© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Intelligent Gaurds against Disaster Prepared Smart Environment using MSP430 Microcontroller

Karthikeyan S*1, Dr. N. Kumaresan2

[1]Department of Electronics and Communication Engineering, Kongu Polytechnic College, Perundurai, Erode, Tamilnadu, India
[2]Department of Electronics and Communication Engineering, Regional Centre of Anna University, Coimbatore, India.

ABSTRACT

Recent years have tremendous advances in information and communication technologies (ICT) implied in infrastructures for disaster management. Sensor networks and web services interoperable provides alert and warning systems at emergencies. Even though people in technically advanced regions remains ill prepared.

The broader spectrum of devices and services makes smart and intelligent environment provides comfort and convenience, safety from intruders, and enhancing our environment for disaster preparedness. The standard-based cyber physical devices are the application system that help to minimize loss of lives and damage to property and enables social connectivity but little or nothing to help us to improve our readiness against killer tornados, major earthquakes, and landslides, floods and so on. Such devices and systems performing predict, detect & alert delivering capabilities.

Keywords: In-situ Monitoring, M2M, Information Communication Technologies, Common Alert Protocol, standard-based cyber physical devices

I. INTRODUCTION

The system Intelligent Gaurds Against Disaster (GaDs) is a cyber-physical Elements[1] of disaster refers to embedded systems, designed to prevent economic hazardous, decrease or minimizing injuries and death and applications that receive, authenticate and process standard-conforming disaster warning messages[2] and respond by taking appropriate actions to enhance our preparedness for disasters. Hereafter, for sake of concreteness, we assume in subsequent discussions that alert messages conform to the CAP standard and sometimes call iGaDs CAP-aware devices [3]. We will use the terms messages, alerts and data interchangeable when there is no confusion. They are designed to respond to warnings of imminent strong earthquakes.

In comparison, technologies to take advantage of machine readable and authenticable alert messages remain immature. Smart and intelligent homes and environments now offer us devices, applications and services for our comfort, convenience, and social connectivity, but nothing to help us prevent loss of lives, reduce chance of injuries and minimize property damages and economical losses when disasters strike [4]. This fact motivated us to propose the pervasive use of iGaDs (intelligent Guards against Disasters) as elements of future disaster prepared smart home and environment.

Objective of Work

In addition to disaster management ICT (Information and Communication Technologies) infrastructures and tools, we also have witnessed great advances in the development and 3 deployments of technologies for the predication and detection of killer storms, earthquakes, debris flows, tsunamis, and so on.

Advanced weather radars and warning decision support systems enables accurate predictions of paths and severities of tornados and hence deliveries of warnings tens of minutes in advance. In developed countries frequented by strong earthquakes (e.g., Taiwan, Japan and parts of USA and Mexico)[1], densely deployed broadband arrays of seismometers and strong seismic motion sensors are networked with computers running advanced auto-location and focal mechanism determination tools. Systems built on such networks of things can deliver early warnings R. Murphy et al.,[8] of earthquakes within seconds after their occurrences, providing receivers of warnings as said by Moore L K et al.,[5] seconds or more before shock waves arrive and ground motion starts.

II. METHODS AND MATERIAL

Literature Survey

A. OSIRIS

In EU, OSIRIS (Open architecture for Smart and Interoperable networks in Risk management based on In-situ Sensors, Providing the necessary technologies that will adapt sensors & network configuration in order to meet final users' needs and getting "In-situ Monitoring sensor web".

The above project Osiris collects the information from sensors such as gas analyser, humidity sensors, temperature sensors and noise sensors and transmits to the server Real-Time Communication Link from the OBUsto the interface control enter and it communicates.

