# Hardware architecture for the evaluation of BCP robustness indicators through massive data collection and interpretation

**Oussema Ben Amara**
IMT Mines Albi, University of Toulouse
oussema.ben_amara@mines.albi.fr

**Daouda Kamissoko**
IMT Mines Albi, University of Toulouse
daouda.kamissoko@mines-albi.fr

**Frederick Benaben**
IMT Mines Albi, University of Toulouse
frederick.benaben@mines-albi.fr

**Ygal Fijalkow**
INU Champollion, University of Toulouse
ygal.fijalkow@univ-jfc.fr

## ABSTRACT

Recently, the concept of robustness measurement has become clearly important especially with the rise of risky events such as natural disasters and mortal pandemics. In this context, this paper proposes an overview of a hardware architecture for massive data collection in the aim of evaluating robustness indicators. This paper essentially addresses the theoretical and general problems that the scientific research is seeking to address in this area, offers a literature review of what already exists and, based on preliminary diagnosis of what the literature has, presents a new approach and some of the targeted findings with a focus on the leading aspects, having a primary objective of explaining the multiple aspects of this research work.

### Keywords

Business continuity plan, social sciences, risk management, robustness, embedded hardware.

## INTRODUCTION

The consequences of harmful and brutal events at the origin of crisis situations (pandemic, fire, flood, terrorist attack, etc.) are constantly rising. In fact, the increasing complexity and densification of our society (i) generates additional events to natural events, (ii) disrupts the environment, thus creating additional natural events, and (iii) increases its sensitivity to events (Elmqvist et al. 2019).

In fact, industrial societies do not only produce wealth but also risks. Those risks do not tend most of the times to be under control and thus their management is a challenging aspect for the recent research works and theories that are trying to solve the risk issues (Beck 2001).

For example, the end of the Cold War promised a move away from nuclear, radiological, biological, and chemical threats. Since September 11, 2001, the fear of large-scale terrorism has been considered at the highest level of national risk prevention policies (Revel 2005).

Another example is illustrated by the fact that the Permanent Observatory of French Natural Disasters and Natural Risks has counted between 2001 and 2017, 1593 events having caused 25,870 victims for a cost of 34,895 million dollars. The COVID-19 health crisis we are facing illustrates, if proof were needed, the acuity of this issue.

These events affect many organizations and can lead to a delay or a permanent cessation of activities.

Crisis management is generally defined by four phases: preparation, prevention, response, and recovery (Altay and Green 2006). In this research work, the preparation phase is the one that is essentially considered. In fact, Anticipatory management has become a priority for many public and private stakeholders: the government, public services, private companies, law enforcement organizations, operators, etc. (Kamissoko et al. 2019)

To meet this major security and business continuity challenge, organizations are required to develop a plan known as a Business Continuity Plan (BCP). It "represents the set of measures designed to ensure the maintenance of the provision of services or other essential or important operational tasks of the company, followed by the planned resumption of activities" according to the French GSDNS (General Secretariat of Defense and National Security) practical guide “A Guide to Implementing a Business Continuity Plan”.

However, one main drawback of BCPs is that they are sometimes not easily deployable, nor are they assessable in real-life situations (Liu et al. 2015). The main reasons that can be suggested are the following: (a) because it is impossible to reproduce risks without their irreversible consequences; (b) because economic losses, the difficulty of mobilizing all resources and stakeholders at the same time, and human behaviors are not easy to anticipate nor to simulate. It is therefore essential to have indicators to measure the feasibility and the robustness of BCPs without having to fully deploy them.

The main question that this article aims at tackling is the following: **How to design and implement robustness indicators which are required in the design of better BCPs, but also in the identification of areas for improvement in the day-to-day management activities of organizations?**

In fact, this paper basically discusses the general and scientific problems that scientific research seeks to solve in this field, provides a literature review of what already exists, introduces a new approach, experimental study, and some of the targeted results, with a focus on the leading aspects and the consequences of the research work.

## GENERAL PROBLEMS AND ISSUES

Studies and methods have attempted to deal with the issue of how to build a better BCP in various ways. With the increasingly growing crisis events, new studies are being undertaken and this research is one of them. In the next following two subsections the general issues that this study is aiming to answer are discussed.

