International Society of Automation
Setting the Standard for Automation™

Benefits and Challenges of AI in Mining and Metals

By Bas Mutsaers, Rob Zwick, Joanne Sun, Mark Harris and Ismael Borrego

Integrating industrial systems with artificial intelligence can provide sustainable outcomes when standards are followed, and best practices are applied.

Abstract

Like many other enterprises, the mining industry is embracing artificial intelligence across the mining operation value chain. Although the technology can bring tremendous benefits, integrating AI into existing operations is not without risks and challenges.

In this article, authors from the International Society of Automation's Mining and Metals Industry Division (**MMID**) share their experiences, discuss emerging AI use cases, and offer advice on applying relevant standards and best practices.

First, we'll explore potential applications of AI technology. Next, we'll detail successful use cases implemented by members of MMID. These illustrate that there is a lot to consider to ensure sound and secure installations before implementing AI in the cloud or on the premises.

This article also discusses the added cybersecurity risks and benefits that AI technologies bring and shares cybersecurity best practices for deeply integrated and sometimes autonomous sites.

Introduction

Artificial intelligence (AI) is the computer system simulation of human intelligence processes. It covers very broad areas and can be grouped with topics such as knowledge engineering, machine learning (ML), natural language processing, image recognition, decision-making and more.

AI can be applied locally and globally across a business's value chain and is a great tool for improving efficiency and autonomy at modern mining sites. AI promises to improve resource discovery, boost operational efficiency by optimizing processes and automation, reduce downtime by improving predictive maintenance, reduce environmental impact and improve health and safety.

Implementing AI is a journey that requires a significant cultural shift within the organization and strong collaboration between subject matter experts, data scientists and multidisciplinary engineers. When integrating industrial systems with AI, it is important to understand the implications, best practices, risks and benefits.

Summary

Key Challenges of Applying AI to Mining/Metals Operations

Data quality and accessibility: Mining operations generate vast amounts of data from various sources, including sensors, equipment, geological surveys and historical records. Ensuring the quality, consistency and accessibility of this data is a significant challenge for AI applications. Data may be incomplete, inaccurate or stored in disparate formats, requiring preprocessing and integration efforts. Using models from other areas can introduce issues.

Complexity of mining processes: Mining operations are highly complex and highly variable. They are also dynamic and involve numerous interconnected processes, such as exploration, drilling, blasting, hauling and processing. Developing AI solutions that can effectively model and optimize these processes requires a deep understanding of the domain-specific challenges and constraints. Suboptimization is the biggest risk here.

Integration with existing systems: Many mining operations rely on legacy systems and infrastructure, which may not be compatible with modern AI technologies. Integrating AI solutions with existing systems, such as fleet management software, geological modeling tools and enterprise resource planning systems, can be challenging and require careful planning and coordination.

Safety and reliability: Safety is a top priority in the mining industry, and AI solutions must be reliable and robust to ensure worker and equipment safety. Malfunctions or errors in AI algorithms could have serious consequences, leading to accidents, equipment damage or production delays. Therefore, it is essential to thoroughly test, validate and monitor AI systems to mitigate risks.

Regulatory and compliance requirements: The mining industry is subject to various regulatory requirements for safety, environmental protection and community engagement. AI solutions must comply with these regulations and standards, which may vary depending on the jurisdiction and type of operation. Ensuring regulatory compliance while deploying AI technologies requires careful consideration of technical, legal and ethical implications.

Skill and knowledge gap: Implementing AI in the mining industry requires a workforce with the necessary skills and expertise in data science, machine learning, computer vision and other AI-related disciplines. When going to the next level of autonomy, robotics and mechanical systems and their limitations must be well understood. However, there may be a shortage of talent with these specialized skills, highlighting the need for training and capacity-building initiatives within the industry. We see the original equipment manufacturers taking an increasing role here.

Cost and return on investment (ROI): While AI has the potential to deliver significant benefits in terms of productivity, efficiency and safety, the initial investment and implementation costs can be substantial. Mining companies must carefully evaluate the expected ROI of AI initiatives and prioritize projects based on their potential impact on operational performance and profitability. Also, having a dedicated team execute AI projects may not always be beneficial for companies. Vendors have high-value AI to offer, but embedding the technology into existing operations is not without risk.

Security and risk management: AI-powered security solutions greatly improve cybersecurity prevention, detection and response capabilities. However, AI technology also introduces unique risks in the mining operation. An organization must set up strategies to manage the additional risks and deploy AI technology securely.

The many considerations of applying AI

We know humans are not particularly well equipped to multitask or quickly process large amounts of data. The opposite is true for control systems that are deployed to automatically make decisions based on process data.