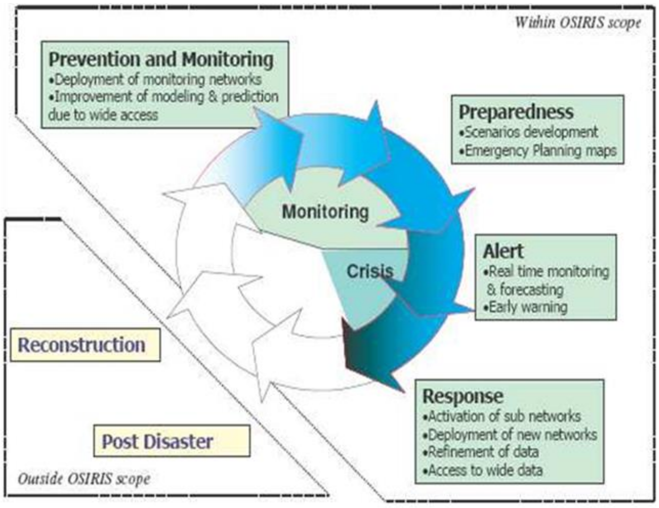

Figure 1: In-Situ Monitoring Enchantment

Since the project Osiris developed as complex device it employed for information collection and information center, further the following drawbacks are

- Limited number of mobile stations(Less sensors are installed)in the sensor web`
- Since the message follows the fixed route path to reach the interface control center, so Study of routes of available mobile units in order to produce a model maximizing the spatial coverage of the network while keeping at the minimum the numbers of unit required.
- Complexity increases as the sensor increases and also the wiring required joining all the elements on board.

B. SANY

The SANY (Sensors Anywhere) project focuses on interoperability of in-situ sensors and sensor networks. It provides quick and efficient way to reuse data and services from currently incompatible sensors and data sources in future environmental risk management applications.

M. Klopfer and I. Simons et al., [3] focuses on interoperability of in-situ sensors and sensor networks, SANY IP is actively required to build an active dialogue with end users of environmental data, service providers and service developers interested in the abilities of the SANY technology. Currently, the Consortium is particularly interested in collecting the concerns. In particular, SANY IP is interested in additional use cases that illustrate the advantages of self con-figuration, rapid deployment and advanced data fusion, as well as all use cases involving combinations of moving, roving, high altitude and EO sensors.

- Cross checking of requirements with developers and service providers of environmental sensor networks, as well as with end users of environmental data.
- As said above SANY concentrates on interoperability of sensors and networks, but not in real-time conveyance of messages between server and to end users.

C. MiRE (Minimal Rule Engine)

Choi C, et al., [4] presented Context-aware services in cellular phones, manages and rule process the key research issues for the resource-limited devices to have context-aware capability, This rule processing engine, called MiRE (Minimal Rule Engine). Implements the minimum cores of the conventional rule for processing facilities and some special policies to achieve resource-saving and light-weight inference engine suitable for resource-limited mobile devices. MiRE, as a part of context-aware middleware system, provides a flexible architecture to adopt various context-aware applications while rules and contexts are dynamically registered at run-time. It maintains the amount of context (i.e., facts) and rules to be optimal in order to save computing resources and processing time. Its design strategy allows MiRE to be conveniently equipped into resource-limited context-aware mobile devices. The performance is limited on a context-aware cellular phone shows the intended efficiency to be achieved.

D. M2M Applications

M2M applications such as Wired Smart Home Wired Smart Home in the scope of energy metering, security, and emergency communications.

N. L. Griffin and F. D. Lewis et al., [5] divided the M2M system into three main domains: M2M Device, Network, and Application Domain and includes the following key elements: M2M Device. M2M Area Network.A network providing connectivity between M2M Devices, M2M Gateways and M2M Applications (servers).

M2M Application (Server). This is the middleware layer where data goes through the various application services and is used by the specific business processing engines. M2M node device capable of replying to requests for data contained within those devices or capable of transmitting data contained within those devices autonomously.

E. Emergency Data Exchange Language (EDXL) Distribution Element (DE)

Together with EDXL-DE, the alert message standard CAP supports message exchanges between emergency information systems and public safety organizations [6]. More importantly for our discussions here, CAP enables automatic reports by sensor systems to analysis centers, aggregation and correlation of warnings from multiple sources and automatic processing of alert messages by smart devices and applications.

