11º Workshop em Engenharia e Tecnologia Espaciais
18, 19 e 20 de agosto de 2020

CEMADEN: A Study of Technological Vulnerabilities in a Natural Disaster Monitoring Network

André Aparecido de Souza Ivo [1 2], Carlos Leandro Gomes Batista [1 2], Fátima Mattiello-Francisco [3]

[1] Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brasil
Aluno de Doutorado do curso de Engenharia e Gerenciamento de Sistemas Espaciais (CSE)

[2]Centro Nacional de Monitoramento e Desastres Naturais, São José dos Campos, SP, Brasil
Divisão de Monitoramento e Alertas - DIMON

[3]Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brasil
Coordenação dos Centros Regionais - COCRE

andre.ivo@cemaden.gov.br, carlos.batista@ieee.org, fatima.mattiello@inpe.br

Abstract. *Due to the vast extension of Brazilian territory, government investment on environmental data collection technologies has been observed since the 90's. Different networks of Data Collecting Platforms (PCD) exist to support environmental monitoring aiming at meteorological forecasting, hydrological control, mitigation of natural disaster consequences, and research and development purpose. In this work, we discuss and examine the major technological vulnerabilities in a Natural Disaster Monitoring Network in order to show unsolved issues related to the network operation, maintenance and expansion. The paper includes a basic description of an approach to the analysis of technological vulnerability in the context of CEMADEN Natural Disaster Monitoring Networks operation. The goal is to share challenges with the scientific community, as opportunities for future research.*

Key-words: Technological; Vulnerabilities, Natural, Disaster, Networks.

1. Introduction

The Brazilian National Center for Monitoring and Alert Natural Disasters - CEMADEN, created in July 2011 with the Presidential Act number 7513, has the mission to monitor the natural hazards in susceptible risk areas of Brazilian counties to natural disasters and issue alerts. CEMADEN also performs research and technology innovation to contribute the early warning system with the final objective to reduce the number of fatal victims and material loss in whole country [da República 2011].

Nowadays CEMADEN works 24/7 without interruptions, monitoring all Brazilian territory, the risk areas of 958 counties classifieds as vulnerable to natural disasters. Beyond its capabilities CEMADEN sends alerts to the Brazilian National Center for Risks and Disasters Management (CENAD), from Brazilian National Integration Ministry (MI), helping the Brazilian National System for Civil Defense.

The CEMADEN monitoring network is composed of 5,857 different types of devices being implanted in the whole national territory risk areas.

The natural disasters more frequent in Brazil are from intense or sparsely rain events [Mendes et al. 2018]. So, the pluviometric monitoring is the main focus of the network, being performed through Meteorologic RADAR and different kinds of Data Collecting Platforms (PCD)[Soler et al. 2013].

The precipitation registers provided in real time by these instruments are direct observations in the risk evaluation for geological disasters (mass displacement)[Ahrendt and Zuquette 2003], hydrological (floods), meteorological (cold fronts, convergence zones, storms), and climatological (droughts, barrenness and fires). These data are combined with indirect information sources (products) to create an alert report, with satellite images and results from numeric modeling [Soler et al. 2013].

All PCDs are equipped with a sensor measure the rain intensity (pluoviometer) and could receive some different sensors to monitor a specific group of the natural disaster. There are five different categories:

1. Pluviometric PCD
2. Hidrologic (fluviometric) PCD
3. ACQUA (simple agro-meteorologic) PCD
4. AGRO (complex agro-meteorologic) PCD
5. Geotech

The river monitoring for overflow and floods is performed by a dedicated network in addition to RADAR and pluviometers they monitor the target hydrological bays [Soler et al. 2013]. For the Brazilian semi-arid region it is performed the agro meteorologic monitoring aiming to minimize the impacts caused by the crop collapse on the small rural proprieties of family farmers. The geotech monitoring, or hydrogeological, is performed by geotech PCD capable to measure the amount of water accumulated at the different soil layers in addition to the Total Robotized Stations (ETR), which monitor possible landslides at mountain regions as hillsides.

The CEMADEN PCD network is the major tool for governmental decision making. As this, the operation, maintenance, and expansion of this network have a great importance. On the other hand, the size of the Brazilian Territory $(8,516,000km^2)$ imposes difficulties.