Along the same lines, humans are not equipped to deal with the multidimensional data and the mounting terabytes produced by modern information technology (IT), operational technology (OT) and sensors at a typical site. AI is far better equipped to utilize this data because it is adept at consuming and analyzing vast amounts of data while producing actionable insights.

For all these reasons, control systems, operational systems and machines—like drilling and hauling equipment—are combining first principles in their model-based controllers with AI.

AI is not a solution that is simply deployed and results are achieved. Instead, it is a tool for human operators that must be tailored to the specific mining technology, operation and environment. Governance of the overall application is key, as with many of the cyber standards, because the result is only as good as the data provided for training the model and used in the operation, along with the personnel skills available to train, apply and maintain the AI.

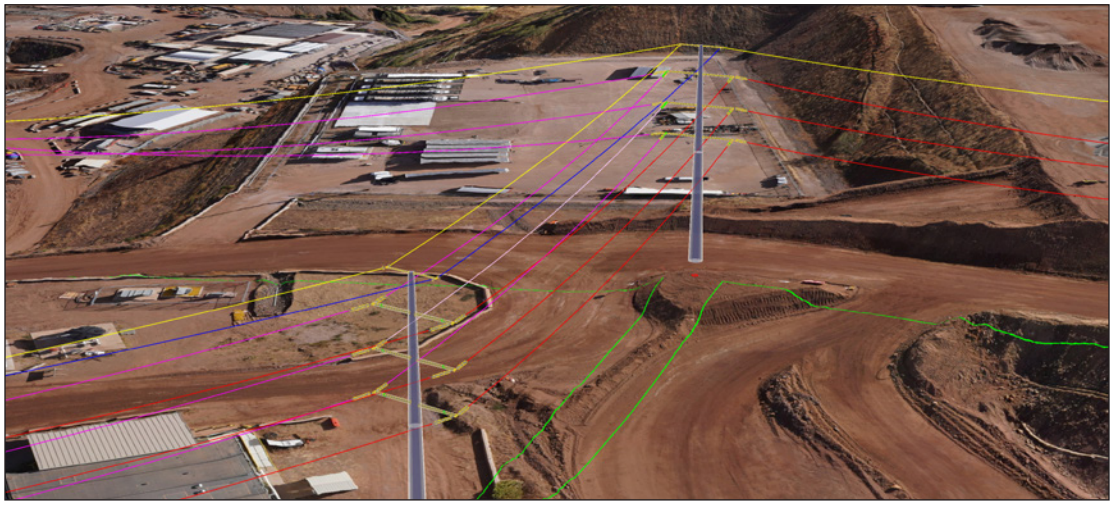
Therefore, security and governance must be applied to the data from source to outcome to keep AI in place and effective for the site. Trust is a big factor, and it can only be achieved if good governance practices are applied throughout the life of the data, including implementing security practices, to make sure the data is not adjusted at any stage.

In modern mining and metals operations, process applications are combined with power grid and energy management applications, which are often collectively called power management applications. Secure industrial process applications are often based on **ISA/ IEC 62443 Series standards**, while power management applications are typically based on different standards: **IEC 62351**, "Power Systems Management and Associated Information Exchange – Data and Communications Security," and **IEC 61850**, "Communication Networks and Systems for Power Utility Automation."

Thus, when bringing secure industrial processes and power management systems together, it is important to understand the implications of such an integrated approach. Similarly, because AI often combines digital processes and digital power information to improve efficiency at mining sites, it is important to understand the concepts and scope of all these standards as they relate to each other.

Another important consideration is best practices, which are often incorporated into standards. Mine sites often play catch up when increasing their knowledge before setting and implementing best practices or challenging them with valid exceptions. This leaves the sites exposed. ISA and other standards incorporate best practices, but we have observed that best practices often suffer from the time pressure of daily operations. Also, AI use and security are evolving rapidly, so it is hard to keep up with new functionality and additional risk exposures.

ISA standards incorporate best practices, but we have observed that best practices often suffer from the time pressure of daily operations in metals and mining sites. Also, because AI use and security are evolving rapidly, it is hard to keep up with new functionality and additional risk exposures. Mine sites often play catch up when increasing their knowledge before setting and implementing best practices or challenging them with valid exceptions. This leaves the sites exposed.



After applying AI to create a model of an area, other layers can be added, such as future electric wiring (pictured here) or a conceptual hauling/charging infrastructure option.

Potential AI applications in mining/metals

Here we'll explore applying AI in the cloud or on-premises in these mixed environments. First, we'll review potential applications of AI technology and then we'll detail successful use cases implemented by members of ISA's Mining and Metals Industry Division. The latter illustrates that there is a lot to consider before implementing AI.