This service provides the exchange of messages in multiple formats to include:

- Hospital Availability Exchange (HAVE)
- Resource Messaging (in development)
- Sit Rep (in development)

If you offer a commercial product or are building a custom application that needs to communicate with other applications to share basic alerts (CAP) or complicated emergency file structures (EDXL-DE), DM-OPEN offers a “write once, use many” interface that uses recognized international standards. If you wish to offer your customers a way to direct connect to the National Weather service for the purpose of broadcasting non-weather emergency messages on NOAA radio, DM-OPEN is the place.

Common Alerting Protocol (CAP)

Moore L K et al., [7] suggested the Common Alerting Protocol (CAP) in a digital format for exchanging emergency alerts that will allow a consistent alert message to be disseminated simultaneously over many different communications systems. FEMA has worked with the Organization for the Advancement of Structured Information Standards (OASIS) to develop the IPAWS standard.

This service provides for the exchange of alerts between responder organizations and for the dissemination of IPAWS Profile alerts to designated IPAWS[20] gateways including Emergency Alert System (EAS), Cellular Mobile Alerting System (CMAS), National Weather Service Radio.

The Emergency Alert System (Eas)

The Emergency Alert System (EAS) is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers, and direct broadcast satellite (DBS) providers to provide the communications capability [20] to the President to address the American public during a national emergency. The system also may be used by state and local authorities to deliver important emergency information.

FEMA Integrated Public Alert and Warning System – Open Platform for Emergency Networks (IPAWS-OPEN)

DMIS is now superseded by IPAWS-OPEN (Integrated Public Alert and Warning System – Open Platform for Emergency Networks) CAP (Common Alert Protocol) and EDXL-DE (Emergency Data Exchange Language Distribution Element

IPAWS-OPEN [20] is a non-proprietary operational interoperability backbone that acts as a “level playing field” to allow disparate third-party applications, systems, networks and devices to share information in non-proprietary, open, standards based format. As Federal infrastructure, IPAWS-OPEN is designed to support the delivery of real-time public alerts and other emergency and situational awareness data to the public and to emergency responders in the field, at operation centers, and across all levels of response management. IPAWS-OPEN serves as test bed to facilitate the development of open non- proprietary standards to support interoperable information sharing for the emergency responder community.

Concept of Cyber-Physical Element

The cyber physical elements such as intelligent Guards against Disasters designed to process and respond to alert and warning messages from responsible authorities and it helps in early readiness to Disaster, These systems collects the signal from various networked sensors(test environment), After conditioning those received signal it transfers to specified authorities to make decision over the received signal.

The respective authorities process it by comparing with standard norms and procedures it will make decision and transfers the messages as conforming to CAP protocol through IPAWS-open and also by GSM that would enable to reach long distance. R.R. Rao, J. Eisenberg, and T. Schmitt et al., [11] The iGaDs could also receive message as a CAP from alerting authorities and it process to authenticate and route the standards based message to Systems through Emergency Information system.

This project advocates the development and pervasive deployment of cyber-physical devices, systems, services and applications designed to take advantage of the current and future disaster predication and detection capabilities T. Sakaki, et al[15] and standard-based alert/warning delivery systems for the purpose of enhancing our preparedness for disasters. When there is no need to be specific, we refer to such devices/systems/services/applications as intelligent Guards against Disasters, or iGaDs for short. Specifically, each iGaD can authenticate and process standard-conforming disaster warning messages and respond by taking appropriate actions. For sake of concreteness, for the most part of this paper, we assume that alert/warning messages conform to the latest version of Common Alert Protocol [24], and will highlight the capability of an iGaD to respond to CAP messages by saying that it is CAP-aware.

