AziSA: An Architecture for Underground Measurement and Control Networks

R Stewart, S J Donovan, J Haarhoff and D Vogt*

CSIR NRE Mining
P O Box 91230, Auckland Park, 2006, Johannesburg, South Africa
Email: sjdonova@csir.co.za

ABSTRACT

AziSA is an architecture for measurement and control networks that can be used to collect, store and facilitate the analysis of data from challenging underground environments. AziSA defines four node classes, two (Classes Four and Three) for interacting with the physical environment and two (Classes Two and One) for managing the system itself. Each class must support a minimum message set that enables the required functionality of the network.

AziSA is intended primarily for use in underground mining environments where there is limited power and communications infrastructure. One of the major design goals of AziSA is the capability to have sensors and actuators that are cost-effective, use very little power, and are suitable for use underground. Typically, the communication between these nodes would also be wireless. AziSA was created because the existing identified protocols could not offer an organized and open architecture for low-power, low-cost, wireless systems.

1. INTRODUCTION

Labor-intensive drill-and-blast mining, as conducted on the major South African gold and platinum mines, is often not tightly managed due to the lack of good information about what is going on underground.

Better real-time management can occur only once three conditions have been met.

1. Parameters to be managed have to be measured.
2. Measurements have to be communicated sufficiently quickly to affect the parameters being managed.
3. Measurements have to be processed into a sufficiently useful form to provide support for decision making.

These conditions can be fulfilled more effectively, if an agreed architecture is put in place to facilitate communication and decision making. The architecture that has been developed at the CSIR is called AziSA, an isiZulu word meaning "to inform". In this paper, the AziSA architecture is described.

2. THE AziSA ARCHITECTURE

AziSA is a specification for an open measurement and control network architecture that will facilitate decision making. AziSA is intended primarily to give rise to systems for use in underground mining environments in which there is limited power and communications infrastructure. As a by-product, the AziSA architecture will also enable a communications infrastructure that covers all places where people are working.

It is envisaged that AziSA will be adoptable as an open standard. As such, it references existing open standards, chaining them together to form the various stages of a network, and only adding to the standards when desired functionality cannot be obtained from an existing standard. AziSA was created because the existing identified protocols could not on their own provide what was required: support for low cost, low power and wireless, as well as organization and openness.

The ultimate goal is an open system in which AziSA-compliant sensors can add themselves to a network with the minimum of human intervention, through a process of self advertisement. The relevant standard in this regard is IEEE 1451, which provides for sensor metadata in the form of Transducer Electronic Data Sheets (TEDS). In this paper, a sensor refers to a sensing platform, a node on the network which can communicate with other nodes, to which are attached detectors (or transducers, used interchangeably), each of which measures an aspect of the surrounding environment.

In addition to accurate measurements with adequate precision, data integrity requires that both the time and the location of each measurement are known. In order to preserve data integrity, each sensor must thus exhibit a minimum functionality. Sensors are required to be able to identify themselves and make their presence known to the network, send data to an aggregator and respond to instructions from the aggregator (e.g. to change a detector's sampling rate), perform a health check and detect if they have been tampered with. It must be known what kind of sensor it is and where the sensor is positioned, even if the sensor cannot store this information itself (in which case, this information becomes the responsibility of the parent aggregator).

A system developed from the AziSA architecture must be robust, since it is required to continue monitoring potentially hazardous conditions and provide for in-mine communications even if the link with the outside world is disrupted. This requirement for robustness implies that processing in the system must be distributed and not totally dependent on central coordination. Decisions should be made as close to the source of data as possible so that local alarms can be raised without the need to consult the central controller. However, the low-power requirement restricts the processing power available at the sensors. This apparent contradiction can be resolved by a tiered architecture in which the sensor sub-networks are coordinated by local intelligent gateway devices, which aggregate the data and alert streams and pass them on to the central controller, while passing instructions back to the network.

