IoT Security Maturity Model
Mining Extraction Profile

An Industry IoT Consortium® Whitepaper

2024-02-07

Authors

Lehlogonolo Ledwaba (Mandela Mining Precinct), Carel Kruger (Mandela Mining Precinct), Frederick Hirsch (Upham Security), Ron Zahavi (Auron Technologies)

Contents

FIGURES

TABLES

The start of the 4th industrial revolution (4IR), also known as Industry 4.0, has enabled significant technological advances in the global supply chain, introducing new and innovative IoT technologies to all sectors of industry. Industry 4.0 represents the merging and blurring of barriers separating various physical, digital, and vertical industries and application spaces. It is being driven by the disruptive technologies such as artificial intelligence, blockchain, the Internet of Things (IoT), quantum computing, Web3 and various other solutions reliant on the rise of data, connectivity, analytics, human-machine interaction, and robotics.[1] These technological advances are set to completely transform the entire supply chain and methods of operation for several sectors including mining.

The digitalization of the minerals extraction process is no exception, having multiple interconnected Internet of Things (IoT) devices working together in a Cyber-Physical System (CPS). This improves mine operation in a number of ways including increasing profitability, providing access to ore deposits which were previously uneconomical to extract, and meeting sustainability, safety and other goals.

However, digitizing the extraction process has resulted in a trend where several loosely coupled, bespoke systems are used for industrial process control. The complex nature and mission critical nature of these bespoke systems has raised concerns in the mining community about the security maturity of such systems and the possibility of losses if the security maturity is not adequate. Potential losses can include intellectual property, especially mining exploration data, impact of theft of business information such as pricing, financial consequences of operational shutdowns, potential harm to individuals or the environment (safety issues), equipment damage and harm to reputation among others. Losses can impact not only the mining companies and industry but even nations in which mining occurs[2].

Given the economic importance of the mining industry, security is an important consideration, especially given the escalating and pervasive occurrence of cyber security attacks. Risks must be considered to all aspects of the system, including governance, technologies, and operations. The Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM) helps organize and manage these concerns, enabling various stakeholders to communicate and determine appropriate maturity targets, assess the current status, and create action plans to address gaps.

---

[1] *https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir/*

https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir

[2] *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

The "IoT Security Maturity Model: Practitioners Guide"[3] defines the SMM and includes detailed general guidance, providing a foundation from which communities can consider their specific needs and concerns. They can extend the SMM by creating profiles which consider industry and device specific concerns.

This document, the "IoT Security Maturity Model (SMM) *Mining Extraction Profile*" is an industry profile extension that specifically focuses on the Industrial Internet of Things (IIoT) devices deployed in the mineral extraction aspect of a mining operation and is intended for the mining community. It draws on the detailed analysis conducted through collaboration of the IIC security and mining groups. This profile can also be extended or combined with other profiles as needed by communities that adopt it.

1 THE IOT SECURITY MATURITY MODEL

The goal of the SMM is to provide a path for Internet of Things (IoT) providers to know where they need to be, and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms. It seeks to help organizations identify the appropriate approach for effective enhancement of these practices where needed. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

An informed understanding of the risks and threats an organization faces is the foundation of choosing and implementing appropriate security controls. The model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

Not all IoT systems require the same strength of protection mechanisms and the same procedures to be deemed "secure enough." The organization determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementation of security mechanisms and processes are considered *mature* if they are expected to be effective in addressing those goals. It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity. Hence, *security maturity* is the degree of confidence that the current security state meets all organizational needs and security-related requirements. Security maturity is a measure of the understanding of the current security level, its necessity, benefits, and cost of its support. Factors to weigh in such an analysis include the specific threats to an organization's industry vertical, regulatory and compliance requirements, the unique risks present in an environment and the organization's threat profile.

[3] *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

Security level,[4] on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner. The SMM does not say what the appropriate security level should be; it provides guidance and structure for organizations to identify considerations for different maturity levels appropriate for their industry and system. It provides guidance for defining and accounting for different levels of comprehensiveness and alignment with industry sector and system, including non-industrial systems. Some users of the model will apply its guidance to create industry- and system-specific profiles, which can then be used by a broader audience, in concert with the model, to help assess maturity in a specific vertical or use case.

The audience for this document includes owners of IoT systems, decision makers, security leaders in various verticals, business risk managers, system integrators, architects, system testers, security maturity assessors, analysts, policy and regulatory authorities, and other stakeholders concerned about the proper strategy for the implementation of mature security practices tailored to the needs and constraints of the specific IoT system.

Those using the SMM should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements[5] and threat landscape, what is my solution's target maturity state?
- What is my solution's current maturity state?
- What is the prioritized action plan for addressing any maturity gap?
- What are the controls, including both mechanisms and processes, that will take my solution's maturity from its current state to its target state?

1.1 THE SMM PROCESS

Organizational business stakeholders define goals for the security posture of the organization and the systems it owns or operates. These systems may be brand new or brownfield. These goals should be mapped to objectives that tie to the risks. Technical teams within the organization, or third-party assessment vendors, map these objectives into tangible security techniques and capabilities, identifying the appropriate target security maturity state. Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture target security maturity states of systems and can act as templates for evaluating security maturity of a specific area of use, common use-case, or system of interest.

[4] *https://webstore.iec.ch/publication/7033*

[5] Namely, business or mission needs, requirements from regulatory authorities, and other similar factors.

1.2 UNDERSTANDING THE MODEL

Figure 1-1 illustrates the structure of the SMM and the breakdown of security maturity domains. *Domains* are the high-level views that capture the key aspects of security maturity: governance, enablement, and hardening. Each of the domains has different key aspects to it, called *subdomains*. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

This hierarchical approach enables maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

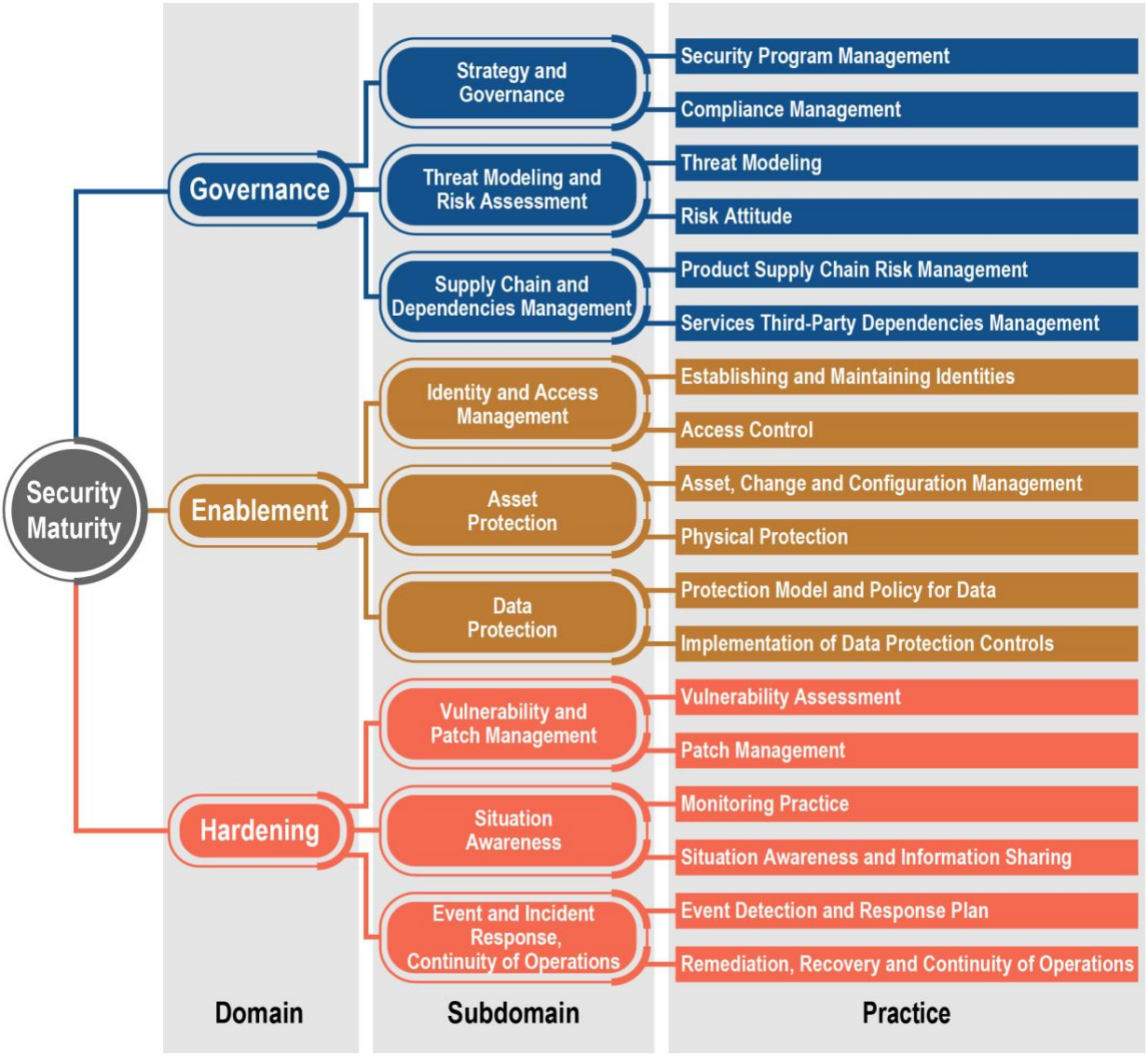

Figure 1-1: SMM hierarchy.

Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.	At the domains level, the stakeholder determines the priorities of the direction in improving security.
Subdomains reflect the basic means of obtaining these priorities at the planning level.	At the subdomains level, the stakeholder identifies the typical needs for addressing security concerns.
Practices define typical activities associated with subdomains and identified at the tactical level.	At the practices level, the stakeholder considers the purpose of specific security activities.

1.2.1 SECURITY GOVERNANCE

Figure 1-2 below describes the elements of the governance domain of the SMM.

The security governance domain is the heart of security. It influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation.	
Security strategy and the governance subdomain facilitates organizational drivers along with providing security, compliance with regulations, laws and contractual obligations. This also can relate to customer expectations and reputation management.	
Security program management practice is vital to the clear planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.	**Compliance management practice** is necessary when strict requirements for compliance with evolving security standards is needed.
Threat modeling and the risk assessment subdomain identifies gaps in specific configurations, products, scenarios and technologies and prioritize countermeasures accordingly.	
Threat modeling practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.	**Risk attitude practice** enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.

Supply chain and the external dependencies management subdomain aims at controlling and minimizing a system's exposure to attacks from third parties that have privileged access and can conceal attacks.	
Product Supply chain risk management practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.	**Services Third-Party dependencies management practice** addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.

Figure 1-2: Security governance.

1.2.2 SECURITY ENABLEMENT

Figure 1-3 below describes the elements of the enablement domain of the SMM.

The security enablement domain is based on established security policy and addresses the business risks using the best available means. Security policy and controls are subject to periodic review and assessment.	
Identity and access management subdomain aims to protect the organization and control the use of resources by the identified agents to reduce the risk of information leakage, tampering, theft, or destruction.	
Establishing and maintaining identities practice helps to identify and constrain who may access the system and their privileges.	**Access control practice** policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.
The asset management subdomain is put in place to protect both physical and digital assets. This is an area of strong collaboration between IT and physical security teams.	
Asset, Change and Configuration Management practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.	**Physical protection practice** policies address the physical security and safety of the premises, its people, and its systems to prevent theft and ensure the ongoing safe operation of equipment.

The data protection subdomain prevents unauthorized data disclosure or manipulation of data, both for data at rest, in transit and in use. This is important for security, privacy, regulatory compliance, legal and intellectual property protection.

The security model and policy for data practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.	**The implementation of data protection controls practice** describes the preferred application of data protection mechanisms to address confidentiality, integrity, and availability.

Figure 1-3: Security enablement.

1.2.3 SECURITY HARDENING

Figure 1-4 below describes the elements of the security hardening domain of the SMM.

The security hardening domain practices support trustworthiness objectives through the assessment, recognition, and remediation of risks with both organizational and technical countermeasures.

Vulnerability and the patch management subdomain policies and procedures keep systems up to date and less prone to attacks.

Vulnerability assessment practice helps to identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.	**Patch management practice** policy clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching such as patch security and update mechanisms and processes.

The situational awareness subdomain aims at understanding the current security state enabling an organization to prioritize and manage threats more effectively.

Monitoring practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.	**Situational Awareness and Information sharing practice** helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.
Event and incident response, continuity of operations subdomain implemented in a combination of policy and technical preparation allows an organization to respond to incidents swiftly and minimize disruption to the rest of the system.	
An event detection and response plan define what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.	**Remediation, recovery, and continuity of operations** represent a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.

Figure 1-4: Security hardening.

1.3 APPLYING THE MODEL

Two aspects are essential for measuring the maturation progress of IoT systems and prioritizing associated security practices: comprehensiveness and scope. These are considered within the context of the target and assessment, namely the system of interest, whether end-to-end, a component or a sub-system under consideration.

Comprehensiveness captures the degree of depth, consistency and assurance of security measures that support security maturity domains, subdomains, or practices. For example, a higher level of comprehensiveness of threat modeling implies a more automated systematic and extensive approach.

Scope reflects the degree of fit to the industry or system needs. This captures the degree of customization of the security measures that support security maturity domains, subdomains, or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

1.3.1 SCORING AND PRIORITIZATION

Any rigorous security self-assessment procedure, including the SMM, needs a scoring and prioritization method to enable evaluation of the current state and the development of a metrics-based security strategy.

Comprehensiveness and scope, which are orthogonal, help score and prioritize security maturity practices. Certain IoT systems may not require the highly sophisticated or narrowly scoped implementation of all security practices. Such implementation may be over-engineered, given the particular system, and the threats that it faces. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

1.3.2 COMPREHENSIVENESS LEVELS

There are five comprehensiveness levels for every security domain, subdomain, and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree of comprehensiveness of security controls. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones.

- Level 0, None: There is no common understanding of how the security practice is applied and no related requirements are implemented. (As this is null, we shall not discuss it further).
- Level 1, Minimum: The minimum requirements of the security practice are implemented. There are no assurance activities for the security practice implementation.
- Level 2, Ad hoc: The requirements for the practice cover main use cases and well-known security incidents in similar environments. The requirements increase accuracy and level of granularity for the environment under consideration. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks. For this assurance, application of measures learned through successful references may be applied.
- Level 3, Consistent: The requirements consider best practices, standards, regulations, classifications, software, and other tools. Using such tools helps to establish a consistent approach to practice deployment. The assurance of the implementation validates the implementation against security patterns, design with security in mind from the beginning and known protection approaches and mechanisms. This includes creating a system with the security design considered in the architecture and design as well as definition defaults.
- Level 4, Formalized: A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. For this assurance, a more complex approach is applied that uses semi-formal to formal methods.

1.3.3 SCOPE

The scope measurement captures the extent to which the specifics of an application, network or system of interest are taken into account during the implementation of the security facet.

There are three levels of scope for every security domain, subdomain, and practice, from Level 1 to Level 3, with higher numbers indicating a narrower and more specific scope. The appropriate scope(s) will depend upon the system and scenarios. Note that in some cases there may be both industry specific and system specific scope considerations in addition to general considerations.

- Level 1, General: This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific IoT sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.
- Level 2, Industry specific: The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sector-specific issues, particularly those regarding components and processes that are prone to certain types of attacks and known vulnerabilities and incidents that have taken place.
- Level 3, System specific: This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

1.3.4 SMM TEMPLATE

All IoT devices, networks and systems do not require the highest comprehensiveness and scope for all security domains, subdomains, or practices. The security maturity target for the system of interest is defined as the set of all desirable values of comprehensiveness and scope characteristics for every security maturity domain, subdomain, and practice.

In case of insufficient details about the system-security needs the stakeholders may initially determine the target levels of comprehensiveness and scope just for domains. These levels determine the relative priorities of security governance, enablement, and hardening. The levels set for the domains will be inherited by the appropriate subdomains and then by the practices according to the hierarchy. The stakeholders may modify the levels to match the risks more closely. This is helpful for the step-by-step recognition of an uncertain security maturity target.

The security maturity target by default is defined when referring to the comprehensiveness and scope for security maturity practices as seen in The Security Maturity Model Practitioner's Guide. [6]

Each practice table has four columns, one for each comprehensiveness level. The objective in each level describes the general considerations that should be met. Guidance is provided in the

[6] *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

form of general considerations.

	Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>

Table 1-1: SMM template.

1.4 Security Maturity Profiles

The SMM is designed to be extensible across a wide array of industries and systems. It addresses the general scope, which looks at common security maturity best practices in the industry. There is an opportunity to add industry-specific and system-specific scope to any or all of the practices.

The IIC will collaborate with a wide range of industry groups to encourage development of profiles—practice tables that go beyond general scope and include industry- and system-specific requirements for different comprehensiveness levels. For example, a retail group may create profiles of some or all practices that include best practices and regulatory requirements specific to the retail industry; they may also create system specific profiles for commonly used devices such as card readers or security cameras. A health care profile may include specific guidance related to *HIPAA*, while a system-specific profile could address considerations for, say, *FDA* pre- and post-market guidance for implanted medical devices.

Industry and system profiles need not be created for every practice in the model. An industry may decide that the general scope is sufficient for most of the governance-related practices but that a few of the enablement practices necessitate an industry-level point of view. When extending for industry or system-specific considerations, the practice table as seen in Table 1-2 expands to include two additional rows. Where appropriate, cells may have no content and may be marked as having no content.

<Practice Name>				
<Practice Description>				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	<List of Level 1 industry specific considerations>	<List of Level 2 industry specific considerations>	<List of Level 3 industry specific considerations>	<List of Level 4 industry specific considerations>
System-specific considerations	<List of Level 1 system specific considerations>	<List of Level 2 system specific considerations>	<List of Level 3 system specific considerations>	<List of Level 4 system specific considerations>

Table 1-2: Template with industry and system specific considerations.

Industry-specific considerations include the sector-specific issues, particularly components and processes that are prone to certain types of attacks, known vulnerabilities, incidents that took place in similar systems and possible harm to this kind of operational technology as well as sector specific priorities including legal and regulatory guidance.

System-specific considerations include the specific security-relevant business needs and risks for the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios that combine the general and domain-specific objectives in a unique manner.

This mining extraction profile provides considerations at the industry-specific scope.

While the general row in the table included headings for achieving the level and indicators of accomplishment, the industry row should include a general description of the industry-specific issues as noted above and for a comprehensiveness level with industry-specific considerations:

- what needs to be done to achieve that level, and
- relevant industry guidelines for that level, and
- indicators of accomplishment that can assist assessors in identifying if the organization has met the requirements of the level.

Similar information should be provided when system-specific scope guidance is provided.

2 MINING EXTRACTION SECURITY CONSIDERATIONS

2.1 MINING EXTRACTION METHODS

Mining can be defined as the action of extracting high concentrations of minerals called ore from the earth. For the purposes of this SMM, underwater mining is excluded from the definition. Ore bodies are usually contained inside a rock mass and are only extracted after exploration has indicated that enough ore is available for economical extraction after which a mining operation is established.

