Nat. Hazards Earth Syst. Sci., 13, 3419–3428, 2013
www.nat-hazards-earth-syst-sci.net/13/3419/2013/
doi:10.5194/nhess-13-3419-2013

Natural Hazards and Earth System Sciences
Open Access

"Last mile" challenges to in situ volcanic data transmission

J. F. B. D. Fonseca[1], B. V. E. Faria[2], J. Trindade[3], G. Cruz[1], A. Chambel[1], F. M. Silva[3], R. L. Pereira[3], and T. Vazão[3]

[1]Instituto Superior Técnico, Lisbon, Portugal
[2]Geophysics Department, Instituto Nacional de Meteorologia e Geofísica, Mindelo, Cape Verde
[3]INESC-ID, 2744-016 Porto Salvo, Portugal, Portugal

Correspondence to: J. F. B. D. Fonseca (jfonseca@ist.utl.pt)

Received: 30 May 2013 – Published in Nat. Hazards Earth Syst. Sci. Discuss.: 9 August 2013
Revised: 11 November 2013 – Accepted: 14 November 2013 – Published: 23 December 2013

Abstract. Scientists play a key role in volcanic risk management, but rely heavily on fast access to data acquired in the vicinity of an active volcano. Hazardous volcanoes are often located in remote areas were telecommunications infrastructure is fragile. Besides being exposed directly to the volcanic hazard, the infrastructure in such remote areas can also suffer from "last mile" limitations derived from lack of market demand for data transmission services. In this paper, we report on the findings of the FP7 MIAVITA project in the topic of volcanic data transmission. We draw on the contribution of partners from emergent or developing countries to identify the main bottlenecks and fragilities. We also present the results of an experiment conducted on Fogo Island, Cape Verde, to test the availability of VSAT services adequate for volcanic monitoring. We warn against the false sense of security resulting from increasingly ubiquitous connectivity, and point out the lack of reliability of many consumer-type services, particularly during emergencies when such services are likely to crash due to excess of demand from the public. Finally, we propose guidelines and recommend best practices for the design of volcanic monitoring networks in what concerns data transmission. In particular, we advise that the data transmission equipment close to the exposed area should be owned, operated and maintained by the volcanic monitoring institution. We exemplify with the set-up of the Fogo telemetric interface, which uses low-power licence-free radio modems to reach a robust point of entry into the public network at a suitable distance from the volcano.

1 Introduction

Volcanic risk management and the emergency response to volcanic crises rely heavily on fast access to critical information by scientists, civil protection agents, authorities and citizens, spread over the affected area and beyond. For this reason, in civil protection as in many other critical sectors, a system must be in place to collect, filter, analyze, structure and transmit data to support the decision-making process (Harrald and Jefferson, 2007), and a robust telecommunications infrastructure is therefore a prerequisite for efficiency.

Scientists play a key role in securing the situational awareness required for effective and timely emergency management, provided that they can have fast access to in situ geophysical, geochemical and geodetic data (e.g. Sparks, 2003). Their observations are an essential input for evaluating the significance of any crisis, since they establish the level of activity of a volcano even in the absence of historical eruptions, and can detect a deviation from baseline volcanic activity weeks or months in advance of an eruption. Combined with geology and geomorphology, geophysical data allow the development, validation and calibration of models of volcanic behaviour (MIAVITA, 2012).

This is illustrated by the 2010 centennial eruption of Merapi volcano in Indonesia (Surono et al., 2012), whereby a combination of in situ and satellite monitoring techniques allowed scientists to issue an advance warning which saved tens of thousands of lives, providing compelling evidence of the importance of volcanic monitoring. The alert level was raised above the normal state 36 days in advance of the onset of the eruption, and continued to rise until it reached its maximum level 23 h before the first exposure, triggering an evacuation order in the radius of 10 km around the volcano (Surono et al., 2012).

Despite the critical role that scientists have in volcanic crisis management, and the stringent operational requirements for their effective contribution to emergency management, very often this sector of the broader civil protection community is the weak link in what concerns telecommunications. In this paper we focus on the technological challenges faced by scientists when they try to access data acquired in the vicinity of an active volcano, in real or near-real time.

Hazardous volcanoes are often located in remote areas of emergent or developing countries, where the existing telecommunications infrastructure is fragile, if not non-existent. Given the increased capillarity of the distribution network, the ratio revenue/installation decreases sharply towards these "last mile" areas, and therefore the operators tend to avoid investments. To complicate matters further, in the vicinity of an active volcano the telecommunications infrastructures are themselves exposed to the volcanic threat.

Satellite communications, and in particular VSAT (very small aperture terminal) networks (Maral, 2003) are often described as available anywhere. In theory at least, a power source, a PC, a modem and a satellite dish are all that is required to establish a link to the Internet anywhere in the planet. This idea seems to be supported by the frequent video streaming over satellite by TV crews in inhospitable regions of the planet. The minimum infrastructure required by satellite communications makes them suitable for hazardous areas, by contrast with techniques relying on fixed landlines and telecommunications towers. However, the high latency inherent to the use of geostationary satellites is an obstacle to stable Internet connectivity. Technical expertise required for set-up, regulations and cost may be other factors precluding the use of satellite communications for volcanic data transmission.

To address these issues and search for remedies, FP7 Project MIAVITA (Mitigate and Assess Volcanic Impact on Terrain and human Activities) conducted a study of the adverse conditions affecting volcanic monitoring data transmission, taking advantage of the participation of several institutions from international cooperation partner countries (ICPC).

