ORIGINAL RESEARCH ARTICLE ADRS

Ann. Disaster Risk Sci. 2019, 1-2, 11-27

CLIMATE RELATED BUSINESS CONTINUITY MODEL FOR CRITICAL INFRASTRUCTURES

Danai Kazantzidou-Firtinidou[1], Ilias Gkotsis[1], Georgios Eftychidis[1], Athanasios Sfetsos[2], Nenad Petrovic[3], Alen Stranjik[3]

[1]Center for Security Studies, Ministry of Citizens Protection (KEMEA), Athens, Greece
[2]National Center for Scientific Research DEMOKRITOS, Athens, Greece
[3]University of Velika Gorica, Zagreb, Croatia

Abstract

Climate change is nowadays more and more acknowledged to be one of the natural hazards for which the society, and its critical infrastructures, need to anticipate and plan. The impact the climate-related hazards have to the functionality of different Critical Infrastructures (CI) is being discussed, focusing on the minimization of the disruption time of their critical services. This is achieved by means of a Business Continuity plan that is based on Business Impact Analysis and Risk Assessment of projected weather-related hazards. Business continuity planning is the essential part of the resilience framework of the CIs, which the EU-CIRCLE project proposes with regards to climate change. Guidelines are presented in order to provide a planned and controlled method for anticipating and responding to events that are likely to interrupt key business activities (Business Continuity Model), and suggestions upon adaptation of CIs to climate change are also given. For this purpose, information was collected from CI operators with regards to existing BC plans and adaptations measurements by means of questionnaires, which is also presented herein.

Keywords: climate change, business continuity, critical infrastructures, resilience, adaptation

Address for correspondence: Danai Kazantzidou-Firtinidou, 1Center for Security Studies, Ministry of Citizens Protection (KEMEA), Athens, Greece, email: d.kazantzidou@kemea-research.gr

1. INTRODUCTION

1.1 Background

According to the Australian academy of science (AAS, 2015), "Climate change is a change in the pattern of weather, and related changes in oceans, land surfaces and ice sheets, occurring over time scales of decades or longer". In other words, it refers to the change of the statistical properties of the climate system within the next decades, usually over 30 years, as defined by the World Meteorological Organization. Contrary to the weather, that is easily predicted at short-term basis, based on actual observations, future climate can only be predicted using highly complicated Earth models also accounting for socio-economic pathways.

It is, also, widely recognized and reported (BSI Group, 2014) that many business activities are directly dependent on the weather and extreme events. In fact, extreme weather events are more and more common in every part of the world and/or different climate conditions make their appearance in areas that have little historical experience on them and thus are not prepared to face them. Meanwhile, the business value follows also an increasing trend, and consequently the value exposed at risk (Trexler and Kosloff, 2013). Hence, a potential business disruption due to weather-related incidents of increasing frequency may lead to important monetary loss, as well as impact the society's smooth function.

Climate change is being recently added within the scope and interests of Business Continuity Management (BCM), and it requires different treatment than traditional natural or man-made hazards businesses usually plan for (BSI Gro-

up, 2014). It is important, also, to differentiate planning for weather events from changes of climate averages, which usually refers to long-term planning with given uncertainty. Moreover, the identification of both threats and benefits, that weather conditions due to climate change may bring in, could provide a market lead to the industry that decides to take into account the dynamic phenomenon of the climate change and plan with a long-term horizon with future projection of combined events, rather than studying historical experience. Finally, it should be noted that the concept of "disruption" due to climate change when referring to the provision of services may be seen as "reduced efficiency" rather than actual business disruption for a certain amount of time, as usually being accounted for. Considering the abovementioned, the establishment of a BC plan to account for requirements and impact of climate change is suggested, based on scientific knowledge on extreme weather events, so as to minimize the uncertainty.

1.2 Impact to Critical Infrastructures (CI)

The EU defines a Critical Infrastructure (CI) as 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" (Horrocks et al., 2010). Thus, CIs refer to technical infrastructures such as hospitals, transportation and energy networks, natural gas pipelines, and others. By extension, a European Critical Infrastructure (ECI) refers to an infrastructure which if destructed or disrupted, and can severely impact at least two Member States (Horrocks et al., 2010). Apart from the vital services these infrastructures provide to the society, the significance lies also within the interdependencies between the different infrastructures which can be responsible for Domino effects in case of a disruptive incident. The different types of interdependencies are defined as physical, cyber, geographic and logical interdependencies (Rinaldi et al., 2001) and various approaches for modelling CIs as a network of networks exist (e.g. Baba et al., 2014), for assessing potential cascading failures and cascading effects, being also part of BC planning.

All kinds of infrastructures, to mention herein the most critical sectors – energy, transport, water supply and sewage, Information and communications technology (ICT) – are crucial for the economy, the societal integrity and function in Europe, at present and future basis. One of the policy areas of the European Union is to assess infrastructures for resilience to current risks and future climate changes. Evidence collected by the European Commission indicates that climate impacts on infrastructures will vary across the EU depending on their geophysical risk exposure, the existing adaptive capacity and resilience, and the level of regional economic development. Their interconnection is also highlighted, considering that impact to one critical sector often affects assets and aspects of function of other sectors, which if uncontrolled may lead to cascading impacts.

In fact, climate impacts show regional and seasonal patterns, e.g. north/south, winter/summer, urban/rural/coastal, requiring complex, site-based analysis of different trends and impact patterns. Climate change will also affect the environmental and social systems around infrastructure assets and their interactions with these systems. Interestingly, as well, many of the impacts are often accelerated or accentuated in built-up areas, and by the installations of the infrastructures themselves that may create unique micro-climates in terms of temperatures, wind, and precipitation. Vulnerability, moreover, is strongly sector-specific and closely linked to the technology used for construction and operation. This highlights the importance of acting in an integrated, cross-sectoral way on climate risks and resilience, from a structural and operational point of view, recognizing, though, the peculiarities of each of the CI sector or the industries themselves.

