Last of the Mile Hazard Warning System (LM-HWS)
ICT Assessment and Community Simulation
Observation Report

Prepared for:
LIRNE*asia*
12, Balcombe Place
Colombo 8, Sri Lanka

By Peter Anderson
Associate Professor
School of Communication
8888 University Drive
Simon Fraser University
Burnaby, B.C.
Canada V5A 1S6
Tel: +1 778-782-4921
Email: anderson@sfu.ca

6 December, 2006

Introduction 3
1. Project Background Objectives 3
2. Concept of Operations 4
3. LM-HWS ICTs 4
3.1 LM-HWS CAP Implementation and integration 6
3.2 CAP GUI and CAP Broker 7
4. Training 7
4.1 HIH 7
4.2 Village Training 8
5. ICT Testing 9
5.1 Silent tests 9
5.2 HIH Dry Runs 9
6. Community Simulations 10
6.1 Trained Villages 10
6.2 Untrained Villages 10
7. Observations 11
7.1 ICT Performance 12
7.1.1 HIH network performance during dry runs and first round of simulations 12
7.1.2 Dialog Disaster and Emergency Warning Network RAD – SMS Alert Systems 15
7.1.3 WorldSpace Disaster Warning Recovery and Response Addressable Satellite Radio (ASR) 17
7.1.4 VSAT – IPAS 23
7.1.5 CDMA Fixed Wireless Phones 24
7.2 CAP General Observations 25
7.3 Alert Message Receipt and Acknowledgement 26
7.4 HIH Setup 27
7.5 ICT Guardian Setup 28
7.6 Intra-community Communication 28
7.7 LM-HWS ICT Maintenance 29
8. Other Considerations 29

Introduction

This report provides a brief review of the Last Mile Hazard Information Warning System (LM-HWS) project and of the progress in implementing and testing its ICT components. In particular, it sets out a series of observations based upon visits (9 Nov-6 Dec 2006) to the Sarvodaya Hazard Information Hub in Moratuwa and selected Sarvodaya district offices and villages during the lead up to and during the first simulation tests of the LM-HWS.

The report builds on previous project reports which include interim reports and reports submitted by Dr. Gordon Gow. Selected excerpts from previous reports and documents are also included in this report for purposes of continuity and to frame recorded observations. Otherwise, all project definitions and related works are assumed within the context of this document.

Preliminary observations and recommendations recorded in this report will be incorporated into the analysis of data collected during the full schedule of village simulations (to be completed before the end of 2006) and into the identification and discussion of requirements to move the project from a pilot project to full implementation (to be completed during a second visit in early 2007).

1. Project Background Objectives

The overall aim of this project is to set the stage for community-driven initiatives at the Last Mile of the Hazard Warning System (LM-HWS). The current phase is not an implementation project but rather a pilot study involving a technology assessment to determine the most cost effective and reliable solutions for a LM-HWS, including an evaluation of their integration into the everyday activities of participating villages.

The primary objective is to evaluate the suitability of various information and communication technologies (ICTs) as the basis of a last mile hazard warning system in Sri Lanka. Six factors are to be considered:

- Reliability of the ICTs
- Effectiveness of the ICTs
- Effectiveness of the training regime
- Level of organizational development
- Gender
- Integration of ICTs into everyday life

A non-profit, non-governmental organization—Sarvodaya—provides oversight, training, and an information hub for the monitoring of hazard threat conditions and for the dissemination of alert and government warning messages to local communities in the Sarvodaya network of villages. Designated first responders selected from the local communities are to be responsible for overseeing emergency preparedness, message dissemination, and emergency response at the local level.

2. Concept of Operations

The LM-HWS project consists of two information reception and dissemination stages:

1. reception and authentication of external hazard event and warning information by monitors located at the Sarvodaya Disaster Risk Management Center Hazard Information Hub (HIH) in Moratuwa (near Colombo) and dissemination to 28 (4 are controlled villages) targeted Sarvodaya communities specially equipped with LM-HWS ICTs, and
2. reception and authentication of HIH generated messages by ICT Guardians in LM-HWS equipped communities and dissemination of the messages to affected local populations.

When fully implemented, trained and certified monitors at the HIH will monitor, on an around-the-clock basis, a variety of hazard and warning networks and disseminate alerts and other messages of interest to LM-HWS equipped communities. There are 5 steps to initiating an alert message: *recording* an event of interest, *consulting* with a Sarvodaya Executive, *deciding* to send the message, *composing* the Common Alerting Protocol (CAP) message, and *issuing* the message. Alerts issued by the LM-HWS are not "public" alerts and are intended only to be distributed to "first responders" who have been trained and certified by Sarvodaya Disaster Management Center as ICT Guardians within the LM-HWS Project.

The ICT Guardians are members of the local community and it is they, or their authorized designates, who are responsible for determining if a local, community-wide (village) warning is to be issued. Upon receiving an alert from the HIH, the ICT Guardian must first acknowledge receipt of the message to the HIH and then proceed with notifying local community officials responsible for activating the community emergency plan.

3. LM-HWS ICTs

The LM-HWS project is testing five information and communications technologies:

1. Dialog Remote Alarm Device (RAD). RADs are stand-alone units that incorporate remotely activated alarms, flashing lights, a broadcast radio receiver to be turned off or on and SMS messages to be displayed, as well as self-test, message acknowledgement and hotline GSM call-back features.
2. GSM Java enabled SMS mobile phones to receive text alerts in Sinhala, Tamil and English (Java Phone), activate a Java applet to sound an alarm, and hotline GSM call-back features.

3. Disaster Warning Recovery and Response Addressable Satellite Radio (ASR). ASR is a WorldSpace system that can issue address hazard information directly to those communities at risk. Global Positioning System (GPS) technology incorporated into the radio set, along with the unique code assigned to every receiver, allows for hazard warnings to be issued to sets that are within a vulnerable area or just to radio sets with specific assigned codes.
4. Very Small Aperture C-Band Satellite Terminals (VSAT). VSAT terminals are being installed in two communities and at the HIH. These facilities will provide up to a 512 kbps Internet connection and enable testing of the Internet Public Alerting System (IPAS). An IPAS client application installed on a computer enables pop-up messages to appear on a PC screen and an audio alert tone to be played on the computer's sound system. This part of the project will also evaluate the extent to which end-user devices can be used to report observations from villages to the Hazard Information Hub in order to improve situational awareness. These evaluations will therefore have downstream (warning) and upstream (reporting) components.
5. CDMA Fixed Wireless Phones with built-in speakerphones to provide voice communication via the public switched (FPs).