As a first step, a functional architecture was developed for communications in a volcanic crisis, enumerating the basic components and functions in the system, characterising the information workflow and clarifying who are the actors, what objects they manipulate and what tasks they execute. The main constraints to reliable volcano data transmission in emergent or developing countries were illuminated through questionnaires to MIAVITA ICPC partners. Then, Fogo volcano and a proxy location in the Sahara desert were used as a test bed for different data transmission solutions. Particular attention was paid to the feasibility of VSAT data transmission in the context of volcanic monitoring.

Several lessons were learned and recommendations were drafted, based on the input from the ICPC partners and on the data transmission tests. This paper attempts to synthesise these lessons, further discussed in MIAVITA (2012), a handbook for volcanic risk management (Chapter 3: living with a volcano – scientific and operational aspects), and in the project's reports (Fonseca et al., 2011; Vazão et al., 2011).

2 A model for volcanic data transmission

2.1 The actors

The following actors use monitoring data for different purposes (analysis, information, education, etc), both in a crisis situation and during routine intra-eruption observations:

- a local volcanological laboratory (LVL);
- one or several remote volcanological laboratories (RVL);
- civil protection authorities and other stakeholders;
- the local authorities; and
- the population in general.

The sensors – seismometers, tilt metres, spectrometers, infrasound arrays, video cameras, etc – are the base data providers. They are deployed in the vicinity of the active volcano, and supply the upward workflow with raw data. Very often the actors are not in the same area, and frequent visits to the site are not always an option, given the exposure to the hazard or other constraints (e.g. budget restrictions). A suitable telecommunications link, interfaced with the sensors, is therefore required to allow remote access to the data.

As a rule there is a trade-off between the proximity to the volcano and the resources available at the laboratory. The nearest observatory to the volcano, here called local volcanological laboratory (LVL), comprises typically a minimum set of processing and analysis capacities, and in remote regions its staff may have limited technical or scientific skills. In most instances, this observatory is in charge of (and in a crisis situation, possibly overwhelmed by) equipment maintenance and basic observation tasks, while more sophisticated analyses may need to be carried out away from the affected area and taking advantage of a distributed research infrastructure. The transmission of raw or partly processed data from the LVL to remote laboratories is therefore an important issue in volcanic monitoring.

The participation of remote volcanological observatories (RVLs), located in the same country or abroad, can prove invaluable for the successful management of a volcanic crisis. It may however be plagued with political difficulties, and should not be improvised at the onset of an emergency. Data sharing, particularly in real time, may be regarded with suspicion by the institutions or individuals who are supporting the burden of maintaining a monitoring network, and mutual confidence must be built through sustained cooperation in routine times.

During an emergency, a civil protection agency (or any other entity endorsing this role) is usually the interlocutor of the scientific and technical community, and in turn passes the information to the local authorities and to the public. While hopefully the ICT resources available to the civil protection agency and the local authorities will be less exposed to "last mile" issues, the latter may affect in a very significant way the communication with the population exposed to the volcanic threat, and locally traditional ways of communication should not be discarded. The presence of the LVL staff, usually well embedded in the local culture, may be a major asset when the science-based advise has to be passed to the population, or their traditional wisdom tapped by the scientific community. A much greater deal or research has been conducted on the best practices for information management by civil protection agencies (e.g. Iannela and Henriksen, 2007; McGuire et al., 2009) and protocols for communication with the public (ITU, 2010). These aspects will not be discussed further in this paper, which focuses on ITC requirements of volcanic monitoring.

2.2 The systems

The actors must have at their disposal systems that allow them to perform the expected data transmission tasks. A sensor or group of sensors require a telemetric interface to handle and forward the data. The LVL requires a local monitoring system with the capacity to receive and store the data sent by the sensors and optionally to share it with remote laboratories, and a specialised reporting system to communicate with the civil protection agency. In many instances it might be advisable for the RVL to operate a remote monitoring system with independent access to the raw data, should the LVL fail to acquire data as a result of the emergency.

2.3 The communications network

The different systems need to be linked in a suitable communications network. The link between the in situ equipment and the LVL should allow remote troubleshooting and maintenance. Very often the tools provided by the manufacturer work only within a local area network (LAN), and in such cases those tasks require either virtual private network (VPN) tunnelling or a field computer attached to each remote site. With the VPN technique, the data are transported over a public network, but a LAN connection can be emulated (simulating a "long cable" connecting the laboratory and the equipment). Alternatively, when field computers are available at the remote sites the software tools may be run locally, but the computers must still be reachable from the LVL through the Internet (see Sect. 4.2 for an example).

Robust and reliable data transmission links must be in operation between the LVL and the RVL monitoring systems, in both directions, to enable an effective cooperation. The RVL monitoring system may have also a direct link to the sensor interface, for redundancy. Figure 1 depicts graphically this model of data transmission for volcanic monitoring, identifying the actors, the systems and the links between systems.

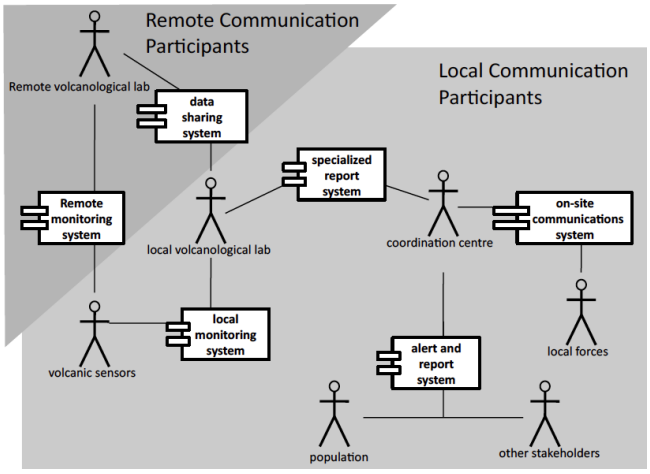

Fig. 1. Actors, systems and links: an abstract functional architecture for volcanic monitoring and emergency management. After Vazão et al. (2011).