As examples of iGaD, when warned by alert messages of earthquakes of a specified strength or stronger, a smart valve shuts down natural gas flow into a condo building to prevent fire and an automatic door controller opens the building doors to ease evacuation. Elevator controllers stop elevators when they reach the closest floor. An application component of the smart environment in hospitals tells surgeons to pause on-going operations, or in supermarkets informs shoppers of relatively safe aisles to be during the quake and so on. As the iGaD part of an on-board vehicular safety system, an earthquake alert device warns the driver of the imminent strong earthquake and may even turn on the hazard flashers, disengages the cruise control or helps the driver to slow down. Smart variable message signs before tunnels and bridges on highways may tell the drivers to slowdown and pull over.

A Message Delivering Capability

This project describes architecture and middleware fora system of intelligent Guards against Disasters, called iGaDs for short. iGaDs are smart devices and applications that can receive, authenticate and process standard- conforming disaster alert messages from authorized senders and respond by taking appropriate actions to help us to be better prepared for nature disasters. They are designed to be used ubiquitously as elements of future disaster-prepared smart homes and environments. The prototype prioritized asynchronous A. Almer,et al [19] alert message delivery service described here is built by using a data bridge to connect Qpid and PubSubHubbub as a way to push alert messages to a large system of iGaDs via GSM.

These examples motivated us to use a light-weight rule engine to provide all iGaDs with decision support. Figure 2 shows how the rule engine and the CAP message processor fit together with other components in a general structure of all embedded iGaDs. Solid arrows represent information flow among the components. A software iGaD does not have a device controller; a CAP-aware application takes its place.

B. Emergency Alert System (EAS)

The Emergency Alert System (EAS) is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers, and direct broadcast satellite (DBS) providers to provide the communications capability to the President to address the public during a national emergency. The system also may be used by state and local authorities to deliver important emergency information, such as AMBER alerts and weather information targeted to specific areas.

The FCC, in conjunction with Federal Emergency Management Agency (FEMA) and the National Oceanic and Atmospheric Administration's National Weather Service (NWS), implements the EAS at the federal level. The President has sole responsibility for determining when the EAS will be activated at the national level, and has delegated this authority to the director of FEMA. FEMA is responsible for implementation of the national-level activation of the EAS, tests, and exercises. The NWS develops emergency weather information to alert the public about imminent dangerous weather conditions.

The FCC's role includes prescribing rules that establish technical standards for the EAS, procedures for EAS participants to follow in the event The EAS is activated, and EAS testing protocols. Additionally, the FCC ensures that the EAS state and local plans developed by industry conform to FCC EAS rules and regulations.

C. CAP Protocol

The CAP message processor is essentially the same for all iGaDs. It is responsible for extracting from each alert message the information needed by the iGaD device controller (or application) to decide whether and how to respond: The information extracted and includes the name and scale of the alert event type and severity of the event, as well as specifications of areas affected by the alert. The message may also provide resources such as human-readable descriptions and URLs of files containing supplement information (e.g., photos, maps, audio, and so on) that may be useful to the public EAS and some iGaDs.

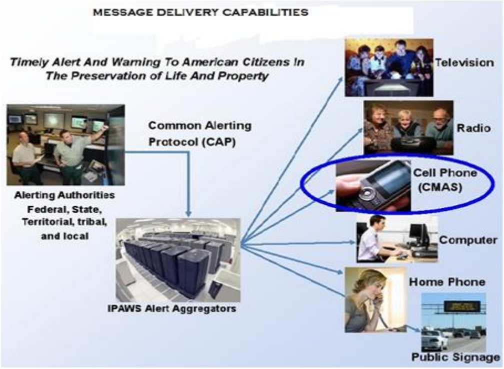
MESSAGE DELIVERY CAPABILITIES
Timely Alert And Warning To American Citizens In The Preservation of Life And Property
Common Alerting Protocol (CAP)
Alerting Authorities Federal, State, Territorial, tribal, and local
IPAWS Alert Aggregators
Television
Radio
Cell Phone (CMAS)
Computer
Home Phone
Public Signage