Device	Network Access	Message Creation/dissemination Interface	Enabling Partner
DEWNS	GSM fixed wireless	Password protected Internet website	Dialog Telekom Mobile Communication Laboratory at the University of Moratuwa, MicroImage
Java phones	GSM mobile wireless	Password Internet protected website	Dialog Telekom, MicroImage
Telephone	CDMA fixed wireless	PSTN	SL Telecom
VSAT, Internet Public Alerting System	Internet via C-Band fixed satellite wireless	Password protected website	Innovative Technologies, Solana Networks
Addressable Satellite Radio	L-Band portable satellite wireless	Password Internet protected website	WorldSpace Global Data Solutions

Table 1 LM-HWS Access and Message Management Attributes

3.1 LM-HWS CAP Implementation and integration

A major component of the LM-HWS project is the use of the Common Alerting Protocol to enable data interchange between the Hazard Information Hub (HIH) and a range of end-user technologies. CAP is a simple, flexible data interchange format designed for collecting and distributing "all-hazard" safety notifications and emergency warnings over information networks and public alerting systems.

CAP as a content standard is deliberately designed to be transport-neutral. In web-services applications, CAP provides a lightweight standard for exchanging urgent notifications. CAP can also be used in data-broadcast applications and over legacy data networks. CAP provides compatibility with all kinds of information and public alerting systems, including those designed for multilingual and special-needs populations. Further, CAP incorporates geospatial elements to permit flexible but precise geographic targeting of alerts. CAP also provides for associating digital images and other binary information with alerts and supports various mechanisms for ensuring message authenticity, integrity and confidentiality where required.[1]

In 2004, CAP was adopted as an international standard by OASIS (Organization for the Advancement of Structured Information Standards), a not-for-profit, international consortium, that drives the development, convergence, and adoption of e-business standards. Since 2004, the CAP standard has been adopted by many national and sub-national emergency management organizations, as well as hazard monitoring and reporting organizations such as NOAA and national meteorological organizations for disseminating hazard information, alert and warning bulletins.

CAP was integrated into the project because of the following perceived benefits and advantages:

- Since it is an open source, XML-based protocol with clearly defined elements, CAP should be capable of supporting data interchange across multiple dissemination channels.
- With CAP, one input at the central information hub can be translated into multiple outputs for downstream alerting.
- CAP provides a standardized template for submitting observations to the central hub (upstream) and thereby supports situational awareness to improve overall management of a critical incident.
- A CAP-enabled system will more easily integrate with other national and international information systems.

Discussions about whether or not, and how to implement CAP within the Sri Lankan context (e.g., language, geographical regions, hazards, etc.) are still evolving with no official government determination yet made at the time of preparation of this report. Similarly, decisions concerned with the long term path dependencies associated with

[1] OASIS Emergency Management Technical Committee, CAP 1.0 - Fact Sheet, 3/1/2004, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency [accessed 29 November, 2006].

future expansion of CAP within Sri Lanka and in the Indian Ocean region are yet to be concluded.

In this regard, the decision and processes used to implement CAP within LM-HWS are important considerations of the pilot study, and will provide lessons for implementing CAP in other organizations in Sri Lanka and in other countries.

3.2 CAP GUI and CAP Broker

An early challenge faced by the project was whether or not the project would need to build a CAP user interface from scratch, or whether there was an application available that could be borrowed. The CAP GUI provides a method (a template) for authorized users to enter data into a computer at the HIH and for the transformation of that information into the appropriate CAP XML elements. The CAP broker is a server that will provide an intermediary point of interconnection between the Information Hub and the relay network to facilitate interconnection of all ICTs and passage of CAP-compliant messages through a single software application.

At this stage of the project, both WorldSpace and MicroImage have developed web browser based CAP GUIs for the LM-HWS project. The WorldSpace CAP GUI (Anny Network Early Warning System) interfaces with the ASR component and the MicroImage (Disaster Early Warning Network) with the Dialog RAD/SMS components. Both the WorldSpace satellite uplink and Dialog Telekom SMS servers are registered as teleports in their respective CAP alerting software. Presently, the ASR and RAD/SMS CAP software operate independently of each other, but in the future, could be integrated and controlled by a single software application. Similarly, the VSAT IP gateway could be added as a teleport and integrated into a common CAP solution along with other ICTs.

The VSAT satellite alerting message software also uses web browser based GUI called Internet Public Alerting System (IPAS). IPAS in its current form is not CAP-compliant but provides a simple and effective means to test sending IP based alerts to PC screens and audio systems.

4. Training

4.1 HIH

In August 2006, HIH staff were given training for certification as Hazard Information Hub Monitors and “authorized users”. The basis of the course is the *Common Alerting Protocol* (CAP) for risk information communication. By the end of the course the Monitors were able to: 1) *identify* an Event of Interest (EOI), 2) *confirm* the EOIs with a Sarvodaya Executive, 3) *construct* a CAP Message, and 4) *relay* the CAP message to LM-HWS ICT devices in designated communities.

The training also emphasized, in the event the government of Sri Lanka issues a public warning, how the Monitor will relay this message directly through the LM-HWS network. If the government does not issue CAP-compliant messages, the Monitor will need to develop a system for translating or reformatting these messages quickly and accurately into a LM-HWS CAP-compliant message.

4.2 Village Training

Training at the village level consists of two training components: 1) general disaster preparedness training for village trainers and 2) specific training for ICT Guardians.

Training of Trainers

The Training of Trainers (TOT) component forms the education component envisaged in LM-HWS as the underpinning training to instill an effective warning response. Those trained (known as HIH Trainers), in turn, are to train ICT Guardians and others at the community level.

The newly trained trainers are expected to be able to:

- Instill awareness of hazards, vulnerability, and risk.
- Conduct community based hazard mapping, resource mapping, risk assessment and identification of vulnerable households and groups of people in the community.
- Create awareness of the early warning mechanism in place and the response activities that need to be undertaken.
- Enable the identification of appropriate dissemination mechanisms to vulnerable households.
- Enable formulation of a response plan, which includes an evacuation plan with clear actions, roles and responsibilities and identify resources needed.
- Instill the competency to conduct an evacuation drill which is comprehensive.
- Provide the ability to measure the effectiveness of response plans carried out as simulations.

TOT took place in Bandaragama in April 2006. Currently, 16 of the 32 participating communities have received training as part of a controlled group in the pilot study.

ICT Guardian Training

In July, 2006, a workshop was held at Sarvodaya in Moratuwa to train the Sarvodaya Village and District first responders with the objectives of:

- ensuring that all participants, namely Sarvodaya first responders, have a good understanding of the Common Alerting Protocol.
- providing ICT Administration and User training to all Village and District first responders.

- introducing the Hazard Information Hub Help Desk functions to the participants.
- giving the technology partners who designed and developed the ICTs an opportunity to demonstrate their solutions.
- handing over the ICTs to the Village first responders. Those responsible for their operation were designated as “ICT Guardians”.

5. ICT Testing

Upon completion of installation of LM-HWS ICT components at the HIH and in participating communities, a series of tests were conducted to verify that the ICTs functioned properly and to enable HIH Monitors and ICT Guardians to become more familiar with their operating characteristics. The tests were conducted in “silent” mode to set the stage for expanded “live” community simulations (exercises).