Although data transmission links may be, and usually are, also present within the systems, we make here the somewhat artificial distinction of considering "system" as what is operated autonomously by the laboratory, and discuss under "communications network" the public services. This reflects the fact that the vulnerabilities are of a different nature, as will be exemplified later.

3 Vulnerabilities of communications infrastructure in a remote volcanic region

The participation of ICPC partners in the MIAVITA project provided an opportunity to inquire into their experiences concerning communications. MIAVITA's ICPC partners were the Institute of Meteorology and Geophysics of Cape Verde (INMG), the Ministry of Industry, Mines and Technological Development of Cameroun (MINIMIDT), the Center for Volcanology and Geological Hazard Mitigation of Indonesia (CVGHM) and the Philippine Institute of Volcanology and Seismology (PHIVOLCS). Target volcanoes were Fogo (Cape Verde), Mount Cameroun (Cameroun), Merapi (Indonesia) and Kanlaon (Philippines), sampling very different types of hazards, societal contexts and risk management practices. Of the four ICPC institutions taking part in the project, we were able to obtain answers from three of them (INMG, MINIMIDT and PHIVOLCS). Although this is a limited sample, it allows nonetheless some insight into the main difficulties experienced in emergent or developing countries. Vazão et al. (2009, 2011) describe the methodology adopted for the collection of information.

In short, the main fragilities identified were

- high vulnerability of the telecommunication towers and landlines supporting the public networks in the vicinity of the volcano to direct physical damage during an eruption, potentially leading to the disruption of services and blackout of communications;
- “blind spots” without network coverage in the vicinity of the volcano, both for public networks and in some cases for networks owned by the local forces (army, police or civil protection agency);
- vandalism affecting the telecommunications infrastructure, and difficult access for repair (the latter may worsen during a volcanic emergency);
- very limited access to non-voice services in the field, with Internet access usually limited to the premises of a local volcanological observatory; and
- reliance, in part or totally, on the public cellular telephone network for emergency communications, and resulting exposure to usage overload and associated system crashes during an eruption.

Other identified hindrances concerned limited or non-existent training of the staff on emergency communications, and the lack of inter-operability of the different equipment used by the local forces (e.g. two-way short range radios and cellular telephones).

Clearly, the limitations are more stringent for data transmission – with less market demand in remote areas – than for voice services, now nearly ubiquitous even if often fragile. The remainder of this paper will focus on non-voice communications.

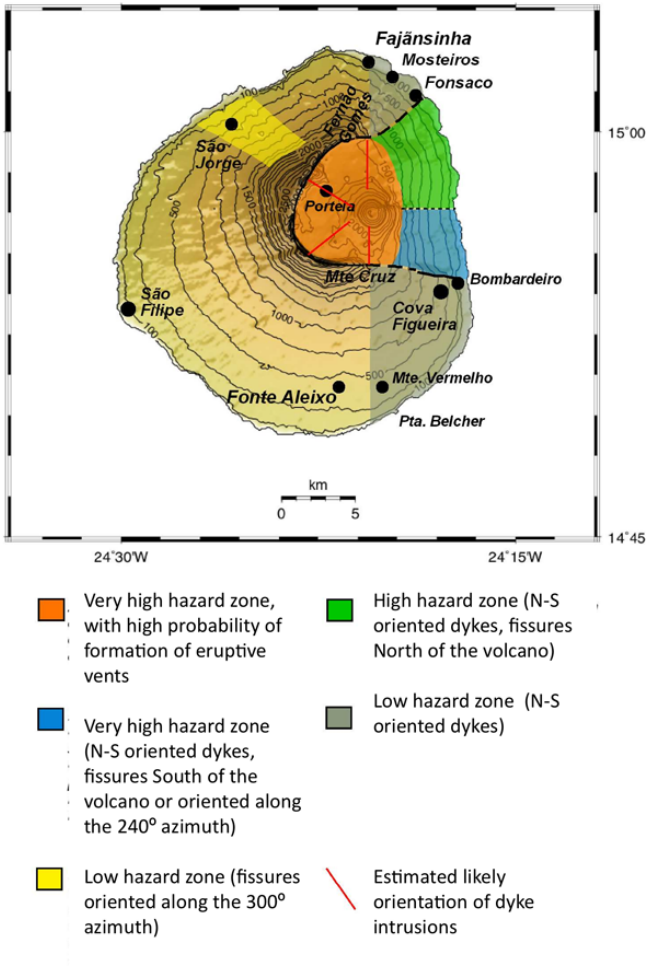

Fig. 2. Lava flow hazard map for Fogo Island, after Faria (2010).

4 The Fogo volcano experiment

4.1 The setting

Fogo is an active stratovolcano in the Cape Verdean island of the same name (Figs. 2 and 3), reaching an altitude of 2829 m a.s.l., or ∼7000 m if measured from the seafloor (Day et al., 1999). The volcano is located in a poorly developed area of the island, inside a 9 km-wide caldera whose floor is at an average altitude of 1750 m a.s.l. The caldera has a fertile soil, farmed by a population of ∼700 inhabitants. Cattle raising and tourism are other economic activities. The volcano has erupted at average intervals of 20 yr since the discovery of the island by Portuguese sailors 550 yr ago. This pace slowed down during the 20th century, with two flank eruptions in 1951 and 1995. Figure 2 depicts the lava flow hazard in the different zones of Fogo Island.