Beyond the physical difficulties for the network maintenance and expansion, this territorial extension creates limitations on communication and information traffic, in special where the orography is very pronounced or at the country side, places where the cellular signal or optic fiber availability are scarce.

As the PCD observational network installed on the field registers the environmental parameters, the data processing systems, at the research centers, process a great amount of information received and translate these data on figures and charts. However, in the majority of cases, the data collected and processed need to be available in almost real time to the stakeholder. So, the data transmission is essential for the full success of the PCD network. Without the transmission services by the cellular network the decision making principal actors would be unable to do their jobs.

With more than 5,000 devices spread around the Brazilian territory, the CEMADEN monitoring network shows other vulnerabilities besides problems during data transmission. This paper presents an analysis about of the major vulnerabilities the CEMADEN PCD network presents and the challenges to keep the network operational.

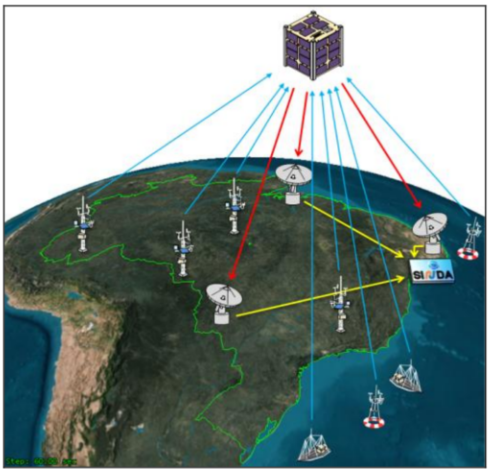

Figura 1. SBCDA Architecture with the Space Segment, Reception Ground Stations, PCD/Buoys and SINDA [Source: [Carvalho et al. 2013]]

2. INPE/SINDA: A Similar Network

The Integrated Environmental Data System (SINDA) is the mission center of the Brazilian Environmental Data Collection System (SBCDA) operated by the Northeast Center of Brazilian National Institute for Space Research (INPE) at Natal, Rio Grande do Norte.

Besides the SINDA this network is composed by around a thousand Data Collecting Platforms (PCD) spread around the Brazilian territory, a constellation of three satellites named SCD-1, SCD-2, and CBERS-4A and two reception ground stations at the cities of Cuiabá and Alcântara. The platform network started in 1993 with the launch of the satellite SCD-1 with about 60 PCDs. In 1996, the Brazilian National Electric Energy Agency (ANEEL) and the Center of Weather and Climate Forecast (CPTEC) became major users of the network increasing the number up to 600 [Santos et al. 2013].

The satellites operate on two different communication frequencies for the SBCDA: UHF for data uplink from PCDs and S-band for data downlink to the reception ground stations as we can see at the Figure 1.

All the data collecting was based on the space segment working as a mirror, once the satellite has view of the PCD and the reception station, at the same time, the link is established and the data is transferred [Carvalho et al. 2013]. Nowadays, the SINDA infrastructure enables the PCDs to transfer data through GPRS or local/internet networks [Santos et al. 2013].

The major applications of the PCDs are hydrologic, meteorologic, oceanographic buoys (anchor or not) and flame risk analysis [Miranda et al. 2013]. But some new activities are being put on account such as animal tracking, fishing ships monitoring and disasters alert.

2.1. Technological weakness

As all other networks, the INPE data acquisition network suffers from some weaknesses.

In this subsection, we will show some of the discussion about the SBCDA network vulnerabilities and limitations.

2.1.1. Time & Revisit

One of the first limitations of the orbital-based network for environmental data collection is the dependence of time and revisit schedule of the space segment.

As there is a limited number of spacecrafts on SBCDA it is impossible to guarantee coverage and low revisit time at the same time with the current configuration.

The SCD-1 and SCD-2 have equatorial orbits (30°) which can provide almost all orbit passing through the Brazilian territory but this orbit limits the revisit time and coverage on regions below latitude $-25°$ [Yamaguti et al. 2009]. The CBERS-4A with a polar orbit has only a few numbers of orbits passing on Brazilian territory per day but can coverage all latitudes even with a low revisit time.