5.1 Silent tests

On 21 of August, 2006 a series of silent tests were conducted at the HIH and among ICT Guardians. Testing at the HIH consisted of creating test messages and sending them to each LM-HWS ICT component installed at the HIH to verify they were set up, operating properly and were correctly receiving alert messages.

The silent testing also enabled HIH Monitors to test and become more familiar with the components’ software, necessary for composing and sending messages. Four of the ICTs, satellite radio (ASR), fixed CDMA phone (FP), java-enabled mobile phone (MP) and the GSM remote alerting device (RAD), were tested. Installation of the VSAT terminal was not completed at time of testing. The tests revealed that all of the installed ICT components were functioning correctly.

On the same day, silent tests were performed on all devices installed in the participating Sarvodaya communities, whereby ICT Guardians could verify to the HIH whether or not their ICTs were correctly installed and functioning properly.

5.2 HIH Dry Runs

On 22 November, a full end-to-end silent test (dry run) was conducted at the HIH to determine how long it would take to complete the entire process of receiving an external hazard event notification, authenticate it, receive approval from the Sarvodaya Executive, convert it to the appropriate CAP formats, input it to the appropriate LM-HWS content dissemination interfaces, and transmit and receive the messages successfully over the installed LM-HWS ICTs.

A subsequent dry run was conducted on 23 November. The results of these tests are discussed later in this report.

6. Community Simulations

With LM-HWS components now in place and preliminarily tested, with HIH Monitors and ICT Guardians having completed basic training and with selected communities trained in basic risk and disaster management principles, the stage was set for a series of community based simulations to test the LM-HWS from end-to-end. To facilitate these community simulations, a number of organizing activities have taken place, including a pre-simulation orientation workshop involving key participants at Sarvodaya in Moratuwa on 17 November, 2006 and pre-simulation mini-workshops in participating Sarvodaya Districts (currently still underway). These workshops have provided an opportunity to present a standardized methodology for the evaluation of simulations, including the capture of data to assess:

- reliability of the ICTs.
- effectiveness of the ICTs.
- effectiveness of the training regime.
- level of organizational development.

A series of simulations have been scheduled from late November through December on a District-by-District basis.

6.1 Trained Villages

Some of the trained communities have elected to run full end-to-end simulations, including the involvement of residents in mock evacuations to test local plans, alerting and evacuation procedures. Others have chosen to conduct simulations on a smaller scale.

The simulations have required considerable pre-planning at District and Village levels including:

- community meetings to discuss the purpose, objectives, goals and needs of the simulation.
- informing community authorities and obtaining necessary approvals.
- scheduling of the event (choosing best time of day and day of week).
- defining roles and responsibilities of the local simulation group.
- preparing residents of the community in advance so they understand that this is an exercise and what is expected of them.
- recruiting observers and evaluators .

6.2 Untrained Villages

After consultation with LM-HWS Districts and Villages at the 17 November pre-simulation workshop, consensus was reached that it would not be appropriate to fully exercise villages that are not trained, to avoid creating confusion among residents about the intended purpose of the simulation.

Further, there are public safety considerations that must be considered in advance whenever public participation is sought in such exercises.

Instead, in each participating untrained village, HIH trainers and District coordinators will conduct a “table top exercise” with relevant officials at the village location when the LM-HWS alert arrives. The table top exercise will be in the form of an around-the-table or group discussion about what steps the village would take in the event the alert message was real, followed by LM-HWS trainers taking participants through an introduction to disaster planning – to be followed by a full training workshop at a future date. In this way, shortly after the completion of simulations, all participating villages will be trained to the same level and all villages will have improved their alerting and response capacity.

A slightly modified version of this table top process can also be applied in trained villages where circumstances prevent them from conducting full community simulations.

All villages, trained and untrained, will be able to complete the HIH-to-village LM-HWS technical simulations.

7. Observations

Based upon a review of the project objectives, supporting documentation and participation in activities at the HIH, pre-simulation workshops and the first simulation test in the District of Galle, the following section offers a preliminary set of observations and recommendations intended to serve as inputs to factors to be addressed as the project moves from pilot to full implementation. These are offered with a caveat that they may be subject to revision when post-simulation analysis of collected data is completed in January 2007. Further, the recommendations will form part of an action plan for the author’s expected return visit in early 2007.