Following the 1995 eruption (Heleno et al., 1999) the area surrounding the volcano was the object of a monitoring effort in the period 1998–2003 (Fonseca et al., 2003), but in the following years it subsided to very low standards. More recently, INMG took charge of geophysical monitoring nationwide and the monitoring network was revamped with partial support from project MIAVITA (Faria and Fonseca, 2013). One of the tasks of the project aimed at testing different solutions for data transmission.

Figure 3 depicts the Fogo monitoring network deployed by INMG in the period 2008–2011 (Faria and Fonseca, 2013), which consists of nine broadband 3-component digital seismometers Guralp CMG-3ESPCD (flat response from 60 s to 50 Hz), seven in Fogo Island and two in the adjacent Brava island. Taken together, the sensors of the Fogo volcano network produce approximately 42 kbit of data per second, continuously. The sites were fitted with telemetric equipment to allow the real-time retrieval of these data in the local volcanological laboratory (see below). This section describes the tests conducted, and summarises the conclusions. We start with the characterisation of the intervening actors and systems, and the links between them.

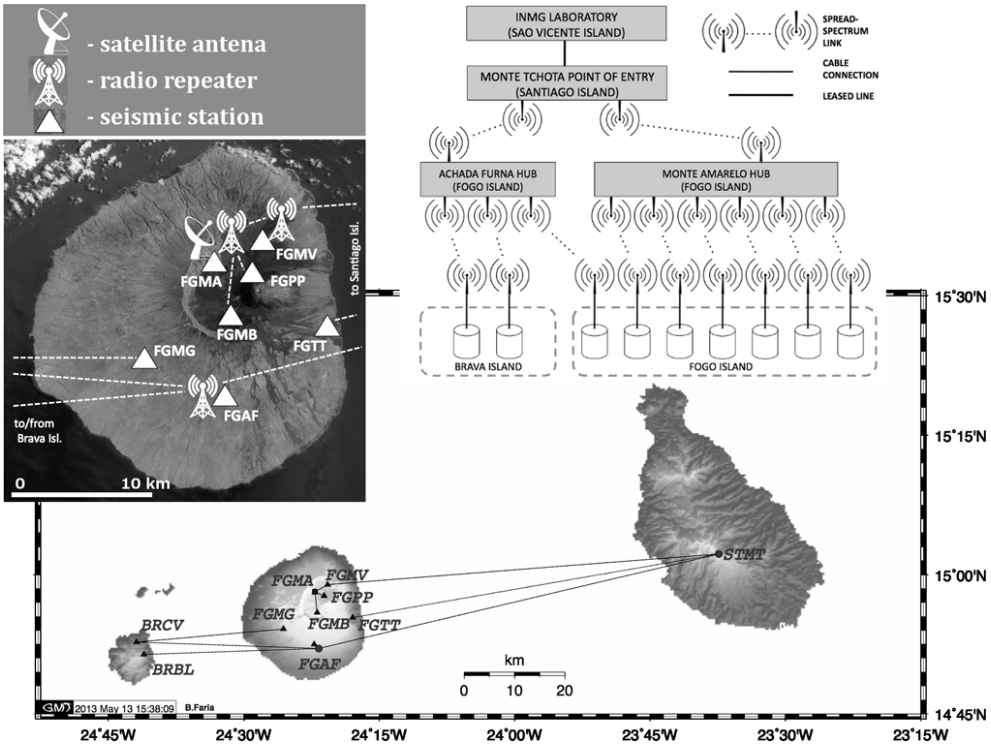

Fig. 3. Fogo volcano data transmission network, showing the different types of links implemented (cable, wireless, commercial leased line). Bottom: overall view, from the remote stations in Brava and Fogo islands (left) to the point of entry in the Internet in Santiago island (right); top left: detail of the network in Fogo Island; top right: schematic representation of the data transmission from the sensors to the INMG laboratory in São Vicente island. A detailed description of the Fogo Geophysical Monitoring Network may be found in Faria and Fonseca (2013).

Geophysical monitoring in Cape Verde falls under the responsibility of INMG, whose Geophysics Department is located in São Vicente island, approximately 230 km to the North of Fogo volcano. At the expense of compromising the proximity, this LVL has favourable operational conditions, being situated in a major city, Mindelo. The LVL is staffed with one PhD researcher specialized in volcanic monitoring, and a limited number of technical and administrative support staff.

For the purpose of the tests conducted under the MIAVITA project, the seismological laboratory of IST fulfilled the role of RVL. Through a number of previous research projects in the field of volcanic monitoring with emphasis on Fogo volcano (Fonseca et al., 2003; Heleno et al., 2006; Helffrich et al., 2006; Faria, 2010), the seismological laboratory has developed over the last decades the relevant competences.

4.2 The systems

The telemetric interface, operated autonomously by INMG, concentrates the data from all the sensors (distributed over a distance of the order of tens of km) at a single point of entry into a commercial service, to avoid the multiplication of services and associated costs (Fig. 3). In a first stage the data are concentrated at two sites, the Monte Amarelo and Achada Furna hubs (Fig. 3). The Monte Amarelo site has been used traditionally by the population of the caldera as a first refuge during eruptions, which attests to its relative safety despite being inside the caldera. This hub is equipped with autonomous power supply (no grid power is available in the caldera), consisting of photovoltaic solar panels with a total power of $\sim$1000 W. The Achada Furna hub is at a telecommunications complex of the Cape Verdean operator CVTelecom, with good conditions for uninterrupted operation.

