

# Geotechnical and technology partnerships in the mining industry: ensuring availability of operational data

Evgeny Shilov <sup>a,\*</sup>, Lincoln Tovey <sup>b</sup>

<sup>a</sup> IDS GeoRadar, Australia

<sup>b</sup> BHP, Australia

## Abstract

*Geotechnical monitoring can be logistically challenging to design, implement and maintain, largely due to the scale and distribution of mining operations in a company's portfolio. Driven by in-field monitoring requirements to reduce operational risks, a considered approach to the underlying technology infrastructure needs to be undertaken to ensure optimal performance, scalability, survivability, supportability, availability and accessibility across the wider business operations. Often ignored by practitioners when designing mines and safety systems are the critically important foundational infrastructure components required to avoid ongoing technical regret. The key topic of identifying important monitoring technologies used in different mining scenarios is covered in the following paper, followed by many elements of infrastructure design decisions that define successful implementation. Irrespective of specific company requirements, a high-level solution design should be mandatory, and more detailed designs covering hosting and storage, communications and networking, cybersecurity and firewalls, and application deployment with user access models should be produced, in parallel with a clear transition to the operations process required for post-implementation support and maintenance. Driving the detail into these designs are decisions regarding confidentiality, solution integrity and system availability, which in turn inform a design team about user access models, data latency, service continuity, disaster recovery, data archiving, alarm propagation modes, and the integration and portability of monitoring technologies. There is no single solution to suit all mining operations, however, the process of translating monitoring requirements into technology designs is paramount to a successful outcome. The intent of this paper is to highlight what decisions need to be considered and why they are important, with a presentation of both good and poor examples of real industry use cases observed by the authors.*

**Keywords:** *geotechnical engineering, geotech, monitoring response, information technology, IT, infrastructure, partnerships, service continuity, disaster recovery*

## 1 Introduction

Effective monitoring by geotechnical engineers is critical to ensuring safe mining operations, in accordance with Government of Western Australia 2022, *Work Health and Safety (Mines) Regulations*.

Monitoring plays a vital role in identifying and mitigating ground stability hazards that have the potential for compromising the safety of mining teams. Tovey et al. (2023) described the importance of business partnerships between geotechnical engineering, information technology (IT) and vendor services in managing slope stability risks around the clock in large-scale open pit mining operations in Western Australia's Pilbara region. Dixon et al. (2022) described some of the challenges faced and decisions required to expand geotechnical monitoring capabilities from desktop- to enterprise-scale in the same mining landscape.

Some of the broad geotechnical concepts discussed in this paper were explored by Sharon & Eberhardt (2020).

This paper will provide a more comprehensive discussion regarding the IT considerations required for all geotechnical instrumentation and data types across a range of mining landscapes, with an emphasis on the

---

\* Corresponding author.

questions a business must answer to provide its customer base with the right solution. Case studies will be presented to highlight what good and bad IT practices look like, with recommendations of how to avoid technical regret and elevated safety risks.

## 2 Geotechnical sensors

The following section presents an overview of the various types of sensors and measurement instruments employed in an open cut mining environment. These instruments can be broadly classified into two primary categories: surface (above-ground) monitoring and sub-surface monitoring.

Above-ground instruments generally require minimal or no installation of devices on the ground and include:

- Ground-based radar: a terrestrial radar system that emits electromagnetic waves and measures phase shift of the returned signals to detect and monitor ground surface or structural displacements in real time
- Automated prism monitoring: a system that consists of a fixed-position laser instrument and a network of reflective prisms installed on the monitored slope. Robotic total stations perform periodic readings of prisms and store the data into the database
- Satellite InSAR monitoring: a service of analysing data acquired by satellites
- Laser scanner (lidar): a laser scanner generating a high-resolution image of a pit wall without needing to install prism reflectors
- Unmanned aerial vehicle (UAV): UAV can take photos, videos and lidar scans, and deploy and retrieve reflective prisms
- Ground-based global navigation satellite system (GNSS): a series of GNSS receivers installed on the ground used for high-precision positional information
- Weather station: a collection of sensors recording different types of data (rain, temperature, pressure, wind) which can be used to perform data corrections for other instrumentation.