Exploration. AI-powered systems can analyze vast amounts of geological data to identify new mineral deposits. By processing geological maps along with satellite, magnetic, multispectral/hyperspectral and historical data, AI algorithms can identify potential areas for deeper exploration.

Challenges include data quality and availability and complex geography. Geological data can be sparse, difficult to collect or inconsistent. AI models rely on high-quality data, so ensuring accurate and comprehensive data collection is crucial. Different geological formations and structures pose challenges to accurate mineral deposit identification. AI algorithms must be trained to handle this complexity.

Predictive and prescriptive maintenance. AI can predict equipment failures by analyzing sensor data from mining and processing equipment, such as shovels, haul trucks, SAG and ball mills, motors and pumps. Detecting issues early enables planned maintenance instead of emergency repairs, which reduces downtime and improves operational efficiency.

A main opportunity for AI in this area is with protocol updates. AI can move analytics into the prescriptive zone where maintenance protocols are updated to prevent failures from happening. Challenges include:

- Sensor reliability: AI-driven, predictive maintenance relies on accurate, timely sensor data; therefore, sensor selection, calibration and connections must be well thought-out and reliable.
- Model calibration: Models must be calibrated periodically to adapt to changing equipment conditions. Regular model updates are necessary for accurate predictions.

Mineral recovery. AI can optimize mineral processing techniques, such as flotation, leaching and gravity separation. By analyzing process variables, AI can enhance recovery rates. AI machine learning models can predict optimal conditions for mineral separation and suggest processing parameters to operators that are superior to the parameters process control systems can recommend. The result is better yields.

Challenges include complex mineralogy. Different minerals behave differently during processing. AI models must be informed of and account for variations in mineral composition. Therefore, in addition to control variables for each unit, operation models must consider product management variables like hardness, density, chemistry and metal content.

Environmental factors. AI can monitor environmental factors, such as water quality, air pollution, vegetation health and noxious weed growth. It helps mining companies comply with environmental regulations and minimize their ecological footprint. An example is applying AI to multispectral data to identify the GPS coordinates of thistle plants, which are then loaded into a drone that spot-sprays each plant. This reduces the amount of chemicals sprayed in a given area. Challenges include:

- Data integration: Combining environmental data from various sources (sensors, satellites, etc.) can be challenging, and performing this without going back to a central server would add one level of complexity. AI systems must also be able to handle diverse data formats.
- Regulatory compliance: AI solutions must align with environmental regulations. Ensuring compliance while optimizing operations is a delicate balance, as hard and soft constraints must be part of these models and change over time as needed. This is easier for first-principles models than digital twins shaped through big data and learning models.

Energy optimization. AI algorithms can be used to optimize energy use in mineral processing plants by adjusting power consumption based on real-time electrical pricing, demand and production requirements. Improving the energy

efficiency of grinding circuits and mineral separation processes can contribute to cost savings. Challenges include:

- Model complexity: Energy optimization models can be complex. Intervening with such systems requires a deep understanding of practical challenges and regulations.
- Energy costs: AI systems in this space must adapt to changing energy costs as well as the ever-changing topology of energy systems, production schedules and constraints.
- Reaching production key performance indicators (KPIs): Adjusting power consumption in real-time can prevent starting or shutting down a mill to lower costs or carbon output.

Actual AI use cases

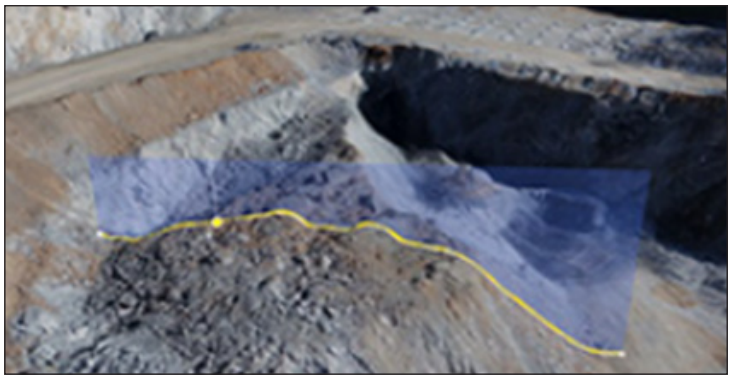
Now that we know some typical mining and processing applications where AI can be applied, here are three practical use cases from existing sites. In the first, we address using drones and AI to gather and analyze data. The second use case discusses AI applications using short-interval control to improve operational performance. The third shows how AI can be used to improve process efficiency.

Use Case #1: AI and data-gathering drones

Drone-based data is a valuable part of Industry 4.0, particularly in the mining industry. Its use is growing exponentially every year. With careful planning and governance, mining businesses can take full advantage of this powerful technology.