Figure 2 : Pictorial representation of Message Delivery Capabilities

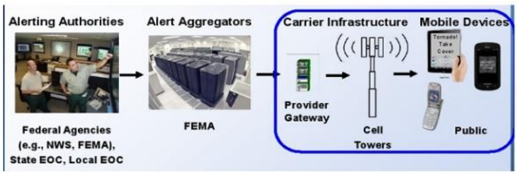

Figure 3 : Pictorial Representation of Commercial Mobile

D. EMS (Enhanced Messaging Service)

Besides the data size limitation, SMS has another major drawback -- an SMS message cannot include rich-media content such as pictures, animations and melodies. EMS (Enhanced Messaging Service) was developed in response to this. It is an application-level extension of SMS [21]-[22]. An EMS message can include pictures, animations and melodies. Also, the formatting of the text inside an EMS message is changeable. For example, the message sender can specify whether the text in an EMS message should be displayed in bold or italic, with a large font or a small font.

The drawback of EMS is that it is less widely supported than SMS on wireless devices. Also, many EMS-enabled wireless devices only support a subset of the features defined in the EMS specification. A certain EMS feature may be supported on one wireless device but not on the other.

CONNECT TO CONTROLLER

In general, there are two ways to send SMS messages from a computer / PC to a mobile phone:

1. Connect a mobile phone or GSM/GPRS modem to a computer / PC. Then use the computer / PC and AT commands to instruct the mobile phone or GSM/GPRS modem to send SMS messages.
2. Connect the computer / PC to the SMS center (SMSC) or SMS gateway of a wireless carrier or SMS service provider. Then send SMS messages using a protocol / interface supported by the SMSC or SMS gateway.

If you do not want to develop SMS software or applications but just want to use your computer / PC to send text messages.

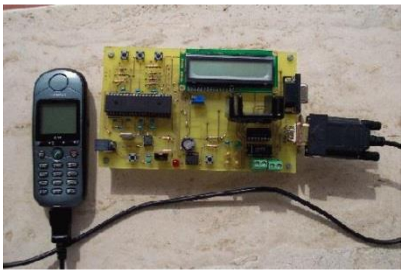

Figure 4 : Interface Module of GSM Kit

E. Interfacing with MSP430 Installation

The MSP-EXP430G2 LaunchPad installation consists of three easy steps:

1. Download the required software.
2. Install the selected IDE.
3. Connect the LaunchPad to the PC.

Then the LaunchPad is readily availabled with the pre-programmed demo application.

Develop an Application With the MSP-EXP430G2 LaunchPad

The integrated development environments (IDEs) shown in Section 2 offer support for the whole MSP430G2xx Value Line. The MSP-EXP430G2 LaunchPad needs only a connection to the USB of the Host PC— there is no external hardware required. The power supply and the Spy-Bi-Wire JTAG signals TEST and RST must be connected with jumper J3 to allow the onboard emulation connection to the device, as shown. Now the preferred device can be plugged into the DIP target socket of the Launch Pad. Both PDIP14 and PDIP20 devices of the MSP430G2xx Value Line and the MSP430F20xx family can be inserted into the DIP socket aligned to pin 1. A complete list of supported devices can be found.

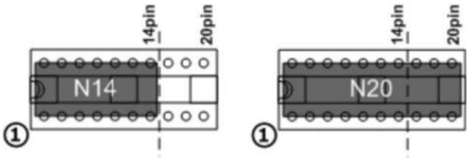

Figure 5 : Insert Devices into Target Socket

As the assignment of jumper J3 has been changed in MSP-EXP430G2 revision 1.5, following are comments in Table to find the assignment for a specific board revision.

Jumpers 4 and 5 connect the UART interface of the emulator to the target device pins P1.1 and P1.2. The direction of the UART signal lines can be selected by the orientation of the attached jumpers. In horizontal orientation, the jumpers connect TXD to P1.1 and RXD to P1.2, as they are used for the software UART communication on the demo application. In vertical orientation, the jumpers connect the TXD signal to P1.2 and the RXD signal to P1.1, as required for the MSP430G2553 USCI.