Sub-surface monitoring instruments require drilling into the surface and placement of instruments in the ground, including:

- Vibrating wire piezometer (VWP): measures porewater pressure using a tensioned wire that vibrates under pressure
- Time-domain reflectometer: monitoring moisture, ground movement and deformation using coaxial cable or waveguide
- Extensometer: measures the amount of strain or deformation
- Shape accel array: a chain of tilt sensors measuring deformation in 3D
- Tilt sensor: a sensor that detects differential settlement on the surface
- Inclinator: sensor that detects the slip surface inside the ground
- Strain gauge: a sensor that measures the amount of deformation (strain) of the material it is bonded to
- Crack meter/crack gauge/joint meter: a sensor designed to monitor the opening/closing of the crack or joint
- Seismic sensor/accelerometer: a device that measures ground vibrations across multiple axis.

### 3 Data types, volumes and integration

Above-ground instruments usually generate larger amounts of data and have more frequent readings compared to the sub-surface sensors.

Data storage could be split into local and cloud, although a lot of providers are now moving into a hybrid model where both options are utilised and provided. Local storage is typically faster and more convenient in terms of accessibility but requires infrastructure set-up on site, at a higher cost. The advantages of cloud storage are that data security and availability are taken care of by the provider, but disadvantages include cybersecurity concerns (having company data in a public cloud) and accessibility (slow internet connection speeds).

Table 1 below illustrates the different categories of data as well as some typical size estimates.

**Table 1 Categories of data and size estimates**

	<b>Instrument</b>	<b>Category</b>	<b>1y data size</b>	<b>Storage</b>
1	Ground-based radar systems	Large	>100 GB	Local
2	Automated prism monitoring	Medium	>5 GB	Local
3	Satellite InSAR	Large	>50 GB	Cloud
4	Laser scanner (lidar)	Large	>100 GB	Local
5	Unmanned aerial vehicle	Large	>100 GB	Local
6	Ground-based global navigation satellite system	Small	<1 GB	Local/cloud
7	Weather station	Small	<1 GB	Local/cloud
8	Vibrating wire piezometer	Small	<1 GB	Local/cloud
9	Time-domain reflectometer	Small	<1 GB	Local/cloud
10	Extensometer	Small	<1 GB	Local/cloud
11	Shape accel array	Small	<1 GB	Local/cloud
12	Tilt sensor	Small	<1 GB	Local/cloud
13	Inclinometer	Small	<1 GB	Local/cloud
14	Strain gauge	Small	<1 GB	Local/cloud
15	Crack meter/crack gauge/joint meter	Small	<1 GB	Local/cloud
16	Seismic sensor/accelerometer	Small	<1 GB	Local/cloud

### 4 Telemetry/network connectivity

Connecting a geotechnical monitoring device to a network versus keeping it offline for manual readings involves trade-offs related to data accessibility, reliability, cost and maintenance.

Advantages of networked (online/automated) devices include:

- real-time data access
- continuous monitoring and quick response to changes (e.g. early warning systems)
- remote monitoring
- elimination of the need for frequent site visits – ideal for remote or hazardous areas

- higher data frequency
- integration with alarms or dashboards
- reduced human error and missed data points common with manual logging.

Disadvantages of networked (online/automated) devices include:

- a higher initial cost
- installation of telemetry units (e.g. LTE, LoRa, Wi-Fi) is required
- consistent power via battery, solar or grid is required
- cybersecurity considerations are necessary when using public LTE networks
- set-up and maintenance (firmware updates or troubleshooting of telemetry hardware) requirements.

Advantages of offline (manual readings) devices include:

- a lower initial cost
- they are easier to install
- a simplified design without external antennas, etc. – more robust in harsh conditions
- lower power requirements.

Disadvantages of offline (manual readings) devices include:

- being labour intensive (regular site visits for data collection)
- providing less-frequent readings (slower detection of changes or events)
- potential human errors caused by manual logging
- no real-time alerts.

