RISK ASSESSMENT OF A SOLAR ATTACK ACCORDING TO ISO 31000 STANDARD

Igor Lavrnić[1] – Ana Bašić[2] – Dejan Viduka[3*]

[1]College of Academic Studies – General Economics" Dositej" Belgrade, 11000, Serbia
[2]Faculty for Applied Management, Economics and Finance, University Business Academy, - Belgrade, 11000, Serbia
[3]VONing, research, consulting and services, Osijek, 31000, Croatia

ARTICLE INFO

***Article history*:**
Received: 24.12.2019.
Received in revised form: 20.6.2020.
Accepted: 26.6.2020.

Keywords:
ISO 31000
Risk Assessment
Solar attack

DOI: https://doi.org/10.30765/er.1566

Abstract:

Energy supply remains *the greatest challenge for many of Eastern European countries and their economy. In post-soviet and ex-Yugoslavian countries, till today there exists a system where some of the power plants rely on high voltage (HV) and medium voltage (MV) power grids in the process of distribution of electric energy (EE) to final consumers. This makes them vulnerable to solar storms due to HV power transformers which are especially sensitive to geomagnetic induced current (GIC). The acquisition of electrical power infrastructure could put the electrical infrastructure out of service from a couple of months to a year or more. Loss of income, for ordinary families, is a primary hazard of a long power outage. Business continuity of industry and other critical infrastructures (CI) is important in this scenario, but it is a significant challenge for small businesses and enterprises as well. This paper introduces ISO 31000 standard to such scenarios with the primary goal of achieving resilience of companies against such disaster as a new method of vial response to avoid scope of similar hazards.*

1 Introduction

The strongest ever reported and recorded solar storm is the Carrington event, September 1st, 1859. Reports from all over the world described that the Auroras provided enough light that people could clearly see the text in newspapers [1], [21]. Telegraph systems in Europe and North America received electrical shocks causing fires and injuries to operators [2], [3]. The projection of the cost to modern society (by the US National Academy of Sciences) if such an event was to happen now days is in the volume of 1 trillion to 2 trillion EURO's in the first 12 months while the time of and recovery is estimated to be 4 to 10 years [4]. In the 21st century, the "Halloween storm" (occurred October 30th, 2003), is the strongest recorded storm causing interferences and collapse of different technical systems of power grids all over the globe [5]. A transformer at a Swedish nuclear power plant suffered from increased oil temperature of 13˚C before the transformer was assisted in cooling down [6]. The same storm in South Africa caused a failure of 15 transformers. It took more than 4 years in some parts of the country for a full recovery. The purchase and delivery of electrical power infrastructure components, in regular conditions, takes up to 12 months. In a case of a super solar storm this estimation goes from 4 years to 10 years [6]. Modern society could not sustain a power outage that could paralyze the nations infrastructures for several years. This paper presents how a risk assessment strategy could deal with the challenge of business continuity of companies and CI. The main goal of a risk assessment as a methodology, in which risk levels are quantified, is to provide required safety systems for protection of operators from possible injuries and damages to the system itself. The International Organization for Standardization (ISO) published the first risk management standard, in November 2009, under the title ISO 31000:2009 Risk Management - Principles and Guidelines [7]. This standard provides the

* Corresponding author
E-mail address: dejan@viduka.info

main principles of risk management from various sources, covering the organizations size, type, complexity, structure, activities, and location.
This paper offers a solution for minimizing the consequences of solar storms by using a risk assessment procedure according to ISO 31000 standard as an integral part of organizational processes [8].

2 The phenomenon of a solar storm

A geomagnetic storm is a significant disturbance of the Earth's magnetosphere, temporarily caused by a solar wind, a shock wave or a magnetic cloud which collides with the magnetic field of our planet [10]. The strong solar wind pressure in the beginning compresses the magnetosphere in the process of interaction with the Earth's magnetic field and transfers a huge volume of energy into the magnetosphere of the Earth. In the main phase of this process, the electric current in the magnetosphere generates a strong magnetic force which pushes out the border between the magnetosphere and the solar wind. The Earth's Magnetosphere is not steady [11]. The process of a slow collapse of the Earth's magnetic field is ongoing for more than the last 150 years. The field strength is already significantly decreased, and its process of declining has recently accelerated, leading Earth towards serious consequences. The hazard of super storms is in direct relation with the sunspot activity level. A solar storm has its own cycle of activities, with peaks approximately every 11 years, when the probability of this phenomenon increases [1], [6].