### Risk and Business Impact Aspect

The purpose of this research work is mainly to solve different issues in various aspects, one of them is the managerial aspect. When risk events happen, the organization should still be able to resume its activities using a pre-defined BCP. To this day, many models, and tools for BCP elaboration are available (Savage 2002). Risk analysis tools have basically two different approaches: quantitative risk analysis (Finney 2005) and qualificative risk analysis (Conrad et al. 2017).

However, the qualification of the BCP itself is still a challenging scientific question because evaluating a tool that its main objective is to assure the activities’ continuity means measuring a purpose-driven assessing tool. On this issue, our main contribution will be the qualification of BCPs in terms of robustness, efficiency, and resilience.

To be able to qualify the BCP in an efficient way, all surrounding data should be considered, particularly the societal events and information, which are discussed within the following subsection.

### Societal Aspect

Most of the present BCP tools and guidelines do not include the societal events and the society’s data while dealing with the risk events that can perturb and even sometimes suspend the organization’s activity (Okrent 1980).

On this point, this research work will include a societal data analysis and interpretation that should be realized objectively. The faced challenge then is to assure the objectivity of this step and to interpret it correctly. Namely, the data will be obtained through result-oriented and objective approaches of surveys, and questionnaires when needed, to identify the relevant data for the organization. The organization that will be considered as the first use case of this research work is the Hospital Center in Albi, France. In fact, the importance of this step is making the organization able to consider different surrounding crucial data, especially from the society’s activities, figures, and aspects.

### Hybridity of the Project

As observed in the two previous subsections, the consideration of both aspects; the Risk impact aspect and the societal aspect, is the key to this contribution.

Risk analysis with considerations to the societal factors will enable the qualification of the BCP and its robustness measurement with even a more realistic sense. In fact, the considered approach for this research work is then the following: **Taking into consideration the variety of societal events that can contribute to the crisis situations making it possible to develop better BCPs throughout a robustness measurement process.**

The following section will include an overview for the scientific issues within this approach.

### Scientific Issues

The interest of this study is basically to proceed using a hardware implementation the data analysis in the risk or crisis management context. In fact, most applications for risk management are implemented only on software and providing then simulated results. The hardware implementation notion in this field of study, which is the industrial engineering applications, is a recent approach. By partially running the data within a hardware implementation to perform the acquisition phase for example, the application case is more customized and hence can perform better in terms of the time delay execution (Aporntewan and Chongstitvatana 2001).

Given the diversity of data sources, the difference in transmission frequencies and the risks of loss (hacking, disruption, failure), defining a hardware architecture could be a challenging task to face since such issues could always occur and should be then treated carefully. There are approaches such as WSN (Wireless Sensor Networks), Multi-Sensor Fusion Technology, Internet-scale resource-intensive sensor network services, IoT. Even though these technologies are improving the performance in many domains, some aspects such as large-scale integration, reliability, security, deployability, transposability to any organization and the capacity of integrating several types of sources (including those from surveys, human expertise, etc.) are still challenging facets to cover during a hardware/software development and especially in the context of risk management (Abdulkader et al. 2018). The hardware implementation can assure a high security for the gathered information in some application and a high speed of data proceeding (Biasizzo et al. 2005).

Treating data using WSN for example can be very useful for different reasons: (i) Minimizing the energy consumption while maintaining connectivity of the nodes (sensors), (ii) Suitable for real-time applications, (iii) Making it possible to gather and aggregate an important amount of data with a high frequency and (iv) WSN is a cloud-friendly approach making it possible to store an important amount of data (Raghavendra et al. 2006).