## 5 Presenting data to the user

Decisions on how to present the data should be guided by the target users, the type of data, how often it changes, whether collaboration is needed, where the data is going to be accessed from (in the field or office) and any technical or regulatory constraints. Each decision involves consideration of simplicity, compute resources, accessibility, complexity and cost.

Web-based applications are usually accessible from any device with a browser, easy to update and ideal for multi-user access. They require an internet connection (if cloud-hosted) and are often limited by browser constraints. Desktop applications may offer better performance and offline capabilities but are platform-specific and harder to distribute and maintain. Mobile applications are great for providing roaming access and native device features, but in turn require more development effort to support multiple platforms. Single-user interfaces, simpler to build and manage, are suited for personal tools or offline applications. Multi-user interfaces require more complex authentication and permission models for security, but offer real-time collaboration features for teams and shared data access. Static outputs, like PDFs or Excel files, can be used for formal reporting and compliance purposes. Interactive dashboards allow users to explore data through filtering and drill downs, additionally providing value for both data analytics and system monitoring. Real-time interfaces are used when instant updates are critical.

## 6 Platform integration and data aggregation

With the increasing deployment of sensors in the field there is a growing need for an integrated platform capable of aggregating data from diverse sources.

Bringing disparate data into one interface provides a comprehensive, centralised view, eliminating the need to manually switch between systems. With all relevant data visible in context, users can make faster and more informed decisions. Cross-referencing becomes easier, helping reveal trends or correlations that would otherwise be missed. Aggregated platforms reduce time spent on manual tasks like data collection, formatting and reporting. This leads to higher productivity and allows teams to focus more on analysis and action. When aggregation is automated and standardised, it reduces human error and ensures that users are seeing consistent, up-to-date information – especially when sources are refreshed on a schedule or in real-time. Once an aggregation framework is in place it's easier to add new data sources as your ecosystem grows, rather than building separate tools for each one. Centralised data access enables teams to work from a single source of truth. This encourages transparency and easier collaboration across departments, especially when role-based access and shared dashboards are used. Users can tailor the interface to highlight the most relevant metrics for their role, department or use case – whether through filters, dashboards or alerts. Aggregated platforms can provide real-time monitoring, enabling anomaly detection, alerts and quick responses to problems across different data domains.

## 7 Using business partnerships to define solution requirements

Prior to any decisions and solution designs, the business needs to formulate requirements based on how their monitoring plans, instrumentation and data are positioned within the organisation. To guide this process, one needs to consider accessibility, operability, availability, survivability, supportability and scalability as six key business tenets for the IT foundations of a geotechnical monitoring solution. When understanding the main elements within these tenets it should also be noted that there will be inherent interdependencies between many requirements. Trade-off decisions may be required but these should always be made with a clear view of why, and what that will mean for the solution as it matures.

To build a successful suite of requirements with the above concepts in mind, Geotech, IT and Technology teams need to work closely together. Geotech will always guide requirements from an operational perspective – for example, types of instrumentation, monitoring standards, and data and system access – and will ultimately define the criticality of the systems, but equally IT and Technology teams will be able to provide details on how the system will be designed for optimised operation. This will include understanding and adhering to any business standards relating to hardware, networks, cybersecurity and permissions modelling. A key failure in too many projects is a technical department buying new instrumentation without consideration of how it will ultimately be integrated into an enterprise organisation.

Considerations from an accessibility perspective, to form an initial view of IT requirements, would be to assess the geographical spread of the instrumentation required, the type and stability of communications networks for connectivity back to a data centre, proximity to an available data centre or data centres, and which business users require access to the software systems and data to make informed safety decisions. For example, a fully localised solution, hosted in a site office with users logging in via physical desktops, may be suitable for some companies. However large-scale companies operating across vast geographical locations and a decentralised user-base will ultimately need a starkly different IT operating model. A final note of interest here may be the potential to enable access for users outside the company network; for example, vendor service teams.