Program Connected eZ430 Target Boards

The MSP-EXP430G2 LaunchPad can program the eZ430-RF2500T target boards, the eZ430-Chronos watch module, or the eZ430-F2012T/F2013T. To connect one of the ez430 targets, connector J4 must be populated with a 0.050-in (1.27-mm) pitch male header.

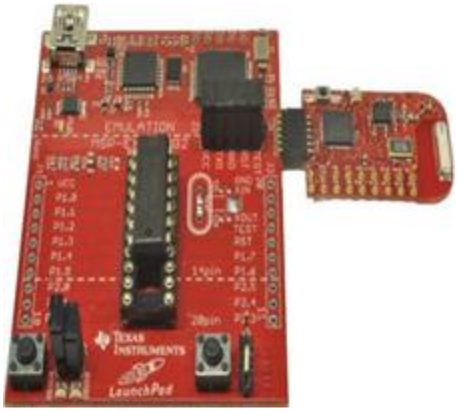

Figure 6 : MSP-EXP430G2 LaunchPad with Attached eZ430-RF2500 Target Board

To program the attached target without interfering with the LaunchPad socket board, jumper connections TEST and RST of J3 must be open. The interface to the eZ430 target board is always connected to the MSP-EXP430G2 emulator, so the programming and debugging of a connected LaunchPad target device is possible only if the eZ430 target is not connected on the same time. The application UART, on the other hand, is connected directly to the LaunchPad target device, and jumper J3 can be closed to monitor the transmission from the LaunchPad target to the attached eZ430. This way both possible connections, from the device to the PC and from the device to the eZ430, can be established without changing the direction of the UART pins.

The VCC connection to the eZ430 interface is directly connected to the LaunchPad target VCC and can be separated with jumper J3, if the LaunchPad itself should be powered via a connected battery on J4. To supply the eZ430 interface with the on-board emulator the jumper J3 VCC needs to be closed. Table 2 shows the pinout of the eZ430 debugging interface J4, the first pin is the left pin located on the emulator part of the LaunchPad.

III. RESULTS AND DISCUSSION

Implementation

It is evident from these scenarios that different types of iGaDs differ significantly in function and that iGaDs of the same type can take widely different actions. Nevertheless, they share many characteristics, including their architec-ture and key components.

Each embedded iGaD has a CAP message processor and a device controller. The proces-sor extracts from each alert message the event's type and severity as well as one or more geographical polygons or circles specifying the boundaries of affected areas. Some-times, alerts also contain pointers to resources, such as audio and video files, to assist the iGaD in performing its actions. Based on this information, as well as device location and sensor data from local sources, the device controller determines whether and how to respond. The controller also interfaces with one or more physical devices, such as a shelter door or search light[23]-[29]. A non-embedded iGaD does not have a device interface; in its place, one or more disaster management applications run on some platforms.

A CAP-aware building management and security system could control the building's battery- or solar-powered devices such as a smart natural-gas valve. It also could broadcast audio and video warning messages (contained in alert elements) on public speakers and video displays in the building.

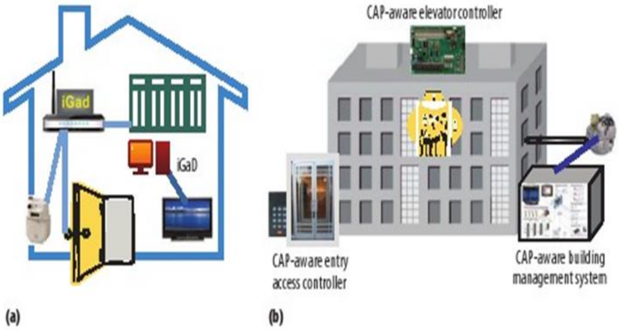
iGaD
iGaD
CAP-aware elevator controller
CAP-aware entry access controller
CAP-aware building management system
(a)
(b)

Figure 7 : Intelligent Guards against Disasters (iGaDs) in smart environments in home (a) or business (b)

Results

Thus the devices were employed in applications automatically validate and process alerts. Their CAP message processors are identical. Each alert element has an enveloped digital signature that lets the processor authenticate the message. An iGaD might be in service for years, and changes over time are inevitable, including key updates. These device reliably validate all alert messages intended for it during and after each key update process.