Mining extraction methods include surface and subsurface mining; with the method used depending on the value of the ore. Surface mining is used to extract mineral resources of lower economical value due to the reduced cost of extraction, while subsurface extraction takes place for valuable minerals where the additional cost of extraction is justified.

Surface mining operations include open-pit, quarry, and strip-mining methods where ore is extracted from the earth`s surface moving downwards or sideways into the ore body. Surface mining results in a pit or open strip of soil which increases in depth or length as the ore is extracted. Surface mining makes use of large excavators, conveyors, explosives, and dump trucks to move ore to either an intermediate storage site or directly to a crushing unit which is the first point of processing for most mining extraction operations.

Subsurface mining can be categorized based on the type of rock the ore is mixed with and is identified as either hard-rock or soft-rock mining. Hard-rock mining includes the extraction of precious metals such as gold, silver, lead, and copper, but is also used for gems, rubies, and diamonds. Hardrock mining primarily makes use of “stope and retreat” as well as the “stope and fill” methods to loosen and extract ore where the decision to either replace the removed rock or leave the cavity open is the differentiating factor.

Soft-rock mining usually deals with the extraction of coal, oil sands, potash, and salt. Popular methods for soft-rock mining include longwall mining as well as room and pillar mining. Longwall mining is the process of extracting a long continuous vertical section of ore using a longwall machine. The cavity produced at the back of the longwall mining machine is allowed to collapse after the machine has advanced. Room and pillar mining extracts ore by creating cavities while leaving pillars behind to support the hanging wall. The size and frequency and general pattern of the pillars depend on the load bearing capacity of the material above and below the pillars.

Access to an underground mine can be obtained via a decline, vertical shaft or Adits; the type of access used to be determined by the depth of the ore. Decline access is where a vehicle makes use of a roadway declining into the mine; like the inclines and declines found in multi-story parking lots. Vertical shaft access is used for deep ore extractions and uses a hoist and wheel system to lower and raise a cage up and down a vertical shaft. The cage is used to transport miners, and equipment in and out of the mine with ore transported using skips. Adits are

horizontal tunnels bored directly into the side of a hill or mountain and allow for horizontal access to an ore body located above the ground level inside a hill or mountain the Adit is driven into. A horizontal shaft inside a mine is called a level or drift.

The type of access to a mine mostly dictates the type of equipment used to transport ore from the stope to the first point of processing above ground, but exceptions do occur as not all mines are the same. Aboveground mining operations make use of large purpose build excavators and trucks to extract and transport ore. Conveyor systems may also be used to transport ore over longer distances or where the terrain is suitable for conveyor-based transport in automated mining operations. In decline access mines ore is removed using a load haul dump (LHD) vehicle and transported to the surface using the LHD or other types of trackless mobile machines (TMM).

Underground decline access mining machines are purposely built to be as low as possible. These machines look like smaller, flattened versions of the aboveground counterparts to fit inside the low height stope cavities. In vertical access mines, blasted material is moved around using a scraper and dumped into a mine wide rail system used to transport miners, equipment, and ore to the shaft. Initial crushing may occur below ground to reduce the ore size to more manageable, transportable sizes before the ore is transported above ground via the skip or a bucket system to the mills where further processing will occur.

2.2 Mining Ecosystem, Architecture and Risks

The mining ecosystem is a collection of various processes and industries working towards the goal of ore extraction and processing. With the numerous processes required for a successful mine, comes many interconnected networks and devices. This also brings with it changing security requirements within each zone of the mining architecture to ensure adequate protection, reliability and availability of data exchanged between devices and end users within the network.

Automation in the mining industry is increasingly looking towards the use of Industry 4.0 technologies, such as the internet of things, artificial intelligence, analytics, robotics etc., to improve efficiency and safety within their operations[7]. With ore reserves becoming increasingly more difficult to locate and extract safely the impact of attacks on mining extraction can have great consequences, especially when considering the reliance on mining activities as part of the economic development of various countries. The introduction of internet-connected devices within the operational technology space brings with it new vulnerabilities and threats that can impact the safety and effective operation of a mine, increasing the risks that can result in these greater consequences.

[7] *https://miningdigital.com/smart-mining/mining-40-how-innovation-shaping-mines-future*

Figure 2-1: The industrial mining operations landscape. (Artist: Kgabo Chuene)

Generally, typical mining operations would be divided into approximately eight main zones; with increasing availability of network processing power, storage, and internet connected devices. Figure 2-1 gives a general breakdown of the industrial mining architecture as visualized by CISCO[8].

At the lowest level of the architecture, the extraction zone, more resource constrained devices are employed, such as sensors, worker monitoring devices, environment monitoring devices, GPS/localization devices, autonomous vehicles, industrial switches, etc. These devices tend to be numerous in number, easily accessible, easily deployed and heavily reliant on industrial broadcast communications protocols such as ISA100 and WirelessHART[9]. This makes them susceptible to more physical types of security threats such as tampering, insertion of rogue nodes, and removal/destruction. Issues of interoperability between the communications and networking technologies could also expose areas of the mining network which are intended to be protected.

Integration and interaction of other safety critical systems within the mining sector such as fire, fall-of-ground could unintentionally lead to the introduction of previously unknown security vulnerabilities. Fall-of-ground (FOG) within mining is the class of events related to the movement of rock mass or release of rock into the mine opening as either a controlled/intended or uncontrolled/unintended operation and causes injuries that are “the most prevalent occupational injury in the South African mining sector.”[10] It is important to adequately address the issues of integration and interoperability within the mining extraction space so that mining extraction operations are protected from the unintentional exposure of sensitive OT systems to cyber threats.

[8] *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

[9] *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

[10] *https://link.springer.com/article/10.1007/s10706-021-02023-3*
https://www.mosh.co.za/falls-of-ground/summary

Of the many cyber security threats, the broadcast nature of the communications infrastructure makes the extraction zone susceptible to eavesdropping, man-in-the-middle (MitM), and Masquerade attacks. A lack of integrity in the exchanged data within this zone therefore affects the overall safety of the extraction process and endangers the lives of the miners working in that area.

Similar devices can also be found within the crushing, processing, smelting, and refining zone of the mining process along with the inclusion of more heavy-duty switches and servers to handle the information exchanged by the Supervisory Control and Data Acquisition (SCADA) network and devices such as crushers, refiners, and smelters. At this level of the architecture, we see the addition of some of the main operations technology devices which have previously been siloed or air-gapped away from other mining operations as a means of protection from security threats. The addition of internet capability within this zone of the mining process allows for more real-time updates and adjustments to be made towards improved output, but it also brings with it larger threats to availability and confidentiality. Physical damage may also be done to the machinery as acts of sabotage should the controllers or any of the human-machine interfaces be infected or affected by a malicious attack.

Some of the more vulnerable devices and systems that are found within the ore extraction and processing zones of the mining architecture include but are not limited to:[11]

- Autonomous haulage systems
- Camera networks
- Collision avoidance and geo-fencing systems
- Command and control systems
- Communications infrastructure
- Conveyor belt monitoring, control, and communications systems
- Dewatering pumps
- Distributed control systems
- Emergency refuges
- Environmental sensors
- Firefighting systems
- Hoist equipment
- Internet connected Human-Machine Interfaces for Industrial Control System (ICS) devices
- Miner tagging systems
- Motion sensors or accelerometers on automated drilling equipment
- Non-ICS devices as entry points into the mining network
- Power distribution networks
- Precious metal vaults
- Process and wastewater treatment systems

[11] *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

- Process knowledge systems
- Programmable logic controllers (PLCs)
- Remote terminal units
- Remotely controlled dozers and excavators
- Sonar, electromagnetic, radar and vibration sensors
- Tailings pile stability monitors
- Ventilation systems