The next line of enquiry, intrinsically coupled with the above, is regarding expectations and requirements for how the system needs to operate: or in other terms, what minimum performance standards are required by the user-base. Cost is significant driver here and often underpins any technical compromise. It may be, particularly for a small mining operation, that the company rents shared data centre facilities in a nearby location, as compared to an established large operation with localised data centres and capacity readily available. In large-scale compute and data transfers, local and wide area networks' (LAN/WAN) bandwidth, stability and latency need to be evaluated for all solution options, as does the availability of CPU, RAM, GPU (if required), storage arrays, database servers, and/or decisions around cloud-hosting services, if applicable.

Given the regulatory requirements for adequate geotechnical monitoring across mining operations, it is critically important to understand the availability and survivability of chosen monitoring technologies, underlying IT infrastructure and related services. One excellent method to assess your business requirements is to understand the CIA triad, with components defined as confidentiality, integrity and availability. Whilst the underlying principles behind a CIA assessment are generally well understood, individual companies will likely have their own definitions and ratings systems. Confidentiality, in broad terms, relates to the protection of data, objects or resources via controlling access to intended systems. Integrity is centred upon ensuring data, objects or resources are reliable, consistent and only modified by authorised means. Availability ensures that authorised users are granted timely and uninterrupted access to data, objects or resources. Each element of the CIA triad can be assessed within a severity-domain matrix. For example, if a significant data breach via unintended or criminal means occurs, the maximum foreseeable loss or impact on health and safety, environmental and legal regulations, reputation and finances, or on the community, drives the confidentiality rating. Similarly for integrity, the maximum foreseeable loss or impact if unauthorised changes occur, and the service, application or data becomes unavailable, defines the accessibility ranking. The impact assessments in each category will ultimately drive decisions regarding service continuity and disaster recovery plans, service level agreements for both internal and external supporting teams, and cybersecurity requirements. Scenario-based workshops can be extremely useful in developing service continuity and disaster recovery plans. Consider impacts such as losing a single data pod or entire data centre to catastrophe (fire, terrorism, 'acts of God'), private or public communications network outages, global service impacts such as the 19 July 2024 CrowdStrike-related IT Outages (Wikipedia 2025a), LAN or WAN outages, and a host of other planned and unplanned IT outages. Think big, understand the maximum foreseeable impact in all scenarios and then develop risk mitigation strategies in your IT designs, or accept the risk and implement business controls and processes to effectively manage these situations. Whilst it can be applied at a macro level, the same principles can be applied at an individual geotechnical sensor level, with the acknowledgement that some sensors and data are less critical than others and may have a significantly lessened impact on mining operations if unavailable for a period.

A common significant oversight in many technology projects is where a solution is designed and delivered to the business's customers but minimal consideration has been given to supporting the array of IT systems on which the service is dependent. As with any mechanical system we use in daily operations, IT systems need both preventative maintenance and break-fix support as required. Storage capacity requires monitoring and management, security patches need to be applied, software updates are required for new features, stability control or security improvements, networks require upgrading to facilitate higher volumes of traffic, hardware expires and, sometimes, things just break. Mining operations in Australia face some of the harshest environmental conditions anywhere in the world, including extreme and sustained temperatures, often over 50°C in the shade during summer months; torrential rain events in the wet seasons, with regular occurrences of 24-hour periods receiving > 250 mm; and fine-grained dust ingress into every nook and cranny. Thus, many of our in-field geotechnical sensors and supporting hardware suffer significantly shorter life spans than expected. Understanding which teams or vendors can support each service for both planned and unplanned events, to maximise service continuity and minimise disruptions, will become the legacy of any project.