A European Commission White Paper (EC, 2009) outlines the main direct impacts of climate change

in the **energy sector** in terms of both supply and demand. Energy is at the core of economic and social activity and, as the European Environmental Agency (EEA, 2014) states, it is essential for the generation of industrial, commercial and societal wealth. In fact, the projected future climate impact differs at territorial level, with more evident discrepancies being between the south and north of Europe, as Green paper (EC, 2007) briefly describes. Hence, different levels of precipitation, temperature and wind speed would lead to different amount of hydropower or wind power production as well as electricity demand, what will lead to destabilization of the energy balance. In addition to this, severe or extreme weather phenomena and sea level rise have also direct impact to the industry installations and their components, structurally or operationally, being in emerging need of upgrade and/or protection.

Climate change also clearly compromises **transport services**, often in a quite important frequency. It is being reported that transport infrastructures, often deteriorated due to aging, already cope with extreme weather events, following an increasing trend in frequency and intensity (EC, 2013). They face different types of challenges depending on their type, territorial aspects and current climate conditions. The operation in extreme (high/low) temperatures that should be taken into account for the rail properties or the roads pavements, sea-level rise and waving threatening coastal infrastructures (ports/harbours), are some examples of structural impact. Moreover, delays or interruption of services due to extreme precipitation, flooding, weather-related landslides or changing wind patterns are main issues to be anticipated aiming to business continuity. High temperatures and droughts often being the reasons for intense wildfires can affect to a smaller or larger extent the operation of the transportation networks.

Water resources, and consequently infrastructures of the water sector, either for drinking water or wastewater, are also directly affected by climate change, mainly due to increase in temperature and alteration of precipitation pattern. The seasonal variation in river-flow depends directly on snow volume and melting and its impact is encountered in the peak threatening flow levels of spring and dry summer water reservoirs. Similarly, increased frequency and intensity of rainfall may multiply the flooding phenomena and, on the other hand, dry prolonged periods can reduce significantly the groundwater recharge, critical for watering. Hence, extreme events will affect directly the raw water supply, the end-users water demand and the infrastructures used. The efficiency of the wastewater management system is also affected, with impacts to the ecosystem or the demand of alternative potable supply sources. Furthermore, the alterations on water supply and demand balance will, in their turn, pose an indirect to climate change pressure, that will further increase the vulnerability of water infrastructure. Finally, as EEA (2014) states, the socio-economic impact of changes in Europe's water resources in a variety of sectors, such as agriculture, forestry, fishery, energy production, drinking water provision and others indirectly linked with water flow is evident, highlighting the cross-sectoral climate impact.

Although the direct impact of the weather and climate change to the **ICT infrastructure** hasn't been thoroughly studied, Horrocks et al. (2010) mention some of the potential climate impacts on ICT, mainly focusing in interruption of its services or quality reduction. First, two large categories of assets are recognized, those *underground*, vulnerable to flooding or drought or other weather-related geological phenomena; and those *above ground*, mostly affected by the precipitation itself or humidity, unstable ground conditions and other environmental stresses which reduce infrastructure's lifespan. As far as the latter is concerned, considering the fast pace of technology change which leads to frequent replacement of ICT components, it may be said that ICT sector is the most flexible and adaptable to climate change of long time-span, provided that evolving risks are taken into account in future design. However,

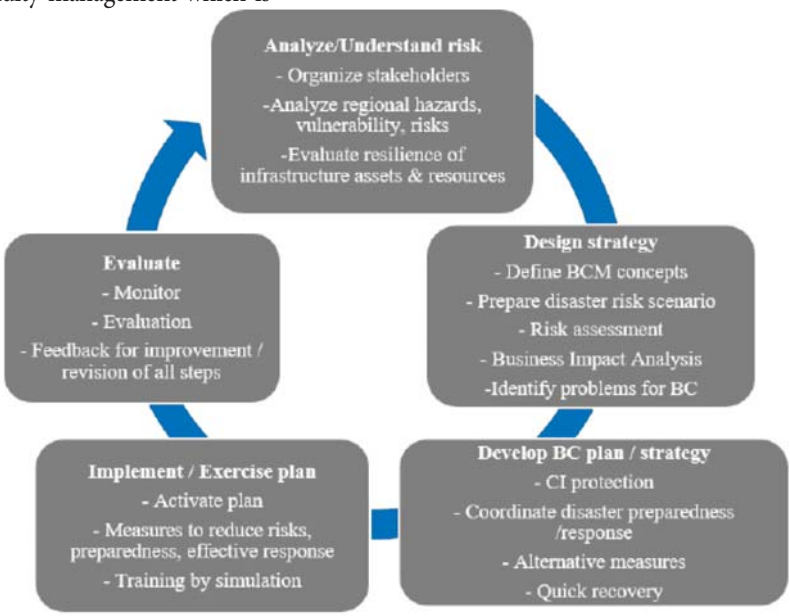
the impact of current extreme weather conditions should be seriously accounted for when acting towards resilient ICT infrastructures, considering the economic and social impact of a potential prolonged failure of any of its critical assets (e.g. data centers, fiber cables, antennas).

From the above-mentioned the emerging need for policy-makers and CI stakeholders to understand the climate-change impacts and to act is revealed, not only towards climate change reduction, which is undoubtedly indispensable, but also towards immediate shielding of infrastructures assets against weather-related impacts. Adaptation measures should, therefore, be taken at national and European level, from public sector and private businesses (EC, 2007), with both inexpensive actions (e.g. water conservation or even awareness raising) or costly defense measures (such as relocation or structural upgrades), depending on the projected environmental stresses, the serviceability time frames and assets criticality. Main scope of all engineering or non-engineering measures will be the enhancement of infrastructures robustness and redundancy at both physical and operational level, in order to ensure provision of the critical services. All the aforementioned are, therefore, challenges to the business continuity management which is called to plan and anticipate actions and backups under a climate change adaptation business strategy. To this, identification of threats, risks (impact with the associated probability) as well as opportunities, is the necessary first step towards the risk mitigation and minimization of disruption of critical activities.