After the processor authenticates an alert, the validator extracts relevant information. A typical alert element is an one to a few thousand characters Cell phones, PDAs, computers, and other devices can extract the information in an alert within a second or two, using one of the lightweight validator now available on popular platforms. In addition, hardware validator has begun to emerge that offer a suitable option for iGaDs.

Hardware Module Images

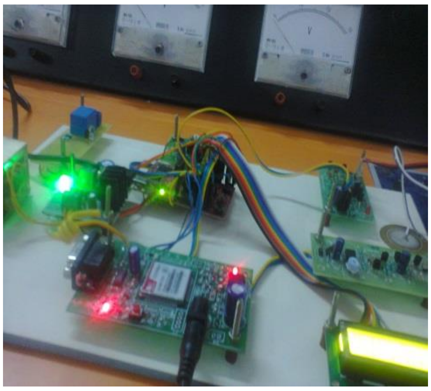

Figure 8: Hardware Module

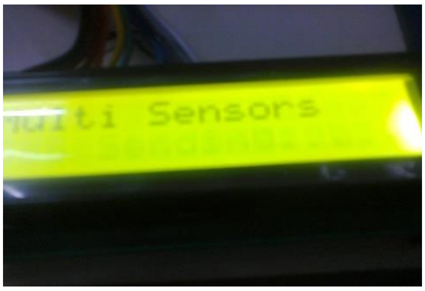

Figure 9: Output

IV. CONCLUSION

Systems with CAP-aware sensors also could be used to trigger safety measures in nuclear power plants, rail and subway trains, and fab-rication lines. For example, typical safety measures in power plants start auto-matic shutdown when local sensors detect ground vibra-tions exceeding the limits accounted for in the plant’s design. This happened at nuclear power plants in Virginia.

A better alternative is to cover the region with an earthquake early warning system and make the safety equipment CA P-awa re. The equipment could then respond to early alerts of strong earthquakes, starting shutdown sequences before local ground vibration begins, thus minimizing damage.

V. FUTURE WORK

It is easy to envision the potential benefits realizable by deploying a broad spectrum of iGaDs throughout future living environments. Pervasive use of iGaDs offers a gigantic new market for smart-device manufacturers and application developers. While these devices offer new opportunities to industries that install, upgrade, and service them, they also create new responsibilities for oversight agencies and organizations. Making iGaDs ubiquitous and as commonly used as cell phones, GPS devices, social media applications, smart appliances, and so on presents numerous challenges.

VI. REFERENCES

[1] Coulter and Phillips T, "New GOES-R to Give More Tornado Warning Time," SJAA Ephemeris,; ephemeris.sjaa.net/1108/d.html. Aug. 2010

[2] Chee E C, Mohd-Yasin E, and Mustaph A K, "RBStrex: Hardware XML Parser for Embedded Systems," Proc. Int’ lConf. Internet Technology and Secure Transactions (ITTST09), IEEE, 2009, pp. 1-6.

[3] M. Klopfer and I.Simons, "SANY - an open service architecture for sensor networks", edited http://sany-ip.eu/publications/3317, 2009.

[4] Choi C, et al., "A Minimal Rule Engine for Context-Aware Mobile Devices," Proc. 3rd Int’l Conf. Digital InformationManagement (DIM 08) IEEE, 2008, pp. 172-177.

[5] N. L. Griffin and F. D. Lewis, "A rule-based inference engine which is optimal and VLSI Implementable," Technical Report, Department of Computer Science. University of Kentucky, 1989.

[6] EDXL-DE: Emergency Data Exchange Language Distribution Element, V1.0, http://www.oasis-open.org/committees/download.php/17227/EDXL-DE_Spec_v1.0.html

[7] Moore L K, "The Emergency Alert System (EAS) and All Hazard Warnings" Congressional Research Service, www.fas.org/sgp/crs/home-sec/RL32527.pdf. Dec 2010; tech. report 7-5700.