Data is collected by uncrewed aerial vehicles (UAVs), also called drones, using a variety of technologies and systems: photography, videography, photogrammetry, light detection and ranging systems (LiDAR), thermographic, multispectral, hyperspectral, magnetometry, ground-penetrating radar (GPR), and more. Drones are being manufactured with AI algorithms built-in to speed up and enhance the data collection workflow.

Mining companies are using AI to identify anomalies in high-resolution 3D images of their mine sites to prevent inefficiencies. For example, AI can quickly

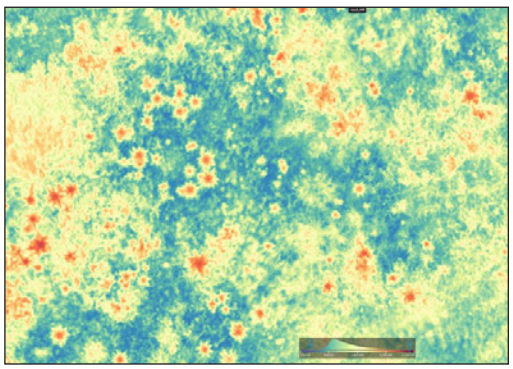


Data is collected by uncrewed aerial vehicles (UAVs), also called drones, using a variety of technologies and systems.

identify changes in the high walls of an open pit mine, helping hydrologists discover water incursion in unexpected areas using color and infrared imagery. Wet rock is generally cooler (occasionally warmer) than surrounding dry rock, which can show up as a sharp contrast in such imagery.

AI is also helping geotechnicians identify risks, such as boulders close to a crest posing a rock-fall hazard. The radar systems that capture ground movement activity cannot detect these situations, making drone-based imagery ideal for this application.

A key focus for mining companies is acting as a good steward of the environment they are operating in. AI is a key element in environmental monitoring as it can use multispectral data to identify noxious weeds like thistles and create a plan to execute drone-based spraying. Spot spraying each plant reduces the amount of herbicide used and associated environmental impacts and costs, which by itself is a great reason to use it. At the end of the mine lifecycle, multispectral data is used to assess desirable vegetation



To monitor environmental factors, AI can be applied to multispectral data to easily identify thistle plants from drone images They show up as red stars when using the NIR spectral band.

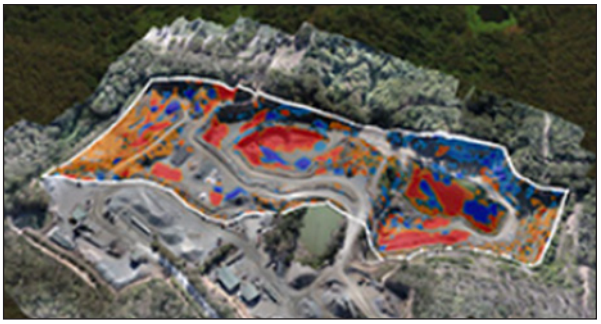
growth and health, which is valuable to regulatory reporting and rehabilitation programs and their assessments.

Cybersecurity is an important consideration for this use case. AI is used to process the 3D and multispectral data locally or load it to the cloud for processing, storage and analysis. To protect the data, miners need to ensure that the data is approved to go to the cloud, the cloud-based software providers are protecting the data and the providers' technology and governance practices are approved by the site cybersecurity team.