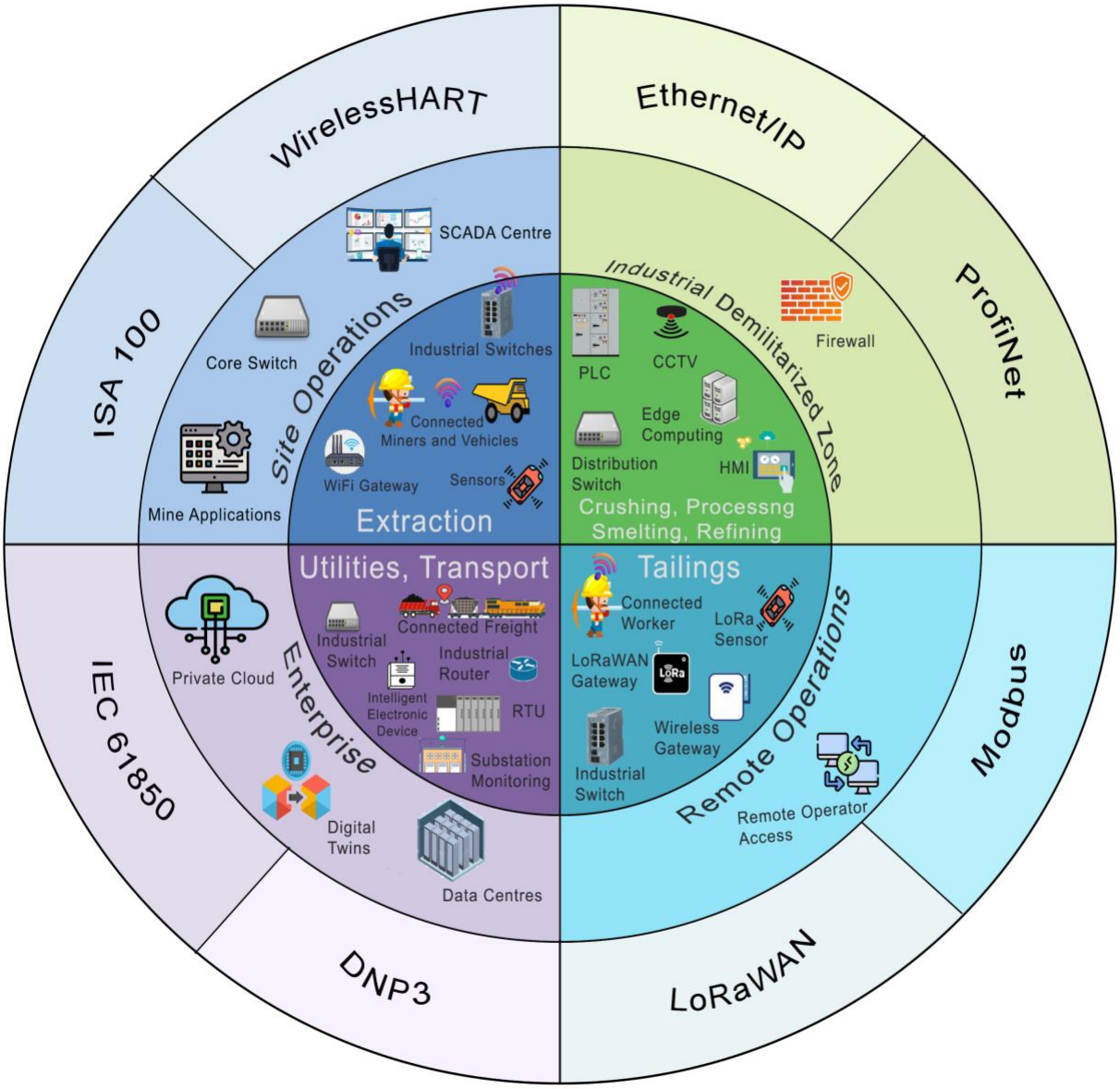

Figure 2-2: The automated mining device landscape.[12]

[12] *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

The resource restrictions on the devices within the extraction and processing zones, the openness of the communications infrastructure, the scale of the deployment and accessibility of the devices make them highly desirable targets to cyber-physical attack. Mining operations are also seeing themselves as targets of attack from actors such as competitor mining houses, organized cybercriminal organizations, environmental hacktivists, terrorists, and foreign nation states.[13] Through eavesdropping attacks on worker, autonomous vehicle and localization sensors within the extraction zones, mines could experience theft of geological exploration data and a loss of confidentiality on real time status updates on mining operations while more active man-in-the-middle attacks could result in malicious alteration of environmental and ore reserves data, unauthorized manipulation of automated equipment, and a disruption to mining operations and monitoring systems through denial of service/flooding attacks. Insiders may also damage or tamper with monitoring devices both on their persons or in the mining tunnels to circumvent seemingly cumbersome safety procedures, to disguise a work inefficiency, or remove evidence related to compliance, environmental or other concerns.

At the processing and refinement zones, a compromise of the human-machine interfaces could lead to unauthorized access to SCADA systems and devices (such as PLCs), which allow malicious actors insight into proprietary refinement environment settings and techniques (resulting in intellectual property theft) or unauthorized control of processing machinery (resulting in damage to refinement equipment and a disruption to the supply chain and mining operations). Malicious data alterations to equipment settings and instructions could also result in damage to refinement equipment or the ruination of the processing ore.

Besides the vulnerability of the equipment found and utilized in the mining process, other architectural considerations need to be made taking into consideration the physical nature of mining sites and their base of operations. In South Africa, for example, mine extraction sites may not necessarily be located within close proximity with the control center and processing locations. This requires ore to be moved by means of road transportation and communications between the extraction sites, processing, and control centers need to be able to send mining data across large physical distances while maintaining confidentiality and integrity. In some instances, these records and data are captured either on physical paper records or on some form of removable media. Management on the use of removable media with mine extraction related

[13] *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

https://www.pwc.co.za/en/assets/pdf/threat-advisory-manufacturing-mining-sector.pdf

https://www.bsigroup.com/globalassets/localfiles/en-za/mining/mining-cyber.pdf?utm_source=website&utm_medium=AfricaMining&utm_content=PDF&utm_campaign=ZA-Information-Security-Mining-2021

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/cyber-risk-in-mining.pdf

systems needs consideration, with the intentions of upgrading to secure network interconnectivity with growing maturity where appropriate, as well as techniques to guarantee the continuous protection of confidential information as records move from paper captures to a more mature, paperless environment.

The role that environmental factors play in the provision of security and the implementation of security mechanisms also need appropriate consideration. Within the mining stope, there can be high levels of dust, humidity, low light, flammable and corrosive gases, and high temperatures. This means that operation of IoT devices employed within the mining space could be compromised, not by malicious actors or any physical tampering, but by the operation environment itself. Issues with biometrics failures owing to dust, incapacitated cameras and optical devices owing to high levels of heat and humidity, failures of sensor devices which do not have a properly sealed enclosure for the mining space are a few examples.

Other than environmental conditions within the excavation (stope), adverse weather conditions could also have an impact on the safe operation of IoT technologies within mining extraction. While not susceptible to many natural disasters, South Africa for example, and especially the Highveld area in which most mines are located, experiences lightning storms and flooding during the rainy season which can compromise the electricity supply to safety-critical systems or may take down communications networks within the mine; leaving the network open to attack. The Highveld also experiences ground tremors because of the many years of mining activity, which could trigger safety events in mines. IoT devices would need to be protected against these seismic events to continue operation to evacuate the miners efficiently and effectively without causing an overcrowding or stampede event.

2.3 SMM Mining Extraction Profile Scope

The minerals extraction profile focuses on above ground as well as below ground mining and does not differentiate between the type of ore extracted or the mining method applied, but rather on the commonalities and differentiators between mining methods relevant for assessing the maturity of security mechanisms.

The system context for the mining ore extraction SMM is thus defined as all equipment, personnel, software, and supporting infrastructure which operates in the ore extraction zone of the mine. It also includes the control room and any communications infrastructure required for the control room operators to monitor and control equipment, personnel and supporting infrastructure inside the ore extraction zone.

The ore extraction zone of the mine is defined as a demarcated zone either above or below ground where additional physical safety precautions are implemented due to the danger posed by using heavy machinery or experiencing environmental conditions such as rockfall. The boundary of the ore extraction zone is thus the first location where additional safety requirements are physically enforced by restricting unauthorized access and requiring the use of

specific personal protective equipment (PPE) before entering. The boundary of the ore extraction zone for below ground operations is thus defined as the entry point to the decline or vertical shaft used to access the mine. The ore extraction zone boundary for a surface mining operation is defined as the point where extracted ore is transported and offloaded at the first point of processing using either truck or belt-based transport.

Major equipment in a mine that operates on electricity includes large autonomous and semi-autonomous grinding mills, ball mill drives, conveyor belts, high-pressure grinding rollers, cyclone feed pumps, mine hoists, dragline excavators, crushers, shovels, bucket wheel, dewatering pumps, ventilation fans, and bucket chain excavators.[14]

Owing to this unique combination of cyber and physical threats brought about by the combination of operation and information technology, the scope of this security maturity model will be limited primarily to the extraction and processing operations of the mining architecture and the associated devices and connectivity technologies that are utilized in those spaces. The higher levels of the mining architecture do not present any unique characteristics not already covered as part of the original security maturity model, which can be applied as-is to set maturity targets, assess and improve the security maturity of mining enterprise operations.

3 PROFILE TABLES

The following tables add the industry and device scope to the general SMM considerations as appropriate.

3.1 SECURITY PROGRAM MANAGEMENT

Cyber security management in mining operations is currently not formally managed across the various mining companies in a unified and standard method. This also tends to be a more formal focus of the IT systems implemented at the head office. At the mine sites, the mining engineers are responsible for the management of security programs but their focus is generally on the operational aspects of the mining devices and not necessarily on cyber security as they lack IT/cyber security skills.

[14] *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

Security Program Management				
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Identify the current state of mining security for safety audits	Establishment of IIoT security training as part of SHEQ (Safety, Health, Environment, Quality) qualification and onboarding	Establishment of organization-wide security training and compliance requirements	Automation of IT/OT security training and certification with refreshers through all levels of the mining organization.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Assessment and comparison of current state of security and policies existing within organization and industry as part of mine safety assessments. Security program management is the responsibility of the IT department (based at head office) and is only reported quarterly at audit and risk committee meetings. Management of	Implementation of security training as part of safety OHSA onboarding. Security program management focuses to include IT and OT systems implemented at mine sites in addition to IT systems implemented at mine head offices. Security program management at local mine sites conducted by cyber-physical security specialist with reporting at audit	Development and implementation of organization wide security programs, training, and compliance with international security and safety standards for control, mining, and embedded systems. Mines implement available security standards and frameworks (e.g. ISO 27000 series, NIST Cyber Security Framework) with appropriate security controls (e.g. Center for Internet Security	Adoption of IT & OT security training software with standard certification and periodic reminders at all skill levels within mining companies which is implemented and coordinated across all mine sites with monthly reporting to mine site managers and head office cybersecurity management teams.

	security program at mine sites is done by mine engineers if implemented.	and risk committee meetings.	(CIS) Critical Security Controls (CSC)) for measurement, monitoring and reporting.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Safety inspection documentation would have indications for state of security and security policy within the mine as part of safety compliance certification.	OHSA certification and compliance by end users will include basic competence levels from security awareness training.	Mines assessment for international standard compliance (e.g. ISO 27001, ISO 99, NIST 800, CIC CSC).	IT/OT security certification training, compliance offered 24/7, 365 with autonomous, periodic refresher courses for various skill levels within and across the mine sites.