[8] Murthy K, "Without Basements, Joplin Had Scant Refuge from Tornado", www.reuters.com/article/2011/05/31/ us-tornado-basements-idUSTRE74U6HT20110531. Reuters News, 31 May 2011

[9] Shinetal T C., "Strong Motion Instrumentation Programs in Taiwan," Handbook of Earthquake and Engineering Seismology, Lee W H K, Kanamori H, and Jennings P C, eds., Academic Press, 2003.

[10] R. Murphy, "A national initiative in emergency informatics," Computing Community Consortium, November 2010.

[11] R.R. Rao, J. Eisenberg, and T. Schmitt, Ed "Improving Disaster Management: Role of IT in Mitigation, Preparedness, Response and Relieve", National Academic Press, 2007.

[12] "Harnessing information and technology for disaster management," The Global Disaster Information Network, Disaster Information Task Force Report, 1993.

[13] UN, Global Disaster Alert and Coordination System, http://www.gdacs.org/about.asp

[14] InSTEDDGeoChat: a unified mobile communications service, MESH4X: an adaptive data integration platform, RIFF, an interactive decision support environment, http://www.instedd.org/technology_overview

[15] T. Sakaki, et al, "Earthquake shakes twitter users: real-time event detection by social sensors," Proceedings of the 19th international ACM conference on WWW, 2010.

[16] S. Vieweg, et al, "Microblogging during two natural hazards events: what twitter may contribute to situational awareness," Proceedings of the 28th international ACM Conferenceon Human factors in Computing Systems, 2010

[17] A. Almer, et al, "Information services to support disaster and risk management in alpine areas," in Taking Geoinformation Science One Step Further, The European Information Society, Lecture Notes in Geoinformation and Cartography, Springer, 2008.

[18] "Sensor Net: Nationwide detection of chemical, biological, radiological, nuclear and explosive threats", http://computing.ornl.gov/cse_home/datasystems/sensornet.pdf, also "SensorNet" by J. Strand, http://www.ittc.ku.edu/workshops/sensornet/john_strand.pdf 2004

[19] "Introduction to Disaster Management Inoperability Services," http://www.cemaonline.org/DMIS/dmisCT.htm#About DMIS Web Service Release 2.3,

[20] FEMA, Integrated Public Alert and Warning System (IPAWS),

[21] T. C. Shin, W. H. K. Lee, H. Kanamori and P. C. Jennings, Ed et al., "Strong motion instrumentation programs in Taiwan," in Handbook ofEarthquake and Engineering Seismology", and BATS (Broadband Array in Taiwan for Seismology), http://bats.earth.sinica.edu.tw Academic Press, 2003

[22] G. P. Hayes, L. Rivera, and H. Kanamori, "Source inversion of the W-Phase: real-time implementation and extension to low magnitudes," Bull. Seism. Soc. Am., 80, 2009.

[23] "Digital signatures," http://capan.ca/cap-cp/reference/?page_id=579 and "Applying XML-signature to CAP-XML," http://capan.ca/cap-cp/reference/?page_id=1024

[24] N. C. Hsiao, et al., "Development of earthquake early warning system in Taiwan," Geophys.Research Letters, 36, 2009.

[25] "Smart networked objects and Internet of things." a white paper of Instituts-Carnot,

[26] E. T.-H. Chu, Y.-L. Chen, J. W. S. Liu and J. K. Zao, "Strategies for crowdsourcing for disaster situation information," WIT Transactions on the Built Environment, 2011.

[27] J. Ferrell, "Crowdsourcing snowstorm's westward model shift," The WeatherMatrix Blog, December 11, 2011

[28] The Geo SMS standard, http://geosms.wordpress.com/the-geosms-standard/

[29] D. Davidrajuh, "Array-based logic for realizing inference engine in mobile applications," International Journal of Mobile Learning and Organization, Vol. 1, 2007