2. BUSINESS CONTINUITY MANAGEMENT (BCM), FUNDAMENTALS

According to ISO 22301 (2012), **Business Continuity Management** (BCM) is a "business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework". Its main purpose is to proactively improve an organization's resilience against operational disruption, to anticipate a methodology for restoring organization's ability to continue providing essential products and services at an adequate quality level and within an agreed time, and to develop the organization's capacity to successfully manage the disruption and conserve its reputation. It is essentially a cyclic process (Figure 1) which starts from risk understanding and impact estimation and comprises the design of the strategy, the development of a holistic business continuity plan, the implementation of the planned actions and preparedness measures, evaluation of the result for continuous improvement and guarantee of business continuity.

Figure 1. Business Continuity Management cycle, modified after Baba et al. (2014) and according to ISO 22301 (2012).



In fact, **Business Impact Analysis (BIA)** and **Risk Assessment (RA)** form the backbone of Business Continuity Planning (BSI Group, 2014). The former focuses on the business impact of the disruption regardless of its source or probability of occurrence, which leads to immediate prioritization of actions and allocation of resources without the need of further complex information, such as statistics. This is usually performed after collection of data from the different sector operators who provide their views of the impact over time based on customer-related, financial, regulatory, operational, reputational, and human criteria. This will allow the BC managers to assess the overall impact in quantitative or qualitative terms and prioritize timeframes for resuming each of the activities. Adaptation measurements and recovery objectives will be decided based on the nature of the impact and its level, the impact over time and the recovery time, as well as the critical dependencies and interested parties (KEMEA, 2019).

Risk assessment, on the other hand, is considered to be the most complete method of assessing the impact with its associated probability (see, risk) and is useful for risk understanding and for decision making in long-term basis, accounting for uncertainties. It provides a holistic view of "how future may develop" accounting for the probability of impact and the frequency of the hazard, the severity of impact, and its speed of development. The collection of information is more demanding, and it is necessary to evaluate the credibility of the sources. Risk assessment, following ISO 31000 (2018), includes all steps of risk identification, analysis, and final evaluation of disruption- related risk that requires treatment. Risk treatment is decided in accordance with BC objectives and risk appetite. Based to the latter, the necessary proactive measures should be taken for reducing the likelihood of disruption, minimizing the disruption period and/or mitigating its impact to the delivered products or services (ISO 22301, 2012).

Setting the **BC strategy** is the main outcome of the BC planning as it implements the conclusions of the BIA and RA process (ISO 22301, 2012). Its main objective is to define alternatives and strategies to follow in case of interruption of the critical services, to implement appropriate measures for reducing the disruption possibility, and to identify the necessary resources for the effective and rapid restoration of the critical services. Core concept of the strategy is the establishment of scenarios which must respond to the contingency assumptions that have been adopted, focusing to the impact rather than to its causative effect. These include assumptions of unavailability of different CI assets and resources, what may refer to unavailability of locations (buildings, data centers, etc.), of human resources (personnel, continuity of operations, etc.), and of supplies or loss of data. For each of the considered scenarios, one or more recovery alternatives should be set and their availability should be guaranteed. For example, alternative buildings, cold, warm and mobile sites may be anticipated, alternative personnel and/or collaboration with other similar service providers might be agreed in advance, technology should be put in place for conservation of data. Finally, the BC strategy should also consider its cost of implementation, as well as the consequences of its non-implementation.

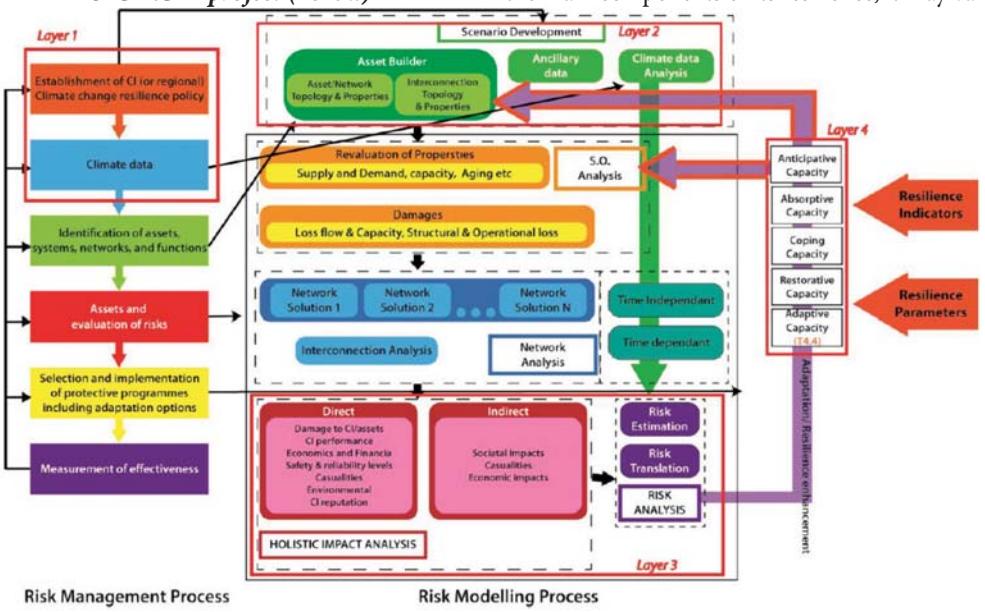
After the design and the establishment of the BC strategy, **implementation of the BC plan** at the pre-disaster phase takes place in order to test the validity of the BC plan and identify its gaps and strengths. The type of exercise is selected according to the scope (e.g. unit, modular or global) and the method used (e.g. hypothetical, procedural, operational or integral). The scenario defines the critical services to be disrupted and the stakeholders required to carry out actions and it may be independent of the cause of disruption (nature of hazard). However, as further explained below, the BC plans related to hazards due to climate change require special policy and study due to the long-term and unprecedent nature of the hazards. After the completion of the exercise, the performance of all steps of the BC strategy is evaluated by the team

leaders, it is documented, and used for revisiting of the plan. A maintenance program should be also foreseen in order to ensure the validity of the plan throughout the time, accounting for all possible operational or other changes.