7.1 ICT Performance

7.1.1 HIH network performance during dry runs and first round of simulations

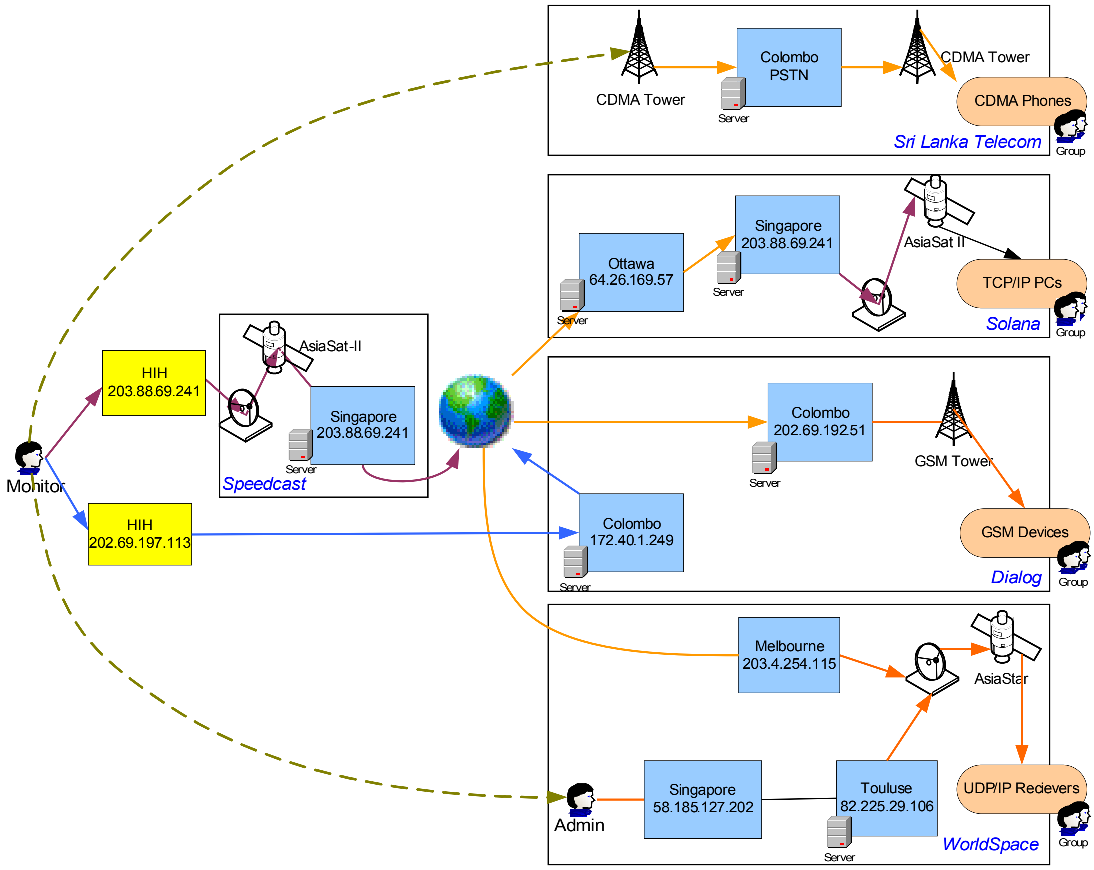

Figure 1 - Communication Gateways and Pipes from HIH to End User Devices

<u>Internet Connectivity</u>

At present, the HIH uses a Dialog 128 kbps fixed wireless link (bridge) for its Internet access. The connection is terminated at the HIH through a modem which in turn is connected to a Local Area Network (LAN) through a data switch and a wireless 802.11g WiFi access point. Dialog provides 5 static IP addresses for use at the HIH.

Leading up to and during the dry runs, a series of problems concerning outbound Internet connectivity emerged and continued to plaque the tests, resulting in both the Dialog DEWN and WorldSpace Anny software timing out before messages could be fully entered into their templates and/or sent. These problems manifested themselves in the form of severe network congestion that caused lengthy delays in logging into the servers. After an extensive investigation, it was revealed that four separate issues were at the root of the problems.

The first problem was caused by an incorrectly connected cable that was routing data packets from the WiFi access point router back into the main Dialog connection. This effectively caused the LAN to be flooded with excess packets, causing severe local congestion. Once correctly cabled, most of the congestion disappeared.

The second problem was caused by the HIH workstations being connected to the WiFi access point, rather than through a cable connection to the Dialog router via the data switch. The WiFi access point appears to intermittently drop its signal, causing the link to time out and PCs to have to reinitialize their Internet connections through a DHCP setup. Each time this occurred, the connection to the CAP servers broke and/or timed out. This problem was solved by connecting the PCs directly to the Dialog connection and assigning them a Dialog static IP address.

The third problem was caused by congestion on the main Dialog backbone connection. This was discovered by conducting a trace route connection between the HIH and the final destination where the server resided. In the case of Dialog DEWN, the server resides within Sri Lanka, whereas, the WorldSpace servers reside in Toulouse, France and Singapore. A trace route test sends a series of data packets through the network and measures and analyzes the quality of the link according to how long it takes to get an acknowledgement back from all of the locations where the packets are routed on their way to the final destination (latency), along with how many of the sent packets were dropped in transit (packet loss). The trace route tests revealed that, at times, there were significant latencies in packet delivery possibly due to congestion or a malfunctioning router at the Dialog gateway, which were resulting in timeouts and excessive packet losses en route to their final destination. Results of the route traces were sent to Dialog who, in turn, made changes to the packet routing. The routing now appears to be stable.

The fourth problem was caused by the Dialog radio antenna being mounted on a tall pipe that tends to sway in the wind, moving the antenna in and out of focus.

Recommendations

1. That the HIH ensure it always has at least one backup Internet connection in the event that the primary link malfunctions. It is understood that when the HIH VSAT terminal installation is completed, a much higher capacity link will be available. It is recommended that this become the primary link when available and that the Dialog link becomes the backup.
2. That the WiFi router be tested for stability and that it be connected only as an auxiliary unit to support non-mission critical applications.
3. That all mission critical applications always have priority access to the most reliable connections and use static IP addresses.

4. That all outside network support facilities (antennas, masts, cables, etc.) be checked for protection – both physical and environmental.
5. That the Dialog radio antenna mast be stabilized using guy wires.
6. That HIH monitors receive training in basic network diagnostics in order to monitor connections for stability and to report problems to the SITU for resolution.
7. That the HIH enter into a formal agreement with SITU for ongoing ICT operational and technical support.

Power outages and voluntary shutdowns

The building which houses the HIH experiences power failures almost on a daily basis due to interruptions of service from the mains electrical grid. These failures result in loss of lighting, air conditioning and power to PCs, printers, data switches and other critical LM-HWS components. Further, as power is being restored, surges and spikes that are potentially damaging to equipment can easily occur. Some, but not all, of the key LM-HWS components are equipped with small battery uninterruptible power supplies (UPSs) that both cushion equipment against surges and provide a time limited alternate source of AC power – sometimes long enough to function until power is restored or to enable PCs and other equipment to be properly shut down.

During lightning storms, which are also frequent at certain times of year, equipment often needs to be shutdown and unplugged from the electrical system to prevent damage from spikes resulting from lightning strikes on the electrical grid. This can incapacitate an operational centre.

However, a recent test, using a battery operated lap top computer connected to the HIH LAN, revealed that the Internet connection can remain functional during a power failure; demonstrating that if provided with an adequate alternate power supply, the HIH can remain functional. Similarly, this would be the case if the HIH was physically disconnected from the mains power grid and switched to a local battery/generator source that was lightening protected. In the event the Dialog fixed wireless connection is lost due to a wide area power failure, the HIH VSAT could still remain operational if self-powered at the HIH. Further, the use of CDMA fixed wireless phones and mobiles at the HIH provide an additional layer of insulation to wireline-based power spikes.

Recommendations

8. That a study be conducted to determine the overall operational power requirements for the Sarvodaya Disaster Management Center that houses the HIH, and to determine how mission critical equipment could be isolated from the building's mains power supply and placed on its own backup power supply. Ideally this would be a large UPS system that serves as the mains power supply, which in turn is continuously charged by either a circuit from the main building power supply or a generator when the mains power is lost. AC power to the UPS is diverted between the mains supply and generator through a manual transfer switch or an automatic switch if the generator is self starting.

9. That, in the meantime, additional larger UPS units and a generator with adequate fuel supply be available and routinely tested to support the most critical LM-HWS ICT components and small lighting fixtures through a short to medium duration power outage.
10. That investigations be conducted to determine the extent to which solar photovoltaic panels could supplement battery charging requirements.
11. That all generator connections be routed through UPS units connected to LM-HWS equipment to provide power stability.
12. That all mission critical ICT components be lightning protected. In some cases, where practical, use of fibre optic rather than copper Ethernet cable can provide additional surge protection.

7.1.2 Dialog Disaster and Emergency Warning Network RAD – SMS Alert Systems

The Dialog Disaster and Emergency Warning Network (DEWN) employs two ICT devices – Java enabled GSM mobile phones with alarm and multi-language display and GSM remote alert devices (RADs) to disseminate alerts. The same MicroImage CAP-based GUI serves as the message creation and management interface for both devices. To create and send an alert message to either set of devices, the HIH authorized user logs into (DEWN) server via an on-line password protected form.