A final consideration in the initial design of a system related to the company's growth plans is whether elements of scalability need to be included. With some forethought regarding 5–10 year company plans, some technical regret can be avoided upfront. Designing a system that is at maximum capacity, or at the limits of serviceability, for today generally will become redundant very quickly. It may be that new mining assets are included, or existing high-grade ore drives wider and deeper pits, or deeper underground tunnels. Or perhaps initial budgets only catered for a coarse network of monitoring capabilities, with infill opportunities for instrumentation and data to be included over time. Additional geotechnical instrumentation will likely be included to support these plans, so consider the cost and ease of plugging directly into existing infrastructure which has capacity versus revisiting the designs and adding new compute resources, switches, storage and cabling each time expansion is required. Consider, too, building an IT system that co-locates workloads in case data aggregation software capabilities change over time. For example, in a large-scale operation it may make sense to deliver a fit-for-purpose GPU-enabled compute cluster with full

failover redundancy between separated physical locations, virtually hosting a range of applications that support radars, prisms, laser scanners, VWPs and GNSS base stations, as opposed to squeezing each application workload onto disparate servers that host unrelated mining or IT systems. The purest view in this scenario is to have ample capacity on the cluster to include new instrumentation over time and, software solutions pending, a tool to automatically view each datatype in a unified environment, and with no requirement for export/imports, additional firewall rules for data to traverse networks in a complex manner or added user authentication across disparate systems.

## 8 IT platforms and hosting

As briefly introduced in the previous section there are numerous requirements which ultimately define the final solution design. Small-scale geotechnical operations may easily be enabled via localised, desktop IT solutions but, as the system expands – in terms of monitoring instrumentation types and requirements, data quantities, flexible user access models and emerging software capabilities – there becomes a point at which a centralised and virtualised system is more cost-effective to run and maintain. Each company must understand their intended instrumentation and associated software options, which usually come with vendor-supplied recommended (or minimum) system requirements. It's a good place to start assessing whether specific instrumentation requires specialised graphics processing via GPU cards, how much CPU and RAM are needed, how data is stored and what network bandwidth is necessary; the latter calculated by how much data per unit of time is sent from an instrument to its software host. Some software creates data in common and open formats, and sometimes in proprietary project format; others write direct into mainstream databases like SQL or Oracle; and others utilise their own versions of databases. As time moves forward the industry is being provided with more public and private cloud-based solutions, so hosting on your own company's premises ('on-prem') may not even be required. And for a large mining company distributed across numerous operations, decisions around hosting per site operation versus hosting via a distributed model at a single site might be a key determination.

Another element which will guide the decision process is the user access model required. Some companies with small geotechnical teams may be perfectly suited to single-user software sessions via local and personalised log-in credentials. Larger companies may need users to access systems remotely from other mining sites or from business headquarters located in a capital city. With large teams and complex software suites, the requirement may call for multi-user and multi-session access: that is, one user may need to access multiple systems simultaneously, but equally, multiple users may need to access a single system simultaneously. And further to this, some industry vendors offer monitoring services, via remote operations centres in other countries, outside your company's network.

Virtualising the compute hosting environment simplifies many of these challenges and, using tools such as multi-factor authentication, publicly available remote desktop management tools and application virtualisation technologies like Citrix, the goals can be met whilst successfully managing cybersecurity risks.

It should be noted that for many companies, commissioning an industry-recognised data pod or data centre for these purposes may not be feasible, but even an old administration area can be modified to serve as a local data centre. Many cities and towns also run data centres for rent, including the new NextDC facility in the town of Newman, Western Australia.

## 9 Best practices and continual improvement

To draw a loose parallel, some of the best written novels begin with the end chapter or sequence in mind. Similarly for a project delivering IT solutions, a considered approach to transitioning to operations is imperative for a successful outcome. When designing and building a technology system to host geotechnical monitoring capabilities, identifying the internal and external stakeholders, and their requirements, is important to support services and tools into the future. Companies will always have different organisational structures within IT and Technology teams, but there are usually specialists required to manage IT networks, compute hosting, storage, site communications networks, power supplies, mechanical devices and technical

instrumentation. A project delivery team needs to engage these final stakeholders early in the solution design and determine what documentation or knowledge needs to be transferred to embed proper preventative maintenance and support for every element of the solution.