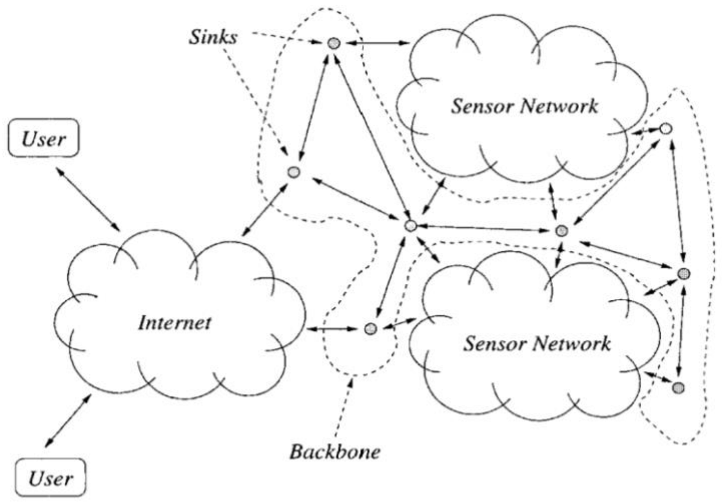


**Figure 1. WSN's nodes and the users' interactions (Raghavendra et al. 2006)**

The objective will be to propose the architecture of a decentralized network of data sources (Figure 1) that meet the previous limitations. The proposal of this architecture will consider the Humanities and Social Sciences (HSS) data collected through the survey. The aim is to facilitate access to information by stakeholders depending on the context (before, during or after the disruption).

The definition of a hardware architecture integrating several data sources is a new aspect especially for risk management application. In this context, the next section will discuss the literature review of this research work.

## LITERATURE REVIEW

The establishment of an efficient BCP in a good shape and form has been a scientific question for a long time. Several studies and approaches mentioned some of the ways to optimize the business continuity policies. In the following paragraphs, some of those studies and approaches will be discussed with a mention to what is missing and how this new study can consolidate the results obtained.

### Business Continuity General Guidelines

W. Lam (2002) in his study "Ensuring business continuity" mentioned the steps to obtain a good business plan. The steps such as identifying the business threats and conducting a risk analysis included several aspects and resources to consider, but very less societal data and societal aspects related to the threats faced. As well, the step of testing the BCP did not consider any robustness indicators or recommendations for reviewing the plan. The aim of this study is to basically to give the recommendation to build a good business plan. For this reason, focusing on this study is what gives a better idea about what aspects are missing in making the BCPs and how to solve them.

A research work called "Business Continuity Planning: A New Road to Nurture Business Growth" held by D. Kumar, A. Kumar Rai, H. Mishra, and P. Srivastava (2013) discussed the key-features of BCP in order to define the goals that should be met when a BCP is implemented within an organization. This work focuses basically on the following milestones: (a) identifying the critical business operation; (b) identifying the risk associated with those operations, and (c) Finding the ways to mitigate or avert the risk. The study takes into consideration the financial and business risks but lacks consideration and explanation of other types of risks. In fact, the risks can be various as they can be the result of different abnormalities in one or many dimensions such as the sociological aspect. It is thus a focused research in the financial sector and taking as a use case the banks' business activity while considering the requirement analysis, design and implementation of BCP based on the business units within the studied structure and the operational risks, especially on the financial aspect and significantly to banks as a use case organization.

Another study called "A new framework for business impact analysis in business continuity management" held by S.A. Torabi, H. Rezaei Soufi and N. Sahebjamnia (2014), considered an analytic network process (ANP) to determine the network structure of the problem and estimate the continuity parameters. Although this study was based on several key products' breakdown, it did not mention the importance of multidimensional data in measuring the risks and thus deducting the well-based business continuity plan. As for the testing part, a use case is studied but only with simulating the internal technical and numeric data. The external data or societal events are not measured or included and as well robustness indicators did not take part of the simulation but a different approach which basically considers the key products is treated.

### Business Continuity within Healthcare Organizations

When it comes to healthcare organizations that should not suspend its activities in any way or form such as hospitals, as of 2000, attacks on hospital staff have made it necessary to rethinking the protection of individuals by putting in place agents, among other things security. Moreover, before the COVD-19, it was terrorism, the heat wave and the H1N1 pandemic (2009-2010) that caused a huge damage to the healthcare system and hospitals in France. This addresses the question of how to maintain hospitals in their best performance of activities when it comes to crisis situations. The research work done by C. Van der Linde (2018) in this context names the nature of the crisis in order to best organize the health response, identifies the cognitive behaviors adapted to stress situations, essential for crisis management steering and tackles the principles, method of reasoning and management tools required steering the organization of the healthcare activity of his health establishment.