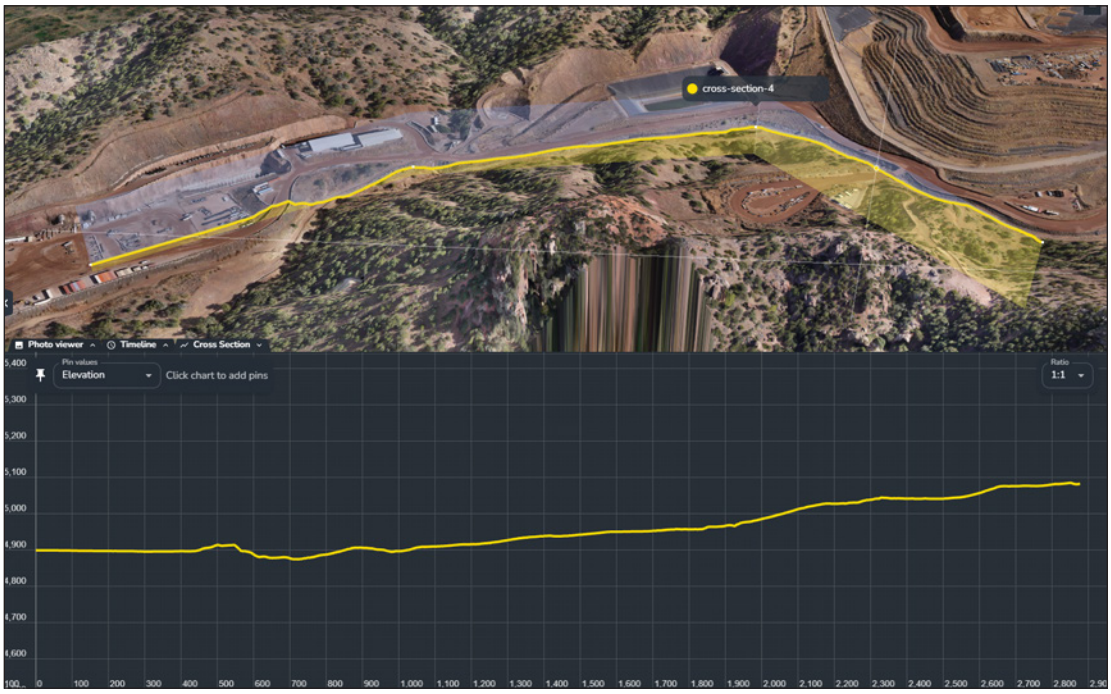
Additionally, data owners must allow access only to trusted team members and partners. Once data is in the cloud, it is easy to add users who can access that data. Policies must be in place to ensure only the necessary, approved personnel are allowed to access, change or combine the data. Others might be given read-only rights.

All mine-site employees should be trained on cybersecurity and data integrity best practices. The proliferation of AI applications and services opens the door to unsafe practices. For example, various vendors are selling AI services directly to mine-site employees, circumventing central procurement in the interest of speed or efficiency. Sometimes, those employees unintentionally engage these valuable providers without proper cyber reviews and protections.

Recently, an employee at a mining site was asked by a new vendor for a large dataset of their process control system for a demonstration of their AI capabilities. The employee almost sent the data over without proper reviews or permissions. Employees need to be reminded that production data can be valuable Intellectual property, as share price could highly depend on the metal content or sampling data.



This image uses AI to show volume changes supporting interval control and planning functions.



Drone-based data can be used to create a cross-section view showing changes in elevation.

Use Case #2 – Help for short-interval control

Short-interval control (SIC) is a management approach used in industrial and manufacturing settings to improve real-time operational performance. Here's a breakdown of what it involves and where AI is being applied. AI is everywhere.

Real-time monitoring. SIC focuses on monitoring and controlling operations frequently and regularly, often in intervals of hours or minutes. This allows for quick adjustments based on current conditions. For example, AI is used to reconcile the volumes of the hauling fleet.

KPIs. SIC relies heavily on predefined key performance indicators (KPIs) to measure performance against targets. These KPIs can include metrics like production output, downtime, quality levels and efficiency rates. In the past, these values were based on equations and first principles. These days AI is involved and is increasing accuracy.

Feedback loop. SIC involves creating a feedback loop where data on current performance is continuously collected, analyzed and used to

make immediate decisions. This helps identify deviations from expected performance and lets corrective actions be taken promptly. AI looks at many factors in the past to predict the future. Accuracy still varies, and closed-loop AI is still in its infancy.

Decision support tools. SIC often utilizes software tools and systems that provide real-time data visualization, analytics and reporting to facilitate effective decision-making. This enables machines, managers and operations to quickly assess situations and make informed decisions based on many smart sensors. Decision support tools combine local and central cloud-based AI for overall and suboptimization.

Continuous improvement. By focusing on short intervals, SIC promotes a culture of continuous improvement. It enables teams to learn from each interval, implement changes and evaluate the effectiveness of those changes in a relatively short timeframe. AI makes suggestions to assist with better decision-making and benchmarking at similar sites or across an enterprise.

Operational flexibility. SIC enhances operational flexibility by enabling agile responses to changing conditions, such as equipment failures, supply chain disruptions or changes in customer demand. Condition-monitoring systems often have local and global AI applied to them to prevent machine downtime.

All data and governance levels must be considered before AI can be trusted and applied for increased efficiency, safety and sustainability. However, SIC aided with AI is more successful in optimizing operational efficiency, minimizing downtime, reducing waste and improving overall performance through a structured, data-driven approach to real-time management and decision-making.

Use Case #3 – Help for improving processing efficiency

Mineral concentrating facilities are focused on throughput and grade recovery, which can be diametrically opposed objectives. This becomes a perfect optimization opportunity. This very complicated optimization problem needs to take into account varying ore types and how they affect the concentrate throughput and quality of product going out the door, versus going into tailings.