3. BCM IN BUILDING RESILIENCE TO CLIMATE CHANGE

Business continuity strategy is planned as a result of an integrated resilience study at CI level (EU-CIRCLE, 2017a). As the framework of Figure 2 demonstrates, the process suggested includes identification of climate hazards (Layer 1) and CI assets, networks and interdependencies (Layer 2), both essential components of risk assessment. Climatic hazard parameters that are taken into account are generally the time frequency of the event, its magnitude and anticipated level of impact on the CI, scientific future climate projections and their reflection on the hazards of interest, the level of uncertainties and their nature. Some of the CI properties included as part of Layer 2 are the location of the installations, their age and state of maintenance, the infrastructure's lifecycle, and the number and level of interdependencies.

Figure 2. Resilience framework according to EU-CIRCLE project (2017a)



Hence, the impact of the weather-related hazard to the CI, main outcome of the risk assessment (Layer 3), is categorized as *direct* and *indirect*. To the *direct consequences*, the damage to the as-built state of the CI assets is firstly reported, together with the casualties among the operators and users, due to physical damage of the assets. Influence to the CI performance, what leads to changes in the provision of services and products to the society, and the associated economic impact, due to loss of income and cost of damage, are also significant direct consequences. To the latter cost, loss of the CI reputation may be added, as well as adaptation measurements within a business continuity strategy. Finally, often direct impact of a CI failure is also reflected to the environment. Furthermore, economic loss and impact to the society is also recognized as *indirect impact*, as the services, no longer offered by the infrastructure, impede economy's and society's normal function. Similarly, dependent infrastructures and their offered services are indirectly affected.

For the final assessment of the CI's holistic resilience, the **resilience capacity** per CI asset is estimated (Layer 4). The capacity of the CI is one of the main components of its resilience, it may vary

per asset and type of hazard and it has to be assessed as such. Discrete resilience indicators quantifying the anticipative, absorptive, coping, restorative and adaptive capacity of each asset lead to the overall resilience estimation, which, in combination with the risk assessment outcome allows for decision-making towards adaptation options. The business continuity module, at the end of this process, provides a framework for consideration of the different *adaptation options* required to increase/maintain resilience in the face of events within reasonable allocation of resources, and it is custom-made to the needs of each business activity or installation.

Adaptation to climate change is particularly challenging given that it refers to the future with, often small availability of related historical data. In fact, there is lack of past experience on the frequency and impact of the projected hazards, while any kind of experience on the business response to disruptive events needs to be exploited. Climate change, by its nature, is a dynamic phenomenon that incorporates a number of uncertainties and assumptions and this is reflected in both the BIA and RA. It may, also, refer to both altered climate averages (e.g. seasonal rainfall or mean daily maximum temperature averaged over a season) and extreme weather events, what may differently affect CI sectors or even different assets within the same infrastructure. Moreover, climate change-related events other than causing disruption, what is often anticipated within BC plans, may also affect business in more subtle ways, yet decisively long-term, such as in terms of process efficiency or manpower productivity. However, of particular concern is the assessment of and the preparedness for scenarios combining different weather events or events occurring during the recovery periods of others (e.g. heavy rain following long dry periods), or prolonged events with the consequent impact. Interestingly enough, the opportunities arising from beneficial effects of the changing weather or the preparation itself of the business towards adaptation, should be also taken into account.

Overall, traditional and one-dimensional approaches often used while incising BC strategy, including BIA and RA processes, may need to be reviewed to account for all the aforementioned. RA, by its definition, is used to identify climate related threats and benefits, based on likelihood and severity judgements (BSI Group, 2014) for prioritizing actions. As said, risk identification should not be limited to what already experienced, on both severity and likelihood, but should be instead oriented to future projections (e.g. level of precipitation exceeding precedent extremes or in a higher frequency). On the other hand, BIA focuses on the business impacts of the disruption irrespectively of the cause, however, it is emerging need to revise existing plans in order to be able to capture the long-term aspect that climate adaptation planning requires.

In fact, **resilience to climate change** has two main time frames: (i) short-term, according to the traditional definition of BC planning which focuses on readiness for immediate resume of the activities and (ii) long-term, linked to the adaptation ability that would result in the CI being able to cope with climate change over a longer time horizon. It is, thus, recognized that challenge of BCM of a CI in a climate changing environment is to primarily identify the climate as main external factor that may influence a number of internal factors of an organization (e.g. activities, services) that involve long planning horizons and, subsequently, to make the plans more relevant to this purpose. Hence, BCM is amended to make future decisions avoiding potential vulnerabilities linked with future hazards and, meanwhile, to estimate whether adaptation measurements against disruptive impacts are cost effective. Adaptation measurements generally focus into three axes (BSI Group, 2014): (i) reduction of the likelihood of disruption (e.g. with technological improvements, physical enhancements); (ii) shortening of period of reduction (e.g. by operational and managerial agreements); (iii) limiting the impact of disruption (e.g. with implementation of technological tools, with

managerial arrangements). The definition of new roles and responsibilities within the business management is necessary, as strong leadership, commitment and resources from across the business, involving different assets and parties are indispensable for a future planning.

3.1 Resilience Assessment Tool

In the framework of EU-CIRCLE project, a Tool measuring the overall Resilience in quantitative terms, by means of resilience capacity indices, has been also developed, as demonstrated in Figure 2 (EU-CIRCLE, 2017c). BC planning affects different sectors of the resilience curve (Figure 3, left): ***anticipative*** capacity that mainly refers to anticipation of equipment and procedures for hazard mitigation, thus reduction of likelihood of disruption; ***absorptive*** capacity focusing to the resistance and robustness of the assets, again towards reduction of likelihood of disruption; ***coping***, aiming to evaluate different BC strategies that will reduce the disruption time and impact; ***restorative*** capacity, less influenced by BC planning since it refers to the restoration of the initial capacities and services; and finally the ***adaptative*** capacity, focusing to the anticipation of adaptation measurements, more precisely, as far as climate related hazards are concerned. In general, the resilience curve indicates the necessary time period for an infrastructure to recover to an acceptable level of functionality, lower or equal to business as usual (restoration), and to preferably reach a better level of performance. In the latter case, the horizontal part of the curve after recovery will be raised to a higher level. Significant slope of the curve is interpreted as low absorptive capacity consequently requiring more effective coping and restorative capacity to restore performance. Hence, the higher the value of resilience capacities, the smaller the slope and the faster the system recovers. Enhanced anticipation capacity may delay or reduce the impact of disruptive event, while adaptation, although being a significant component of resilience, does not lie within the system's performance during response and recovery time. Figure 3 (right) depicts the score of all the aforementioned resilience capacities contributing collectively to the Overall resilience Index after prioritization by the user. The higher the score of each capacity, the larger is the covered area of the polygon representing the level of the overall resilience. This is directly linked with the resilience curve on the left, having an inversely proportional relation with the "triangular surface" which is formed within absorption-coping-recovery phases, and which decreases as the surface of overall resilience on the right increases.