2.1 Geomagnetic Induced Current

During coronal mass ejections, charged particles collide with our planet resulting in the appearance of energized auroras electro – jets. The generated electro-jets follow high altitude circular paths in Earth's magnetosphere containing multimillion amperes and more [9]. The Earth's geomagnetic poles in the magnetosphere are at an altitude of approximately 100 kilometers. Mirror currents appear near Earth's surface as a direct result of the induction of electro-jets from higher to lower magnetosphere. The main problem is created by these mirror currents which can flow into power transmission grids, pipelines, telecommunication cables and railroads tracks. The disaster that a Geomagnetic Induced Current (GIC) has made, could be easily compared to a nuclear bomb-Electro-magnetic Pulse effect [2], [6], [9]. The major focus during this research was on the relations and connections between the Space Weather phenomena and the hazard to HV power transformers and the Power Grid through the prism of the ISO 31000 standard.

A systematic research of theoretical studies of the ISO 31000 standard, up to and including 2018, was conducted with a strong focus on the specific nature of the subject – space weather and power outage. This paper investigates what is currently known about the benefits and limitations of the ISO 31000 standard implementation according to existing literature. The process of collection, study and analysis of existing literature were conducted during the research. Moreover, the comparative analysis of the research findings, included the analysis and synthesis based on acquired knowledge and experience.

2.2 Geomagnetic Induced Current impact on transformers

Several amperes only are enough to create a failure in a transformer's operations. An induced voltage (GIC) from 1 to 2 V in the neutral of the high-voltage winding's is enough to create a saturation of the HV transformer in less than a second. Inside the transformers tank, temperatures could increase by a hundred degrees within several minutes [1], [6], [11]. The highest temperature that has been measured was 750° F. The HV transformer switches, on average, 60 times per second between a saturated and unsaturated condition; consequently the normal hum of a transformer becomes increased. Areas of opposed magnetism in the core steel plates crash about and vibrate the 100-ton HV transformers. This kind of saturation can create excessive evolution of gas within the transformers. Final results in both circumstances is a major failure in the electrical systems voltage, and overloading of long transmission tie-lines. Moreover, a third harmonic could mislead protective relays to operate improperly and shunt a capacitor banks to overload [2], [10].

2.3 Solar Flares

A solar flare is a large energy release over the Sun's surface. During the flare's appearance, the Sun ejects a large cloud of atoms, electrons, and ions through the Sun's corona into space. These ejected clouds reach the Earth's magnetosphere within a day or two after the ejection [6]. The solar flares can disturb both

satellite communications, and radar due to ionosphere radio interference. Furthermore, solar flares can produce shortwave radio fades, blackouts, and effects on ground level systems.

2.4 Solar Proton Events

A solar proton event can reach Earth between 15 minutes to a few hours, and its effects can last for days. The instant effects produced by the Solar Proton Event (SPE) and later effects produced by the Coronal Massive Ejection (CME) has a strong influence on daily death rates due to heart attacks [12]. During SPE and CME death rates increase up to a maximum of 70%. In active/stormy geomagnetic days the K index increases up to 40 NT compared to quiet geomagnetic days where the K index is measured at less than 40 NT. A study by Stoupel presents research results showing that 788 Sudden Cardiac Deaths (SCD) happened during a 36-month period in Baku, Azerbaijan, clearly indicated correlation between SCD and solar storms [13], [14], [15]. These findings are relevant to business continuity and the ISO 31000 standard implementation due to a huge impact on human factors and normal operations of companies and CI [16], [17].