Furthermore, this work considers also that the culture of questioning must take precedence over that of the plan. It is a question of creating and putting in action a transverse management privileging collaborative intelligence (Van der Linde 2018).

On the other hand, the threat of an influenza pandemic is a serious risk, mentioned as one of the major crisis scenarios by the U.S. Department of Homeland Security, due to its significant impact on society. This risk requires a preparation, by means of an anticipative and proactive approach and the whole of society, in each of its areas of activity (Breton-Kueny and Segovia-Kueny 2008). In this context, the covid-19 that the world is experiencing recently makes the healthcare organizations an interesting and justified choice as a first use-case to be considered in this specific period. In fact, healthcare services are affected in their organization (activity, overload, capacity breakdowns, staff fatigue and absence, priority management of the pandemic, deprogramming), in their environment (patients, providers, etc.) and by the local national and international context (global spread of the pandemic, political decisions, media information, standards and regulations).

The crisis is not uniform and can evolve over time. Indeed, there may be different levels of severity that disrupt the day-to-day running of the hospital (human resources, equipment, etc.). Thinking in this way means first identifying the activities that are essential for the hospital and knowing how to adapt. Example: the COVID-19 pandemic in March 2020 was associated with a widespread containment and deprogramming of the healthcare services. This is not the same situation that we are living today while the health crisis is still present.

Breton-Kueny and Segovia-Kueny (2008) proposes a model for the development of BCP based on several successive stages. However, this model, despite its relevance in terms of planning different actions to be undertaken chronologically in the specific case of a “flu pandemic” crisis, it lacks some subtlety because it mainly applies to a general case that does not necessarily integrate the real situation.

### The Particularity of this Research Work

The hardware architecture that this research work is aiming to tackle will make it possible to consider the types of data available in the organization, particularly the healthcare ones, since the first use case of this study is Albi’s Hospital Center. The previous study mentioned the cognitive behaviors adapted to stress situations and some of ways to act in these situations. The way to develop a hardware implementation and the robustness keys for qualifying the BCP is the horizon of this study and here comes this research work to answer the future questions of how to make a better BCP.

Based on the previous studies, this research work is covering some of missing aspects for making BCPs such as the consideration of societal data but also proposes a new approach to proceed the gathered data through a hardware implementation. In fact, the hybridity within this study consists of integrating both technical and societal data which is a key point. Moreover, the hardware architecture for proceeding all the collected data through a data-gathering process and the proposal of robustness indicators along with recommendations for the BCP is what makes it possible to efficiently review, consolidate and iterate the process of building BCPs for a variety of organizations.

## THE PROPOSAL

Our contribution is mainly to assure the quantification of BCPs. To meet this goal, the principal idea is to include the societal data into the quality measurement and to propose some robustness indicators for the under-test plans making it possible to suggest recommendations in a further step.

The methodology of the study is based principally on the following milestones:

- Proposal of a knowledge gathering process: Including several types of technical data and societal data. The types of data and the approach to collect them will be more detailed in the following section.
- Proposal of a hardware architecture: Storage and interpretation of the collected and aggregated data using a physical type of memory such as SRAMs and ROMs, a cloud storage or a hybrid storage combining both technologies depending on the need.
- Proposal of robustness indicators: Indicators taking into consideration the data gathered through the first process and making it possible to qualify the BCPs of multiple types of organization. By studying the gathered data and representing the aggregations within the organization’s type or model, the robustness indicators are possible to build.