When one adds imperfect instrumentation (or a lack thereof), coupled with a very subjective understanding of how that ore can or should be processed, the result is a problem perfectly suited to AI big data solutions.

Big data can be used to establish historically derived relationships between the type of ore and the most likely processing strategies. These big data correlations can be supplemented with "underlying" fundamental models or even experiential learnings.

Implementation of real-time control using this AI big data approach is difficult because control networks seldom have this level of processing power. Then there are the additional cybersecurity risks associated with two-way business-network communication into the process network.

Today, there are implementations of such AI big data solutions in the business network that provide proven, advisory plant-control strategies to operations. However, such an AI-driven solution is not yet implemented in the process control network providing direct control of the plant processes. It will, at some point in the future, become a reality.

With the major risks of bad actors directly affecting people, equipment or the environment, the most significant concern with AI big data solutions the issue of cybersecurity. End-users are just not confident about the security of AI-based systems for direct control of plant processes today.

An AI-implemented plant advisory control solution can be more successful if KPIs are included that provide relevant feedback for continuous improvement of the AI. These KPIs should include the number of successful recommendations adopted by the plant; the established extent of the "success"; and the reasons why any of the advised strategies were not adopted. With an enhanced machine-learning model, this KPI-based feedback mechanism can create an adaptive, self-learning, self-improving AI model.

The Perdue model and standards

As indicated by the three cases we just covered, AI has many applications that can be applied to the control system architecture as described in the

Purdue Enterprise Reference Architecture (PERA). PERA, or the Purdue model, was developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing in the 1990s to model enterprise systems architecture.

Multiple standards—such as the **ISA 95** "Enterprise-Control System Integration" series of standards—use this architecture structure because the Purdue model provides a framework for segmenting industrial control system networks from corporate enterprise networks and the internet. The Purdue model is also used as a baseline architecture for industrial control system frameworks such as American Petroleum Institute **API 1164**, "Pipeline Control Systems Cybersecurity," and National Institute of Standards and Technology **NIST 800-82**, "Guide to Operational Technology (OT) Security."

The Purdue model is incorporated into the ISA/IEC 62443 standards as a model for industrial control system (ICS) network segmentation. The **ISA/IEC 62443** standards define six layers within these networks, the components found in the layers and logical network boundary controls for securing these networks.

The standards also describe the zones that typically contain the IT and the OT systems. It is that part of the standard that is going out of fashion somewhat, with control system technology now available in the cloud and enabled by some of the most trusted brands of process control companies. The standard also applies at the edge for local loop control and AI applications influencing local loop control—or stronger—setting and directing the controls.

The Purdue model might be considered outdated, but only partially. Defense-in-depth still leverages Purdue-model thinking without applying it to the physical implementation alone. Like AI, which exists in all the layers of the Purdue Model, security also needs to be layered. This concept of networking is called segmentation and is still very relevant today.

While the Perdue model sets a high-level architecture and can be seen as creating defense-in-depth practices, it doesn't prescribe detailed security principles and measures for each layer or describe how to handle AI applications. These are addressed in the following sections.

Secure AI for OT systems

Operational technology (OT) security is addressed in the ISA 62443 standards. These standards offer comprehensive guidance on security controls, risk assessment and strategies for securing conduits between zones. The ISA 62443 standards are submitted to the International Electrotechnical Commission (IEC) for global adoption as the international ISA/IEC 62443 standards. The ISA/IEC 62443 series of standards with use cases from more than 20 industries, including mining and metals, are endorsed by the United Nations.

The ISA/IEC 62443 series of standards have demonstrated their utility in all industry verticals that use operational technology. In 2021, IEC recognized the series as a horizontal standard, meaning that the standards have been proven to apply to a broad range of industries.

AI technology is built on computer technologies, which enables it to bring tremendous advantages to the mining industry through automated decisions and actions. It enables optimizing operational processes, improves health and safety, reduces environmental impact, and allows faster, more effective workforce training.

The following is the definition of AI systems from the Organisation for Economic Co-operation and Development "Recommendation on Artificial Intelligence (AI)" adopted in 2019 and **ISO/IEC 22989:2022**, "Information technology – Artificial intelligence – Artificial intelligence concepts and terminology":

> *An AI system is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.*

AI implementations technically reside in the information technology (IT) and OT domains. The solutions often bridge these domains when central AI assists or adds to local AI decision-making at the edge. Security solutions must be applied to all of these AI implementations.

AI-powered security solutions greatly improve cybersecurity defense capabilities to prevent, detect and respond to cyberattacks. For example, AI security solutions can analyze large volumes of events and signals for vast numbers of threats to identify, predict and detect potential cyberattacks.