Table 3-1: Security program management.

3.2 COMPLIANCE MANAGEMENT PRACTICE[15]

The mining industry must adhere to various regulations and laws as part of their operational processes. These regulations vary from country to country, and, for the mining companies, compliance is dependent on the issuing and maintenance of an operational mining license. A detailed example of some of these compliance regulations as related to the South African mining industry are given in Annex C.

[15] *https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/overlay-repository/nist-developed-overlay-submissions/industrial-control-systems*

Compliance Management				
This practice is necessary when strict requirements for compliance with evolving security standards is needed.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Mining companies establish and maintain internal rules and policies for compliance management, with specific considerations to maintaining health and safety standards.	Identification and compliance with all local regulations related to mining and mining security.	Identification and compliance with all regulations related to mining and mining security within all countries where the mining house is listed on the stock exchange. Dedicate manpower and manhours to ensure and maintain regulatory compliance through all levels of the mining organization.	Employ automated tools for compliance assessment, regulation monitoring, breach reporting and frequent report generation within compliance departments.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Daily reports and checks are conducted in house to ensure that health and safety rules and regulations are being upheld with a zero-tolerance attitude towards mining related deaths.	Mining companies are to establish and publish regulatory frameworks detailing requirements, benefits, and objectives of compliance with local regulators as part of their operational procedures.	Mining companies are to establish and publish regulatory frameworks detailing requirements, benefits, and objectives of compliance with regulators in all operational countries as part of their compliance procedures, highlighting key differences from local regulations.	Mining companies employ the use of compliance management software solutions to assess, track, and flag mining and environmental regulation and compliance requirement changes across jurisdictions with provision of autonomous maintenance of

			Develop compliance departments with appointed managers for each departmental level to highlight key legislation with potential impacts, track and update regulatory changes, establish compliance policies and procedures, and engage with assurance providers and a local and international level.	mining license renewals.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Health and safety (SHEQ) documentation is captured daily and audited internally for any potential violations.	Mining companies produce documentation of operational procedures illustrating compliance with local regulations (including training strategies and reporting responsibilities) regarding security to obtain and maintain a mining license.	Mining companies produce documentation of operational procedures illustrating compliance with regulators within all stock exchange listed countries (including training strategies and reporting responsibilities) regarding security to obtain and maintain a mining license. Dedicated compliance management activities are implemented at various levels of	Compliance department reporting to include more detailed statistics, active regulatory monitoring, and frequent reports back to stakeholders and board of directors as to the compliance health of the mines across operations in various jurisdictions. Regulatory compliance reports are made continuously available by

			mining operations to track compliance and ensure requirements are up to date as part of the mine's annual reporting.	compliance department to mining regulators in all operational countries for autonomous renewal of mining licenses.

Table 3-2: Compliance management.

3.3 THREAT MODELING PRACTICE

Threat Modeling				
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Identification of unsafe/insecure behaviors in mining operations (including contractor behavior) which could lead to security vulnerabilities being introduced.	Perform threat modeling of critical mining devices and machinery.	Implementation of international standards for security and threat modelling in mining operations.	Introduction of autonomous threat and vulnerability detection software solutions and artificial intelligence models for mining operations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Identification and flagging of common user behaviors leading to security vulnerability within the mines. Identification and flagging of common devices introduced by contractors which lead to security vulnerability within the mine.	Identify highly critical devices and machinery within the mining ecosystem ('Crown Jewel' Devices) and associated security threats in terms of AIC triad for patching, access points, connectivity, and user behavior.	Threat assessment procedures and policies developed in guidance by NIST 800, ISO 62443 and other appropriate security standards for industrial control systems.	Adoption of autonomous threat detection and vulnerability scanning software within the mining edge and organizational structure (e.g. operational security software). Use of AI-enabled software as appropriate.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Identified common devices introduced by contractors and user behaviors leading to security vulnerability included as part of regular reporting.	Documentation of threats against highly critical devices and machinery, the number and location of restricted access points within highly critical machinery is regularly generated and updated.	Implementation of threat assessments standards are evaluated by compliance officers with appropriate certification issued.	Reporting by autonomous threat detection software is generated in real time with alerts issued for highly critical incidents with suggested mitigation actions, associated risk, vulnerability detected, and time period by which mitigation should occur.

Table 3-3: Threat modeling.

3.4 Risk Attitude Practice

Risk Attitude				
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Identification and establishment of local regulations regarding risk management in mining.	Establishment of industry-recognized risk management methodology to minimize risk as much as practical.	Adoption of international safety risk management standards in mining related operations e.g. operation of autonomous mining machinery, risk management of unmanned, drivable vehicles, managing and maintaining gas/FOG detection devices.	Establishment of autonomous risk management tools and controls that apply international standards for safety risk management in mining operations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Risk management controls identified and implemented should satisfy local regulatory requirements.	Apply industry recognized standards, guidelines, and practical methods for showing appropriate risk management.	Establish and maintain a safety case for the mining operation including a preliminary case, an interim case, and an operational case.	Implementation of software-based risk controls implementing with international standards for safety risk assessment.

		Ensure equipment is being used as intended and that the standard enables risk reduction to as low a level as is practicable and practical.	Conduct business impact analysis of associated risks within the mining industry and capture as part of the risk management documentation.	Ensure vendor certification according to international standards such as ISO 13849 or ISO 19014-4 (ISO 2015, ISO 2020). Utilize software risk and safety control schemes such as software development lifecycle, unified software languages and operating environments.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Local risk regulation compliance certificates	ISO certificate of compliance	Comprehensive safety cases for mining operations are captured, regularly updated, and audited along with business impact analyses.	Development and implementation of a comprehensive and complete software-based risk and safety management plan. Implementation of testing methodology and appropriate document completeness, and competencies of software development and maintenance personnel.

Table 3-4: Risk attitude.

3.5 PRODUCT SUPPLY CHAIN RISK MANAGEMENT PRACTICE[16]

Within the overall mining context, supply chain management needs to consider all operations stemming from procurement of product for mining quarries all the way to the selling of mined ore to end users. This overall process includes planning, implementing, and monitoring day to day operations within the mine to procure adequate materials and machinery to support mining operations, increase visibility, improve time management, and achieve the quickest and highest quality delivery to customers.[17]

In the mining supply chain, providers are external to the mining house and could be suppliers of raw materials, partially finished or fully finished goods that support mining and processing of ore. While mining has four main sectors in which supply chain is a main driver of operations, as this SMM profile is focused on the extraction layer of mining operations, we shall consider supply chain operations related to exploration and extraction within mining.[18]

Currently, there is no formal third-party risk management procedure implemented for mining equipment as the focus of existing procedures is on IT systems from IT vendors. This forms a vulnerability as involvement from head office is occasional and mining engineers lack the IT and cybersecurity skillset to be able to review procured devices thoroughly and accurately prior to introducing them into the mine environment.

[16] *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/dttl-er-mining-how-secure-is-your-supply.pdf*

https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/mining-metals/ey-top-10-business-risks-and-opportunities-for-mining-and-metals-in-2023.pdf

[17] *https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/mining-metals/ey-top-10-business-risks-and-opportunities-for-mining-and-metals-in-2023.pdf*

[18] *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/dttl-er-mining-how-secure-is-your-supply.pdf*

Product Supply Chain Risk Management				
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Implement security requirements clauses within requests-for-purchase (RFP) and/or procurement contracts. Mining engineers responsible for security checks on procured equipment with occasional review by head office cybersecurity team for the compulsory minimum security standard checks.	Implement tight security controls for and inspection protocols for vendor supplied products prior to installation within the mine including security handshaking for new SW/HW, cryptographic check sums for SW mining products, physical inspection, and x-raying (if possible) of new vendor products, security scan in isolated, containerized environment etc.	Establish a database of approved vendors including product provided, security mechanisms included with product, international security verifications/certifications and past product performance (counterfeit, zero-day vulnerabilities, infrequent security patching etc.).	Supply chain database is frequently updated with tracking updates and delays from suppliers with automated adjustments to maintenance/deployment schedules and identification of alternative solutions and suppliers should security vulnerabilities be listed by international security auditors-including breaches to vendor company and/or associated parent companies.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Identify essential suppliers within the current mining supply chain and request specifications for security mechanism implemented in solutions that can guarantee availability, integrity, and confidentiality (AIC) prior to procurement and installation into the mine as part of solution identification and contracting processes.	Supply chain sourcing to include local* suppliers/manufacturers of same or similar mining solutions and good business viability. *Local meaning within the country or continent Employ supply risk management strategies to minimize disruption within the mines. Regular, formal review of supply chain equipment by head office cybersecurity team prior to installation/dispatch to the mines.	Supply chain sourcing to include alternative international suppliers/manufacturers of same or similar mining solutions with continuous updates on end-to-end supply chain timelines. Effect an overarching track and trace monitoring mechanism of mining infrastructure inbound supply chain to increase visibility. Mine products are evaluated by trained cybersecurity, professionals as review at head office and at mines prior to procurement, and on delivery.	Automated system employed to track and update supply chain products, update maintenance schedules accordingly, and identify alternative vendors and solutions should delays continuously affect mining schedule. Trained formal security review of mine equipment under procurement and in line for procurement on regular basis across all mines with a centralized policy.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	New inventory introduced into the mining space has security mechanisms guaranteeing AIC already implemented as part of the solution design from manufacturer.	Supply chain databases to include alternative local vendors able to supply or manufacture same or similar mining devices.	Supply chain databases expand list of viable international vendors with ordering priority based on updated supply chain timelines.	Up to date supply chain databases with autonomous end-to-end timeline updates provided as part of vendor risk reporting.