*Corresponding author

2.1. AziSA device classes

There are four AziSA device classes. Each device class is defined by the functionality that it must be able to exhibit in order to enable the required functionality of the system as a whole. This functionality must support the unit of communication comprising a message, which can be of three basic types: queries and their responses, commands and their confirmations, and notifications (data and alerts). Messages that have been defined include the following:

- Getting device identification and capabilities, for detector discovery;
- Setting and getting device time, for synchronization;
- Setting and getting sampling rates for detectors;
- Setting alert conditions;
- Getting data and alerts.

The four device classes naturally fall into two groups:

1. Measurement nodes, which can be simple devices which are not expected to do anything computationally intensive (Classes Four and Three);
2. Management nodes, which will typically need more computing power and which will be required to buffer data and perform some preliminary data analysis (Classes Two and One).

2.1.1. Class Four devices

Class Four devices produce local data measurements. A Class Four device will typically be a low-power battery-operated device transmitting data from a few detector transducers over a wireless network. It will measure at least one quantity at regular time intervals and send the result to a Class Two parent device. It is required to respond to commands, at a minimum providing information about itself, its detectors and their positions, and providing data on request. It may implement a simple scheme such as sending only samples that have changed by more than a given tolerance or after a maximum time period has passed; if so, it must respond to commands to change the tolerance and time period. It may have a real-time clock; otherwise the Class Two parent device must provide reliable time-stamping.

2.1.2. Class Three devices

Class Three devices also produce local measurements as well as making local decisions. In addition to the Class Four functionality, a Class Three device must be able to raise alerts based on its own data and continue monitoring this data and logging the alert information even if communication with the Class Two parent device has been interrupted. It is required to have a clock deemed sufficiently accurate for this purpose. It must be possible to reset the clock remotely and to examine the contents of the log. The Class Three device may buffer data during disconnected periods and it may raise a visible or audible alarm if unable to notify its controller; if so, this behavior must be remotely configurable.

2.1.3. Class Two devices

Class Two devices each coordinate a sub-network of Class Three and Four devices, aggregate the data produced by those devices for transmission to a Class One device (caching the data in the event of any communication disruptions) and make autonomous decisions based on the data available to them, raising alerts as required. They translate between different communication protocols as necessary.

2.1.4. Class One devices

Class One devices occupy a central locus of control for the network (via the Class Two devices) and are responsible for data storage. They also facilitate decision support by allowing client applications to subscribe to all or part of the data stream. They are responsible for routing received alerts to responsible parties, and may present data and information through various standard interfaces, such as web services.

2.2. AziSA topology

The diagram in Figure 1 shows an example of what the topology of an AziSA-compliant network might look like. A Class Two device on the network serves as a local management node for Class Four and Class Three devices, which cannot communicate amongst themselves (although they might be connected to one another through a mesh network). Multiple Class Three and Class Four devices can consider a single Class Two device as being their parent. All the Class Two devices on a network report to a Class One device which would typically be located on surface. Class Two devices can also form peer relationships with one another if one Class Two deems it necessary to view incoming data on another Class Two.

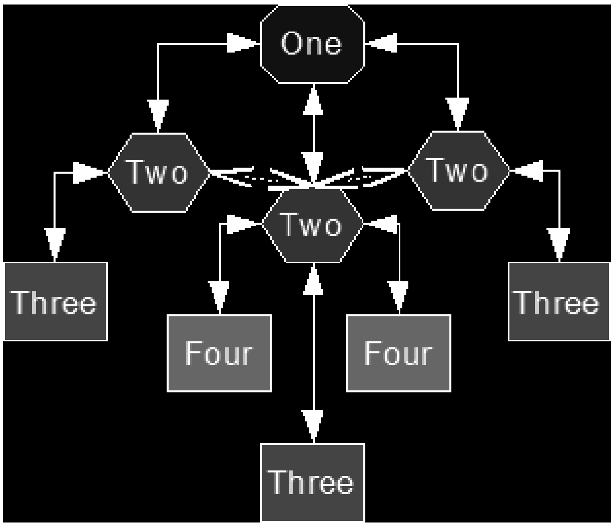

Figure 1: *AziSA class diagram*

By design, there is no point-to-point communication among the third tier sub-networks; all traffic goes through the Class Two aggregator. If one sensor node needs to know the state of another, it would have to pass the request through the aggregator (or even the Class One controller) – however, our position is that decisions depending on the data from more than one sensor should be handled at or above the Class Two level.