As discussed in Section 7, the CIA ranking for the solution will guide the requirements for service continuity and disaster recovery plans. Service continuity plans usually contain elements such as: the contact details of all supporting services, both internal and external teams; recovery point and recovery time objectives (RPO, RTO) after an outage; specific plans for an array of single failure points (for example, instrument communication device failure) or uncontrolled systems failures (for example, storage, application and licensing, WAN, LAN, virtualised access and compute resourcing failures); controlled system outages (for example hardware and software upgrades, security patching, preventative maintenance); and data recovery due to accidental or unplanned events. Disaster recovery plans address the next level of significant incident, with the goal of establishing defined responsibilities, activities and procedures to recover technology services resulting from unplanned, calamitous events. This plan is designed to mitigate the risk of system and service unavailability by documenting effective contingency solutions for the continuation or resumption of mission-critical technology services in the event of a disaster. Overall disaster recovery objectives include the following:

- recovering services within the established RTO and RPO
- minimising business impact, direct costs and indirect costs resulting from a technology service disruption
- ensuring that service application performance is not degraded for recovered services
- ensuring that recovery plans are cost-effective.

Preventative system maintenance is also a great way to avoid unplanned and uncontrolled outages. Implementing dashboards or systems to remotely and continuously monitor disk space, application uptime, licensing services, solar power inputs, battery voltages, generator fuel levels and other important system elements can save money and effort, particularly when instrumentation can be difficult to physically access.

With an array of instrumentation continuously collecting important data, plans to protect, archive and restore the data should also be part of the overall IT solution. In addressing the criticality of data and any legal or regulatory requirements, data management systems with ongoing capacity can range from periodic backups of data (to external media or the cloud) to a fully formed technical archiving data strategy. There is no one solution here, but any decision should reflect the CIA assessments and be consistent with both the service continuity and disaster recovery plans. It should also be consistent with the most appropriate IT tools available to the company at the time. Some storage terms to be familiar with are:

- Online/hot: still available to applications and users, usually on a fast disk with low latency
- Near-line/warm: can be made available to applications and users relatively quickly but is isolated from the main working areas to reduce unintended modifications
- Offline/cold: usually on low-cost media, including magnetic tape, cheap cloud services or a low-speed disk, and with a longer retrieval time for applications and users.

Any IT system will require periodic maintenance in the form of software and firmware upgrades, operating system (OS) patching and new functionality testing. Implementing processes and controls to effectively manage planned outages includes provisioning a separate QA (or testing) environment and following a robust IT change process to consult with both technical and business stakeholders to schedule in fully tested system changes, including both implementation and rollback plans. By following some simple best practices, the risk to safety and mining production is minimised and managed effectively.

Continual improvement to meet evolving technology, process and regulatory requirements needs to be factored into any solution. We have discussed designing a solution to cater for more instruments, greater volumes of data and adapting software, but sometimes internal and external reviews, for example by a

geotechnical review board, will highlight deficiencies in existing operational practices. Varying state, county or national regulations may also influence changes to a company's monitoring requirements. This may include modifications to both safety and environmental management systems, or even to reporting and data retention for compliance. Flexibility in a designing a geotechnical monitoring system can be crucial to being able to rapidly meet fluctuating demands, especially in a cost-effective manner.

## 10 Examples of good practices

As described by Dixon et al. (2022), BHP designed and built a technology solution from first principles, guided by many of this paper's discussions points. Starting with only two radars, each monitored via a simple desktop solution at two separate site locations, a program of work to expand the radar fleet to 11, and finally 22, over a three-year timeline required a significant investment for a sustainable and maintainable solution. Using the processes and principles discussed in this paper, a dedicated technology project team worked closely with both geotechnical engineering and IDS GeoRadar consultants to ultimately deliver a highly available, standalone compute cluster, hosted in BHP's OT network, with the provision for user access from any geographical location around the world, including support for external vendor accounts.

Leveraging vSphere vMotion (Wikipedia 2025b) technology, the hosting environment was designed to provide full disaster recovery failover, with virtual machines able to move silently between physical servers and with no impact to applications or licensing. Capacity was such that all relevant applications supporting an array of other slope monitoring capabilities were co-located, thus provisioning for future data aggregation applications.