Table 3-5: Product supply chain risk management.

3.6 SERVICES THIRD-PARTY DEPENDENCIES MANAGEMENT PRACTICE

Mines heavily rely on the use of external contractors to provide support services to the operational infrastructure. Mechanisms to extend trust across the organizational boundary are thus required. Hidden threat sources may include sabotage of equipment, violation of mining safety rules, theft of intellectual property, planting of clandestine surveillance devices, installing unauthorized software or malware and dishonest procurement practices. There is thus a need to exchange trust information on all actors in the mine linked to various systems such as procurement, access control and reporting services.

Services Third-Party Dependencies Management				
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	References need to be provided before procurement of services from external parties. Screening of all contractors is conducted before procurement of services.	Contractors to provide background checks.	A mine-wide trust database is maintained for all internal and external staff as well as suppliers.	A company-wide trust database is maintained for all internal and external staff as well as suppliers. The database is linked to procurement, security, and access control systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Internal reference checks are conducted on suppliers before allowing a supplier to register on the company procurement system. The individuals providing services on behalf of the external companies are subjected to a background check. Contactors or vendors are onboarded through a general procurement management process in which a minimum security standard and posture check is conducted.	Individuals to provide report of background check conducted by third party prior to contacting within the mine (security screening within the mine). Cyber security questionnaires are used to vet cyber security controls of third party as part of the onboarding procedure.	Company and individual trust information is captured in a database and the database is updated as violations occur by procurement, security, and the HR department. The type of activity resulting in a violation needs to be clearly defined and agreed upon. Contractor equipment is temporarily blocked from usage in the mine environment during the posture checks while cyber security controls are reviewed by the mine head office's cybersecurity team.	The trust database is integrated with other company-wide ICT systems. Vulnerability management procedures are implemented to ensure monitoring within the mining edge network.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Onboarding policy within mine companies regarding contractor references approved and available for review.	Provision of background check reports to relevant parties within the mining house including police clearance certificates, tax certificates, company registration certificates.	An electronic database has been established and is actively maintained and updated by procurement, security and human resources as violations occur. Policy on contractor equipment checks and prohibited activities available.	Procurements are automatically rejected if a supplier is deemed unfit to provide services to the company. Hiring of individuals or contractors are automatically rejected if a violation exists in

		Onboarding procedure for contractors includes cybersecurity controls developed by third party security company.		the company database. Vulnerability management systems generate monitoring reports for the mining edge network.

Table 3-6: Services third-party dependencies management.

3.7 Establishing and Maintaining Identities Practice

A level 3 (consistent) target for establishing and maintaining mining identities is probably appropriate for extraction, especially for mining traffic management and digital twin initiatives, but this target decision is up to the mining stakeholders in the specific instance. In the typical mining operation identity is associated with people (with verified competency and skills checks determining which role is allocated to personnel), locations, as well as physical things.

Identity is mostly used to enforce safety and access control related to dangerous equipment such as explosives drills and trackless vehicles. Identity can also be coupled to capability where a specific person with a unique identity is associated with a specific skill or craft such as artisan, electrician, or shift supervisor. The identities are associated with a "type" (or role), limiting access. For example, an electrician is allowed to access dangerous areas such as high voltage sub stations and perform repairs, but not allowed to operate a mining machine or to use a transport vehicle to provide transportation to the specific area if not authorized.

The identity of machines is also an important consideration for mining environments. Machines of a specific identity may be operated by multiple operators during several shifts and a human identity needs to be matched to a machine identity taking specific policy and standard operating procedures into consideration.

Most mines make extensive use of contractors to implement and maintain infrastructure. Differentiating between contractor and employees as well as the privileges associated with the specific identity and the regular review of the identity is thus a key requirement.

Establishing and Maintaining Identities				
This practice helps to identify and constrain who may access the system and their privileges.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Mining companies establish contractor and employee identities on ad hoc basis based on current needs and available skills.	Operators acting as legal appointments manage allocation of roles in mining stope.	Operator identities within the mine are autonomously linked to license, asset, and access database.	Autonomous management of identities based on compliance, conduct, and competence status.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Mines establish separate contractor and employee identities with contractors being afforded privileges specific to their area of operation within the mine.	Legal appointments have a shift list of miners and contractors in the stope and allocate identities and relevant access within the stope based on listed licenses/competencies.	Mine operator access cards are linked to the associated machinery and operational licenses.	Mine identities are linked to biometric identification and are automatically managed to maintain current status of mine operator. Access and machinery requiring specialized privileges are biometrically secured and only operational based on correct privileges being linked to biometric identity.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Separation of contractor and employee identities with further	Legal appointments allocate and manage identities and roles of workers in the mining	Operator license status is autonomously linked to operator	Autonomous identity management of operators within

	separation of contractor identities based on area of operation.	stope based on indicated competencies/licenses given on shift list.	identities and roles within mine with appropriate permissions being granted.	the mining space implemented through biometric identification linked to mine identity and role.

Table 3-7: Establishing and maintaining identities.

3.8 Access Control Practice

Access to the mining stope is highly restricted owing to the limited space, large amounts of equipment and general danger associated with underground mining. Prior to being allowed access to the active mining area, personal protective equipment (PPE) needs to be allocated. Miners also need to pass a medical fitness test to be allowed into the stope. In addition to restricting access into the stope, access within the mining areas needs to be modifiable at a moment's notice should safety concerns arise. Personnel should not be permitted to access dangerous zones of the mine while being directed in an orderly manner towards either a safer area of the mine or to an evacuation point. Additionally, owing to the size, expense, and danger associated with certain types of mining equipment, personnel should be restricted from accessing areas in which they are being operated or stored unless they are properly accredited to be operating that machinery and are scheduled to use that machinery at a particular moment. Currently, access control in mining operations and to mining equipment is not well implemented with default credentials sometimes in use.

Access Control				
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Access control is managed manually with access being granted once basic access control requirements (PPE, medical screening etc.) are met.	Access requirements are checked more frequently and manual inspections (with some tracking technology employed) are conducted within mining stope to	Localization and adjustment of personnel access is conducted through access control software in near real-time.	Access control is integrated with safety systems and access is adjusted autonomously for currently occurring or future unsafe events.

		identify unauthorized personnel during blasting/unsafe activities.		
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Basic human access control requirements are met, e.g. turnstile access, access to mine dependent on being equipped with appropriate PPE etc. Access control in the mines is done through a segregation of duties where personnel should only be allowed to access what is authorized for work responsibilities. Rely on standard operating procedures and people to control their access during events such as blasting. Paper based systems.	Identification and restriction of access points (e.g. USB ports) to highly critical devices and machinery with adoption of appropriate security mechanisms to guarantee AIC triad. Manually inspect and restrict areas for unauthorized personnel before blast to disallow access, enforce physical access control on blasting site through use of barriers, and enforce shift control.	Know location of people in near real-time and implement the ability to adjust the access of areas and resources on a zone basis. Contractor device access restricted to exclusion zones within mining ecosystem until cleared for potential vulnerabilities. Autonomously manage access to highly sensitive/unstable areas through real time activation or deactivation of employee identification cards based on role and location. Access control systems (e.g. gates, access cards etc.) are integrated with safety systems.	Establish mine wide, real-time track and trace access control system on people and equipment currently deployed within the mine. Use automated human tracking and access prevention to implement access control policies according to miner's current status/role and mine operational policies. Machine vision systems to be used as part of PPE verification with appropriate access control restrictions should miners not be correctly equipped for the hazard/task indicated for that mine area.

	Rely on standard OHSA operating procedures to revoke access for unsafe incident such as fall of rock or blasting incidents.	Environmental monitoring systems, blasting systems, logistic stores, data, and control rooms dedicated to the programmable logic controllers (PLCs) require limited or strict access control for both safety and security reasons.	Electronic systems are implemented to provide blast warning and to limit access to blast zones, zones where an unsafe incident has occurred, or evacuation routes. Access to licensed machine types and restricted areas are autonomously granted or revoked based on operator identity, and status of linked license. Combination of biometrics and locally managed access control by mining engineers with cybersecurity experience.	Rely on standard OHSA operating procedures to revoke access for unsafe incident such as fall of rock or blasting incidents.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Human-based checks are conducted to ensure that access is only granted after needed personal protective equipment (PPE) is worn and appropriate medical tests have been conducted and passed e.g. to go through turnstile.	Human PPE and other mining equipment is checked more often in addition to upon entry, e.g. when entering mine, and before going down shaft.	Location tracking and access adjustments are conducted in near real time after an incident has occurred within the mine.	Access control systems are integrated with mine safety systems and are autonomously able to adjust personnel access based on current roles as well as detection of current/future unsafe incidents within various zones of the mining stope.

	*Lamp and rescue pack is issued before person can gain access into mine. This log is checked against paper-based register of workers and visitors. The proximity detection system is tested prior to arriving at turnstile or at turnstile. * Induction/training required for access. * Medical checks are necessary to be allowed access into the mine.	More frequent inspections are conducted, and physical barriers are implemented in areas where unsafe incidents have or will occur. This is combined with basic localization/tracking software to help identify where personnel are stationed within the stope.	More formally defined, role-based access is implemented and enforced using access control software and technologies. Electronic systems are able to forewarn personnel to zones where access has been restricted in near real time as well as direct personnel to nearest evacuation routes. Security reports are generated from exclusion zone regarding health of external contractor devices with appropriate risk levels awarded prior to connection into the main mining network.	*Lamp and rescue pack is issued before person can gain access into mine. This log is checked against paper-based register of workers and visitors. The proximity detection system is tested prior to arriving at turnstile or at turnstile. * Induction/training required for access. * Medical checks are necessary to be allowed access into the mine.