In Table 1, the indicators defining the resilience capacities are listed, together with their categories and subcategories. All the answers lead to 1-10 indices and subindices (e.g. assuming as 10 the "yes" answer), while Risk or BC manager, in charge of the resilience assessment of the organization, has the possibility to prioritize the indicators according to his/her experience and the particular CI needs. Should the Overall index is low, corrective actions are strongly recommended to be taken throughout the entire resilience curve, for guaranteeing maintenance of the critical services and overall resilience upgrade.

Figure 3 Conceptual resilience curve, adapted for EU-CIRCLE project (left); Overall Resilience Index from Resilience Assessment Tool (right)

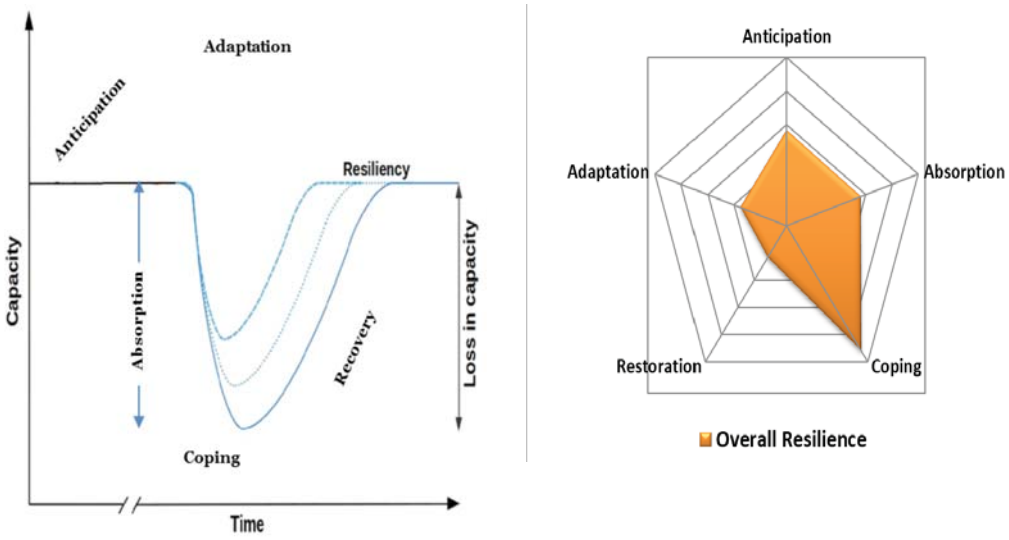


Table 1 Capacity resilience indicators according to Resilience Assessment Tool (EU-CIRCLE, 2017c)

Anticipative Capacity Resilience Indicators	**Resilience Categories / Subcategories**
Awareness	Users awareness of number of threatening hazards vs existing hazards (%)
Quality extent of mitigating features	Equipment and procedures for hazard mitigation
	■ Procedures documents (Y/N)
	■ Procedures regularly revised (Y/N)
	■ Equipment of hazard mitigation (Y/N)
	■ How many climate related hazards they cover vs hazards impacting the area? (%)
	Early warning system exists
	■ How many climate related hazards they cover vs hazards impacting the area? (%)
Quality of disturbance planning/response	Response plans exist
	■ Plans are up to date (Y/N)
	■ How many climate related hazards they cover vs hazards impacting the area? (%)
	■ Climate changes are covered (Y/N)
Communication systems	Plans of communication and information sharing between CI operators and public sector exist
	Communication system for communication and information sharing between CI operators and public sector exist
	Backup of communication system for communication and information sharing exist
Learnability Training	Training system exist
	■ How many climate related hazards is covered by training vs hazards impacting the area? (%)
	■ How many hours of training is performed vs necessary hours of planned training? (%)
	■ Last training was within a year (Y/N)
	■ Number of people in need to be trained vs number of trained people (%)

Absorptive Capacity Resilience Indicators	**Resilience Categories / Subcategories**
System failure	Acceptable time vs actual time that CI is not able to serve its function (%)
	Acceptable cost vs cost of damage (%)
Severity of failure	Loss of performance for certain hazard level (%)
Resistance	Probability of failure (%)
	Age of CI vs CI lifetime (%)
	Safety design standards
	■ How many relevant standards are applied vs exist? (%)
	■ How many climate related hazards they cover vs impact the area? (%)
	Regular maintenance of the asset is performed
	■ Maintenance plan exist? (Y/N)
	■ Maintenance is performed according to the plan (Y/N)
	■ Critical Infrastructure is fully operational (Y/N)
Robustness and redundancy	Asset backup exist
	■ After how much time backup is available, real vs acceptable time? (%)
	■ How long backup is available, real vs acceptable time? (%)
Coping Capacity Resilience Indicators	**Resilience Categories / Subcategories**
Response	Needed response time vs acceptable response time
	Emergency plans for Climate Hazards (in the context of climate change) exist
	■ Plans are up to date (Y/N)
	■ How many climate related hazards they cover vs hazards impacting the area? (%)
	Business continuity plans for Climate Hazards (in the context of climate change) exist
	■ Plans are up to date (Y/N)
	■ How many climate related hazards they cover vs hazards impacting the area? (%)
Economics of response	Cost of response (for CI only)
	Backup cost vs acceptable cost (%)
Interoperability with public sector	Procedures exist (Y/N)
	Communication system exists (Y/N)
	Joint action plans exist
	■ Plans are tested (Y/N)
	■ Plans are up to date (Y/N)
Restorative Capacity Resilience Indicators	**Resilience Categories / Subcategories**
Post-event damage assessment	Stage of change from base state after event (%)
Recovery time	Recovery plans exist
	■ How many climate related hazards it covers vs hazards impacting the area? (%)
	■ Climate changes are covered (Y/N)
Economics of restoration	Actual cost of restoration vs acceptable cost of restoration (%)
	Actual loss of income during restoration vs acceptable loss (%)
	Actual loss due to possible penalties from violating service level agreements with buyers vs acceptable loss (%)
	Actual maintenance costs after hazard vs acceptable costs (%)
	Actual cost of reputation vs acceptable cost (%)
	Actual insurance costs vs acceptable costs (%)