The digitizer at each station outputs the data through a serial connection, and the first data transmission task concerns the concentration of these data streams from the different sensors at Monte Tchota, via the two hubs (Fig. 3). The distances to be covered in the first stage – stations to hubs – range from a few metres (for the sensors co-located with the hubs) to 35 km (signals transmitted from Brava island to Fogo Island), but are typically of the order of 5 km. One of the Fogo sites (FGMG) required a link to Brava island and back to Fogo, given the rugged topography.

Wireless data transceivers (Freewave FGRplusRe) were chosen to connect each remote digitizer to a hub. These radios, operating in the 900 MHz frequency band (but this will

change from country to country), are licence-free, have very low power consumption (5 mW to 1 W) and use the TCP/IP protocol. Embedded Guralp CMG-EAM computers at the hubs handle the incoming data using the Guralp Data Interchange (GDI) protocol, and serve as backup storage if the forward link is temporarily lost.

In a second stage, the data are transmitted from the two hubs to the Monte Tchota point of entry, located at a CVTelecom telecommunications complex in Santiago island (Fig. 3). From the hubs to Monte Tchota, the distance is ~ 80 km. Despite the low power, the solution used to connect the sensors to the hubs proved also reliable to cover the distance from each hub to Monte Tchota, where an embedded CMG-EAM computer and a router were installed to add flexibility to the remote management of the equipment.

Hosted by the Geophysics Department of INMG, the local monitoring system consists of an acquisition and processing computer and a data centre with a 2 TB network-attached storage (NAS). It operates a specialised reporting system, whereby updates on the state of Fogo volcano are passed to the civil protection agency on a routine basis or as per request. The system has a reliable connection to the Internet, and therefore can share the data with other laboratories if needed (e.g. during an emergency). Part of the data are transmitted in real time to the seismological laboratory of IST on a routine basis.

The seismological laboratory at IST played the role of remote monitoring system. It hosts a data centre with 6 Tb storage capacity, adequate computational hardware, and a range of specialized scientific software. The laboratory has state-of-the-art ICT infrastructure, with a 10 Gb s^{-1} connection to the European research and academic network GEANT. In addition, the system is equipped with a VSAT antenna and modem.

4.3 The network

From the Monte Tchota site to INMG (in São Vicente island), a commercial service was selected for data transmission. A careful analysis of the options available commercially was required at this stage, weighing service reliability versus cost. Whereas most providers offer corporate-type services that meet high standards, the associated costs are likely to render a monitoring network unsustainable – an issue that should not be overlooked in cooperation projects, whose funding is typically limited in time.

The figure for the total data production rate of the monitoring network (42 kbit s^{-1}) is modest by comparison with the bit rates on offer by most providers, and may therefore hide the critical aspect that continuous operation leads to an accumulated monthly traffic of the order of 10 GB. Unlimited-traffic tariffs are sometimes advertised that seem adequate for these volumes of data, but the bandwidth is often throttled down once some volume is exceeded, despite the name. The Cape Verdean company CVTelecom provides a comprehensive range of commercial services, including (at the time of writing), GPRS/EDGE mobile broadband services, ADSL and leased lines over most of the territory. To avoid competing for bandwidth with the general public, a leased line was negotiated with CVTelecom between Monte Tchota and the LVL. At INMG, data reception is handled by a CMG-EAM embedded computer with the GDI protocol.

All the radios and computers of the data transmission network were configured as a single local area network (LAN). Remote access from an authorised computer to the equipment in the LAN was possible through Network Address Translation (NAT) on the Monte Tchota router's public interface. This allows full remote control of the infrastructure (troubleshooting, reconfiguration, etc) from INMG (or elsewhere). Remote access to the station's digitizers is also possible with this configuration.

4.4 The link to the RVL

Because both the LVL and the RVL are equipped with reliable Internet connections, standard options such as SFTP (Secure shell File Transmission Protocol) were deemed adequate to transmit files between the two sites, since it provides reliability and privacy. Real-time data transmission from the LVL to the RVL was dealt with, reliably, by SeisComP's (Hanka et al., 2010) SeedLink protocol, therefore no additional steps were taken to reinforce the existing link. We focused instead on the establishment of a direct back-up link from the monitoring network to the RVL, to secure full redundancy with respect to the LVL link. As a key part of the experiment, we tested the feasibility of setting up a VSAT connection from the Monte Amarelo hub to the RVL at IST.

The first stages of the tests were conducted from a proxy site located in seemingly similar conditions, the seismographic station MTOR, operated by IST jointly with the Scientific Institute of Rabat in the Sahara desert village of Aouint Torkoz (28.49° N; 9.85° E). The MTOR site hosts VSAT equipment (ViaSat LinkStar modem, 1.8 m Ku-band antenna), and is located outside but near the edge of the 40 dBW contour of the footprint of Eutelsat's satellite 12 WA. We were able to establish a stable VSAT link between MTOR and IST with a residential-type (i.e. cost-sustainable) service provided by a major European operator. A backup CDMA (Code Division Multiple Access) link provided by Maroc Telecom was also set up at the MTOR site alongside the VSAT link to have redundancy. However, to achieve this an additional PC with the Windows operating system had to be installed at the site with the single purpose of hosting the drivers of the CDMA modem provided by the operator, because no Linux drivers could be obtained. This detail illustrates the challenges that can be presented by the use of commercial services in remote areas.