<u>Java-enabled Mobile SMS Phone</u>

Four advantages of the Java-enabled SMS phone alert device are that it: is portable or mobile, is increasingly in common use, sounds alerts and can display text in different character formats to support multiple languages in addition to English (especially Sinhala and Tamil). However, the GSM mobile phone needs to be pre-loaded with a special Java applet in order to receive sound alerts and text in Sinhala and Tamil. Without the applet, the mobile phone can only receive English language text messages. Other potential limiting factors are gaps in signal coverage in various locations around Sri Lanka and a limited capacity for text display (154 characters). In the latter case, only a small portion of a CAP generated alert message description can be displayed. Its key advantage then is it’s alerting – attention getting characteristics.

Acknowledgement of alert message receipt is accomplished by using the call back function to enable a voice callback with an option to save the number for subsequent text messaging.

A few challenges have been experienced in configuring phone sets, including downloading the Java applet (required to display Sinhala and Tamil characters) over a GPRS link, and the fact that configuration requires additional technical expertise beyond that to be expected of an average user. The weak signal strength of the GPRS connection does not allow for easy download and installation. Once configured, however, usage requires little or no extra training beyond normal SMS usage. However, at time of first simulations, not all phones were fully configured.

Recommendations

13. That HIH establish a technical/maintenance shop to pre-configure and test all devices before they are sent to communities.
14. That ICT Guardians receive additional instruction (including a technical manual) in use of the phone's call back features for alert message confirmation.

Dialog GSM Remote Alert Devices (RADs)

As indicated earlier, the RAD device is a stand-alone unit that incorporates an array of alerting features, including remotely activated alarms, flashing lights, a broadcast radio receiver that can be remotely turned off or on, and SMS messages to be displayed, as well as self-test, message acknowledgement and hotline GSM call-back features. The unit also possesses a built in backup battery power supply.

Of all of the current LM-HWS ICTs, the RAD is by far the most intrusive (attention getting) device. Its alarm is loud enough to be heard from any room within most households and its flashing light is very bright. This feature is very useful for attracting attention, especially for those with hearing disabilities.

A few observed disadvantages of the current version are that:

- as with the Java-enabled mobile phone, its SMS message capacity is limited and can only display a small portion of a CAP generated alert message description.
- it can only display text messages in English.
- when all features are enabled and operating without mains AC power, the units appear to draw down battery capacity quickly.

Despite these issues, early feedback from ICT Guardians indicated that they especially liked the flashing light and alarm features.

Recommendations

15. That an option be added to connect an external antenna to the device where indoor reception is poor.
16. That the text display features be modified to have the same capabilities as the Java enabled mobile SMS phones, to allow text to be displayed in English, Sinhala and Tamil.
17. That a DTMF pad be added to enable the end user to initiate general GSM calls in the event that the HIH hotline number isn't downloaded and/or programmed in the unit.
18. That methods be examined to reduce current draw on battery units when operating without mains AC power and/or to add an auxiliary 12 volt connector to supplement the DC capacity of the unit, including a solar powered charging unit.

DEWN CAP Interface

Once logged in to the web-based system, the HIH monitor can create new and view existing users, view and delete existing messages and/or create new ones in Sinhala, Tamil and English, assign a Hot-line number, create new and view exiting recipients, create and configure alarms and send SMS and Alarm messages. To enable Sinhala and Tamil functionality, corresponding drivers must first be installed on the HIH monitor's computer.

However, the GUI requires these actions to be completed through a number of separate window screens, and SMS and Alarm messages must be sent separately. All of these actions can add additional time to creating and sending a CAP alert message.

Some other issues relating to DEWN functionality include the following:

- DEWN is not fully supported by the Mozilla browser. For example, text menus overlap in the windows.
- All RAD unit IDs, including non-Sarvodaya units, appear in the on-line forms. To choose only Sarvodaya units, the HIH monitor must go into the CAP management software and manually delete all non-Sarvodaya listings.
- Similarly, to test individual units, all other units must be deleted from the recipient list. Once this is done, results cannot be saved for future quick configuration.
- The SMS Message Log feature is not functional – the "Use Calendar Feature" does not presently work.

Recommendations

19. That the DEWN software be modified to enable all messages to be composed in one stage, and that the number of templates be reduced to simplify and better integrate common data fields.
20. That HIH work with Dialog – MicroImage to further customize features based upon HIH common operating procedures.
21. That Dialog – MicroImage be informed of the SMS Message Log malfunction and that they be encouraged to modify DEWN software so it can be used with other Internet Browser Applications such as Mozzila Firefox and not exclusively with Microsoft Internet Explorer

7.1.3 WorldSpace Disaster Warning Recovery and Response Addressable Satellite Radio (ASR)

Among its many features, ARS supports a variety of functions including text alerts, both short and extended (through an auxiliary box), audio broadcasts of unlimited length, geographical, individual and group based message targeting.

Further, because the receivers' signals are fed from a geostationary satellite, and receivers can be DC battery operated, ARS can operate independently of local or national infrastructure. This is a very useful feature during hazard events that can impact domestic infrastructure and utility services.

However, programming and loading message content into the system is still dependent upon having a reliable Internet connection, which, at the HIH, is currently being supplied by a domestic land-based Internet service provider.

Observations about the ARS hardware and software functionality and usage are briefly described below.

CAP GUI

The CAP GUI software named, “Anny Network Early Warning System (Anny)”, is accessed via an Internet web-based connection to the WorldSpace gateway in Toulouse, France. The authorized user logs in and proceeds through a sequential 3-screen process to create and compose a CAP-compliant message.

The following observations were recorded during silent tests of the software.

Overall, once properly oriented, authorized users should be able to compose and send text messages fairly quickly using Anny. However, some software modifications and enhancements could improve the timeliness of alerting and efficiency of message management. Some data entry issues were also observed and are noted below.

Timeliness of message creation - The Anny software will time out if there are delays in data entry, requiring the HIH Monitor to log out and log in again and start a new entry.

Precision of data entry - Some data fields are very particular about what characters can be entered. For example, the ID description field only accepts numbers and letters and not characters such as “/”. Doing so results in receipt of an internal system error message.

Another example is use of the “Countries” drop down field in the third CAP page. Selection of “Sri Lanka” results in the alert not being sent, even though it shows up as having been sent. It was discovered that this field should not be used, as apparently the system defaults to Sri Lanka when the HIH Monitor logs in.

Documentation and trouble shooting - Many of these issues are not documented and required follow up calls and emails with WorldSpace technical staff in Singapore and Toulouse to resolve. The character entry issue was uncovered at the HIH through trial and error.

Help menu - The current version of Anny does not offer an on-line help menu.

Message creation and transmission logs - The current version of Anny does not offer authorized users access to system logs, although it is understood that they are available to WorldCom system administrators.

Recipient Layout and Configuration - The Anny Recipient List contains a complete list of all ASR units – many of which are not part of LM-HWS. It may be possible to send alerts to non-LM-HWS recipients if they are selected accidentally.

