network crosses.

As a civil engineer, when looking at the system from a dynamic perspective, you can imagine that once you are at level four from the static perspective that you are first curious as to how a road network within a region works. In this case, you would first be interested in where the cars enter the system and where they exit the system. Here you would again be looking at the road network at a very high level of abstraction, and some would say that you are looking at the road network of the region as a black box because no information is known that will help understand how the resulting flow is determined. Next, you might progress to understand how many vehicles enter the system at each entry point and how many leave the region at each exit point. In such a case, you are investigating the system at a lower level of abstraction, since more information is being obtained. Some would consider this to be a grey box because no details on how cars behave within the road network are given. You might then advance to an even lower level of abstraction and determine functions that represent the number of vehicles that would turn left at the intersections within the network, and the ones that turn right. You would then be looking at the system as an even lighter grey box as you have additional insights on the flow model. Once this information is obtained, you might advance to determining functions that incorporate the speed at which vehicles are travelling through the network, which would allow you to assess the traffic flow through the network in units of time, where travel speeds may be a function of the road configuration and condition as well as number of vehicles travelling on the network. This would be a white box because the behavior of cars is fully explained.

Perhaps you have already realised it, but what one defines as a black box, a grey box or a white box depends on how you are looking at the system. The descriptions above in no way mean that an assessment of where the physical shape of a network, e.g., cars enter and exit the system, is always to be considered as a black box. When analysing a dynamic system an analysis in which the system is treated as a black box is also sometimes referred to as being environmentally oriented, a grey box – as being effect oriented, and a white box as being structure oriented. The reference to environmentally oriented is used to emphasise that your interest is focused on the environment surrounding your system and how your system reacts with the environment. The reference to effect oriented is used to emphasise that your interest is focused on the effect that your system is having on the environment or vice versa. The reference to structure oriented is used to emphasise that your interest is how your system is structured and working.

2.4 Think of possibilities

The principle that one should think in possibilities helps to ensure that you, due to some embedded biases obtained from personal experience for example, do not omit the optimal solutions to your problems. Examples to facilitate the understanding of this principle are given in the following text for civil engineers, making use of Figure 3.

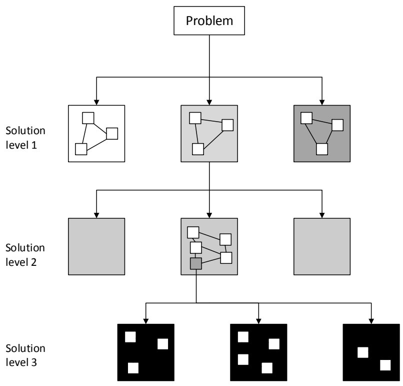


Figure 4. Illustration of multiple possibilities at multiple levels of abstraction

As a civil engineer, you can imagine being given the challenge to build a dam. If so a reasonable first project phase would be to investigate in general what type of dam should be built, e.g. an earth dam, a concrete gravity dam or a concrete arch dam. In determining what type of dam should be built you should not from the start simply decide to build a concrete dam because you like concrete. It might be that an earth dam would be much cheaper and more environmentally friendly, even if perhaps, at least to you, not as beautiful. If your analysis in this phase shows that a concrete dam is indeed the best of the general possibilities (level 1) than in the next phase of the analysis you can analyse variations of concrete dams (level 2). Again, you should not select a specific type of concrete dam without giving thought to other, perhaps more beneficial, possibilities. Once the type of concrete dam is selected you can progress to the next level of analysis which may involve the investigation of multiple types of valves to be used in the dam. This would continue until all details of the dam are selected.

The principle of think of multiple possibilities is one, which will help ensure that each time you are confronted with a problem you will think of multiple possible solutions at the appropriate level of abstraction and assess which one of these is best, before moving on to a more detailed level of abstraction or the next problem. Making use of this principle will help ensure that you find the best solutions to problems.

3 Process

3.1 General

The proposed process to modify a system to ensure acceptable levels of infrastructure related risks due to natural hazards is shown at the highest level of abstraction, alongside the problem solving process, in Figure 5. It is compatible with the even higher level process for assessing and evaluating risk proposed in [ISO 31000, 2009] and is consistent with the principle of following a basic structured process to solve problems.

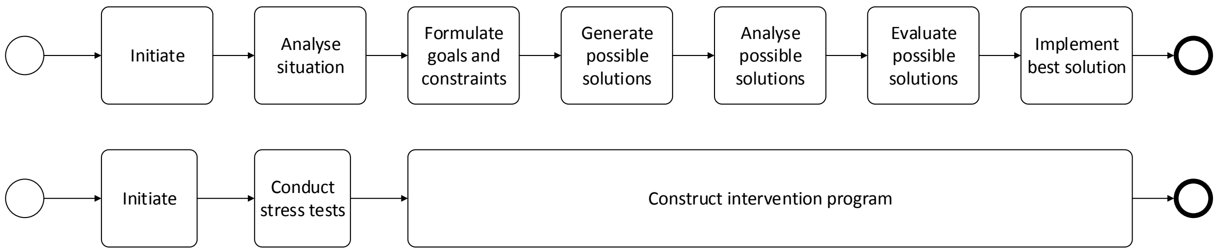


Figure 5. Process

Following the principle of work in phases, work is grouped and decisions are made stepwise, at each level of abstraction with which work is done. You can see this even at the highest level (Figure 5), as the stress tests are conducted and completed before work begins on constructing the intervention program. You can see it even better in section 4 where the iterations within the conduct stress test task are explained, i.e. the stress tests are first done at a high level of abstraction and then, if decision makers are not happy with this once they see the results, redone at a lower level of abstraction.