2.5 Coronal mass ejection

CME is a huge cloud of hot and magnetized plasma that, in the case of strong CME, can arrive to the Earth's magnetosphere within 18 hours. More typical travel time is 2 to 4 days. It can cause an array of negative destruction including ozone layer depletion and its effects on the magnetic field can last for days. The strongest recorded CME's happened on April 16th, 1938, (1,900nT), then October 12th, 1859 (1,760nT) and September 25th, 1909 (1,500nT). It is important to know that the Halloween storm in 2003 recorded 422nT [6] [1].

3 The impact of a solar storm

Losing one's job and consequently a source of income for ordinary families is the greatest hazard of all, that will follow a solar storm. Most of the population can only survive a few days without access to unpolluted drinking water. The collapse of an EE power supply drives the water pump to failure, leading water systems to poor performance. An even more serious issue if the failure of Waste treatment facilities, because the untreated waste stream can flow back into rivers, streams, or lakes. Eventually the lack of clean drinking water will be the worst consequence of a solar storm [2], [3], [4], [6], [17].

Road traffic would be significantly affected by loss of working traffic lights. Lack of fuel in cars, or money and operative gas stations to refuel cars will be a huge problem all over the country. Moreover, the revitalization of the banking sector would be government's highest priority since an EE power grid collapse will disable access to funds in banks. Suddenly, credit card usage, bank transactions and ATM cash withdrawals will be the only source of funds for living for an ordinary family. The whole economy of the country will face the same problems due to an interruption of EE power and water supply. Business continuity science, will prove that companies who implemented ISO 31000 and provided their own reslient resource for EE, both in power and water supply (as well as their major suppliers and buyers) will become leaders in the market in a very short period of time [8], [18].

4 Standard ISO 31000 concept

In the ISO 31000:2018 standard, risk is defined as the effect of deviation from the projected (expected) outcome of flow of events that can be positive or negative to companies' business. Risk is usually defined as a mixture of consequences of an event and the probability of its occurrence. ISO 31000:2018 cannot be used for certification only because it encourages organizations to make a comparison of their current risk management practices to ISO 31000:2018 good practice and experience in order to develop the most effective strategy for a company's improvement [4], [7], [17].

The first edition of the ISO 31000:2009 provided a definition and explanation based on long experiences of implementation of previous standards, and provides an excellent connection between the principles for managing risk, the framework for managing risk and the risk management process itself.

The second edition of the ISO 31000:2018 explains the interrelation between the risk management principle, the risk management framework (RMF) and the risk management process (RMP). Moreover, ISO 31000: 2018 does not include any examples on how to adapt and implement the framework [22].

4.1 The risk management principles

The ISO 31000 standards define major principles which are basic qualities required for risk management to be effective [7], [8]. The principles are [7]:

- Risk management is an integral part of all organizational activities.
- A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
- Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.
- Risks can emerge, change, or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.
- The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders.
- Human behavior and culture significantly influence all aspects of risk management at each level and stage.
- Risk management is continually improved through learning and experience.

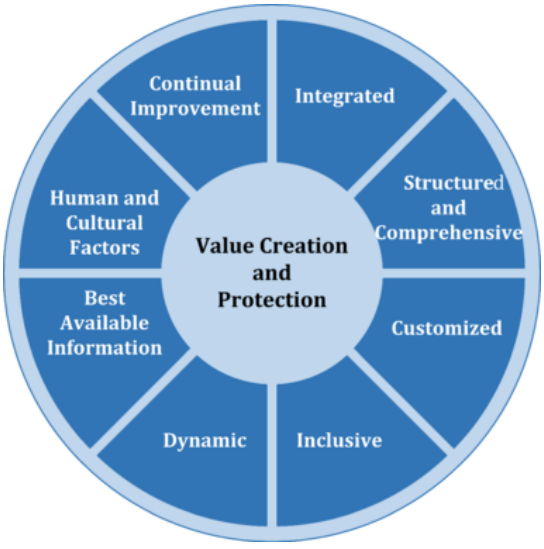

Figure 1. Major principles defined in standard ISO 31000:2018 [7].

4.2 The risk management framework

The "Plan, Do, Check, Act" cycle of constant improvement must be used as the basis for a risk management framework [7], [8]. Framework development encompasses integrating, designing, implementing, evaluating, and improving risk management across the organization [7]. Components of the risk management framework are shown in Figure 2.