Table 3-8: Access Control.

3.9 Asset, Change and Configuration Management Practice

Assets in the mining extraction process can be grouped into four different asset types. Each asset type may require a varying change and configuration management implementation strategy based on the level of expertise, limitations imposed by the physical environment and device maintenance required.

Type 1: Machinery or mining support devices which are stationary or may move occasionally.

Typically, not removed from the mining area unless replaced and serviced in place. The list of underground heavy machinery assets will include but is not limited to scrapers,

winches, drills, conveyer belts, rail systems and locomotives. Support devices may also include pillar supports, jacks, rams, and other lifting equipment.

Type 2: Heavy machinery which is fully mobile and able to be moved above ground for maintenance.

Examples include TMM, LHD and personnel transport.

Type 3: Assets carried by miners are lightweight mobile devices and are taken below ground as well as above ground and returned to a central point after every shift.

Assets could also include PPE such as a self-rescue device, cap lamps and mobile gas meters, seismic sensors, Collision avoidance devices and voice or communication devices such as walkie talkies and cellular phones.

Type 4: Infrastructure assets which are permanently installed above or below ground, providing operational support to the mineral's extraction process.

Examples of above ground systems may include a WAN communications system connecting mobile dump trucks to a control room or electrical reticulation supplying power to conveyor belts and lights, servers, SCADA systems, environmental monitoring systems, blasting systems, logic control systems etc. Examples of below ground systems include a ventilation system, turnstile access control, shaft signaling system, electrical reticulation, and transformers as well as compressed air systems and water delivery systems.

Efficiency and ability of remote management will depend on the associated asset type.

Asset, Change and Configuration Management				
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Asset configurations are captured in an asset change log and accurately represented according to the type, function, and location of the device.	Assets are routinely maintained based on a schedule and limitations as described in the asset management database. Asset change and configuration data is manually maintained.	Asset change and configuration data is automatically reported for IT and OT networks.	IT and OT departments are merged, and Asset, Change and Configuration Management is maintained holistically for all technology systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	An electronic or paper-based asset change log is maintained by the mining engineers. Equipment reaching end-of-life (EOL) typically is not replaced until broken with manual, decentralized asset management.	Conduct risk-based inspections of Type 1 and 2 assets to regularly reassess maintenance requirements and equipment and configuration management. Implement IT Asset Management (ITAM) principles for management of type 3 and 4 assets. Staging environments exist for testing IT infrastructure before changes are implemented. Standard change controls are applied for decommissioning older systems when implementing newer systems into the mine environment.	Staging environments are used to test IT and OT infrastructure before changes are implemented in the production environments. IT and OT assets can communicate but are managed and governed by different departments and policies. OTA updates for mining equipment are used whenever units are connected to the mining network when appropriate (centrally management) to extend asset lifecycle.	No organizational separation between IT and OT systems exists. Asset, Change and Configuration Management is applied to all technology systems to ensure autonomous checking of SHEQ and license to operate (Type 1 and 2 assets). Meet regulatory compliance with real time digital twin modelling of asset movements and status. A single staging environment exists for testing integrated IIoT applications from surface to scope. Regular asset assessment and change management are used across the mine ecosystem.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

	Policy on the management of Asset, Change and Configuration Management exists and is implemented by mine engineers.	Comprehensive risk-based and IT Asset Management (ITAM) policies on the management of Type 1-4 mining assets exist and are implemented.	The different requirements for IT and OT infrastructure are clearly defined according to end-user application requirements and reflected in organizational policy including policies regarding OTA updates of mine equipment.	Holistic Asset, Change and Configuration Management policies in place without departmental differentiation or organizational boundaries.

Table 3-9: Asset, change and configuration management.

3.10 PHYSICAL PROTECTION PRACTICE

Physical protection will be determined by the safety of the people and the physical integrity of the machines. People need to be protected from being crushed by machines, environmental conditions such as fires, methane explosions and heat exhaustion which is primarily a function of ventilation. Machines need to be protected primarily from a mine collapse (goaf), and secondarily from vandalism, inappropriate use, and insufficient maintenance. Integrity and protection of the communications loop which supplies physical protection information between the machine and maintenance team / control room is thus important. Investment in machines is extensive so their protection is important.

We may also comment here on a physical separation between the IIoT network (OT and IT) as well as the physical safety network. The IIoT network can fail and only incur financial loss while if the safety network fails, human loss will be incurred. Safety networks must be fire, explosion, and goaf proof while the other types of networks are not required to be so robust as there may be cost and performance tradeoffs between the design philosophy between the general IIoT and safety critical networks.

Physical Protection				
This practice's policies address the physical security and safety of the premises, its people, and its systems to prevent theft and ensure the ongoing safe operation of equipment.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Basic systems in place for the physical protection of equipment and personnel as required by legislation.	Implement ad hoc physical protections on high risk 'crown jewel' mining systems.	Enhancement of physical security of critical infrastructure within and surrounding type 1-4 assets.	Physical security assessments and further enhancements of all infrastructure.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Adhere to the best practices and requirements as set out by local mining regulations regarding safety systems.	Maintain a database of the physical protection requirements for all systems. Ad-hoc initiatives in place to identify and enhance harden the physical security of high-risk systems.	Scheduled initiatives to enhance, test, and improve the physical security of mission and safety critical infrastructure. Additional devices and spare parts are kept on-site to repair or replace malfunctioning systems of critical importance. Store highest risk mining data within security hardened storage with continuous, timestamped tracking on read-	Same as comprehensiveness level 3 but for all systems organization wide above and below ground. Continuous training and refresher courses for staff on inspection and testing of physical security and protection measures with automated role updates to linked mine identities.

			write data access and appropriate physical security measures.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Successful audits by the relevant standards body or legislative entity.	Evidence of inspection and enhancement of physical security measures of high-risk systems.	Evidence of scheduled inspections and updating activities taking place based on pre-determined priorities.	Evidence of scheduled inspections and update activities for all systems organization wide above and below ground.

Table 3-10: Physical protection.

3.11 Protection Model and Policy for Data Practice

Mines deal with a lot of medical data due to the occupational health and safety regulations requiring yearly examinations of workers to declare them fit for work. An identity thus has the possibility to also have medical training and job performance associated with it.

There is an increasing trend in the mining community to make use of contractors who remotely monitor and maintain in-mine above and below ground systems. Data is extracted and sent to the cloud and results in a situation where the mine no longer has access to historical data on production processes.

Data protection laws such as the Protection of Personal Information Act (POPIA)[19] are a major driver behind the way data is gathered and stored. Also affecting data protection is the ability of devices that are capable of sharing what is classified information about the mine structures, equipment, processes, and procedures. As personal devices get more sophisticated, it becomes important as part of data protection strategies to assess what are the capabilities of the devices that visitors, employees and contractors bring in to mine sites to ensure that a loss of data confidentiality is not the result of such devices being present at the mines. This device protection policy would have to adjust based on whether the mines sites are above or below ground level.

[19] *https://popia.co.za/act/*

Protection Model and Policy for Data				
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Protection models includes allowances for personal devices based on type of mine site and device capability.	Protection models include allowances for personal devices based on type of mine site and device capability with allowances for specific roles.	Protection models allowances for personal devices are adjusted with implementation of data protection technologies.	Protection model allowances implemented across mine sites and include verification prior to authorization.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Strict Yes/No allowance policy of personal devices implemented on above and below ground mine sites based on ability to record audio, video, and store and share offsite at portions of mine sites where confidential and proprietary mining processes, infrastructure and information may be unintentionally shared.	Allow personal device use exceptions according to documented policy.	Adhere to local regulations regarding the protection of personal identifiable and healthcare data. Store highest risk mining data within security hardened storage with continuous, timestamped tracking on read-write data access and appropriate physical security measures. Allowances for devices are based on device capability	Allowances for personal devices are based on activation/deactivation of device capability with pre-testing in isolated lab prior to authorization with authorization list shared and implemented across mine sites.

			and risks assessments based on the device allowances above and below ground allowances get more sophisticated, with implementation of rudimentary transmission blocking technologies and disabling of prohibited capabilities prior to granting access.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Compliance assessment reporting for data protection to include guidelines and assessment of employed data confidentiality mechanisms (e.g. POPIA). Allowance of personal devices with prohibited capability is not permitted on mine sites depending on mine style (above/below ground) and associated safety concerns.	Access to high-risk mining data is limited for read-write operations and appropriate data protection practices are employed to maintain continuous confidentiality. Allowance of personal devices with recording and transmission capability is adjusted based on device capability and role of visitor to mine site.	Implement policy surround data protection such that it is employed using standard protection algorithms based on associated risk for all mining data. Access policies are to describe actioning towards increasing physical protections that are employed for storage facilities at which high-risk mining data is kept. Allowance of personal devices with prohibited capability is	Intrusion detection reports allow for the identification of unauthorized data accesses for further persecution. Back-up power solutions minimize mining data losses and availability reduction impacts in instances of power disruption. List of pre-inspected and authorized devices is distributed across all mine sites with regular updates.

			adjusted once technological safeguards are implemented by mine cybersecurity technicians as backup protection.	

Table 3-11: Protection model and policy for data.

3.12 Implementation of Data Protection Practices Practice

Implementation of data protection for mining extraction must take into account protection of personal information and techniques appropriate to mining extraction.