The principle of think of possibilities is followed, for example, in that in the initiate phase you are to think through the multiple ways in which you can envision doing the stress tests, and in the multiple ways you would like to stress test the system. You will notice examples of this principle at each step in the process at each level of abstraction.

The process is constructed keeping in mind that for more detailed quantitative evaluations, computer support will be required. The tasks within the process are explained in the following subsections, with each subsection being labelled with the task name when it is being discussed.

As it is possible during each task that you might discover that work done earlier in the process is not correct, or no longer the way you would like it to be, it is possible to return to an earlier part of the process and make appropriate adjustments. To avoid clutter in the diagrams and redundancy in the text, these returns are only shown / discussed when particular emphasis on them is desired.

3.2 Initiate

The *initiate* task is required to form general ideas of how the entire process is to be conducted. The work done in this task is the generation of first thoughts on all tasks to come, in both the *conduct stress test* and *construct intervention program* tasks. In the *stress test* task, this includes generating first thoughts on, for example, the levels of abstraction and the models and software to be used to determine if the infrastructure related risks are acceptable. This task is to take a relatively short amount of time when compared to the expected amount of time for the entire process, e.g. 10%. This task ends with a clear, or at least clearer, idea of what is to be included in each iteration of the process to ensure acceptable levels of infrastructure related risk due to natural hazards. The task is ended when the decision is made to go further with the process and formally conduct stress tests. This might coincide, for example, with giving a contract to an external company to conduct stress tests.

At this point it is worthwhile to explain, at least generally, what an acceptable level of risk is, beyond that is one where the infrastructure manager is not required to execute interventions to reduce risk. The level of risk that is considered acceptable varies from situation to situation. For example, it depends on whether there are possibilities to reduce the risk and how costly these are. This concept is sometimes referred to as the economically optimal level of risk, and was first proposed in the safety science domain by van Danzig, 1956. He referred to the acceptable level of risk as being the one where the sum of the costs for a safer system were equal to the expected value of the damage.

In addition to this method others such as Jonkman et al., 2006 have proposed to determine acceptable risk levels by comparing the actual risk with norms on individual - and societal risk, where individual risk indicates the distribution of the risk over the potentially affected individuals, and societal risk describes the relationship between frequency and the number of people suffering from a specified level of harm. The acceptable level of risk is considered to be one that is below that described in norms.

3.3 Conduct stress tests

In the *conduct stress test* task in the process you determine whether the level of infrastructure related risk due to natural hazard is acceptable. This step consists of stress testing the system by simulating its behaviour in specific situations and estimating and evaluating the risk. The system is to be modelled first at a relatively high level of abstraction and then repeatedly at increasingly lower levels of abstraction, until it is decided that the level of risk is either acceptable or not. At appropriate iterations in the process, tests on parts of the system can be required to ensure that appropriate models are used. Once decided if the system passes or fails the stress tests, the process continues to the *construct intervention program* task in the process. If the risk is acceptable, the intervention program contains no interventions. If the risk is not acceptable, the interventions to be included in the intervention program are determined. The sub-tasks are 1) *define the stress tests*, 2) *determine approach*, 3) *define system representation*, including the definition / determination of the system boundaries, events, scenarios, relationships between events, and models, 4) *estimate risk*, and 5) *evaluate risk*. These sub-tasks are explained in section 4.