This framework has a major role in assisting the process of risk management integration into its management system. That is why organizations must adapt the components of the framework to their specific needs.

Figure 2. Components of the risk management framework defined in standard ISO 31000:2018 [7].

4.3 The risk management process

The risk management process defined in ISO 31000 is illustrated in Figure 3 [7]. It consists of six key activities:

- Communication and consultation.
- Establishing context.
- Risk assessment (risk analysis and risk identification, in the end risk evaluation).
- Risk treatment.
- Monitoring and review.
- Recording & reporting.

The process of risk management must be an integral part of a company's management, deeply involved in the culture and practice and adjusted to a wide scope of business processes in the organization [7], [8].

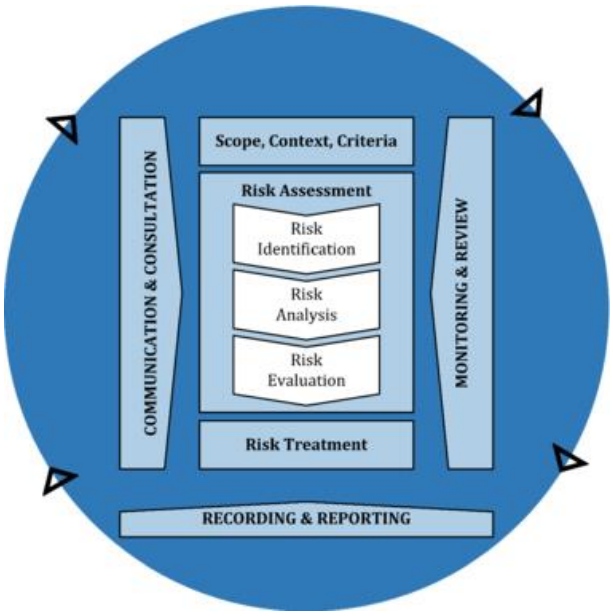

Figure 3. The risk management process defined in standard ISO 31000:2018 [7].

5 Risk management process of a solar attack

According to the authors of this paper, every organization must integrate risk management principles into a wide scope of business activities to achieve good business practice. The ISO 31000 sets out main principles; the most important is the framework and a process for core management at the beginning of the implementation. During implementation good practice must be implemented on all levels of the company. The risk in the business, especially a long power outage and good health of special equipment operators and key management is applicable to any type of organization in the public or private sector. In this chapter, special emphasis is placed on a solar attack as a high impact risk [7], [8].

5.1 Communication and consultation

Communication and consultation with all stakeholders is essential in all phases of the risk management process. Communication is used to obtain information about participants of the team analysis, priorities and main objectives, outputs from individual phases, and their database of the risks or the manner of implementation analysis. This step is essential for each of the decisions taken. At this stage of the risk management process, work should be done to spread awareness of the organization and individuals, the existence of the risk of a solar attack and its consequences on the organization's business and population. Any organization whose business may be affected by a solar attack must consider this kind of risk in a system integration of risk management into their business. A solar attack is a low frequency risk but with a very high impact of risk!

It is essential to introduce the public with the risk from a solar attack and measures which should be taken in case of such a disaster. This can be achieved by involving the media in spreading awareness about the solar attack [7], [8], [1].

5.2 Establishing context of risk management process

During the process of establishing context in the scope of a risk management process, it must be more focused on setting the parameters or borders around the company's risk and risk management roles and duties of an implementation team. Main requirements relate to external factors: 1. social, 2. cultural, 3. political and 4. economic and alignment with internal factors such as: 1. strategy, 2.resources and 3. capabilities.