An important concept captured in this object model is the idea of *monitors*. Our general architecture is a three-tier tree structure, with a single Class One controller at the apex and a tier of Class Two aggregators each controlling separate sub-networks of Class Three and Four devices. However, any aggregator on the second tier can request a data or alert stream from any other aggregator using a monitor; this can currently be restricted to monitoring particular node ids. These peer-to-peer relationships can allow decisions to be made using the data from more than one second-tier sub-network. Once they are initially brokered by the Class One, the relationships persist independently and can thus function if the link to the controller is lost.

It is also useful to monitor the Class One, which is used by our client front-end software to inspect and display the data coming into the database. (It is possible for the Class Two aggregators to monitor the Class One's data stream, although this is probably not generally useful.) These monitoring relationships allow for a very flexible, distributed software system which can be dynamically updated without disruptions to other services.

2.3. AziSA functionality

A new node should be able to join a network, register its type and position, and provide enough information about its detector transducers that it can be incorporated automatically into the whole sensor system as a source of reliable measurements. In this way, the system can dynamically grow from the bottom up and remain reliable with minimal human intervention. For instance, there is no need to manually add records to the database to accommodate a new sensor. After installation, the data should continue to be trustworthy in three ways: location, time and measurement. If any of these becomes doubtful, the system needs to know as soon as possible so maintenance can take place.

The Class Two aggregators coordinate the data from a number of sensors and pass this on to the Class One controller, which is responsible for ensuring the long-term storage of the data and for making the data available for processing into information which can be used as the basis for decision making.

The Class One interacts passively with the Class Two in terms of receiving data from the network. The Class Two registers sensors with the Class One and receives a reference to a data reporter in return for each sensor registration. This registration includes the identification and position of the sensor as well as of its component detectors. The nature and capabilities of each detector are also registered: each detector is associated with a physical phenomenon concerning which measurements are made, and with information relating to its calibration and for the processing of raw data values to derive information about the particular phenomenon. The detector will also be registered as reporting data in a particular form: a physically stationary device might send discrete measurements (e.g. single temperature or humidity values) or bursts of measurements (e.g. images or seismic waveforms), while a mobile device might report data from a different physical location on each occasion, and provision will be made for the storage of all such data.

Each registered sensor then sends data measured by each of its component detectors to the Class One via the data reporter. The data reporter sends the data on to the database manager (for storage in the database) and also to the Class One controller (for distribution to any registered monitors).

The Class One can also interact more actively with registered sensors by sending instructions (e.g. to change sampling intervals) via the Class Two devices. The setting of alert conditions and the raising of alarms on the basis of alert events are also supported via the Class One controller; these messages are appropriately translated in both directions by the Class Two aggregators.

The Class One also exposes an interface which allows data monitors to register to receive some portion of the live data stream. User interfaces can thus be constructed which provide the user with real-time information based on the measured data.

Data values reported from a registered sensor are tagged with the necessary metadata, including the sensor and detector identification and the time of measurement, as well as the physical location where necessary. It is thus possible to query stored data by originating sensor and detector, or by phenomenon as monitored by numerous sensors. Queries can be constrained by time and spatial boundaries.

2.4. AziSA profiles

The architecture is flexible about the actual communications technologies needed and encourages interoperability between the products of different vendors. In general, the AziSA specification defines only what functionality must be available at each class of device without stipulating how that functionality should be achieved. The AziSA specification is deliberately permissive in terms of its actual requirements, so that application designers are free to choose which communication protocols they will use, as well as the form of the application layer for the required messages.