As the SBCDA depends on the spacecraft viewing the PCD and reception station, simultaneously, the revisit time becomes a limitation and vulnerability if we need it to monitor natural disasters, for example.

2.1.2. Satellites

Another issue concerning the INPE network takes place on the current status of the constellation of satellites.

The SCD-1 and SCD-2 were launched in the decade of 1990, 1993 and 1996 more precisely. And now they overpassed its expected life and works on degraded mode. After 14 years of life, SCD-1 had problems with its nickel-cadmium batteries and now they do not work when the satellite is on Earth's shadow [eoP]. Even the CBERS-4A mission was not designed for environmental data collection just carrying the DCS payload as piggy back [Yamaguti et al. 2009].

So, the health of the network lays on the working state of these already degraded spacecrafts and it needs an upgrade urgent [Sato et al. 2011, Carvalho et al. 2013].

2.1.3. PCD Maintenance

INPE is responsible for all PCD homologation. The PCDs work with the ARGOS System, a global environmental data collection, and location system, so INPE is responsible to guarantee the transmitter works as the ARGOS standard specify. But the user, owner of the PCD, is responsible for its maintenance and the quality of the data acquired by the sensors.

A preventive maintenance of PCDs is crucial for the correct function of the network but this process is sometimes unfeasible due to the location of some PCDs [Yamaguti et al. 2009].

3. Vulnerabilities Analysis Design

This section proposes a simple approach to the analysis of technological vulnerability. When we talk about vulnerabilities we also talk about the risks embedded in them and it is at this point where it can generate confusion about this subject [Martin 1996].

Understanding what is the risk it is the first step to understanding what is a vulnerability. A risk is just an fault, event possible or uncertain condition which if occurs will affect positively or negatively on an at least one objective of the system or project [Institute 2013]. The vulnerability is precisely the faults [de Oliveira e Souza and de Carvalho 2005], events or uncertain conditions that can affect the system or the project.

The risk analysis is part of a process known as risk management [Institute 2013]. This paper presents a summary of the negative points to be considered about the technology used on the CEMADEN PCD network. Risk Management process, by definition, takes part in anything that can cause financial or organization damage.

1. **Vulnerability Analysis:** Its major activity is the process of risk identification and mapping failures which can expose the system to hazards. These failures could be physical/environmental (e.g. weather events), technological (e.g. faults on electronic devices) and/or human (e.g. vandalism). From this information, we can start mitigation techniques to avoid the vulnerabilities trying to guarantee more reliability to the system.
2. **Risk Evaluation:** The role of risk evaluation is to know the real potential of the vulnerability, with processes to define and evaluate, systematically, the risks to the system healthy. During this phase, the risk is analyzed as a whole, its origin, probability, and possible consequences. Three question should be proposed:
   (a) What could happen?
   (b) What the probability to happen?
   (c) What are the consequences if it happens?
3. **Mitigating Risks:** This process aims to define actions and/or activities to ensure that the risk embedded in a vulnerability have been extinct or attenuated to a point where it does not cause harm to the system operation.
4. **Capabilities Analysis:** It is the process responsible to review the risk response capability. The term capability is defined as the ability of people, organizations, and systems to execute actions to mitigate the risk in an effective and sustainable way.

4. Vulnerabilities Analysis

On this section, we present a brief study about the vulnerabilities of the CEMADEN PCD network as demonstrated in the Section 2. A great similarity with the technological weaknesses of INPE network has been identified.

4.1. Vulnerability Analysis

The Table 1 shows the major vulnerabilities of CEMADEN natural disasters monitoring network. These vulnerabilities are the more frequent causing the PCD devices services interruption.

Tabela 1. Main vulnerabilities of CEMADEN Natural Disaster Monitoring Networks

Vulnerability	Physical	Technological	Human
Rain gauge clogging	x		
Theft, vandalism and damage			x
Battery		x	
Communication failure		x	
No telephony signal		x	

The physical and human vulnerabilities presented in the Table 1 demands less effort to be resolved.