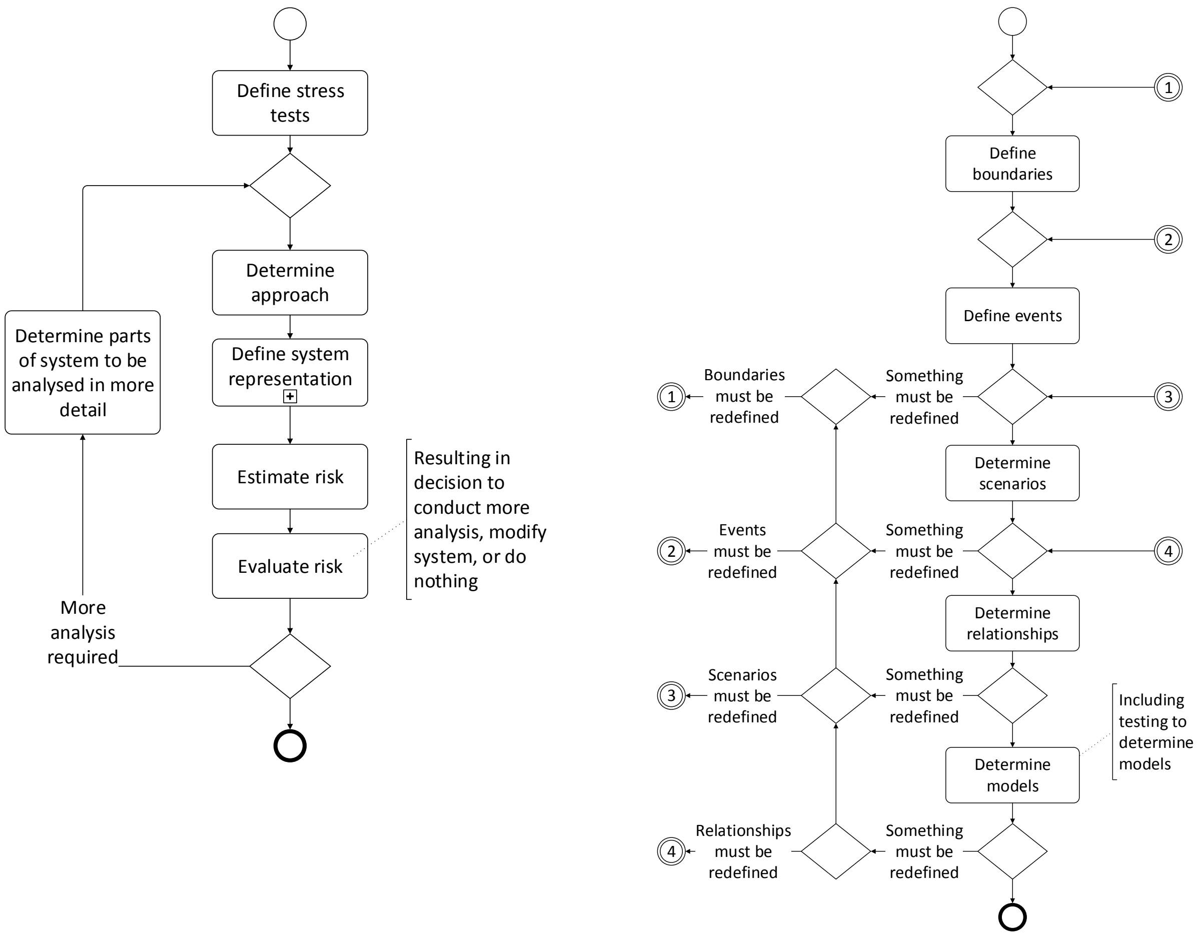
3.4 Construct intervention program

If decided that the risk level is not acceptable, then an intervention program needs to be constructed that will bring down the risk level to an acceptable level. The interventions included in the intervention program may be on any part of the system, e.g. the diverting of a river so it does not come in contact with infrastructure during a flood, the strengthening of infrastructure so that it can resist the flood waters during a flood, and the construction of a second road so that there is little disruption to traffic flow if the first road is washed out from flood waters. The planned interventions cannot require the use of more resources than are available and ideally will use the available resources optimally. The basic subtasks are 1) *identify the possible interventions*, 2) *identify the possible intervention programs*, 3) *determine the risk reduction if each intervention program is implemented*, 4) *identify the constraints*, 5) *identify synergies associated with each intervention program*, 6) *determine the intervention program to be implemented taking into consideration the constraints and synergies*. This task ends with the implementation of the agreed upon intervention program to bring the infrastructure related risk to an acceptable level. Descriptions of these tasks will be included in future work.

4 Conduct stress tests

4.1 General

The *conduct stress test* task is described in Figure 6. The process has been constructed keeping in mind that different decision situations will require different types of models and models that will provide different levels of detail, as well as the fact that in many cases it is desirable to conduct stress tests iteratively. This is consistent with the principles of working in phases, e.g., qualitative analysis over a short period of time first, quantitative analysis over a longer period of time later if required, working from a higher level of abstraction to a lower level of abstraction, e.g., first analysis deliver less detailed information, and later analysis deliver more detailed information, and thinking in possibilities, e.g., there are many possible stress tests to conduct and many ways to perform stress tests once they are set.



a) Conduct stress test

b) Define system representation

Figure 6. Stress test process

4.2 Define stress test

The *define stress test* task is to determine what needs to be checked to be able to say that there are acceptable levels of infrastructure related risks due to natural hazards or that risk reducing interventions need to be planned and executed. This includes the definition of what the acceptable levels of risk are, e.g. there is an acceptable level of infrastructure related risk due to earthquakes if an earthquake of magnitude 8 does not collectively cause losses in infrastructure restoration costs and lost travel time in access of 1 % of GDP. This task includes the generation of preliminary thoughts on the area to investigate and the time period to be considered. It will affect the definition of the system representation, and the requirements to conduct the stress test, in terms of both input, e.g. man-power, and output, e.g. the accuracy of the results or the number and types of scenarios to be investigated. It will also affect the scope and the level of detail of the assessment. Particular thought needs to be given here to the levels at which the stress tests need to be conducted, e.g. do you want to have a cumulative risk due to both floods and earthquakes below a threshold value, or do you want to have the risk due to floods below one threshold value, and the risk due to earthquakes below another threshold value, or both.