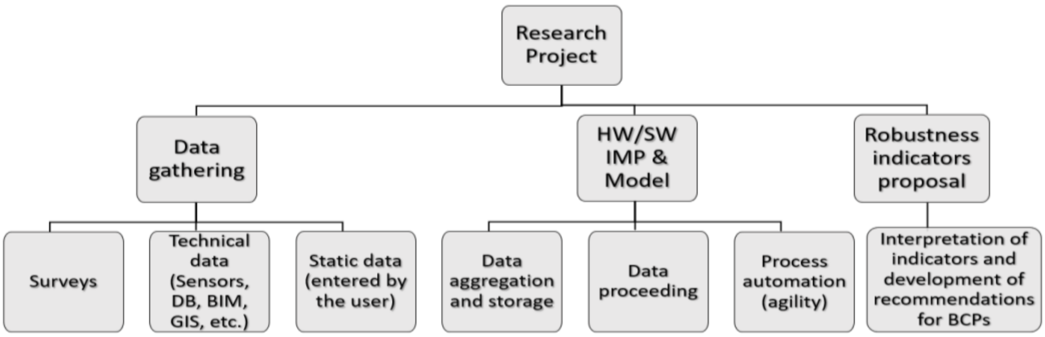


**Figure 2. The proposal's methodology overview**

Figure 2 below shows how the three different milestones are implemented. Starting from the data gathering process (*8-10 months process*), then the hardware model (*12-16 months process*) and finally the robustness indicators' proposal (*6-8 months process*) which will make it possible at the end to interpret the quality of the BCPs and follow up with recommendations accordingly.

The particularity in this proposal is to integrate effectively different types of data at the same time such as societal data, financial data, physical data (sensors and interconnected objects) and use them to perform a complete data analysis of the organization's environment. This approach will make the evaluation of the BCP in an integral and multidimensional aspect possible which will lead to performing better results in terms of both risk and business continuity management.

### The Experimental Study

Based on what is mentioned previously, the experience traits of this study are basically including three forms:

- ***The societal data collection:*** To gather the societal data some voice and written surveys are held. The surveys with the relevant organizations aim to provide proper data for one or more use-case. Noting that the surveys are held on a defined period such as some months of a real happening pandemic like covid-19, the collected data have enough pertinence to be interpreted and result into the societal aspect definition for one or more organizations in a risk or crisis event. This type of data is thus forming one form of the experimental purpose of this study.

  In this context, this research work concerns an exceptional health situation (EHS). For the French authorities, this refers to "the occurrence of an emerging, unusual and/or little-known event that goes beyond the scope of routine alert management in terms of its scope and seriousness (particularly in terms of its impact on the health of populations or the functioning of the healthcare system) or its media nature (actual or potential) and which may go as far as a crisis" (Nahon and Michaloux 2016). Which is given by the Instruction No. 274 DGS/DUS/CORRUSS 2013 of June 27, 2013).

  The specificity of the proposed approach is to use a past case, the history of the crisis experienced (beginning of the organization's exposure to the Covid 19 crisis). The social data are gathered from feedback from practitioners (hospital staff) and users (patients) through interviews and a survey type of inquiry concerning a lived history. As S. Huberson and B. Vraie (2015) wrote: "the philosophy of the BCP is to prepare for war in peacetime, except that we can use what happened during the war to build a more robust BCP".

- ***The technical data collection:*** The technical data can have many forms but also sources such as physical sensors, information systems, databases, knowledge models, BIM (Building Information Modeling), GIS (Geographical Information System), simulation models and more. The collection of this data will be based on a hybrid and customized approach that involves both the consultant and the organization. To require the data to gather, the consultant must take into consideration the data available within the organization but also relevant to the use case of this study.

- ***The hardware architecture testing:*** As the final aim of this study as mentioned before is to propose a hardware architecture for the evaluation of robustness indicators, the collected data should be physically implemented within a hardware architecture. Simulations at first can provide some initial results and thus the expected results from the hardware architecture should be in match the simulation aims and outputs. The purpose of this part is to propose robustness indicators by exploiting the data stored in the physical architecture.

### The Targeted Results

The key results of this study are the proposition of robustness indicators and their evaluation within the hardware implementation. These robustness indicators will be based as discussed previously on the societal aspects, deducted from the surveys' information, added to the technical data obtained within the organization's different services or departments. This evaluation will allow the qualification of BCPs of different use-case organizations.