We tested several VPN options between the Linux computer at MTOR and a server located at IST, with variable degrees of success. The popular IPSec tunnelling protocol suite

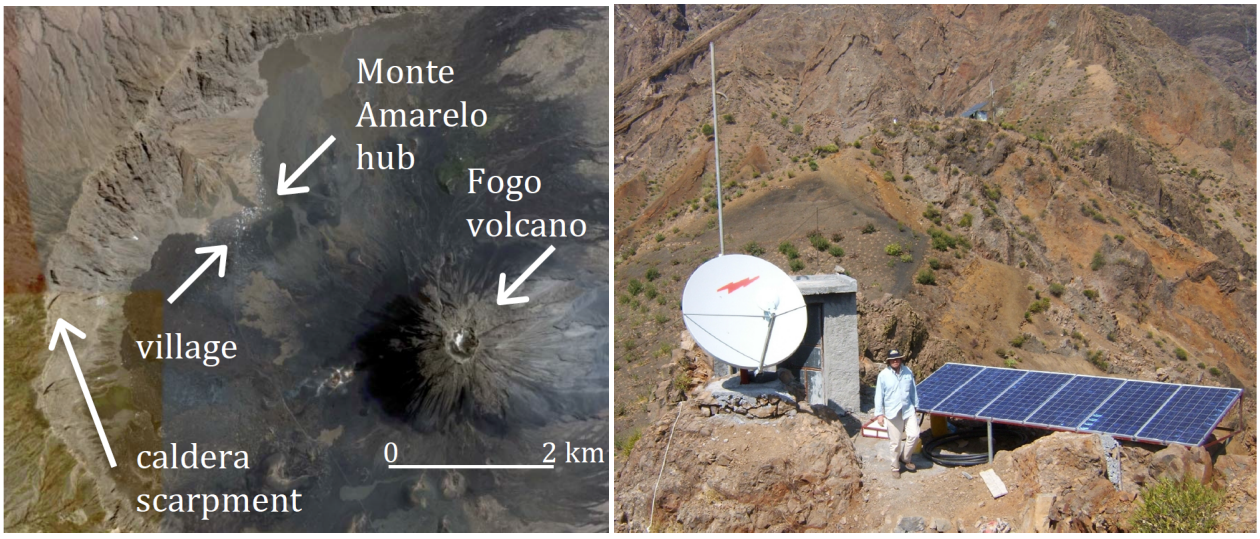

Fig. 4. The VSAT station in Fogo volcano’s caldera. Left: Google Earth view, showing Fogo volcano, the caldera scarpment and the site of the Monte Amarelo hub. Right: setting up the satellite antenna and power supply. The mast behind the dish will receive the antennas of the local links.

(Frankel and Krishnan, 2011) was tested, but we were not able to reconcile it with the large time delays introduced by the ground-to-satellite paths. This is due to the fact that the data encryption introduced by IPSec collides with the operation of performance-enhancing proxies (PEP) introduced by the VSAT operators (Totsline, 2002). This issue will be further detailed in the discussion. We tested also a “mediated VPN” solution, a commercial service whereby a company’s server manages the VPN. This implied an additional pair of gateways, one at the MTOR site and the other at IST, which were able to communicate with the third-party server over the VSAT links, coping with the latency through proprietary PEP techniques. This equipment were also able to deal in a transparent manner with the connection failover. The drawback of this solution was the addition of another fail point in the data transmission chain.

An additional difficulty was introduced by the fact that the VSAT service provider blocked traffic between the two VSAT modems (one at the remote site and the other at the RVL) as it passed through its network operations centre, probably to protect other corporate-type services on offer which supported VPN at a premium. We were nevertheless able to circumvent this difficulty when testing the “mediated VPN” solution, because the gateways had a third-party server between them.

Finally, with OpenVPN (Huyghe, 2004) we successfully established a tunnel over the VSAT link (through the third-party server, to avoid the operator’s blockage). OpenVPN uses the UDP (User Datagram Protocol) transportation protocol, which does not check delivery of the data packets, and is therefore immune to latency, but data integrity could not be guaranteed at the outer tunnel level. However, since the VPN encapsulates a TCP/IP tunnel, data integrity is in fact guaranteed, at the cost of a higher latency in the encapsulated link.

After the moderately encouraging results at the MTOR site, we shipped VSAT equipment to Fogo Island, to test the feasibility of establishing a Ku-band link, outside but close to the 40 dBW contour of EUTELSAT’s 10 A Ku-band satellite (i.e. in seemingly similar conditions to those that applied to the MTOR site). Figure 4 shows the installation at the Monte Amarelo hub. The attempts to establish a Ku-band VSAT link from Fogo were plagued with adverse conditions. Although the service was provided by a major European company, a very long chain of intermediaries (service provider based in Italy > commercial services based in Spain > representative based in Portugal > installer based in Cape Verde) led to a dilution of responsibilities that affected the process, as well as a degradation of the technical support provided to the end user.

Several subsequent attempts to establish the link led to negative results, and doubts gradually emerged about the feasibility of using the Ku-band in Cape Verde. Informal consultations with the Cape Verde Atmospheric Observatory (a German–British–Cape Verdean project) revealed that the use of Ku-band VSAT had been attempted and abandoned by them, due to low and unstable signal strength. It became apparent that Ku-band was not a suitable option in Fogo Island. Consultations with C-band service providers revealed that this option was not sustainable in view of its costs. We concluded that VSAT was not a cost-effective option for data transmission in Cape Verde, and terminated the tests.

As an alternative, we installed at the Monte Amarelo hub a satellite telephone terminal, to allow emergency voice or data communication via the Broadband Global Area Network

(BGAN) service. Tariffs being prohibitive for always-on data transmission, the purpose of this link is the remote troubleshooting and maintenance of the monitoring equipment if the primary link fails, remote repair of the primary link if possible, limited critical data transmission and emergency voice communication in the event of a blackout in the Fogo caldera.