The overarching service and individual components were transitioned to relevant operations teams which, over time, have supported and maintained the system with minimal downtime. Regular maintenance is managed via standard IT Change processes, including software updates and regular OS patching. Break-fix support for individual components such as physical and virtual servers, communications devices and data storage arrays are managed via business incident management tools.

Real-time alarming and alerts are issued to ancillary systems, including to geotechnical engineers via text messaging services, to the BHP Incident Remote Operations Centre and via an external, 24/7 service provided by IDS GeoRadar (described by Tovey et al. [2023]). This ensures that all critical mining areas are always monitored, backed up with a robust trigger, action, response process.

A fully separate QA/test environment is hosted on a different subnet to the production servers, allowing the technology team to test new software capabilities with very low risk. Fully automated data transfer protocols are leveraged to enable data archiving and retention in low-cost backup storage facilities.

## 11 Examples of bad practices

Across the global mining industry, numerous examples illustrate suboptimal and potentially hazardous configurations of IT infrastructure. The following are illustrative cases detailing how individual companies identify and assess risks differently, leading to varied solutions that are shaped by both the specific risk perception and the constraints of available budgets.

Radar monitoring system is widely regarded as the most critical among geotechnical instrumentation due to its ability to deliver real-time data and alerts. In many mining operations, pit activities are directly reliant on radar monitoring systems. A commonly adopted policy among operators is 'no monitoring, no mining', indicating that mining operations are suspended if radar monitoring systems are not fully operational. Indeed, in certain jurisdictions, legislation mandates that monitoring instrumentation must be installed and fully operational as a prerequisite for conducting any open cut mining activities.

## 11.1 Example 1

This site deployed a radar monitoring system within the pit to collect geotechnical data, which was transmitted to an office-based computer for processing and the generation of alerts. The receiving computer, a standalone desktop unit, lacked redundancy in terms of power supply, data storage and network connectivity. During night shifts, when geotechnical engineers were not present onsite, alerts were automatically dispatched via email and SMS to operators working in the pit. Upon receiving an alert pertaining to their active work area, operators were required to evacuate immediately, contact a geotechnical engineer and await further instructions.

One particular night the desktop PC, located unsecured beneath a desk, was inadvertently powered off when a cleaning staff member accidentally made contact with it. Unaware of the shutdown, the cleaner did not report the incident. Consequently, the operations team continued working in the pit under the assumption that the radar monitoring system was fully operational and would issue alerts in the event of ground movement. A ground movement event subsequently occurred but no alerts were dispatched, leading to a near-miss incident. The post-incident investigation identified several critical risks, including the absence of system redundancy and the lack of a monitoring mechanism to detect system downtime.

In response, numerous corrective actions were implemented. The desktop PC was replaced with a rack-mounted server featuring redundant power supplies, network interfaces and storage. This server was installed in a secure onsite server room to prevent unauthorised physical access. Additionally, a secondary alerting system was introduced to monitor the operational status of both the server and radar data availability, thereby enhancing system reliability and situational awareness.

## 11.2 Example 2

As with the previous example, this site operated a monitoring system that transmitted data to an office-based computer for processing and alert generation. This system relied on a standalone desktop computer without redundancy. During a day shift a geotechnical engineer experienced an unexpected failure of the computer, which abruptly stopped working. Initial troubleshooting efforts were unsuccessful and the machine could not be powered on. An urgent IT support request was raised to repair or replace the computer.

However, due to the absence of spare equipment onsite, a replacement desktop unit was not available for several days. Monitoring capabilities were eventually restored, but the absence of backup solutions resulted in the permanent loss of several years of data.

Following this incident, backup systems were implemented, and a secondary (standby) computer was procured and stored onsite to ensure rapid recovery in the event of future hardware failures.