The system as shown in figure 3 consists of five main phases which are the acquisition of data, its storage, processing to perform the indicators' calculus and then finally the assessment of the elaborated indicators which will result in the predictions and recommendations given for the considered BCP of a particular organization. The datapath that will invoke the targeted results is given below by figure 3.

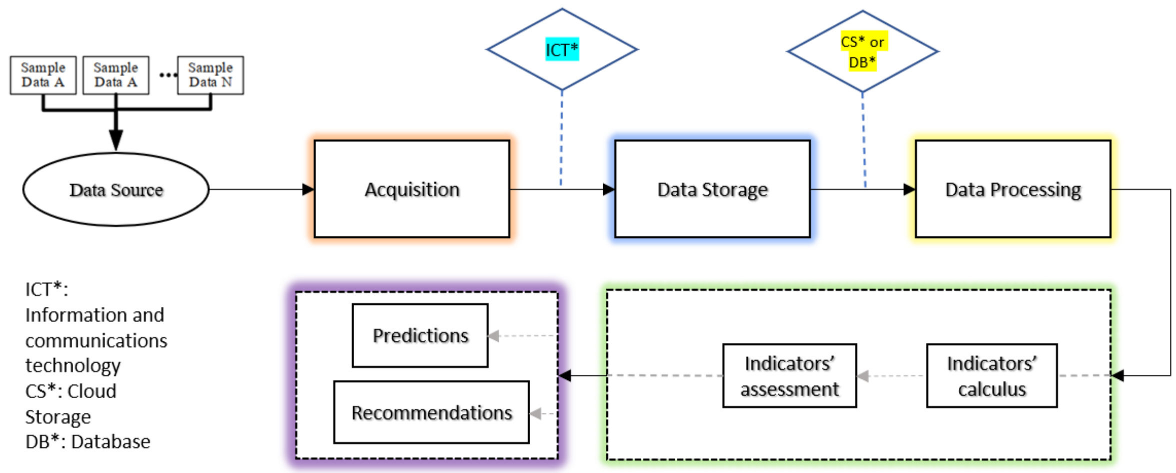


**Figure 3. The system's overview**

The results should as well include an "advisory" option. This option will treat the BCPs robustness case by case and define their profile as well in terms of resilience, efficacity, reliability, etc.

The outputs of this study and architecture in general will allow the optimization of risk management methods within the organizations by characterizing their evolutionary paths and possible improvements in terms of BCPs. In fact, firstly this research work is considering the societal aspects throughout the data collected using the surveys. Secondly, the technical data will be obtained from the different equipment such as GIS, BIM, sensors and more. This data will be then proceeded within the hardware architecture. Finally, the proceeded and aggregated data will be used to test the robustness indicators making it possible to deduct the adequate recommendations for the qualified BCPs.

Using those results, the organizations such as Albi Hospital Center, which is our first use case, will be able to face crisis events using more solid plans adapting to the complex and multidimensional real-life situations.

## CONCLUSION

Studies and approaches tried in different ways to treat the question of how to make a better BCP. With the crisis events that are constantly rising, new studies are being held and one of them is this study.

The originality of this study is to go beyond the technical data by fully considering other dimensions, in particular social factors to be applicable to any type of organization to make the link with the steering and decision support processes. The results will make organizations less vulnerable to crises by proposing more robust BCPs and identifying critical components and resources.

On another side, this developed hardware architecture resulting of this research work should let it be possible for organizations with different types to consolidate their BCP with robustness indicators generated by the proceeding data within the hardware implementation. The implementation should be transposable and generic to multiple types of applications. The tests on the use cases should on their part qualify a structured methodology to be adopted on several structures of organizations.

Having a main objective of explaining this recent research work, this paper discusses basically the scientific and general issues that the scientific research is trying to solve in this field, gives a literature review of what already exists and proposes a new methodology and some of targeted results with a focus on the leading aspects. The next step following this research work will be the proposition of a knowledge-gathering process and the aggregation of both the technical and societal data. On the long term, this research work will be followed by the hardware architecture proposal after the full definition of the data-gathering process.