The definition of the stress tests is a difficult task in that it requires multiple persons bringing together their opinions and feelings into multiple coherent questions to be answered. In this task, it is often realised that although there is a general agreement to what the problem, which was perhaps determined in the initiate step of the process, is there are many differences as to why there might be unacceptable levels of infrastructure related risks due to natural hazards, i.e. which stress tests, and how the stress test should be conducted. Structured brain storming such as that conducted in general morphological analysis [Ritchey, 1998] is often helpful, especially when groups of people with substantially different opinions and backgrounds are involved. It is also often useful to scan large databases, such as that develop by [Gavin et al., 2014], to have an idea as to what scenarios could be of particular interest. Descriptions of what can be found in such databases in the case of infrastructure related risk due to natural hazards can be found in [Cheng et al., 2014].

This task results in a set of clear questions which, once answered, will either tell you that the current levels of infrastructure related risks due to natural hazards are acceptable or, alternatively, that risk reducing interventions need to be planned and executed

4.3 Determine approach

The *determine approach* task involves making numerous decisions about how the stress tests will be conducted. These decisions include 1) which type of approach, e.g. qualitative, semi-quantitative or a quantitative approach will be used, in which form, and at what point in the process, 2) whether or not computer support will be used, and if yes, which form and at what point in the process, and 3) the level of involvement of representatives from different stakeholder groups, in which form and at what point in the process. It also involves decisions about how multiple risks are to be aggregated.

4.4 Define system representation

The *define system representation* task involves 1) defining the boundaries of the system both spatially and temporally, 2) defining the events to be included, 3) defining the relationships between the events, and 4) the scenarios to be considered. Remembering the principle to work from a high level of abstraction to a low level of abstraction, the type and number of events considered vary depending on the level of detail required in the analyses / model. This means, for example, that the infrastructure events to be included in a first iteration of the process might be defined through modelling a 10 km road link as 3 bridges, 4 road sections and a tunnel, which can each either be working or not working. In the second iteration of the process the infrastructure events to be included might be defined through modelling the 10 km road link as in the first iteration, except subdividing each of the bridges into elements, such as columns, bearings, decks and abutments.

Although some thought has been given to each of these sub-tasks in each of the previous sub-tasks, you end each sub-task by making a clear statement as to what you think. As it is impossible to take into consideration everything perfectly simultaneously, it is also impossible to imagine that the *define system representation* task is one that you will done without many loops. This is emphasised by drawing in the loops in Figure 6b. Each of the sub-tasks are explained in the following subsections.

4.4.1 Define boundaries

The *define boundaries* task involves defining the system that is going to be analysed / modelled, both spatially and temporally. This system includes all things required to determine if there are acceptable levels of infrastructure related risk due to natural hazards, including the natural environment, e.g. amount of rain, amount of water in rivers, the physical infrastructure, e.g. the behaviour of a bridge when subjected to high water levels, and human behaviour, e.g. traffic patterns when a road bridge is no longer functioning. As it is necessary to model the system over time, it is also necessary to model the spatial and temporal correlation between events and activities within the investigated time period. This includes the consideration of assumptions, agreements as to how the system will react in specific situations, and the consideration of cascading events.

It should be kept in mind that conducting stress tests requires taking into consideration realisations of all relevant stochastic processes within the investigated time period. This in turn requires that models be built that are sufficiently good representations of the hazards, infrastructure, and consequences, as well as the interactions between them so that there is an appropriate understanding of the system and that the risks and the effectiveness of the intervention programs can be determined.

The definition of spatial boundaries defines the part of the natural and man-made environment to be specifically analysed / modeled, as well as how it is to be subdivided. This includes the definition of where the objects are located, where the source and hazard events can occur, and where the consequences could take place. The spatial boundaries are different depending on the part of the system being analysed. For example, the infrastructure to be considered might be that inside the physical boundaries of a city, but the rainfall to be considered might be that of a catchment area that is much larger than the physical boundaries of the city.

It is usually easy to specify the possible locations of the events, hazards and objects that are of direct concern. It is more difficult, however, to specify the locations of the events, hazards, and objects that might be included in the scenarios to be analysed in a stress test. This is more difficult because it is required to think through scenarios, in which there are events that you might not have yet identified. For example, you are interested in the flooding of a region, which might happen because a dam far up the river, in a region outside your originally defined area, fails. This becomes even more difficult when the location of possible consequences is to be specified. Consequences can be far away from the location of the events, hazards, and infrastructure, and may be outside the direct area of responsibility of the infrastructure manager, e.g., the collapse of a highway bridge on a trans-European highway network can have consequences on the free flow of goods in many countries.

The definition of the temporal boundaries defines the time period over which the natural and man-made environment to be specifically analysed / modelled, as well as how this time period is to be sub-divided. It is worthwhile to emphasise that a system can be analysed / modelled as being static or dynamic. When the system is analysed / modelled as being static, the changes over time are not considered, e.g. the growth in traffic flow. When it is analysed / modelled as being dynamic, they are. The decision on which is used is situation dependent.

As with the spatial boundaries, the temporal boundaries are different depending on the part of the system being analysed. For example, the rainfall event to be considered might be the maximum to occur in the upcoming year, but the consequences of this event might be measured over the following two years after its occurrence, or until the system is restored to normal.