## 11.3 Example 3

As in previous examples, this site had a monitoring system in place which was hosted within a server room. Whilst the devices within this server room were equipped with full redundancy, there was no replication to an external or secondary server facility. A fire in an adjacent room triggered the activation of the server room's fire suppression system. Due to a design flaw, the system employed an inappropriate powder-based suppressant which dispersed particulate matter throughout the server room. The cooling fans in the equipment drew the powder into the internal components, resulting in widespread hardware failure. The incident led to catastrophic system downtime, with recovery taking approximately one week, and significant data loss occurred due to the lack of offsite redundancy. In response to the incident, a comprehensive review of fire protection protocols was undertaken, and a secondary server room was subsequently constructed to ensure future redundancy.

## 11.4 Example 4

Network changes were implemented on this site without a comprehensive assessment of all systems potentially impacted by the modification. Consequently, the slope monitoring system was inadvertently

taken offline. Due to the complexity of the network architecture the troubleshooting process extended over several days, during which time monitoring data was unavailable.

The post-incident investigation revealed that the monitoring system had not been properly registered in the critical asset register. As a result, when the networking change request was submitted, the monitoring system was not identified as a dependent component of the affected network service. This oversight contributed to a prolonged outage and highlighted deficiencies in the site's change management and asset registration processes.

## 12 Conclusion

Effective collaboration between geotechnical engineers, IT departments and specialised vendor services is essential for developing robust solutions that minimise operational risks. Whilst the ultimate design of a comprehensive monitoring solution will be directed by a company's requirements, the process for arriving at the solution should be conducted in a considered, project-oriented manner, with respectful and active participation and communication between all stakeholders. Balancing requirements against constraints is an absolute must, as are risk assessments for every element of the intended solution.

The principles articulated in this paper are universally applicable across mining enterprises irrespective of organisational scale, with the resultant outcomes being inherently influenced by the magnitude and availability of organisational resources.

Geotechnical engineers will drive the technical requirements for instrumentation required to safely monitor mining areas and need to be conversant in industry best practices and regulations. They will be able to provide expertise regarding the intended criticality of a given service, and influence both internal and external service level agreements for managing downtime and incident response. Financial impacts due to the loss of an instrument or entire service will need to be considered.

Equally, the IT and Technology teams should work with respective vendors to provide architecture covering all aspects of how to deliver the solution, including compute hosting, networking designs, application deployment, cybersecurity, user access models, data storage policies and system redundancy. A considered approach to IT Change management for ongoing system maintenance will minimise the risks associated with unplanned, uncontrolled outages and will keep the overall system in the best health. Identifying stakeholders is a critical component of a robust transition to an operations process, allowing every element of the service and the components to be supported by the correct expertise.

## Acknowledgement

The authors would like to acknowledge the contributions of the BHP technology project team, the entire BHP WAIO Geotechnical team (past and present), and the teams at IDS GeoRadar and Hexagon Mining.

## References

- Dixon, R, Tovey, L & Shilov, E 2022, 'Slope radar monitoring – a partnership and infrastructure case study of scalability, reliability and availability', *The Australian Ground Control Conference: An ISRM Regional Symposium*, The Australasian Institute of Mining and Metallurgy, Melbourne.
- Government of Western Australia 2022, *Work Health and Safety (Mines) Regulations*, Perth.
- Sharon, R & Eberhardt, E 2020, *Guidelines for Slope Performance Monitoring*, CSIRO Publishing, Clayton.
- Tovey, L, Dixon, R, Morgan, M & Shilov, E 2023, 'Rocks around the clock: a 24/7 approach to radar slope monitoring', in PM Dight (ed.), *SSIM 2023: Third International Slope Stability in Mining Conference*, Australian Centre for Geomechanics, Perth, pp. 741–756, [https://doi.org/10.36487/ACG\\_repo/2335\\_51](https://doi.org/10.36487/ACG_repo/2335_51)
- Wikipedia 2025a, *2024 CrowdStrike-related IT Outages*, viewed 16 September 2025, [https://en.wikipedia.org/wiki/2024\\_CrowdStrike-related\\_IT\\_outages](https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages)
- Wikipedia 2025b, *VMware*, viewed 16 September 2025, <https://en.wikipedia.org/wiki/VMware>