Rain gauge clogging: This vulnerability represents the greatest number of occurrences, there was a total of 35,185 occurrences in 2017 which affected 2,671 devices. The correction of these damages caused by this vulnerability pass by only the cleaning of the devices once the majority of the cases is caused by falling dry tree leafs. The devices more affected are the pluviometers type tipping bucket. They have the best relation cost/benefit. A solution for this problem would be the use of models disdometer laser. As this model has a high cost, there is no economically feasible solution for this vulnerability.

Theft, vandalism and damage: This vulnerability is more frequent in the Brazilian semi-arid region. This is because in this region is very common the cattle raising of goats, the animal with a rustic diet. The goats eat green and dry leaves, besides they gnaw tree barks, bushes and thorns. These animals with this peculiar diet gnaw also the PCD cables, sensors, and even the holding box. Only at this region, from a total of 559 devices, 30 (5.37%) suffered from damage caused by these animals in 2017. In metropolitan regions, these cases are rare, around 1 per year. To solve this vulnerability it is building a fence to avoid the animals to get close to the devices and the damage correction passes through maintenance campaigns and replacement of the damaged parts.

Battery: This vulnerability is a "consumable"item, the battery has a short life cycle and it needs to be changed in 2 years tops. Despite recurrence, the correction is known just a right schedule for the battery substitution at the maintenance campaign.

Communication Failure: This failure is quite significant at the CEMADEN network, the transmission technology used is the GSM/GPRS based on the mobile telecommunication infrastructure. In the matter of fact, there are two motives which affect the signal quality: great distances between the telecommunication tower to the PCD and obstructions causing interference.

As the mobile telecommunication coverage is based on telephony towers organize on strategic positions, the mobile devices connect automatically from tower to tower. Different from the mobile devices, the PCDs are fixed in a strategic point to evaluate potential risks, so they should not suffer from signal variations once they are connected always to the same tower. As this what could affect the signal is the physical obstruction between the tower and the PCD, known as telephony shadows loss.

In other words, the shadow loss areas are caused by physical barriers (i.e. mountains, hills, buildings, lifts, metal fences and concrete) even a strong rain or storm could attenuate the signal and other technical factors from the telecommunication enterprises can interfere on the signal correct reception.

On the PCDs case, the more common causes to the shadow loss are the strong rains, buildings built between the device and the tower, trees and even the relocation of a tower and other technical factors from the mobile enterprises [Zhou et al. 2002] [Zhi 2006]. CEMADEN has no control over these factors. In 2017, CEMADEN registered 706 devices affected by data transmission problems with a total of 18,750 cases. At the majority of these cases, the correction of the damage caused by this vulnerability is solved by relocating the device, changing the mobile enterprise or opening a help-desk call when the problem is technical. The correction is always complex and slow (could take months) detecting the real cause for the communication failure is the major problem once the telecommunication operators do not expose the real motive. The solution to this vulnerability is still open due to the network characteristics. One possibility to be evaluated is the use of a satellite communication like SINDA/INPE network. This solution needs future studies to evaluate the applicability to CEMADEN needs.

No telephone signal: An extension from Communication failure this vulnerability represents the limitation for the expansion of the CEMADEN network. The cellular telephony coverage is on its majority distributed on the coastal zone of Brazil. At the country side the offer for telephony signal is reduced as we can see at the Figure 2.

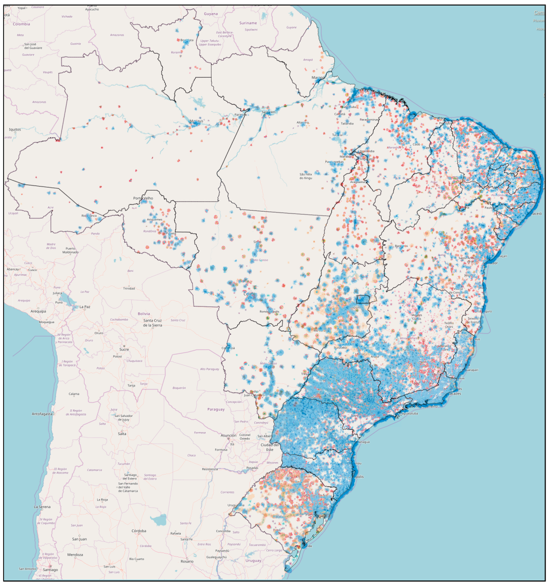

Figura 2. Telecom coverage area. [Source: Telecommunication companies (Vivo, Oi, Tim, Claro)]

Nowadays, CEMADEN does not have any PCD in areas without telecommunication coverage. The solution for this vulnerability is still open as happens on other Communication failures and represents the opportunity for future works including studies with transmission applications using satellites.