5 Discussion

5.1 General requirements of robust communications

The following general principles apply to a robust communications system for emergency management (MIAVITA, 2012):

- The system must not compete with the general public for access to “best-effort” services with high contention ratios (number of users that may be sharing the same bandwidth); during an emergency a peak of demand by the general public must be expected, which may degrade the network performance.
- The system must be redundant and self-healing (i.e. able to re-configure itself automatically in case of failure of one of its components), including the support infrastructure, and in particular the power supply.
- The system used for emergency management must also be used for routine operations; in this way the staff is familiar with the procedures, avoiding an additional factor of stress during a crisis, and the working order of the communications channels is tested regularly.
- The system must be cost-effective, in order to secure sustainability of operation (this principle may conflict with the previous ones, especially when the funding conditions are not favourable).

5.2 Internet access everywhere: a false sense of security

Access to mobile broadband 3G and 4G services is increasingly pervasive, and mobile network data traffic has already surpassed voice traffic (Bold and Davidson, 2012). This increase is even more notorious in emerging countries, where landline services face more challenges since in most places a conventional cable infrastructure was never implemented. Such ubiquity of mobile broadband may lead to a false sense of security in what concerns the access to in situ data from a volcanic monitoring network, since in a remote volcanic region the infrastructure supporting non-voice transmission services will most likely be fragile, due to limited consumer demand (the “last mile” effect). This fragility is compounded with exposure to physical damage during an eruption. Even without physical damage, the service may not provide the required quality of service due to excessive demand by the general public during the emergency. Most Internet service providers publicise the data rates that are guaranteed between the terminal equipment and a local branch office, but from that point onwards the traffic is merged in a link that may have significantly less capacity than the sum of all the incoming tributaries. The quotient of incoming capacity over onward capacity, called contention ratio, is typically in the range $20:1$ to $50:1$ for residential-type (i.e. cheaper) services, making them unsuitable for the transmission of critical monitoring data.

Satellite Internet services can be competitive with cable services in developed countries, but the scenario tends to be very different in emergent or developing countries. Africa, for instance, is in general well covered with expensive C-band VSAT services, but residential-type Ku-band coverage is very limited. When available, services may suffer from poor technical support for installation or maintenance. The Fogo volcano experience revealed that satellite communications are strongly market driven, hampering its potential impact on the reduction of the digital divide.

In addition to cost, VSAT raises some additional difficulties when data integrity and security are required. TCP (Transmission Control Protocol), the most popular protocol in the Internet, requires the acknowledgement of data packets by the receiving computer, and the efficiency of the protocol decreases significantly over geostationary telecommunications given the long round-trip delays associated with the high altitude of the underlying satellite link. VSAT service providers introduce PEPs at both ends of the VSAT link (also known as “protocol spoofing”), as an expedite way around this limitation. However, when a third-party VPN tunnel is established over a VSAT link, the TCP protocol is not accessible to the accelerators because it is hidden by the tunnelling encryption, and this may lead to congestion, reduction of data throughput and data loss.

6 Conclusions

Both in routine monitoring and the wake of an eruption, telecommunications are extremely important for effective volcanic risk management. The design of the systems that enable these communications – from in situ sensors to local or remote laboratories to civil protection agencies – must take into account this need, anticipating and mitigating all the conditions that may hamper the links. This concern must be present at all stages of the design: technology selection, site selection for the elements of the physical infrastructure, network planning.

Critical data for volcanic monitoring should not be transmitted over public networks that may suffer degradation during a volcanic emergency. An in-depth survey of available services must be conducted to ensure adequate performance. Also, the characteristics of the data to be transmitted

(required bandwidth, burstiness, etc...) must be considered in the selection stage.

The Fogo experiment revealed that although satellite communications are often advertised as available everywhere and the ultimate solution for remote areas, the offer is highly market driven and VSAT may prove not feasible for cost-effective volcano data transmission.

For the region that is exposed directly to volcanic hazard, we strongly advocate the use of data transmission equipment owned, installed and operated autonomously by the local volcanological laboratory. Low-power licence-free radio modems are usually suitable to transmit the data, either all the way to the laboratory or until a reasonably safe point of entry into the Internet is reached. With a modest initial investment and no operation costs, this solution is robust and resilient, avoiding the drawbacks of relying on the public networks during an emergency.

Last but not least, we point out that it would be beneficial if national regulations of the electromagnetic spectrum contemplated the use of satellite communications for humanitarian purposes at accessible prices.

Acknowledgements. The MIAVITA project was financed by the European Commission under the 7th Framework Programme for Research and Technological Development, Area "Environment", Activity 6.1 "Climate Change, Pollution and Risks". This work was partially supported by national funds through FCT – Fundação para a Ciência e a Tecnologia, under project PEst-OE/EEI/LA0021/2013. CVTelecom kindly hosted the equipment of the Fogo volcano monitoring network at the Achada Furna and Monte Tchota premises. V. Bosi, S. Auclair and editor Goneri Le Cozanet reviewed the manuscript and helped us to improve it with their constructive criticisms.

Edited by: G. Le Cozannet
Reviewed by: S. Auclair, G. Le Cozannet, and one anonymous referee

References

Bold, W. and Davidson, W.: Mobile Broadband: Redefining Internet Access and Empowering Individuals, in: Living in a Hyperconnected World, The Global Information Technology Report 2012, edited by: Dutta, S. and Bilbao-Osorio, B., World Economic Forum, Davos, 2012.