Add/Edit Recipients Function - Recipient records do not appear to be write protected, possibly enabling non-LM-HWS authorized Anny users to view and edit them. Once a recipient is created it does not appear that the recipient name can be changed without deleting the entire record and creating a new one.

Create/Edit Group Function - New Groups can be assigned names, but the names do not show up in the drop menu in the CAP form when creating a new group message. Groups are listed only by their numerical ID requiring the HIH Monitor to remember groups associated with the Group ID. This may be difficult during an alert phase.

Group records – Group records do not appear to be write protected, possibly enabling non-LM-HWS authorized Anny users to view and edit them or any authorized user to accidentally add an outside recipient to their group list.

Recommendations

22. That the LM-HWS project recommend to WorldSpace
    - the establishment of:
        - a toll free phone and/or Skype/MSN Messenger on-line help desk.
        - an authorized users technical support and documentation section possibly with a bulletin board (accessed via a drop down menu in ANNY).
        - an Email/SMS list for sending updates and notifications to authorized users.
    - The Anny database restrict access to only closed recipient groups and only grant write privileges to records for authorized users within their respective groups.

23. That HIH create a table of Group names and ID numbers – print it out and post it beside the HIH workstations as a lookup table.

HIH configuration of Anny

Personal Messages – Presently LM-HWS ARS receivers are not listed in a consistent manner requiring the HIH monitor to scroll through a long list of receivers to search and select the appropriate receivers.

Recommendation

24. Rename the LM-HWS receivers using a standardized naming convention for easy searching.

ARS Audio Recording Mode

A special advantage of ARS is its ability to datastream audio to ARS receivers. The audio can be any form – music, sound alerts, voice, etc. Creating audio alert messages involves a four stage process. The HIH monitor first records a message using a microphone and a software program installed on the workstation. The audio file is then transferred to a WorldSpace server located in Melbourne, Australia, via an Internet file transfer. The file is then transferred on-line to an appropriate directory for scheduled datastreaming to the designated Sarvodaya WorldSpace audio channel (channel 950) and is monitored by an audio player client installed on the HIH workstation.

The pre-loaded audio files are then linked to the ARS DAMB-R receivers through entering "950" in the Alert BCID/SCID CAP field found on the second page of Anny. When the alert is sent, this field causes the DAMB-B receivers to automatically switch to channel 950.

Quality of Audio Recordings – It has been observed that audio recording levels can vary significantly (more than 20 dB) and at times the Melbourne gateway has rejected it.

Sarvodaya Channel Content – Presently, channel 950 remains undeveloped as a broadcast medium. Its capabilities extend well beyond being available as a simple audio alert system and, if properly supported and organized, could become the primary means for Sarvodaya to distribute hazard and other program content in electronic form to its extensive network of villages.

During district pre-simulation meetings, concern was voiced about the lack of relevant content being aired to retain listener interest and the need to make content distinctive enough to enable the listener to distinguish between general content and alert messages.

Recommendations

25. That a small audio mixer and recording system be installed in the HIH control room to ensure high quality and consistent recording levels.
26. That HIH staff receive basic training in audio production techniques including scripting, audio recording and editing, announcing and on-air presence.
27. That a series of pre-scripted messages be composed and recorded including a distinctive alerting sound to precede all audio alert messages, "please standby" messages, etc.
28. That HIH work with other branches in Sarvodaya to explore ARS capabilities and identify associated usages.

ARS Text Display – DAMB-R

The current model of the DAMB-R can display a limited amount of alert text, including the following CAP field contents:

- Identifier
- Sender
- Status
- Scope
- Category
- Event
- Urgency
- Severity
- Certainty
- Response Type

These are all inputted in the first Anny page. Unfortunately, there is insufficient capacity to display the actual alert description (which can contain qualifying information specific to each event, and in the case of an official government warning message, would contain the entire unmodified warning message). This deficiency effectively relegates the basic, yet sophisticated, DAMB-R unit to a simple alerting device, if used only in this mode. However, there are two supplementary features than can rectify this message limitation. The first is the audio broadcast feature built into the device (as discussed above) and the second is the addition of an auxiliary display device connected to the DAMB-R via a USB cable.

Auxiliary Display Unit – The auxiliary display unit has the capacity to display the full range of selected CAP fields including the description field. However, the text display does not support Sinhala/Tamil text.

Recommendations

29. That auxiliary display units be supplied and attached to village DAMB-R units.

30. That LM-HWS encourage WorldSpace further to enhance units to include a small built-in speaker, flashing light and other alerting features such as multi-language text display.

ICT Guardian DAMB-R Usage

Audio reception – Most ICT Guardians only received a set of ear plugs for monitoring ASR audio service. In Guardian houses, visited during the first round of simulations, many did not have an auxiliary speaker attached, although units possess an audio “line out” connector. Instead, they had adjusted the volume control to a maximum setting and were attempting to use earphones as mini speakers. Unfortunately, this restricted coverage to only a few meters from the ASR device.

Recommendation

31. That a set of DC powered speakers be provided for all ICT Guardians using DAMB-R receivers.

Antenna placement – two bars of signal strength appear adequate to receive ASR audio programming, but are insufficient to trigger the alert functions. This was discovered during the first simulation in Galle District, where two communities failed to receive the alerts. After moving the antennas to receive a better signal strength (minimum three bars), the units functioned properly. It was fortunate that the glitch was discovered during a simulation, since a unit could have functioned properly the first time and, then, have been moved afterwards with audio service still functioning, but with poorer signal reception. The ICT Guardian would be unaware that the unit would not be triggered in subsequent alert transmissions. Similarly, since ASR units possess no message receipt acknowledgement capabilities, without ICT Guardians possessing a second means to acknowledge receipt of ASR alert messages, HIH Monitors would also be unaware of non-delivery of the messages.

This issue is being corrected by site visits to each community to test and verify functionality of all alert systems before subsequent simulations take place.

Recommendations

32. That regular updates be provided to ICT Monitors, along with tips on how to ensure proper functioning of units.
33. That the HIH schedule regular silent tests with Guardians and have them maintain logs, copies of which should be periodically sent to the HIH for analysis.

Power outages and lightning storms – ICT Guardian residences do not possess backup power and ASR units go off-line during frequent power interruptions or when unplugged during lightning storms, unless backed up by batteries. The ASR units have provision for two AA size batteries. However, some Guardians reported that the batteries did not last long. Further, units need to be unplugged and tested regularly to check battery levels and supplies of replacements must be on hand.

Further, when using the attachable auxiliary alert box, power is provided to the ASR unit from the auxiliary box via a USB cable. However, the current version of the auxiliary box relies on an AC-to-DC power supply. Although it is capable of operating from a DC source, it does have a back up battery compartment.

These power issues also affect all of the other LM-HWS components. Even those such as the SMS Java mobile phones and RADs ultimately require an alternative power source to recharge their internal batteries during prolonged power interruptions.