Adaptive Capacity Resilience Indicators	Resilience Categories / Subcategories
Adaptability and flexibility	Adaptation of asset is possible
	■ Technically is possible (Y/N)
	■ Financially is possible (Y/N)
	Adaptation to new climate conditions on time is possible (acceptable vs real time) (%)
	Adaptation plan exist
	■ How many climate related hazards it covers vs hazards impacting the area? (%)
	■ Climate changes are covered (Y/N)
Impact / consequences reducing availability	Relocation of existing facilities is possible (Y/N)
	New investments made considering climate change (Y/N)
	New facilities are built according to climate-ready standards (Y/N)
Economics of adaptation	Increase of clientele by improving the service / climate adaptation polices (%)
	Reputation is increased by implementing climate change adaptation options (Y/N)
	Decisions on adaptation adopted due to market forces (Y/N)

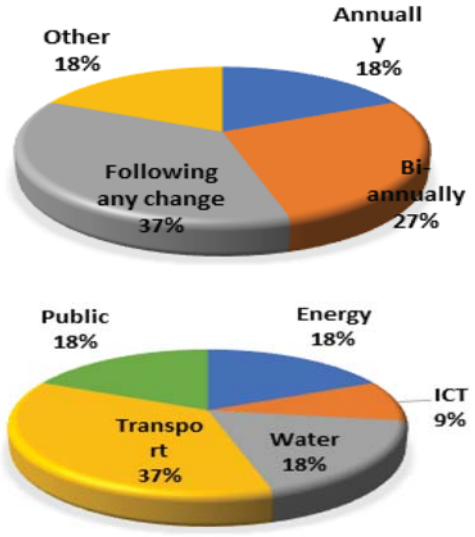
4. EU-CIRCLE BUSINESS CONTINUITY MODEL

For the establishment of a BC framework tailored to the needs of the CIs exposed to climate change-related hazards, information on existing BC planning and current measurements adopted for adaptation to climate change by CI operators, was collected in the form of questionnaires (EU-CIRCLE, 2017b). It is interesting to visualize their responses and interpret them for better addressing of their needs. Based on these findings and further collaboration with CI representatives, a BC model is proposed together with the main steps to be followed.

4.1 Analysis of BCM Questionnaires

The responses are provided by nine CI representatives who belong to the following CI sectors (Figure 4, left) from UK, Poland, Germany, and France. Among them, 7 responded that their organization has BCM system, which is updated in the frequency depicted in Figure 3 (right). The two CIs that do not have a relevant system belong to the public Transport sector, and one of them, despite the fact that it does not have an explicit BCM system, it does have defined procedures for some emergencies.

Figure 4 CI sectors interrogated (up), how often BC plans are updated (down)



Initially, the CI operators after indicatively communicating some of the critical services of their organizations, have also recognized incidents that could lead to disruption of the abovementioned critical services, and would trigger activation of BC planning. These are: shortage of personnel, loss of electrical power, loss of significant communications, loss of critical material or supplies, loss of critical system or process, loss of critical facility

or equipment, and disruption to financial system or cyber-attack. Potential impacts identified are to CI's managing company reputation and to physical property, both requiring protection; to contractual and regulatory compliance, what has to be anticipated with managerial arrangements; to consumers/users confidence and thus financial viability. To a lesser extent, life safety and public health threatening and cascading impact to other dependent CI services, such as water and waste water service, is imprinted. In Table 2, some critical operations per CI sector have been enlisted with potential disruption events affecting them and the acceptable Recovery Time Objectives (RTO), time to resume activities. Finally, all operators have declared the existence of alternative or redundant solutions for their organizations.

Table 2 Recovery Time Objectives (RTO) per critical operation and potential disruption

CI sector	RTO	Department/ Process	Critical Operations	Disruptions/Incidents
Transport	varies	Asset management	Maintain drainage systems	Lower line speeds
	From hours to 1-3 days		Road network	Typical road accidents
	Weekdays: Until next morning	Bus	Bus operation	Computer-based operations management system
	120 minutes	IT department	Maintain communications equipment	Loss of communication
	24 hours	Financial and accounting department	Provide additional financing sources	Inability to finance shipping services
	24 hours	Purchasing department	Provide additional supplies	Inability to operate vessel
	12 hours	Logistic department	Provide additional services	Inability to load/ unload vessel
Energy	15 minutes	Maintenance traffic	Maintain operational process	Loss of electrical power
	3 hours	Technical	Loading/ Unloading oil products	Pumping unit damage
	6 hours	HR	Provide additional personnel	Physical and intellectual fatigue of personnel during long time response
	Supply must be restored to 90% of the clients in max 5 days	Network control	Maintain supply	Supply to distribution networks
	Depending on each contract (confidential)	Network control	Maintain supply	Supply to industrial clients
	12 hours between the alert and the start of the intervention	Maintenance	Maintain supply or control by critical equipment availability	
Public	15 minutes	IT	Maintain communications equipment	Loss of communication

Moreover, it is interesting to analyze the CI operators' views as far as adaptation of existing BCM to climate change is concerned. Based on the responses in almost all of the cases, CIs basically admit that they have not conducted any action related to climate change adaptation yet. The majority of the respondents gave negative answers to questions on

the definition of factors related to climate threats, the amendment of BC policy and BIA due to the recognized climate change, the performance of climate RA, the study of maximum tolerable frequency of disruption, the monitoring of the impact of weather events to CIs operation, the definition and implementation of climate change adaptation measurements. However, many among them have provided examples of climate-driven disruptions to their infrastructures, e.g. blocked roads and damage to tram network due to the catastrophic 2002 flash flood event in France, massive energy interruptions after long lasting snow due to Cyclone Kyrill in 2010 in Polland.