This task ends with clear definitions of the spatial and temporal boundaries of each part of the system to be analysed.

4.4.2 Define events

The *define events* task involves identification of all events (cascading and non-cascading) that are to be analysed / modelled. These events are, in general, grouped from source events to societal events. Source events are ones that, at least from a modelling perspective, are considered to simply happen. Societal events are events to which human activity can be associated and, therefore, can be quantified when estimating risk. All events other than the societal events are only precursors to societal events and cannot be directly quantified in the estimation of risk.

Although the number of element types considered can vary depending on the specific type of problem and the desired level of detail in the analysis / model, the five basic types of events considered are source events, hazard events, infrastructure events, network use events, and societal events. All events are described in space and time, and measures of the intensities of interest should be given. The areas range from local, e.g., a tunnel collapse, to global, e.g., to traffic patterns being interrupted across Europe. The time periods range from a few seconds, e.g., earthquake to over a few days, e.g. flood, to several months, e.g., heat waves. Measures of the intensities of the events should represent the values of event attributes that are of interest. The number of intensity measures used to describe the events depends on the problem investigated and the level of detail required in the analysis. Details are given in Table 2. Additional examples of hazard events are given in D'Ayala et al., 2014.

The necessary detail to be used depends on the specific problem and the level of detail desired. If events at any level, or complete ranges of the values of intensity measures are excluded, it should be explicitly explained and documented why, because in the following risk estimation, the risk coming from those events will be excluded.

This task ends with the generation of a list of all events to be included in the system representation.

Table 2. Basic event types

Event type	Description	Examples	Comments	Example intensity measures
Source	An event that may lead to a hazard event.	Rainfall, Tectonic plate movement	It is the first event in a scenario that will lead to a societal event. A source event may also be referred to as an initiating event.	For a rainfall source event, rainfall of pattern *x* with water per minute of over y mm^2/s for more than 5 hours.
Hazard	An event that may lead to an infrastructure event. A hazard event may also be referred to as a load event.	Flood, Earthquake, Landslide	A hazard event is normally considered to have source event, but is sometimes modelled directly as a source event itself. In addition to leading to an infrastructure event, a hazard event may also lead to another hazard event, e.g. earthquake triggers landslide.	For a flood hazard event, water levels reaching x m depth in locations a, b and c, and amounts of water per second coming in contact with bridge *i* over $j\ m^3/s$.
Infra-structure	An event that is a change in the infrastructure that may lead to a change in infrastructure use or a change in human behaviour	The state of all infrastructure objects being considered during at each instance of time during a flood	In the determination of the infrastructure events thought must be given to which infrastructure object is affected by which hazard and the likely condition states that the object may have if subjected to a hazard. This is a difficult task as in many cases many objects could be affected but the effect might range from very small, e.g. yielding of a reinforcement bar in a bridge during an earthquake, to very large, e.g. collapse of the bridge.	For a bridge collapse, damage resulting in full closure of the road, damage results in the closure of one lane of traffic, damage resulting in no closure of the road.
Network use	An event that is a change in how the infrastructure is used that may lead to a change in human behaviour	The state of use of the network following closure of part of the network.	The probabilities of these events occurring are particularly difficult to estimate as their occurrence depends on spatial and temporal correlation, and physical relationships between initiating events, hazards and infrastructure events. The latter, which can lead to cascading events.	For example, due the freight corridor between Rotterdam and Genoa being closed 50% of goods is put onto trucks, 40% of goods is diverted over other train routes and 10% is not delivered.
Societal	An event that is a change in human behaviour	The actions of persons or groups of persons to which a value can be placed	In order to model the actions of persons or groups of persons it is often beneficial to group them into categories based on their general behavior, which in turn is coupled with how their behavior is to be modelled. Societal events may lead to other societal events. If they, however, do not then a value needs to be assigned to the event. This value then enters the risk assessment as a consequence.	Amounts an infrastructure manager spends on reconstruction amounts users spend in additional travel time

4.4.3 Define scenarios

The *define scenario* task involves linking the events together from the source events to the societal events, in the form of an event tree. A very simple example is given in Figure 7. A very simple example is used for clarity, but it should be clear that the event trees required in most situations will have many more branches and many more sub-categories of the events used in Figure 7. To build the event tree it is necessary to determine the value of the intensity measures defined in the *define events* task that will provide clarity on how events are considered to be related. The identification of the scenarios should be done in this task without an explicit estimation of their probability of occurrence or putting a value on the consequences.