5.3 Risk assessment

Risk identification techniques should be utilized in every risk assessment process in an organization, especially brainstorming, work breakdown analysis and expert facilitation. Risk analysis must include possible causes, sources, likelihood, as well as consequences to establish the inherent risk. At this step, the existing control measures in the system and the risk quantification should be done. Quantification of the identified risk involves defining quantitative and qualitative risk assessment. Quantitative risk assessment involves numerically expressed risk assessment [1], [7], [8]. Risk is the product of the probability of unwanted events and the damage caused by this risk. Probability of unwanted events is given by the frequency of events per time unit or activity. Consequences caused by the appearance of risk are given by monetary value. Based on the obtained values; risk is evaluated. Qualitative evaluation includes defining the magnitude of risk, the probability of a risk event and its determination. The authors of this paper emphasize that the risk of solar attack consequences must be considered. This is especially important for risk assessment procedures in organizations such as power distribution companies, telecommunication companies, aircraft, railway, etc. The evaluation of the level of risk is required to make decisions about further risk treatment, after the above-mentioned analysis. If the level of remained risk is not acceptable, risk treatment is obligatory.

5.4 Risk treatment

Risk treatment includes a set of measures, procedures and actions aimed at eliminating or controlling the causes of possible unwanted events and limiting its effects on business processes. At this stage, it is extremely important to choose the correct management strategyy, which involves risk control, risk reduction,

keeping the risk and risk transfer minimal. The strategy which is applicable to risk management of a solar attack is risk control. This strategy cannot eliminate risk, but using it is very useful for finding ways for risk control and the probability of its occurrence and effects on the system. Like any other response to a potential risk, there are actions that public and private organizations can or must take to counter or at least mitigate geomagnetic storms.

The resilience to a power outage could be achieved by installing a generator system (also known as cogeneration), using clean pipeline natural gas as a fuel source due to the fact that natural gas pipelines are less jeopardized by GIC [16]. The science of magnetic events and engineering solutions are both evolving, and much still needs to be studied, tested, and implemented to reduce our vulnerability to solar storms. There are, however, some strategies and engineering solutions that specific industries may employ now to mitigate the effects of a magnetic storm [4], [11], [18]. As mentioned power distribution companies will be the most immediately affected by an extreme geomagnetic storm. Although scientists are at work to identify a better set of strategies and solutions, there are already some:

- Turning off some systems before the time of highest activity may provide protection to the grid and its components. While electric power may be reduced or eliminated the equipment will survive the attack and be able to respond as needed once operations return to normal.
- Grid managers can increase excess capacity on lines to withstand spikes in current.
- High-density power lines can be replaced with low-density lines that are more favorable to Geomagnetic Induced Current.
- Installing Current Blocking Devices, as well as, transformers, neutral resistors in large transformers, allows neutral ground connection to significantly reduce Geomagnetic Induced Currents.
- Cathode protection is a technique that should be applied on long lines of EE power grids and telecommunications lines.
- Purchasing of Emporiums Transformer Neutral Blocking Devices which block Geomagnetic Induced Currents and installing them in the Power Distribution System.
- Installing a metal oxide varistors which provide an over-voltage protection.
- Provide water to the plant's engine-generators to provide emergency power and maintain water supply. Provide petrol stations with engine-generators to provide normal fuel supply.
- Educate the community, the greater public sector, and the general public.
- Engineer protective measures and motivate organizational changes that will empower responders
- Create space weather centers.

Government regulations should increase the minimal level of spare parts of the Power Distribution System, especially unique parts which will take some time to acquire due to a lack of power supply that will paralyze the nation. Aircrafts should avoid exposure to unsuspecting commercial travellers to harmful doses of radiation. To reduce the risk of equipment failure, airlines can divert proposed paths to lower latitude, or a lower altitude for radiation mitigation, even if flights are prolonged and fuel consumption is increased. Communication systems are also highly vulnerable to geomagnetic storms. Radar and radio operators also need to institute preventive measures. They can turn off communication devices during a severe storm which may prevent damage to internal components caused by static or GIC.

Police departments, courts, hospitals, water supply systems and other CI should organize an alternative power supply (natural gas EE generators, Solar EE generators, BIO gas EE generators etc.) and better data protection against the above-mentioned threats in order to remain operative [19], [20], [21].

It is not enough to know how to avert an energy catastrophe. Our larger task is to find ways to implement these strategies and solutions too:

Thus, the formation of a central early warning center with the mission of collecting, analyzing and producing space weather intelligence is essential [22]. Once organized, the center's primary focus should be to:

- Identify the vast network of emergency managers and first responders.
- Build and maintain direct channels of communication with this network to alert them of a potential or a detected geomagnetic event in near real-time.