4.2 Proposed BCM model

Business continuity strategy essentially means "the development of options and the selection of the most appropriate strategies that allow the organization to align with requirements" (Zawada, 2018). To align with the requirements outlined in Clause 8.3 of ISO 22301, a step process should be followed:

1. Identify possible BC strategies that will reduce the risk identified in the BIA and RA to acceptable level, addressing three categories of BC strategy:

- Risk Mitigation: reducing the likelihood of a disruption and limiting the impact should a disruption occur. For example, consider implementing back up power generation to address the concern about a loss of commercial power at a critical facility.
- Incident Response
- Recovery of Activities and Resources: identifying alternate sources of resources or alternate methods of performing required activities in order to meet downtime tolerances and obligations (alternate facilities, personnel, equipment, information technologies, and even third-parties)

2. Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process, asset or CI, in terms of resilience as described hereafter. From a CI's point of view, there are three important factors in the selection process:

- functionality: the degree to which the replacement functionality supports the production of a minimum acceptable level of output for a given core business process,
- deployment schedule: the time needed to acquire, test, and implement, and
- cost: life-cycle cost, including acquisition, testing, training, and maintenance.

5. IDENTIFY AND DOCUMENT CONTINGENCY PLANS AND IMPLEMENTATION MODES

According to the above steps, the following Table 3 is proposed as a general template to be filled, in order to identify and describe BC activities within the organization of a CI.

Table 3 General template for BC planning for climate change-related incidents

Phase	Time Frame	Activity
Phase I- Activation and Relocation	Approx. 0-12 Hours	■ **Alert and Notification**. The agency has established specific procedures to alert and notify the [executive director/general manager], senior management staff, and members of the advance team, operations team, support teams and contingency teams that BC activation is imminent. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Initial Actions**. The agency has identified specific actions to be taken to terminate primary operations and activate BC team, communications links, and the alternate facility. [*Briefly describe actions or refer to list of actions in appendix.*] ■ **Activation Procedures Duty Hours**. The agency has established procedures for an efficient and complete transition of direction and control from the primary facility to the alternate facility, and includes measures for security at both sites. These procedures complement the transportation agency's evacuation plans and emergency response plans. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Activation Procedures Non-Duty Hours**. Procedures for the notification of key staff when not at primary site have been developed. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Deployment and Departure Procedures (Time-Phased Operations)**. Allowances have been made for partial pre-deployment of any essential functions that are critical to operations; determination will be based on the level of threat. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Transition to Alternate Operations**. The transportation agency has established minimum standards for communication, direction, and control to be maintained until the alternate facility is operational. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Site-Support Responsibilities**. The transportation agency has developed a checklist to guide activation of the alternate facility; procedures include provision for notification to alternate facility manager to ready site for operations. [*Briefly describe procedure or refer to procedure or checklist in appendix.*]
Phase II- Alternate Facility/ Work Site Operations	Approx. 12 Hours to Termination of Emergency	■ **Execution of Essential Functions**. The transportation agency will perform any essential functions determined to be critical to operations from the alternate facility or using temporary work orders or procedures. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Establishment of Communications**. The transportation agency will re-establish normal lines of communication within the agency, to external agencies, and to the public. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Support and Contingency Team Responsibilities**. Responsibilities will be assigned to transportation personnel to perform essential functions. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Augmentation of Staff**. As the situation comes under control, additional staff will be activated to provide other services and functions, as necessary. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Amplification of Guidance to Support and Contingency Teams**. Additional guidance will be provided to all transportation personnel in regards to duration of alternate operations and include pertinent information on payroll, time and attendance, duty assignments, etc. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Development of Plans and Schedules for Reconstitution and Termination**. As soon as feasible, the operations team will begin preparation of communication, vital records and databases, and other activities to transfer operations back to primary facility. Circumstances may dictate that a new primary facility is designated and subsequently occupied. [*Briefly describe procedure or refer to procedure or checklist in appendix.*]

Phase III-Reconstitution	Termination of Emergency	■ **Reconstitution Process**. The transportation agency will develop general guidance and policy on ending alternate operations and returning to a non-emergency status at the designated primary facility. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **Reconstitution Procedures**. The transportation agency will establish specific actions to ensure a timely and efficient transition of communications, direction and control, and transfer of vital records and databases to primary facility. [*Briefly describe procedure or refer to procedure or checklist in appendix.*] ■ **After-Action Review and Remedial Action Plans**. The transportation agency will develop a task force to assess all phases and elements of the alternate operations and provide specific solutions to correct any areas of concern. [*Briefly describe procedure or refer to procedure or checklist in appendix.*]

6. CONCLUSIONS AND PERSPECTIVES

The fundamentals of Business Continuity Management with its main component of Business Impact Analysis (BIA) and Risk Assessment (RA), have been presented herein focusing on the exposure and response of Critical Infrastructures to weather-related hazards due to climate change. The unprecedent, or of very low frequency, nature of these events makes the RA to provide low probability results, BIA to lack of evidence-based data and the BC plans of most organizations managing CIs, to exclude them. However, discussing the more frequent development of extreme weather events due to climate change and their impact to critical infrastructures, whose services need to be maintained more and more nowadays, reveals the emerging need to account for them in future BC planning, incorporating new ways of thinking and sources of information. More precisely, BIA should implement effects of future weather events focusing on critical services for allocation of resources, while RA requires a more thorough analysis on "how future may develop" based on scientific data and work. Key issues into BC process are timely recovery and impact mitigation. Adaptation measurements are strongly recommended, which directly affects the overall resilience of an organization. These should be viewed as a cornerstone to good corporate practice and society's normal function, embracing risk, security, insurance, legal, operational and safety issues.