4.2. Risk Evaluation

The CEMADEN network vulnerabilities affect directly the environmental data availability needed to risk prediction. The direct consequences caused by the lack of information are the loss of quality of alerts send by the center operation room and in extreme cases the complete incapability to send it. The indirect could be considered severe as the population is exposed to natural risks who depend on the alerts to save their lives.

There are not enough data to calculate the vulnerability occurrence probability distribution. On the other hand with the historical data, it is possible to calculate how many devices were affected in 2017 by the vulnerabilities, as may be seen on Table 2.

Tabela 2. Percentage of affected devices by the vulnerabilities

Vulnerability	**% affected devices**
Rain gauge clogging	45,60%
Theft, vandalism and damage	5,37%
Battery	4,49%
Communication failure	12,05%
No telephony signal	–

4.3. Action definitions for Risk mitigation

The actions to mitigate the vulnerabilities Rain gauge clogging and Battery are linked to an effective preventive maintenance schedule campaign. Nowadays the devices have one take one visit of predictive maintenance every eighteen-month average. Decrease the time between the predictive maintenance operations will certainly aid to mitigate the risk of these vulnerabilities.

For the vulnerability Theft, vandalism and damage, in the semi-arid region, the more indicated action is the installation of fences around all devices. In metropolitan regions, an informative board will help to mitigate these cases.

For the cases of Communication failure and No telephony signal, there are not proposals to mitigate the risks of these vulnerabilities.

4.4. Capability Analysis

CEMADEN as a governmental center has its capability limited by the human resources available at the center and the financial budget from the Ministry of Science, Technology, and Communication. The greatest challenge to mitigate risks is to execute the maintenance with a bigger time resolution with the same human resources and budget available. Future studies could be developed to decrease the predictive maintenance dependence enabling the devices self-sufficient during the bigger time as possible.

5. Unsolved Challenges

As can be seen, the CEMADEN network presents great challenges in its operation and maintenance. One of the unsolved challenges is to promote the devices self-sustainability, turning them more resilient o the presented vulnerabilities. New studies could be conducted to retrofit the devices or even more replace the network with new and more resilient devices.

About the vulnerabilities Communication failure and No telephone signal, it is important to see the CEMADEN network was developed with the objective of monitoring the natural events disasters triggers, e.g. the amount of rainfall accumulated in a determined region. Some events present a quick answer when a disaster is triggered. This characteristic demands to CEMADEN network a set of rigid requirements, e.g. the frequency of center data acquisition, one time every ten minutes. Beyond the data availability, between 90% and 100%, with the maximum effort to be next to 100%, differently from SINDA which aims essentially research and development.

As this, the communication solution with satellites present on INPE/SINDA network shows an important constraint in function of the revisit time, average 100 minutes with the actual satellites [Yamaguti et al. 2009]. Besides the SCD-1 does not operate 24h due to its degraded situation and all space segment of SBCDA needs an upgrade to maintain its operations.

6. Conclusion

Nowadays the public sector, i.e. CEMADEN and INPE, is being targeted for systematic financial cuts due to a national economic and politic crisis for the last couple of years. This scenario affects directly the actions to mitigate, correct or solve the vulnerabilities of the natural disasters monitoring network.

This work shows a summary of the major technological vulnerabilities with the main goal to foment the research and development (R&D) of new technologies in order to aid the network operation, maintenance and expansion.

The R&D for new sensors and devices more accessible could be the tool to improve the network maintenance and resilience to vulnerabilities which demands predictive maintenance with bigger periodicity.

The solutions to the vulnerabilities Communication failure and No telephone signal could come from researches and development of new methods and standards for Machine to Machine (M2M) [Fadlullah et al. 2011] [Lawton 2004] communication, new knowledge and concepts derived from industry 4.0 [Lasi et al. 2014] and Cyber-Physical Systems [Lee et al. 2015].