There are many other industries we could address here with suggested strategies particular to them. These are only meant to show that there are actions we can take now to mitigate the threat to some degree.

5.5 Monitoring and review

An independent review of the risk management framework should be implemented on a monthly or quarterly basis by risk owners. Documenting the risk is a mandatory procedure within each phase of risk management and consists of all plans, estimates and reports or records that provide the basis for improving methods, tools, and the overall risk management process [7], [8], [23], [24].

6 Conclusion

Disaster recovery and rehabilitation efforts require enormous funds that are taken out from other developments in modern society. Therefore, it is important that alternative disaster mitigation actions such as an increase in resilience of companies and other CI to a long power blackout occur. Strong development production of EE from renewable sources for local communities to be more independent from the supply of power grids, should be an integral part of the developmental strategy for modern society of post-soviet and ex-Yugoslavian republics. At the same time, efforts to enhance the capacities of communities and coping systems at various levels and sectors towards self-reliance and self-sufficiency in managing disasters effectively must be sustained [20]. In particular, the focus of disaster management should be on the following:

- Organization of buildings or adjusting existing shelters in local communities with a water belt to protect citizens from deadly energetic solar cosmic rays during a strong solar attack.
- Founding an agency who will organize and coordinate all actions and educate and advise citizens on how to survive during an attack.
- Organization of better preparedness of power distribution systems regards purchasing of spare transformers, transformer neutral resistors and blocking devices, and installing them to the power distribution network.
- Organization of data storage and alternative power supply of all organizations that represent national infrastructure (police, social security, medical care system, courts etc.).
- Organization of life in big cities during a power outage regarding water supply, sewage, traffic etc. with procedures and delegation of duties for responsible persons.

When solving the problem of risk management, we can always keep in mind the thought by Ross Wright, CEO, Standards Australia International: „Ignoring a risk is like sleeping on a time bomb”.

References

[1] Thorberg R., (2012.) "Risk analysis of geomagnetically induced currents in power systems," Industrial Electrical Engineering and Automation TEIE-5296/1-54/2012, Lund University, Lund.

[2] James M., (2007.) "Solar Storm Analysis," Nuclear Physicist and Engineering Impact.

[3] Lavrnić I. and Viduka D., (2014.) "Kontinuiano poslovanje i Oporavak od katastrofa i izazovi Solarnog udara na Srbiju," Singidunum Journal of Applied Science DOI: 10.15308/SINTEZA-2014635-641, pp. 635 -640.

[4] Hapgood M., (2006.) "Space Weather its impact on Earth and implications for business," lloyd's Risk Insight, London UK.

[5] Cooper C., (2011.) "Preparing the North American Power Grid for the Perfect SolarStorm - White Paper 2011," Institute for Energy & Environment, Vermont Law School, Vermont, USA.

[6] Kappenman J. G., (2005.) "An overview of the impulsive geomagnetic field disturbances and power grid impacts associated with the violet Sun-Earth connection events of 29-31 October 2003 and comparative evaluation with other contemporary storms," Space Weather, DOI: 10.1029/2004SW000128, vol. 3.

[7] ISO 31000:2018, Risk Management- Guidelines.

[8] Purdy G., (2010.) "ISO 31000:2009 - Setting a new standard for Risk Management," Risk Analysis, vol. 30, pp. 881-886.