Further to the study presented here and the respective work that has been conducted within the framework of EU-CIRCLE project, there are several other projects that confirm the importance that European Union pays to Resilience of Critical Infrastructures under climate change pressure. More particularly, H2020 has funded projects such as RESILENS (GA653260), DARWIN (GA653289), RESOLUTE (GA653460), which have prepared tools and Resilience Management Guidelines for Critical Infrastructures to address, among others, climate-related extreme natural events. Ongoing projects, such as ANYWHERE (GA700099) and beAWARE (GA700475) create technologies for early warning and situational awareness emerged by extreme weather and climate events, primarily addressed to first responders, incorporating also needs and requirements of CI operators. The resilience of CIs, being essential part of a city's functional system, is also included into European Resilience Management Guideline of SMR (GA653569) project, which provides guidance to cities and local governments in assessing and strengthening their resilience status. The latter guidelines are included among the guiding documents of the database of the European Climate Adaptation Platform Climate-ADAPT, a partnership between the European Commission and the European Environment Agency (EEA), with the support of the European Topic Centre on Climate Change Impacts, Vulnerability and Adaptation (ETC/CCA).

As a matter of fact, EU Adaptation Strategy of Eu-

ropean Commission has as key objective the "climate-proofing" action which, among others, targets to the enhancement of Europe's infrastructure resilience. Climate-ADAPT platform, part of EU strategy, with its strategic planning until 2021, aims to address gaps in knowledge about adaptation at different societal components, to facilitate the uptake of relevant knowledge by decision makers and to promote relevant collaboration among different sectors. Climate adaptation and CI protection are, furthermore, included among areas in which EU is oriented to strengthen under the next research and innovation framework programme of Horizon Europe for 2021-2027. A cluster for enhancement of civil security research is envisaged to be incorporated under Pillar II "Global challenges and European Industrial Competitiveness", within which research and innovation activities in relation to Union Civil Protection Mechanism, EU Adaptation Strategy, Sendai Framework for disaster Risk Reduction (2015-2030) and Paris Agreement (2016) will support implementation of relevant policies and development of technological tools for improved security and resilience of infrastructure and vital societal functions, with the climate-related hazards being a priority among natural hazards affecting infrastructures. In this direction, not only Business Continuity but a holistic Security climate change related approach, from one hand should be developed and prioritized by CIs, and from the other hand it should be integrated to support civil protection and disaster relief mechanisms and initiatives.

ACKNOWLEDGMENTS

The current study has been performed within EU-CIRCLE project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant agreement No 653824. Please see http://www.EU-CIRCLE.eu/ for more information.

REFERENCES

ANYWHERE (GA700099). EnhANcing emergencY management and response to extreme WeatHER and climate Events (ANYWHERE), funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 65460, during the period 2016-2019. More information: http://anywhere-h2020.eu/

Australian Academy of Science (AAS, 2015). What is climate change? Retrieved from: https://www.science.org.au/learning/general-audience/science-booklets-0/science-climate-change/1-what-climate-change

Baba, H., Watanabe, T., Nagaishi, M., Matsumoto, H. (2014). Area Business Continuity Management, a new opportunity for building economic resilience, Procedia Economics and Finance, 18, 296 – 303.

beAWARE (GA700475). Enhancing decision support and management services in extreme weather climate events, funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 65460, during the period 2016-2019. More information: https://beaware-project.eu/

BSI Group (2014). Adapting to Climate Change using your Business Continuity Management System.

DARWIN (GA653289). Expecting the unexpected and know how to respond, funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 653289, during the period 2015-2018. More information: https://h2020darwin.eu/

EU-CIRCLE (2017a). Deliverable 4.3 – EU-CIRCLE Resilience Framework. "EU-CIRCLE – a pan-European framework for strengthening Critical Infrastructure resilience to climate change", Project funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. More information: http://www.eu-circle.eu/.

EU-CIRCLE (2017b). Deliverable 4.4 – CI climate related business continuity model. "EU-CIRCLE – a pan-European framework for strengthening Critical Infrastructure resilience to climate change", Project funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. More information: http://www.eu-circle.eu/.

EU-CIRCLE (2017c). Deliverable 4.5 – CI resilience indicators. "EU-CIRCLE – a pan-European framework for strengthening Critical Infrastructure resilience to

climate change", Project funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. More information: http://www.eu-circle.eu/.

European Commission (EC, 2007). FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – Adapting to climate change in Europe – options for EU action, COM(2007) 354, Brussels.

European Commission (EC, 2009). Adapting to climate change: Towards a European framework for action, WHITE PAPER COM(2009) 147/4, Brussels.

European Environment Agency (EEA, 2014). Adaptation of transport to climate change in Europe - Challenges and options across transport modes and stakeholders, EEA Report No 8, Denmark.

European Commission (EC, 2013). Adapting infrastructure to climate change, COMMISSION STAFF WORKING DOCUMENT, Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – An EU Strategy o adaptation to climate change, SWD(2013) 137, Brussels.

Horrocks, L., Beckford, J., Hodgson, N., Downing, C., Davey, R. and O'Sullivan, A. (2010). Adapting the ICT Sector to the Impacts of Climate Change – Final Report, Defra contract number RMP5604. AEA group, published by Defra.

ISO 22301 (2012). Societal security - Business continuity management systems – Requirements, International Organization for Standardization, Geneva.

ISO 31000 (2018). Risk management – Guidelines, International Organization for Standardization, Geneva.

KEMEA (2019). Handbook for planning critical infrastructures security, Center for Security Studies-KEMEA, Athens.

RESILENS (GA653260). Realising European Resilience for Critical Infrastructure, funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 653260, during the period 2015-2018. More information: http://resilens.eu/.

RESOLUTE (GA653460). RESilience management guidelines and Operationalization appLied to Urban Transport Environment, funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 65460, during the period 2015-2018. More information: http://www.resolute-eu.org/.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems, 21(6), 11-25.

SMR (GA653569). Smart Mature Resilience, funded by European Union's Horizon 2020 Research and Innovation Programme, under Gran Agreement no 653569, during the period 2015-2018. More information: https://smr-project.eu/home/.

Trexler, MC and Kosloff, LH (2013). Adapting to Climate Change, 2.0 Enterprise Risk Management, Taylor & Francis Group.

Zawada B. (2018). Implementing ISO 22301: The Business Continuity Management system standard, Avalution Consulting.