Recommendation

34. That ICT Guardian monitoring sites be provided with solar power charged HD 12volt UPS battery systems that operate independently from the mains AC supply. Systems are always powered by the battery supply to be impervious to mains power failures. If the UPS battery fails during an emergency it can easily be replaced by an automobile battery.

7.1.4 VSAT - IPAS

At time of writing this report, the VSAT terminal components of LM-HWS were not yet functional. Consequently, an evaluation of their performance cannot be undertaken at this time. However, the VSAT component essentially provides a wideband (512 kbps) IP based connection through an out-of-region satellite Internet gateway. The VSAT system is intended to provide network support for an alerting system known as Internet Public Alerting System (IPAS) developed by Solana Networks in Canada.

IPAS allows authorized users to issue hierarchical alerts to subscribers via the Internet. That is to say, alerts can be issued on a national, regional or community wide basis. Further, IPAS alerts can be issued according to a scale of severity from 1 to 5 (5 being the highest severity).

Although not CAP-compliant in its present form, IPAS possesses some similar features to CAP. The IPAS GUI is accessed through a web-based form. The authorized sender logs in and can then select the “Issue Alert” page to begin composing an alert message. Among the features, users can set the send time, duration of the alert, geographic target area, type of message, level of alert, and compose an alert message. The message box feature is equivalent to the message description in the CAP template. One advantage of IPAS is that unlike SMS and the basic ARS DAMB-R2 components, IPAS appears capable of carrying the equivalent of the entire CAP description field. IPAS alerts can also be received on any Internet enabled MS Windows computer.

For receiving alerts, IPAS utilizes an alert window, visual and audio approach. Users download and install a Java applet on their computers and then register for the types of emergency alert notifications that they want and can filter them according to geographic scope and severity. In the event of an emergency alert broadcast, the alert message will pop-up in a window on the subscribed user's computer screen with an audible alarm.

In tests performed with IPAS, the message system appears to be very efficient and straightforward for composing and sending alerts. However, certain peculiarities were observed that will be important for both HIH Monitor message senders and ICT Guardian receivers to take note of.

For sending alerts, it is necessary to ensure that the correct time zone field is selected. The same is true for choosing the geographic scope and level of event. These latter combinations must match those set by the alert receiver clients; otherwise the alerts will not trigger the client. This situation particularly applies to event level. A client set to level 1 and an alert message set to a level 5 or visa versa will not trigger the client.

If the Internet connection is broken, the client may lose its subscription record and thus its configuration for receiving alerts. When this occurs, the client still appears to the user to be functioning correctly in its standby mode, but will not be triggered by an alert message until it is closed and restarted. At that point, its subscription record is reloaded and the client will function correctly again.

The Alert Log lists the status of alerts, including dates and times, but the time zone defaults to Eastern North American time. The logs do not register which end users have acknowledged receipt, although this data may be recorded by the IPAS server software.

Finally, the IPAS client does not contain a “help” feature or hyperlink to an on-line manual to assist users in configuring their clients and carrying out basic troubleshooting.

Recommendations

35. That the LM-HWS project team work with Solana Networks to determine how the IPAS server software might be modified to:
    - be CAP-compliant.
    - enable authorized users access to recipient message receipt and acknowledgement logs.
    - enable IPAS alerts to be ported to GPRS and/or 1XRTT enabled mobile phones to support display of longer alert descriptions.
    - Correct the log time stamp anomaly and provide improved end-user help features.

36. That a standard configuration for “levels” of event be established and programmed into all LM-HWS clients and be used whenever alerts are composed.

7.1.5 CDMA Fixed Wireless Phones

The CDMA fixed wireless phones provide standard dial-tone voice phone services and are very useful, especially in rural areas that have limited or no wire-line services. Also, because of their portable nature, they can be easily re-located. Further, usage requires little or no training.

The current LM-HWS versions support voice and 160 character text messaging, although an advanced version also supports an Internet connection via a 1XRTT data service.

Alerts sent to ICT Guardians are placed through personal calls initiated by the HIH. However, this form of alerting requires each CDMA equipped ICT

Guardian to be contacted separately – a process that can be time-consuming and human resource intensive when a number of recipients must be reached.

On the benefits side, HIH monitors will receive instant acknowledgement of message receipt when a call has been received and answered. Additionally, all units are powered by batteries that are charged by a mains AC power source. In this regard, they can remain functional during electrical interruptions.

Early simulation tests indicate that it is important to ensure units have a proper level of signal reception and that units are regularly charged.

Also, on some units whenever attempting to place a call, the user was prompted for a PIN. Although only a simple PIN code was necessary to unlock the calling features, this requirement was not documented.

Recommendation

37. That the PIN check feature be disabled or a PIN ID be included in a Standard Operating Procedure.

38. That ICT Guardians conduct regular checks to ensure signal reception levels are sufficient and, if necessary, external antennas be installed to correct any deficiencies.

39. That the DEWN CAP software be examined to determine how it can integrate text message alerting for the CDMA phones.

40. That the current CDMA service be upgraded to support 1XRTT to enable Internet connections. This would provide a third method of receiving alerts over the CDMA units – IPAS alert messages.

7.2 CAP General Observations

Presently, the LM-HWS project relies upon four different software interfaces to compose/upload, manage and send alert messages. Only two of these are CAP-compliant.

<u>Compatibility and consistency</u>

WS and DEWN CAP software interfaces have different looks and feels. Some fields are used differently. For example, The Message Type field for ARS lists the following:

- Personal Message
- Group Message
- BroadCast Message

whereas DEWN lists its Message types as:

- Alert
- Warning

Integration of all CAP interfaces

The CAP protocol chosen by the LM-HWS project is the most recently approved version by OASIS (Version 1.1). Unfortunately, it is not entirely compatible with the earlier 1.0 version preventing automatic importation of alert field data from version 1.0 sources. For example, NOAA is still using the older 1.0 version for dissemination of tsunami information bulletins.

On-line Access to CAP GUIs and Brokers

Presently, HIH depends exclusively upon its external Internet connection in order to connect to off-premise servers to compose and issue all of its text and audio recorded alerts. While one advantage of this setup is that the HIH does not have to manage the servers, these arrangements also make the HIH vulnerable in the event of loss of network connectivity.

A properly designed CAP broker residing on an HIH server could reduce this vulnerability and data entry for HIH Monitors. As originally envisioned in the LM-HWS project, the CAP broker program would provide an intermediary point of interconnection between the HIH and the relay network to facilitate interconnection of all ICTs and passage of CAP-compliant messages through a single software application. In this way, in the event of a connection failure to any individual alerting server, the broker would continue to pass alerts to the remaining functional systems.

Recommendations

41. That consideration be given to installing a CAP broker on a local server, rather than one outside the HIH, to ensure that if an external network link is lost to one of the alert components, the remaining ones will continue to be accessible.