[9] Joseph R.Pinion, J. R. I., (2012.)"Geomagnetic Storms, the natural threat to our energy infrastructure".
[10] Klinger C., Landeg O., and Murray V., (2014.) "Power outages, extreme events and health: a systematic review of the literature from 2011-2012," PloS One, no. PloS One.
[11] Foster J. S., Gjelde E., Graham W. R., Hermann R. J., Kluepfel H. M., Lawson G. R. L., Soper G. K., Wood L. L., Woodard J. B., (2008.) "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," US Critical National Infrastructure Commission, Washington DC USA.
[12] Denton, M. H.; Kivi, R.; Ulich, T.; Rodger, C. J.; Clilverd, M. A.; Horne, R. B.; Kavanagh, A. J., "Solar proton events and stratospheric ozone depletion over northern Finland," ELSEVIER Journal of Atmospheric and Solar - Terrestrial Physics, vol. 177, no. -, pp. 218-227, 2018.
[13] Stoupel E. G:, Zhemaityte D., Drungiliene D., Martinkenas A., Abramson E., Sulkes J., (2002.) "Klaipeda cardiovascular emergency aid services correlate with 10 cosmo-physical parameters by time occurrence," Journal of Clinical and Basic Cardiology, pp. 225-227.
[14] Stoupel E. G:, Petrauskiene J., Kalediene R., Sauliune S., Abramson E., Shochat T., (2015.) "Space weather and human deaths distribution: 25 years observation (Lithuania 1989-2013)," De Gruyter - J Basic Clin Physiol Pharmacol DOI:10.1515/jbcpp-2014-0125.
[15] Stoupel E. G., "Space weather and Tachysytolic sudden cardic death (Scd) - Lessons from clinical cosmobiology," International Journal of Cardiology and Heart health DOI: 10.25141/2575-8160-2017-1.009, Vols. -, no. -, pp. -, 2017.
[16] Mees H., Crabbé A., Alexander M., Kaufmann M., Bruzzone S., Lévy L. and Lewandowski J., (2016.) "Coproducing flood risk management through citizen involvement: insights from cross-country comparison in Europe," Ecology and Society DOI: doi.org/10.5751/ES-08500-210307, Vols. 21-3-7.
[17] Sarmiento J. P., Hoberman G., Jerath M., Jordao G. F., (2016.) "Disaster risk management and business education: the case of small and medium enterprises," AD -Minister ISSN 1692-0279-elSSN 2556-4322, vol. 28, no. Universidad EAFIT, pp. 73-90.
[18] Casalas M. R:, Valverde S. and Solé R. V., (2007.) "Topological vulnerability of the European power grid under errors attack," Unevesitat Politecnica de Catalunya, Barcelona, Spain.
[19] Marx M. A., Rodriguez C. V., Greenko J., Das D., Heffernan R., Karpati A. M., Mostashari F., Balter S., Layton M., and Weiss D., (2006.) "Diarrheal illness detected through syndromic surveillance after massive power outage: New York City, August 2003," American Journal of Public Health ISBN 0-87553-035-4, vol. 96 No3, pp. 547.
[20] Weaver M., (2004.) "Halloween space weather storms of 2003 NOAA Technical Memorandum OAR SEC-88," NOAA and Space Environment Center, Colorado, USA.
[21] Pulkkinen A., E. Bernabeu A. Thomson, A. Viljanen, R. Pirjola, D. Boteler, J. Eichner,P. J. Cilliers, D. Welling, N. P. Savani, R. S. Weigel, J. J. Love, C. Balch,C. M. Ngwira, G. Crowley, A. Schultz, R. Kataoka, B. Anderson, D. Fugate, J. J. Simpson, and M. MacAlester. (2016) "Geomagnetically induced currents: Science, engineering, and applications readiness" AGU Space Weather, https://doi.org/10.1002/2016SW001501.
[22] Edly F. Ramly; Mohd Soffian Osman (2018), Development of Risk Management Framework - Case Studies, Proceedings of the International Conference on Industrial Engineering and Operations Management Paris, France, July 26-27, 2018; IEOM Society International;
[23] Asep Syihabuddin, Yohan Suryanto, Muhammad Salman (2019); PROCEEDINGS OF THE 1st STEEEM 2019; Volume 1, Number 1, 2019, pp. 341-352; Universitas Ahmad Dahlan, Yogyakarta-Indonesia, December 30, 2019; ISBN: 978-602-0737-35-5.
[24] Yaser Rahimi; Reza Tavakkoli-Moghaddam; Seyed Hossein Iranmanesh; and Maliheh Vaez-Alaei (2018); Hybrid Approach to Construction Project Risk Management with Simultaneous FMEA/ISO 31000/Evolutionary Algorithms: Empirical Optimization Study Journal of Construction Engineering and Management, © ASCE, ISSN 07339364.; https://doi.org/10.1061/(ASCE)CO.1943-7862.0001486.