## REFERENCES

Abdulkader, O., Bamhdi, A. M., Thayananthan, V., Jambi, K., & Alrasheedi, M. (2018, February). A novel and secure smart parking management system (SPMS) based on integration of WSN, RFID, and IoT. In 2018 15th Learning and Technology Conference (L&T) (pp. 102-106). IEEE.

Altay, N., & Green III, W. G. (2006). OR/MS research in disaster operations management. European journal of operational research, 175(1), 475-493.

Aporntewan, C., & Chongstitvatana, P. (2001, May). A hardware implementation of the compact genetic algorithm. In Proceedings of the 2001 Congress on Evolutionary Computation (IEEE Cat. No. 01TH8546) (Vol. 1, pp. 624-629). IEEE.

Biasizzo, M. M. F. N. A., Mali, M., & Novak, F. (2005). Hardware implementation of AES algorithm. Journal of Electrical Engineering, 56(9-10), 265-269.

Breton-Kueny, L., & Segovia-Kueny, S. (2008). Le plan de continuité d'activité « pandémie grippale » dans les organisations. Annales des Mines-Responsabilite et environnement (No. 3, pp. 78-82). ESKA.

Conrad, E., Misenar, S., & Feldman, J. (2017), Chapter 1 - Domain 1: Security risk management, Editor(s): Eric Conrad, Seth Misenar, Joshua Feldman, Eleventh Hour CISSP® (Third Edition), Syngress, pp. 1-32, ISBN 9780128112489

Elmqvist, T., Andersson, E., Frantzeskaki, N., McPhearson, T., Olsson, P., Gaffney, O., ... & Folke, C. (2019). Sustainability and resilience for transformation in the urban century. Nature sustainability, 2(4), 267-273.

Finney, M. A. (2005). The challenge of quantitative risk analysis for wildland fire. Forest Ecology and Management, 211(1-2), 97-108.

Huberson, S., & Vraie, B. (2014). La continuité d’activité est une philosophie d’entreprise qui consiste à préparer la guerre en temps de paix. Securite et strategie, 18(3), 24-26.

Kamissoko, D., Nastov, B., Benaben, F., Chapurlat, V., Bony-Dandrieux, A., Tixier, J., ... & Daclin, N. (2019). Continuous and multidimensional assessment of resilience based on functionality analysis for interconnected systems. Structure and Infrastructure Engineering, 15(4), 427-442.

Kumar, D., Rai, A. K., Mishra, H., & Srivastava, P. (2013). Business continuity planning: A new road to nurture business growth. International Journal of Computer Theory and Engineering, 5(1), 151.

Lam, W., (2002). “Ensuring business continuity”, IT professional, 4(3), 19-25.

Liu, B., & Bi, J. (2015). On the deployability of inter-AS spoofing defenses. IEEE Network, 29(3), 82-87.

Nahon, M., & Michaloux, M. (2016). Dispositif d’organisation de la réponse du système de santé en situations sanitaires exceptionnelles (ORSAN). Journal Européen des Urgences et de Réanimation, 28(2-3), 100-104.

Okrent, D. (1980). Comment on societal risk. Science, 208(4442), 372-375.

Raghavendra, C. S., Sivalingam, K. M., & Znati, T. (Eds.). (2006). Wireless sensor networks. Springer.

Revel T. (de), 2005, Menace terroriste, approche médicale : nucléaire, radiologique, biologique, chimique, Eurotext.

Savage, M. (2002). Business continuity planning. Work study.

Torabi, S.A., Soufi, H. Rezaei, & Sahebjamnia, N., “A new framework for business impact analysis in business continuity management (with a case study)” Safety Science,Vol. 68,2014,pp. 309-323, ISSN 0925-7535.

Ulrich Beck, La société du risque. Sur la voie d’une autre modernité, trad. de l’allemand par L. Bernardi. Paris, Aubier, 2001.

Van der Linde, C. (2018). Chapitre 5. La gestion des situations sanitaires exceptionnelles et de crise. Dans : Michel Louazel éd., Le management en santé : Gestion et conduite des organisations de santé (pp. 493-524). Rennes, France: Presses de l’EHESP.