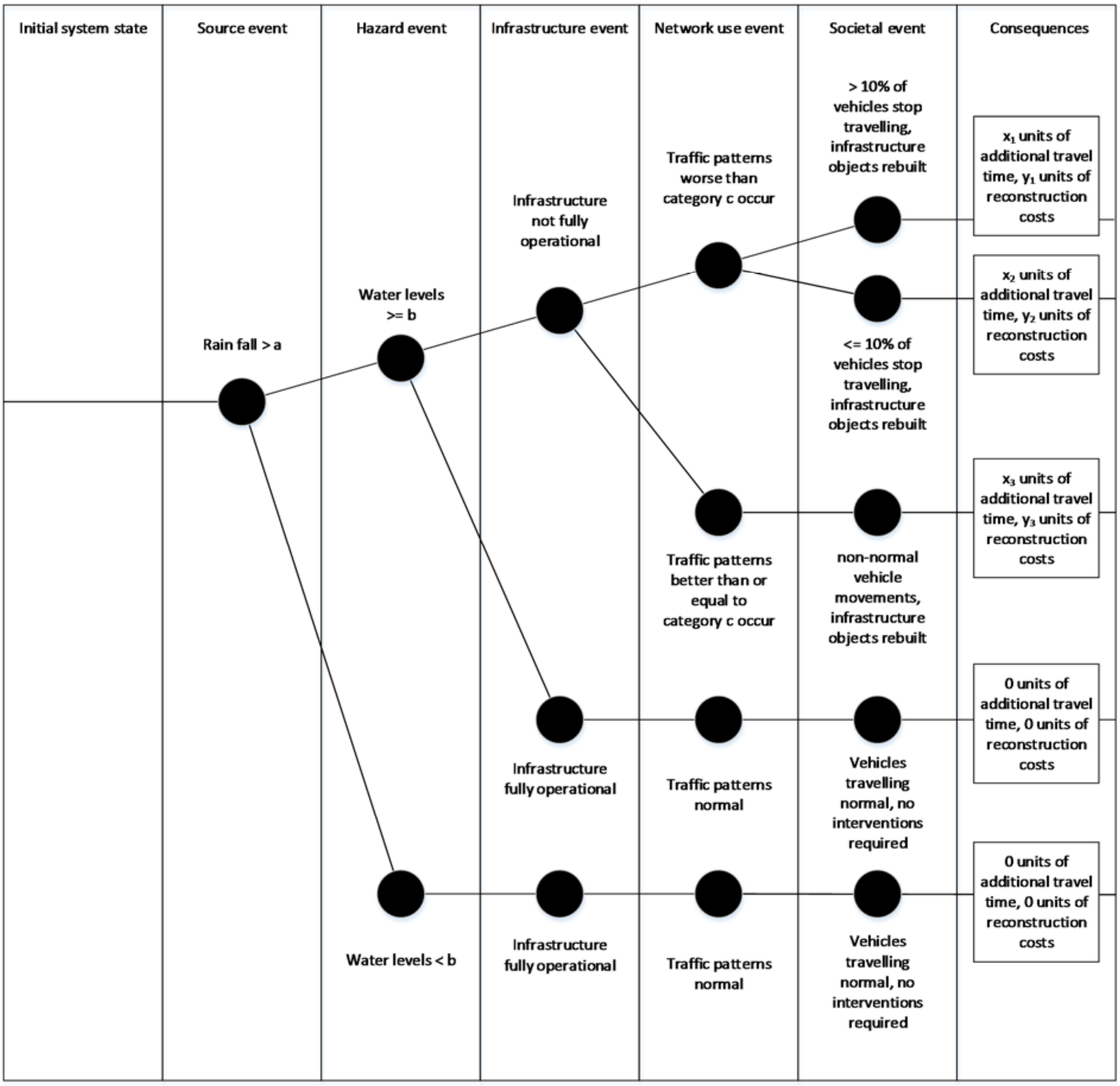


Figure 7. Example of a simple event tree for the definition of scenarios

As you can imagine, for each system representation there are an infinite number of scenarios, i.e. an infinite number of ways for reality to unfold, and an infinite number of ways to represent these scenarios, i.e. an infinite number of ways to represent reality. Particular care needs to be used in the selection of the appropriate scenarios to analyse. In order to generate a sufficient set of scenarios, it is useful to consider the following three possible starting points for your scenario generation:

- start with the source events and think forwards through how the infrastructure will be affected and then how humans will react to this,

- start with the societal events and think backwards through how the infrastructure would have to behave to cause such events, and
- start with infrastructure events and think through in both directions.

Comprehensive identification of relevant scenarios is critical, because scenarios excluded in this task will not be included in further analysis and may result in an incorrect estimation of risk. To minimise the possibility of this happening it is important that experts in each area are involved.

This task ends with a list of all scenarios to be analysed.

4.4.4 Define relationships

In order to estimate the likelihood of each subsequent event in the scenarios, models of the relationships between the events are to be developed. For example, in order to determine the amount of water coming in contact with a bridge during a flood, it is necessary to model how the water, which falls as rain, reaches the river, taking into consideration, for example, the amount of water that seeps into the ground or evaporates, or is held in temporary retention ponds.

The amount of effort to be spent on this depends on the exact problem and the level of detail desired. For example, in some cases it may be sufficient to use one dimensional fragility curves based on expert opinion to estimate the amount of damage that a single building might incur during an earthquake. In other cases, it may be desirable to use composite fragility curves such as those proposed by D'Alya et al., 2015 to estimate the amount of damage a large dam might incur during an earthquake given the large number of components that may fail. In general, extra effort should be spent to achieve more detail when it is suspected that the results will add additional clarity for decision-making. If additional clarity is not provided the extra effort is not worth it.