Referências

Scd (satelite de coleta de dados) - data collection program of brazil. `https://directory.eoportal.org/web/eoportal/satellite-missions/s/scd`. Accessed: 2018-07-11.

Ahrendt, A. and Zuquette, L. V. (2003). Triggering factors of landslides in campos do jordão city, brazil. *Bulletin of Engineering Geology and the Environment*, 62(3):231–244.

Carvalho, M. J. M. d., dos Santos Lima, J. S., dos Santos Jotha, L., and de Aquino, P. S. (2013). Conasat-constelaçao de nano satélites para coleta de dados ambientais. *XVI Simpósio Brasileiro de Sensoriamento Remoto-SBSR, INPE*, pages 13–18.

da República, P. (2011). Decreto nº 7.513, de 1º de julho de 2011.

de Oliveira e Souza, M. L. and de Carvalho, T. R. (2005). The fault avoidance and the fault tolerance approaches for increasing the reliability of aerospace and automotive systems. In *SAE Technical Paper*. SAE International.

Fadlullah, Z. M., Fouda, M. M., Kato, N., Takeuchi, A., Iwasaki, N., and Nozaki, Y. (2011). Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, 49(4):60–65.

Institute, P. M. (2013). *A Guide to the Project Management Body of Knowledge: PMBOK Guide*. PMBOK® Guide Series. Project Management Institute.

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., and Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, 6(4):239–242.

Lawton, G. (2004). Machine-to-machine technology gears up for growth. *Computer*, 37(9):12–15.

Lee, J., Bagheri, B., and Kao, H.-A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3:18–23.

Martin, B. (1996). Technological vulnerability. *Technology in Society*, 18:511–523.

Mendes, R. M., de Andrade, M. R. M., Tomasella, J., de Moraes, M. A. E., and Scofield, G. B. (2018). Understanding shallow landslides in campos do jordão municipality – brazil: disentangling the anthropic effects from natural causes in the disaster of 2000. *Natural Hazards and Earth System Sciences*, 18(1):15–30.

Miranda, G. P., da Silveira, S. W. G., and Yamaguti, W. (2013). Desenvolvimento e avaliação de uma estação de recepção em banda s para incrementar o desempenho do sistema brasileiro de coleta de dados ambientais. *XVI Simpósio Brasileiro de Sensoriamento Remoto-SBSR, INPE*.

Santos, M., Mattielo-Francisco, M., and Yamaguti, W. (2013). Sistema nacional de dados ambientais e a coleta de dados por satélite. *Anais XVI Simpósio Brasileiro de Sensoriamento Remoto-SBSR, Foz do Iguaçu, PR, Brasil*, 13.

Sato, L. H. S., Yamaguti, W., and Fernandes, D. (2011). Itasat-1: uma proposta de continuidade do sistema brasileiro de coleta de dados ambientais. *Proceedings of the XV Simpósio Brasileiro de Sensoriamento Remoto, Curitiba, Brasil.[Links]*.

Soler, L. S., Gregorio, L. T., Leal, P., Gonçalves, D., Londe, L., Soriano, E., Cardoso, J., Coutinho, M., Santos, L. B. L., and Saito, S. (2013). Challenges and perspectives of innovative digital ecosystems designed to monitor and warn natural disasters in brazil. In *Proceedings* *of the Fifth International Conference on Management of Emergent Digital EcoSystems*, MEDES '13, pages 254–261, New York, NY, USA. ACM.

Yamaguti, W., Orlando, V., and Pereira, S. d. P. (2009). Sistema brasileiro de coleta de dados ambientais: Status e planos futuros. *SIMPÓSIO BRASILEIRO DE SENSORIAMENTO REMOTO*, 14:1633–1640.

Zhi, W. (2006). Calculation of shadow fading loss in the rlb of wcdma. *Telecom Engineering Technics and Standardization*, 7:020.

Zhou, J., Kikuchi, H., Sasaki, S., Muramatsu, S., and Onozato, Y. (2002). Performance of cdma cellular system with effects of soft handover under log-normal shadow channels. In *Communications, Circuits and Systems and West Sino Expositions, IEEE 2002 International Conference on*, volume 1, pages 332–336. IEEE.