AI security solutions also improve vulnerability management by applying AI to continuously monitor the exposed attack surfaces for risks and identify high-impact vulnerabilities. By raising early warnings, AI solutions enable security incident response teams to act early and prevent threats from entering the site or wider enterprise environment.

AI applications create new attack surfaces

There are also disadvantages to adopting AI technology. Notably, it increases the risks of cyberattacks.

Malicious actors can leverage AI tools to spread malware, steal information and exploit vulnerabilities. GenAI can create large volumes of personalized phishing attacks, and AI models can be manipulated through training to provide malicious decision recommendations. Hence, AI systems must be treated as extended attack surfaces of an organization.

AI system lifecycles are similar to those of non-AI software technologies (design, development, deployment, testing and operation) with an additional phase of model training. Therefore, AI systems are exposed to similar security risks.

There are additional risks associated with AI systems related to the trustworthiness of AI algorithms and model training. An automated AI system is only as good as the reliability and trustworthiness of its model and the secure implementations and practices of the many connected data sources.

AI implementations technically reside in the information technology (IT) and OT domains. The solutions often bridge these domains when central AI assists or adds to local AI decision-making at the edge.

To be successful in adopting AI technologies in an enterprise environment, an organization must secure the entire AI system lifecycle and should follow the NIST "Artificial Intelligence Risk Management Framework" to minimize security risks to govern, map, measure and manage AI risk. Refer to the NIST publication **NIST-AI-600-1**, "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile" for details.

In addition to the security controls outlined in the NIST Artificial Intelligence Risk Management Framework, refer to the **NIST "Cybersecurity Framework."** Unique security controls are required to protect AI models, data storage and application program interface (API) integrations to mitigate AI risks. The Australian Cybersecurity Center (ACSC) provides security best practices in adopting AI technologies at **Artificial intelligence | Cyber.gov.au**.

A conceptual AI architecture used in the mining industry is shown in the following diagram, where operational data is collected and sent to data analytic platforms for training AI models. The AI models are then downloaded into control networks to improve mining operational safety and efficiency.

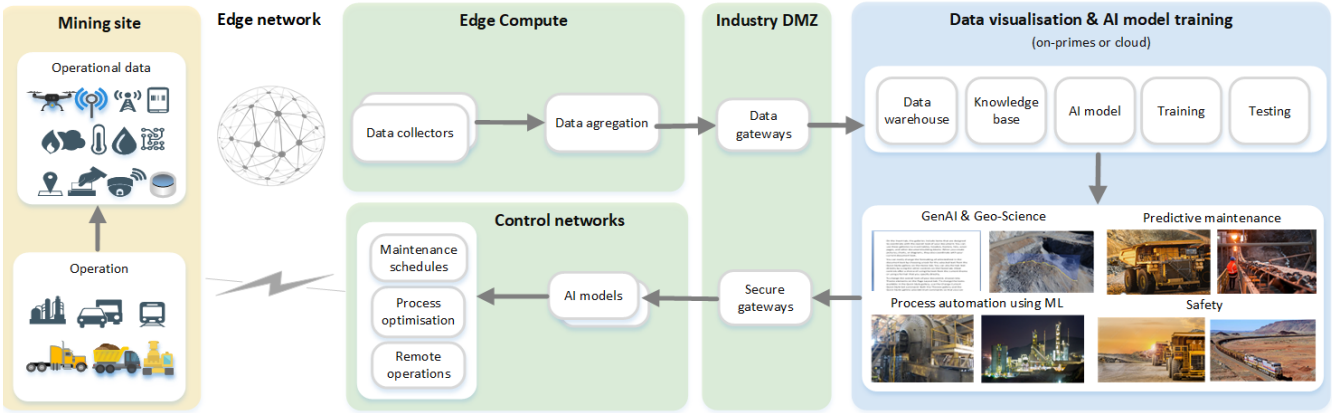
Security risk mitigation

The following sections highlight the security risks in three key applications of AI technologies in the mining industry and recommend key security controls to mitigate the risks.

Computer vision for operational health and safety. When applying AI technology to analyze truck driver behavior and monitor fatigue and equipment malfunctions, any error or inaccuracy in the AI analytical model can potentially cause human fatality. Therefore, the AI analytical model must be trained with reliable, nonbiased and up-to-date data in a secure environment.

The model must be updated regularly, securely deployed and regularly revalidated. If the AI system is developed and/or managed by a third party, the third party must be transparent about how the AI system is secured, trained and tested. It is important to define the ownership of risk and accountability clearly.

Conceptual AI Architecture used in Mining Industry



In this conceptual AI architecture, operational data is collected and sent to data analytic platforms for training AI models. The AI models are then downloaded into control networks to improve mining operational safety and efficiency.

