AziSA: An architecture for underground measurement and control networks

R STEWART, SJ DONOVAN, J HAARHOFF, V BRINK, D VOGT
CSIR Natural Resources and the Environment
PO Box 91230, Auckland Park, 2006, Johannesburg, South Africa
Email: rstewart@csir.co.za

PROBLEM

Labour-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. As a result, mining operations tend to be dangerous and unhealthy as well as expensive. In addition, there are human-resource challenges at all levels due to the lack of appropriately-skilled workers.

OBJECTIVE

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 timeously to affect the parameters being managed
3. Measurements have to be processed into a sufficiently useful form to provide support for decision making, and so reduce the need for routine highly-skilled interpretation.

These conditions can be fulfilled more effectively, if an agreed architecture is put in place to facilitate communication and decision making. This architecture should be open to encourage interoperability among products from various manufacturers.

SOLUTION

The architecture that has been developed at the CSIR is called AziSA, an isiZulu word meaning 'to inform'.

The AziSA architecture

AziSA is a specification for an open measurement and control network architecture that will facilitate decision making. AziSA is intended primarily for the design of systems that will operate 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 networks, as well as organisation 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 that can communicate with other nodes. Detectors are attached to such sensors, each transducer measuring 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 these 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.

Device classes

There are four AziSA device classes. Each device class is defined by the functionality that it must be able to exhibit to enable the required functionality of the system as a whole. The AziSA messages follow from these requirements, inter alia identification, metadata, location, sensor self-management and location change notification.

The four device classes naturally fall into two groups:

1. Measurement nodes, which can be simple devices 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).

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 is required to respond to commands, at a minimum providing information about itself, its detectors and their positions, and providing data on request.

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.

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.

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.

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 among 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.

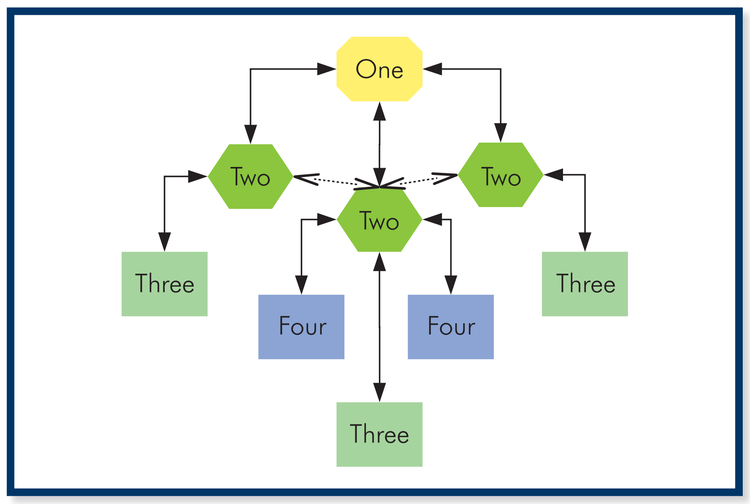

Figure 1: AziSA class diagram

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.

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.

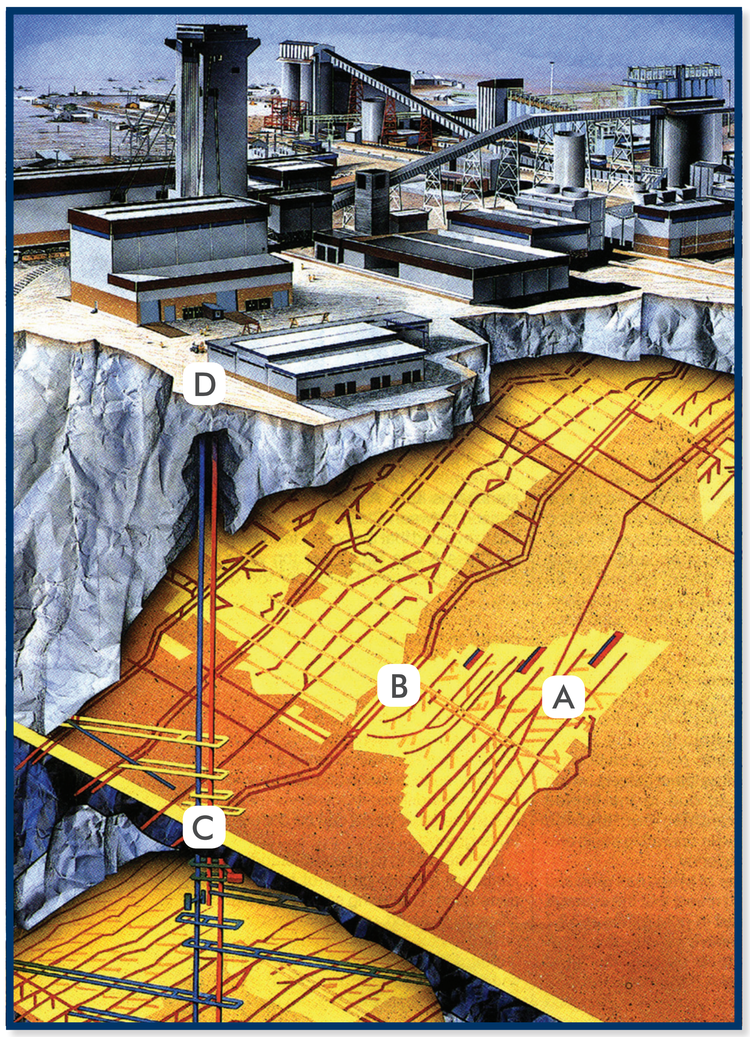

Figure 2: Schematic of deep-level mine

To make our mines safer and more productive, CSIR researchers have developed a technology architecture that will help mines make better use of information obtained underground, where there is limited power and communications infrastructure.

IMPLEMENTATION

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-localisation remains difficult and might not be possible for small sensor devices.

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 fibre-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.

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.

CP0-0005