    Another option is a client residing on a local HIH workstation that has many of the same server functions and that updates the database of an external server whenever a connection is restored. For example, this is a feature built into the Sahana software.

7.3 Alert Message Receipt and Acknowledgement

A fundamental requirement of a warning system is the ability to verify that an alert message has been properly sent to and received by a human operator at the receiving end, and that the message is properly authenticated so only a simple return acknowledgement is required.

Presently, there is no standardized means of acknowledging and authenticating LM-HWS alert messages. Some components possess two way response capabilities but are not yet configured for use in acknowledging receipts of messages, while others can acknowledge receipt to their servers, but their associated GUIs do not enable access to this data by HIH Monitors. In other cases, the component only provides a one way message capability, requiring ICT Guardians to use a second component to form acknowledgement.

Message authentication is a related issue as ICT Guardians and community first responders need to be able to distinguish between real and test messages, and that the content has been verified and pre-cleared by the Sarvodaya Executive. As such, the LM-HWS must demonstrate that it is secure, reliable and can be trusted.

In the absence of an integrated alert message receipt and verification process, the default process becomes a return contact with the HIH by ICT Guardians, usually in the form of a telephone call.

While this process may work for small scale tests and minor real events of limited alerting scope, it can create enormous challenges for HIH staff who must juggle their time between getting alerts out and responding to the feedback. Further, at certain times of the day or night the HIH may also have limited staffing capacity.

At the same time, it is important to have a system in place to be able to monitor confirmation of message receipt in order to identify alerting gaps. In some cases the devices may have malfunctioned and in other cases, recipients were not present at time of a receipt of an alert by their LM-HWS devices.

Recommendations

42. That HIH, in conjunction with Sarvodaya, establish an appropriate call centre to receive alert message acknowledgements and to field follow up enquiries.
43. That the call centre be staffed separately and not rely upon HIH Monitors.
44. That the call centre have a 24/7 capability.
45. That incoming hotline number(s) be private and restricted to authorized users.
46. That additional private hotline number(s) be made available to government and those other agencies and community groups that are likely to be providing advance notice of a hazard event, including local first responders.

7.4 HIH Setup

There are many potential options for enhancing the HIH facilities, which will be explored in more detail during the author's next visit. The following recommendations pertain only to more immediate enhancements based upon recent observations.

Recommendations

47. That at least one workstation should be devoted exclusively to the central monitoring and alerting functions and the workstation should be accessed only through a password protected user profile to enhance security and authentication.
48. That databases, pre-composed templates and sound files be developed and organized for quick access during alert events. ARS sound files be uploaded and placed in a quick access special directory on the WorldSpace audio gateway.
49. That a special LM-HWS home page be created and placed on each HIH workstation that has hyperlinks to all of the LM-HWS on-line log-in pages and appropriate external information sites as well as internal templates and pre-composed messages.

7.5 ICT Guardian setup

Visits to local communities revealed that all ICT Guardians were able to apply the training they had received, but could use some additional assistance in the form of advice and tips on basic setups, location of components, power considerations, etc.

Recommendations

50. That HIH develop some LM-HWS basic set up, operational and maintenance checklists and guidelines, and that they be distributed in all appropriate languages.
51. That HIH examine how LM-HWS components could be used to deliver regular updates to ICT Guardians – especially the ARS audio service.
52. That refresher and advanced user courses be considered.
53. That a TOT program for ICT Guardians be offered to encourage inter-community self-help.

7.6 Intra-community Communication

While beyond the current scope of the LM-HWS project, concern was voiced in community meetings about the need for improved capacity to warn residents once alerts were received by ICT Guardians, and to have a reliable intra-community communication system to coordinate subsequent activities of community first responders.

Recommendation

54. That to Phase Two of the LM-HWS project be added a new module that would include community-based emergency communications planning, incorporating a needs assessment based upon community emergency plan concepts of operation, an inventory of communication means, capacity and vulnerability assessment and gap analysis along with planning and operational training.

A ‘tool kit’ guide to local warning methods prepared by the author for British Columbia, Canada, rural and remote communities might serve as a useful starting point.

7.7 LM-HWS ICT Maintenance

To ensure that LM-HWS components remain functional, regular inspections and tests need to be conducted as well as provision for replacement of defective units and limited-life parts, such as batteries.

Recommendation

55. That a set of operating manuals be prepared for basic and advanced users of each LM-HWS component. The basic user guide would be a “quick start” guide and the advanced guide would contain additional instructions in basic configuration, testing and troubleshooting.
56. That consideration be given to decentralizing maintenance and trouble shooting to the district or provincial levels, with centralized oversight via the HIH, such as facilitating repairs and inventory control.

8. Other Considerations

Due to the limited duration of the author’s first visit, it was not possible to examine all associated areas of the project. The following list is offered as a preliminary identification of some of the other key topic areas requiring further assessment, and which will be addressed during a planned return visit in early 2007.

Terminology

- Standard definitions (e.g., alarm, warning, events of interest)
- Simulation/exercise
- Glossary that is posted
- Types of messages

Continuity Planning

- Backup of software, configurations and databases (copies on and off-site)
- Backup site in event DMC cannot be used or loses basic support functions (power, telecommunications, etc.)
- Alternate access to external servers
- Proper documentation and manuals
- Physical and electronic security arrangements
- Standard operating procedures
- Availability of technical and operating staff for restoration
- Insurance/replacement arrangements

Security

Electronic

- Password protection (type and control – e.g., forced password conventions and changes
- ftp vs. secure ftp file transfers
- https and ssh logins
- authenticating concurrent logins of systems (verifying who is logged in)
- protection of confidential information

Physical

- maintaining proper inventories
- access to HIH
- physical protection of computers (e.g. locked down)

Standard Operating Procedures and Checklists

- HIH
- ICT Guardians
- Set up
- Testing
- Trouble shooting
- Maintenance
- Logs

Best Practices Guidelines

- Simulations
- Planning
- Message composition both at HIH and village levels

Certification and Training of HIH Monitors and ICT Guardians

- Introductory, intermediate, advanced
- Recognition/rewards
- Managing volunteer turnover

HIH Enhancements

- Equipment ergonomics
- Server capacity
- Network redundancy and diversity
- Power supplies
- Ensuring 24/7 support
- HIH – ICT Guardian help desk
- Automated telephone notification for fixed and mobile

ICT Guardian/First Responder Enhancements

- Equipment ergonomics
- Power supplies
- Intra-village alerting and communication
- Inter-village communication
- Emergency communication planning
- Evacuation safe area and reception centre communication

Other Activities for Follow Up Visit

- Analysis of simulation evaluation data
- Applying lessons learned
- Cross check with other ICTs not tested (e.g., facsimile, VoIP, IXRTT, GPRS)
- Integration of HIH within Sarvodaya Community Disaster Risk Management Center
- HIH organization and management enhancements
- Scaling of project to include additional sites
- Outreach and promotion