The industrial internet of things (IIoT) is the group of common technologies used to collect required data/images to feed into AI systems. The reliability, performance and security of the end-to-end IIoT network communication must be ensured.

ML used in process optimization. When applying machine learning technology to optimize processes, such as crushing, loading, flotation and refining, errors or inaccuracies in the ML analytical model can potentially cause equipment damage and interrupt operations. Several security practices can help reduce security risks:

- The AI system should be deployed close to the control system location to reduce network latency and allow real-time data input into the ML model.
- When an ML system is integrated with an OPC server to provide recommended settings in the human-machine interface or directly control the settings in a programmable logic controller, authentication and authorization controls must be implemented. A safety threshold must be set in the control system to protect against an incorrect output from the ML model due to incorrect training or malicious data manipulation.

- When a control system setting is influenced by multiple control inputs, including an ML system, the ML system-generated output should not outweigh or dominate other control input decisions.
- Include manual intervention points between the ML and control systems to allow human intervention when the ML system functions abnormally.
- If the ML system also communicates with systems external to the OT environment to obtain updates, the communications must follow the security controls on authentication, authorization and encryption. Any downloaded ML model must undergo integrity validation and thorough testing for abnormal outcomes, well beyond the design thresholds.
- AI system input/output must be logged and monitored.

Natural language processing to improve productivity. Natural language processing (NLP) is used to analyze textual data from sources such as exploration reports, geological surveys and regulatory documents to extract insights and support decision-making processes. NLP relies on large language models (LLMs) that must access a huge amount of raw data from different sources.

Tech companies, such as Google, usually open source these big models for others to build on, but the data used to create the models and in-house data used to fine-tune them can affect model behavior. Hence, LLMs are prone to "hallucinations"—delivering inaccurate or conflicting responses due to errors in the training datasets.

There's also a risk that LLMs can be built without the necessary understanding of privacy and data confidentiality. Further, prompt-based models are insecure by design. Prompt-based models are vulnerable to prompt injection attacks, which are difficult to prevent or defend against.

The following security practices can help reduce these security risks:

- When in-house data is used to fine-tune LLMs, it must be validated to ensure accuracy and compliance with various regulations. The model training environment must be secured, access to data must be under privileged access control and data must be encrypted while being transmitted and stored.

- NLP tools must be thoroughly tested/scanned to identify any vulnerabilities.
- Any integration with external systems must be secured using secure APIs and communications. Ensure the external data source is trustworthy and secure.

Conclusion

Although AI brings tremendous benefits to many industrial operations, there are challenges when applying AI to the mining and metals industries. When integrating industrial systems with AI, it is important to understand the implications, best practices, risks and benefits of an integrated approach.

This paper outlines all the benefits and challenges, of AI and the use cases highlight the upside business opportunities and potential of the technology. Applying the standards mentioned should make governance easier and well-considered.

Addressing the challenges requires collaboration between mining companies, technology providers, research institutions and regulatory bodies to develop tailored solutions that meet the industry's specific needs and constraints. By overcoming these challenges, AI has the potential to drive innovation, improve competitiveness and foster sustainable growth in the mining sector.

All images courtesy of ISA MMID.

About the Authors

Bas Mutsaers is the director of the Mining and Metals Division (**MMID**) at ISA and is heading strategy, technology and marketing for mining, minerals and metals at Schneider-Electric. His co-authors are members of MMID.

Rob Zwick is manager of Process Automation Systems for Freeport McMoRan Inc.

Joanne Sun is principal security architect for BHP.

Mark Harris is principal adviser for Automation and Remote Vehicles for Rio Tinto.

Ismael Borrego is instrumentation and control engineer for South32.

Benefits and Challenges of AI in Mining and Metals

By Bas Mutsaers, Rob Zwick, Joanne Sun, Mark Harris and Ismael Borrego

ISA TECHNICAL RESOURCES

Explore the extensive range of authoritative technical resources available from ISA, meticulously developed and evaluated by industry professionals.

- **Books**
- **Digital magazines and ebooks**
- **Long-form technical articles and whitepapers**
- **Automation.com technical articles, news and insights**
- **ISA Interchange Blog**

Training

Improve efficiency and reduce downtime, maximize safety and security, fill in knowledge gaps, and develop your workforce with expert-developed, unbiased, and accredited training and certificate programs from ISA.

Standards

Streamline industrial processes and improve plant safety, cybersecurity, efficiency, and profitability by implementing ISA standards. Over 150 standards and guidelines reflect the work and knowledge of more than 3,000 participating experts worldwide.

International Society of Automation
Setting the Standard for Automation™

www.isa.org