Day, S. J., Heleno, S. I. N., and Fonseca, J. F. B. D.: A past giant lateral collapse and present-day flank instability of Fogo, Cape Verde Islands, J. Volc. Geotherm. Res., 94, 191–218, 1999.

Faria, B. V. E.: Monitorização Geofísica e Níveis de Alerta do vulcão do Fogo, Ph.D. thesis, Universidade Técnica de Lisboa, Lisbon, 2010 (in Portuguese).

Faria, B. and Fonseca, J. F. B. D.: Investigating volcanic hazard in Cape Verde Islands through geophysical monitoring: network description and first results, Nat. Hazards Earth Syst. Sci. Discuss., 1, 4997–5032, doi:10.5194/nhessd-1-4997-2013, 2013.

Fonseca, J. F. B. D., Faria, B. V. E., Lima, J. N. P., Heleno, S. I. N., Lazaro, C., d'Oreye, N., Ferreira, A., Barros, I. J. M., Santos, P., Bandomo, Z., Day, S. J., Osorio, J. P., Baio, M., and Matos, J. L. G.: Multiparameter Monitoring of Fogo Island, Cape Verde, for Volcanic Hazard Mitigation, J. Volc. Goetherm. Res., 125, 39–56, 2003.

Fonseca, J. F. B. D., Faria, B. V. E., Cruz, G., and Silva, F. M.: Recommendations for improved LVL-RVL communications during crisis, FP7 Project MIAVITA Deliverable-D6.e, 2011.

Frankel, S. and Krishnan, S.: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, Internet Engineering Task Force Informational Memo, ISSN: 2070-1721, available at: http://www.rfc-editor.org/rfc/pdfrfc/rfc6071.txt.pdf (last access: 27 May 2013), 2011.

Hanka, W., Saul, J., Weber, B., Becker, J., Harjadi, P., Fauzi, and GITEWS Seismology Group: Real-time earthquake monitoring for tsunami warning in the Indian Ocean and beyond, Nat. Hazards Earth Syst. Sci., 10, 2611–2622, doi:10.5194/nhess-10-2611-2010, 2010.

Harrald, J. and Jefferson, T.: Shared Situational Awareness in Emergency Management Mitigation and Response, Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.

Heleno, S. I. N., Day, S. J., and Fonseca, J. F. B. D.: Fogo Volcano, Cape Verde Islands: seismicity-derived constraints on the mechanism of the 1995 eruption, J. Volc. Geotherm. Res, 94, 219–231, 1999.

Heleno, S. I. N., Faria, B. V. E., Bandomo, Z., and Fonseca, J. F. B. D.: Observations of high-frequency harmonic tremor in Fogo, Cape Verde Islands, J. Volc. Geotherm. Res., 158, 361–379, 2006.

Helffrich, G., Heleno, S. I. N, Faria, B. V. E., and Fonseca, J. F. B. D.: Hydroacoustic detection of volcanic ocean-island earthquakes, Geophys. J. Int., 167, 1529–1536, 2006.

Huyghe, S.: OpenVPN 101: introduction to OpenVPN. Informative article, August, 2004, available at: http://openvpn.net/papers/openvpn-101.pdf (last access: 27 May 2013), 2004.

Iannela, R. and Henriksen, K.: Managing Information in the Disaster Coordination Centre: Lessons and Opportunities, in: Proceedings of the 4th International ISCRAM Conference, edited by: Van de Walle, B., Burghardt, P., and Nieuwenhuis, C., Delft, the Netherlands, 2007.

ITU: Utilization of ICT for disaster management, resources, and active and passive space-based sensing systems as they apply to disaster and emergency relief situations, ITU-D Study Group 2, 4th Study Period (2006–2010), Question 22/2, Guidelines on the Common Alerting Protocol (CAP), International Telecommunication Union, 2010.

Maral, G.: VSAT Networks, 2nd Edn., Ed. John Wiley and Sons Ltd, Chichester, 2003.

McGuire, W. J., Solana, M. C., Kilburn, C. R. J., and Sanderson, D.: Improving communication during volcanic crises on small, vulnerable islands, J. Volcanol. Geoth. Res., 183, 63–75, 2009.

MIAVITA: Handbook for Volcanic Risk management, Prevention, Crisis Management and Resilience, BRGM, Orleans, 2012.

Sparks, R. S. J.: Forecasting volcanic eruptions, Earth Planet. Sci. Lett., 210, 1–15, 2003.

Surono, Jousset, P., Pallister, J., Boichu, M., Buongiorno, M. F., Budisantoso, A., Costa, F., Andreastuti, S., Prata, F., Schneider, D., Clarisse, L., Humaida, H., Sumarti, S., Bignami, C.,

Griswold, J., Carn, S., Oppenheimer, C., and Lavigne, F.: The 2010 explosive eruption of Java’s Merapi volcano – A “100-year” event, J. Volcanol. Geoth. Res., 241–242, 121–135, 2012.

Totsline, G.: Issues When Using IPsec Over Geosynchronous Satellite Links, SANS Institute Reading Room, available at: http://www.sans.org/reading_room/whitepapers/vpns/issues-ipsec-geosynchronous-satellite-links_770 (last access: 27 May 2013), 2002.

Vazão, T., Silva, F. M., Varela, A., Trindade, J., Pereira, R., and Santos, L.: Definition of a functional architecture for communications in a volcanic incident, FP7 Project MIAVITA deliverable D6.a, 2009.

Vazão, T., Trindade, J., and Pereira, R.L.: Recommendations for improved local communications, FP7 Project MIAVITA deliverable-D6.f, 2011.