For the sake of interoperability between system components, the concept of AziSA Profiles was introduced, the idea being that the choice of a certain communication protocol by an application designer requires the use of the defined application layer for that profile. For the current version of the AziSA specification, there is an AziSA-ZigBee Profile, applicable between Class Three or Four and Class Two devices if the communication protocol chosen is ZigBee. ZigBee is the name of a specification for a suite of high-level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks[1]. The ZigBee Cluster Library (ZCL) provides standard message formatting and a general attribute reporting system which is a good fit to our sensor applications.

If the Common Object Request Broker Architecture (CORBA) is chosen as the application layer for Class Two to Class One communications, the AziSA-CORBA Profile specifies the implementation of a particular object model, described in the AziSA Interface Definition Language (IDL) file. This IDL file provides abstract interfaces for AziSA

[1] en.wikipedia.org/wiki/ZigBee

concepts such as Aggregator, Sensor, Detector, etc, as well as concrete types which allow the specification of detector information and alert conditions.

2.5. Typical scenario

Maintenance of wire-based communications and power supply in deep-level South African gold and platinum mines is very difficult due to the harsh environmental and challenging working conditions. Sensors in underground mine working areas (A in Figure 2) would thus typically be small battery-powered devices that communicate wirelessly with the aggregators, which would be situated at the nearest source of electrical power. Several detectors, each monitoring various aspects of the environment, might be attached to each such sensor, of which there might be a large population in any given area. The sensors should be low cost and maintenance free (preferably disposable, with battery life as long as the sensing functionality is required), and would ideally have the capability of determining their own physical position. The process of commissioning could involve providing the new sensor with its position, since underground self-localization remains difficult and might not be possible for small sensor devices.

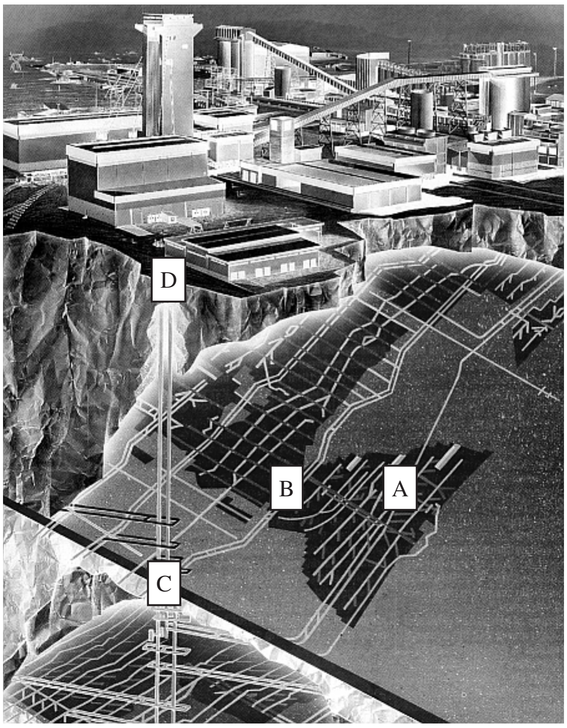

Figure 2: *Schematic of deep-level mine*

The aggregators would typically transfer the data received from the sensors via a power-line carrier out of the working area (A to B in Figure 2) to some point at which a more conventional IT infrastructure is available to send the data on to the shaft (B to C in Figure 2), from which fiber-optic communication might be used to convey the data out of the mine (C to D in Figure 2) to the network controller. The Class Two aggregator devices thus also act as protocol translators between the wireless sensor sub-networks and the central Class One controller device.

3. CONCLUSIONS

The specification for the AziSA architecture has been documented and is available from the authors on request.

Several relatively small systems have been implemented using AziSA principles. These include systems for monitoring waste and ore separation, safety in the workplace, and the underground environment.

It is hoped that CSIR efforts to develop AziSA as an open standard will cause a rapid uptake of the technology on South African mines, and lead to widespread use, with consequent benefits to safety, health and production.