Although specific examples are given here, the general thoughts apply to all events, i.e. source events, hazard events, infrastructure events, network events and societal events. If possible the availability of data to be used to model the relationships should be taken into consideration in determining the level of detail to be used.

This task may involve the testing of parts of the system to ensure that the relationships between events are defined at the desired level of accuracy. For example, data can be collected on rainfall patterns, water levels in rivers can be collected during rainfall events, bridge columns can be tested to see how they react to water pressures, roads can be closed to observe traffic patterns that might be associated with road closures, and tests can be done to see how long it takes to restore failed infrastructure.

This task ends with clear explanations of the relationships between all events.

4.4.5 Determine models

Once the boundaries, events, scenarios and relationships to be analysed are determined, the specific models to be used to estimate the risk are determined. This includes the selection of the software packages to be used if computer support is required [Adey et al., 2014, Hackl et al., 2015]. This task ends with the selection of all models and software required to estimate risk.

4.5 Estimate risk

In the *estimate risk* task the probability of occurrence of each of the scenarios and the values to be attributed to the societal events associated with each scenario if it occurs are to be estimated and, when desired, aggregated. This task can be done with or without computer support, which, of course, can also be with varying degrees of detail, depending on the specific problem, the information, data and resources available.

Special attention is required to the certainty with which both the probabilities of occurrence and consequences of each of the scenarios can be estimated. It is advised to investigate the sensitivity of these values to the modelling assumptions and to consider this in interpreting / evaluating the results. Indicators of the sensitivity of these values are the divergence of opinion among experts, the availability of information, the quality of information, the level of knowledge of the persons conducting the risk analysis, and the limitation of the models used. The parameters varied in the sensitivity analysis should be the ones thought to have the most dramatic effect on the risk values.

This task ends with the estimation of the risk levels for all stress tests defined in the stress test task.

4.6 Evaluate risk

In the *evaluate risk* task, you verify the meaning of the estimated risk to persons that may be affected, i.e. stakeholders. This is true regardless if a qualitative, semi-quantitative or a quantitative approach is used. A large part of this evaluation is the consideration of how people perceive risks and the consideration of this over- or under-valuation with respect to the analyst's point of view used in the *estimate risk* task. Another part, however, is stepping back from the analysis and reconsidering if everything important was modelled in a sufficient way. As systems are never modelled perfectly, it is reasonable that this task may lead to a decision maker deciding something different than the risk estimation alone would say. The deviation should, however, be explained.

In this task, decisions are made as to whether not the stress test has been satisfactorily done, including consideration of the appropriateness of the definition of the stress test, the approach used, the system representation used and the estimation of the risk itself. This task ends with one of the following decisions being made:

1. Stress tests conducted satisfactorily and risk levels acceptable (Stress test passed)
2. Stress tests conducted satisfactorily and risk levels not acceptable (Stress test failed)
3. Stress tests not conducted satisfactorily (Stress test provisionally passed or failed and more analysis is required)

When the stress tests are judged not to have been conducted satisfactorily it means that they have not been done to a level of detail or in a way where you can say whether or not the risk levels are acceptable or not. This might happen because the system, or parts of the system, were not modelled in sufficient detail, or because there is too much uncertainty associated with the models used. If the stress tests have not been done satisfactorily you proceed to determine the parts of the system to be analysed in more detail.

If the stress test is either passed or failed then you proceed to develop the intervention program, i.e. determining the risk-reducing interventions to be executed in the near future. If the stress test is passed there will be no interventions included in the intervention program, and you are finished.

4.7 Determine parts of system to be analysed in more detail

In this task, the parts of the system that must be analysed in more detail in the next iteration, if any, are determined. The parts that are likely to generate the most reduction in uncertainty in the risk estimation are selected.

Care must be given here to not only select parts of the system where risk is likely to be reduced in a way that will result in a passing of the stress test, e.g. to select parts of the system where it is believed that a conservative bias was introduced in the model but to neglect parts of the system where it is believed that non-conservative biases were introduced. To avoid preferential selection of system parts, the uncertainty related to each part of the system need to be determined. In many cases, this will be done using expert opinion. For example, there is high uncertainty in the expected rain fall and in the traffic patterns that might emerge following the collapse of a bridge, but there is low uncertainty in how the bridge will behave if in contact with water of x m^3/s and in how long it will take to reconstruct the bridge following failure.

A list of ways to reduce this uncertainty, along with their likely benefits and costs, following the principle of think of possibilities (see section 2.4), should be generated. This list of possibilities should include conducting tests on parts of the system, e.g. load testing bridges as suggested in Avdeeva et al., 2014 and running more detailed flood simulation models. The parts of the system to be analysed in more detail can then be determined taking into consideration the available resources, including both effort and time frame. If there are resource constraints, the parts of the system to be analysed in more detail should be the ones that will yield the largest reduction of uncertainty for the available resources.

5 Discussion and conclusions

In this paper, a process is proposed to ensure that infrastructure is managed so that levels of infrastructure related risk due to natural hazards are acceptable. The process consists of three main tasks, 1) *initiate*, 2) *conduct stress tests*, i.e., determine if there are acceptable levels of infrastructure related risk due to natural hazards, and 3) *construct intervention program*, i.e., determine the risk reducing interventions to be executed to reduce the risk to acceptable levels. The process is described making appropriate references to four principles of systems engineering. Emphasis is given on the second of the three main tasks, i.e., *conduct stress tests*. The main sub-tasks of the *conduct stress tests* task are 2.1) *define stress test*, 2.2) *determine approach*, 2.3) *define system representation*, 2.4) *estimate risk*, 2.5) *evaluate risk*, and 2.6) *determine parts of system to be analysed in more detail*. The first and the third of the three main tasks will be subjects of future work. The process can be used for a wide range of natural hazards, infrastructure networks and at any level of abstraction. It can be used to take into consideration both simple and complex system representations. It can be used with and without computer support.

Future work related to the further development of this process, should include:

- Determining the stress tests that should be conducted in specific situations,
- Determining the best way to appropriately define the system representation amongst the infinite number of possibilities, including which simulations should be run, which parts of the system should be modelled in which way and which parts of the system need to be tested and to what degree,
- Defining the *construct intervention program* step in the process at a lower level of abstraction,
- Conducting a realistic example of the use of this process,
- Developing appropriate models to be used in the *determine model* subtask to determine infrastructure related risks due to natural hazards at appropriate levels of abstraction, and
- Determining useful ways to illustrate temporal and spatial risks to be used in the *evaluate risk* subtask of the process.

6 Acknowledgement

This project has received funding from the European Union’s Seventh Programme for research, technological development and demonstration under grant agreement No 603960.

7 References

Adey, B.T., Hackl, J., Heitzler, M., Iosifescu.I., 2014, Preliminary Model, Methodology and Information Exchange, Deliverable 4.1, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960 July, 93 pages.

Adey, B.T., Birdsall, J., Hajdin, R., 2010, Methodology to Estimate Risk Related to Road Links, due to Latent Processes. 5th International Conference on Bridge Maintenance, Safety and Management, IABMAS, Philadelphia, USA, July 11-15, 2010.

Adey, B.T., Hajdin, R., Birdsall, J., 2009. Methodology to determine Optimal Intervention Strategies for Structures Adversely Affected by Latent Processes. Transportation Association of Canada, Annual Conference, Vancouver, Canada, October 19-22, 2009.

Avdeeva, Y., van Gelder, P., 2014, Stress Test Methodologies, Deliverable 6.1, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960, 49 pages.

Buritica Cortes, J.A., Sanchez-Silva, M., Tesfamariam, S., 2015, A hierarchy-based approach to seismic vulnerability assessment of bulk power systems, Structure and Infrastructure Engineering, Vol. 11, No. 10, 1352–1368.

Cheng, T., Taalab, K., 2014, Integrated Spatio-Temporal Database, Deliverable 5.1, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960, 35 pages.

D'Ayala, D., Gehl, P., 2014, Hazard Distribution Matrix, Deliverable 3.1, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960, 128 pages.

D'Ayala, D., Gehl, P., 2015, Single Risk Analysis, Deliverable 3.4, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960 July, 69 pages.

Danzig D. van, Economic decision problems for flood prevention, Econometrica 24, p. 276 -287, 1956.

Dehgani, M., FLintsch, G., McNeil, S., 2014, Impact of road conditions and disruption uncertainties on network vulnerability, Journal of Infrastructure Systems,

Gavin, K., Martinovic, K., 2014, Critical Infrastructure Database, Deliverable 2.1, Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960, 19 pages.

Hackl, J., Adey, B.T., Heitzler, M., Iosifescu-Enescu, I., 2015, An overarching risk assessment process to evaluate the risks associated with infrastructure networks due to natural hazards, Special Issue of Performability Engineering on Transport System Safety, Risk and Asset Management, 11:2, March.

ISO 31000, 2009, Risk Management - Principles and Guidelines. International Organization for Standardization (ISO).

Jonkman, SN, Vrijling, JK & Gelder, PHAJM van (2006). A generalized approach for risk quantification and the relationship between individual and societal risk. In Guedes Soares & Zio (Eds.), safety and reliability for managing risk (pp. 1051-1059). London: Taylor and Francis Group.

Meacham, K., Sabeur, Z., 2014, IDST System Specification v1.0 Novel indicators for identifying critical, INFRAstructure at RISK from Natural Hazards, grant agreement No. 603960 July, 51 pages.

Moini, N., 2015, Modeling of Risks Threatening Critical Infrastructures: System Approach, Journal of Infrastructure Systems, ASCE, DOI 10.1061/(ASCE)IS.1943-555X.0000263.

Nourzad, S.H.H., Pradhan, A., 2015, Vulnerability of Infrastructure Systems. Macroscopic Analysis of Critical Disruptions on Road Networks, Journal of Infrastructure Systems, ASCE, DOI 10.1061/(ASCE)IS.1943-555X.0000266.

Ritchey, T., 1998, General Morphological Analysis: A general method for non-quantified modeling, 16th EURO Conference on Operational Analysis, Brussels.