Implementation of Data Protection Practices				
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Health and PII collected by mining companies are appropriately protected.	High risk data related to mining operations is protected to ensure confidentiality is maintained in the event of a breach and accesses are minimized.	Mining data is categorized by risk to mining operations with highest risk data isolated and access restricted.	Data intrusion detection mechanisms are employed with backup power supplies as part of continuous data protection strategies.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Ensure POPIA compliance for health and other personally identifiable information (PII) gathered and stored	Identify high target data and information regarding mining operations, production, and sales and limit read-	Conduct internal and external risk assessment on mining data (ISO 31010, 3100) and employ international data	Autonomous intrusion detection of high to medium risk mining data with immediate flagging and lock-

	on mine premises by securing it with appropriate encryption algorithms and modes.	write access to appropriate personnel and employ appropriate encryption.	protection standards on a risk hierarchy. Implementation of system level fault tolerance processes to maintain availability of critical mine processes.	out of unauthorized account or device. Autonomous switching to backup power supply and backup recovery processes to ensure appropriate protection and shut down procedures can be completed for mining data and storage operations during power disruption events.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Compliance assessment reporting for data protection to include guidelines and assessment of employed data confidentiality mechanisms (e.g. POPIA).	Access to high-risk mining data is limited for read-write operations and appropriate data protection practices are employed to maintain continuous confidentiality.	Data protection should be employed using standard protection algorithms based on associated risk for all mining data. Access log is generated for high-risk mining data with increased physical protection employed for storage facilities.	Intrusion detection reports allow for the identification of unauthorized data accesses for further persecution. Back-up power solutions minimize mining data losses and availability reduction impacts in instances of power disruption.

Table 3-12: Implementation of data protection practices.

3.13 VULNERABILITY ASSESSMENT PRACTICE

Vulnerability assessment of networked and non-networked embedded devices in the IIOT network is usually overlooked in the mining industry and needs to be specifically addressed. The mining sector makes use of many embedded devices, which are operated in remote locations where “getting the job done” takes precedence over following recommended security architecture and design considerations.

Vulnerability Assessment				
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Vulnerability assessments are conducted on new Type 1-4 equipment on an ad hoc basis when new systems are procured and prior to installation within the mining stope as well as on new contractors prior to work commencing in the mine environment.	Vulnerability assessments are conducted on critical "crown jewel" infrastructure as part of maintenance activities as well as on contractor equipment in regular use within the mine.	Vulnerability assessments on the entire mining IIoT system are conducted according to industry standards such as the Common Vulnerability Scoring System (CVSS).	Vulnerability assessments are done on all systems within the organization taking into consideration the internal as well as external federated systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	In compliance with the threat assessment conducted, potential vulnerabilities are assessed and catalogued manually and on an ad hoc basis on new equipment that is to be introduced into the mining environment.	Vulnerability assessment includes potential zero-day vulnerabilities emergent over time requiring patching/updates on crown jewel infrastructure and contractor equipment that is regularly introduced into the mine environment.	Scheduled physical security assessments and hardening of critical infrastructure are prioritized according on the level of importance and vulnerability as determined by standard vulnerability assessment scoring system.	Vulnerability assessment conducted autonomously with threat detection software with generation of real-time assessment and action report.

	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment
	Vulnerability assessment report for introduction of new system into mining ecosystem, associated risk strategy and mitigation plan to be compiled and implemented on ad hoc basis.	Vulnerability assessment report to include assessment of maintenance risk, mitigation strategy and potential frequency required for mining systems and contractor equipment. Documentation of highly critical devices and machinery, the number and location of restricted access points within highly critical machinery and security implemented to reduced vulnerability presented by the access points is regularly generated and updated.	Vulnerability assessment report developed according to international standard reporting and scoring with focus on IT/OT risk.	Vulnerability assessment report available in real-time through continuous scanning by threat detection software with action report from highest to lowest risk.

Table 3-13: Vulnerability assessment.

3.14 PATCH MANAGEMENT PRACTICE

Patch management is like maintenance in the mining context and in the same way computers need to be updated. A system is required to ensure that the latest firmware, hardware and maintenance activity are completed for the machines used in the extraction operation. Patch management could thus be considered as a measure of how mature and secure the logistical management of machines is done from a security point of view.

Machine management generally may go beyond software specifically. Thus, a wider view of patching may need to be implemented when considering certain mine assets. Sensors within the

mine itself would need to be assessed as to whether they are operating correctly and up to date in their firmware as well as identifying what is being monitored for both quality of the data and correctness.

Patch Management				
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Unscheduled patch management is applied for all IIOT operating systems and software.	Scheduled patch management is applied for all IIOT operating systems.	Scheduled patch management is applied for all IIOT operating systems and embedded firmware.	Patching is applied to all IIOT operating systems and embedded firmware as patches are released by vendors.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Patching is done as deemed necessary by the system administrators. OT patching is managed locally and manually by the mining engineers and IT patching is managed by head office cybersecurity teams and only updated when vulnerabilities detected (manually).	Patches are identified by the system administrators and installed for IIoT software and operating systems on a fixed time interval.	Patches are identified by the system administrators and installed for IIoT software, embedded firmware, and operating systems on a fixed time interval. IT and OT patch management is managed by head office across multiple mine sites and is coordinated	The organization is automatically informed of new patches by the manufacturer for software, operating systems, and embedded firmware. Patches are applied autonomously as soon as received. Patch authenticity is verified by mining company teams and pushed autonomously OTA.

		IT and OT vulnerability patches are managed concurrently and coordinated in a single mine when detected by head office cybersecurity teams and mining engineers. Zero day vulnerabilities are immediately and manually patched through to relevant mine infrastructure.	per vendor. Guaranteeing authenticity of the firmware code is left up to the relevant vendors. Zero day vulnerability patches are deployed immediately to relevant mine infrastructure and by the end of business to the entire mine network and infrastructure.	Patches can also be generated for mining teams if detected prior to official firmware update from vendors.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Policy and approval framework exists for unscheduled patch management when vulnerabilities are detected by head office and mine sites individually.	Policy and approval framework exists for scheduled patch management procedures that are coordinated per mine for IT and OT equipment as a coordinated effort with head office and mine sites.	Policy and approval framework exists for scheduled patch management across mining sites per vendor installed within the mines, including embedded firmware for IIoT systems, with appropriate documentation of authenticity added for installed firmware versions as part of maintenance records.	Policy and approval framework exists for immediate patch management including embedded firmware for IIoT systems with OTA push and in house patch development and authentication of vendor firmware.

Table 3-14: Patch management.

3.15 MONITORING PRACTICE

The control room is the heart of monitoring practice and has a direct link with the sophistication of the "SCADA" system. A differentiating factor for monitoring practice will be human in the loop versus automated response monitoring. A mature system will be able to automatically respond to varying levels of alerts with preprogrammed remedies once at comprehensiveness level 4 whereas an unsophisticated system will just alert and require manual intervention to correct.

Monitoring Practice				
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Monitoring of all relevant in-mine process variables.	Comprehensive monitoring of all relevant in-mine process variables as well as IIOT system performance metrics.	Comprehensive monitoring of all relevant in-mine process variables as well as IIOT system performance metrics with the ability to automatically respond to setpoint changes.	Integrated monitoring of all relevant in-mine process variables and IIOT systems on an organizational level.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Relevant in-mine process variables should be automatically monitored and reported to a control room operator for manual intervention or setpoint changes.	Relevant in-mine process variables as well as IIoT system performance should be automatically monitored and reported to a control room operator for manual intervention, setpoint changes or maintenance activities.	All relevant in-mine process variables as well as IIoT system performance metrics should be reported and automatic setpoint changes should be supported for known changes without human intervention. Notifications with audio/visual alarm should be triggered alongside automatic emergency shutdowns depending upon the implications and severity of a problem detected by monitors.	In-mine process variables as well as IIoT system performance metrics should be available to key stakeholders on an organizational level for planning and decision-making purposes as well as to implemented AI model and digital twin simulation sources.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Process variables defined and monitored for manual intervention.	Process and IIoT performance variables defined and monitored for manual intervention.	Automatic setpoint changes are supported for process variables that are monitored.	Variables are available for reporting in the organization.

Table 3-15: Monitoring practice.

3.16 Situational Awareness and Information Sharing Practice

Situational awareness and information sharing is specifically applicable to the mining industry in case of an emergency. Well-defined procedures and automated systems need to be in place to assist with disaster management and planning. Known data formats should be used to share information and automatically updated via IIoT systems where possible. No additional profile information was identified for this practice.

Situational Awareness and Information Sharing				
This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	No Additional Profile Information	No Additional Profile Information	No Additional Profile Information	No Additional Profile Information
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**

Table 3-16: Situational awareness and information sharing practice.

3.17 Event Detection and Response Plan Practice

Event detection can be categorized into two categories. The first is events related to safety and security, with safety and the preservation of human life taking highest priority, and the second is events pertaining to productivity and business objectives. Safety and security events are in general more important than productivity and business objectives but are still closely interlinked in the mining industry. A mine which is not profitable will not be able to continue operating and if an accident occurs a mine closure will lead to a substantial loss in productivity and reduce profitability. The level of automated detection of events using IIoT systems will determine the

maturity of detecting events while the level of human interaction required to respond to the event will determine the maturity of the response plan practice.

Event Detection and Response Plan				
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Event detection and response is limited to unplanned detection and decision making.	Event detection is semi-automated with manual response plan implementation activities.	Event detection is automated with manual response plan activities executed by human participants.	Event detection and the associated response is fully automated making use of IIoT systems to gather and respond to events without human intervention.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Monitoring of individual devices and network behavior is done by local mine engineers with periodically inspected, and incidents responded to by a system administrator at head office. Security events are only detected when notified by	Predefined alert thresholds are set to alert a system administrator of events using instant alerts such as SMS or e-mail notifications on critical, local mine device behaviors. Operations are air-gapped or separated from corporate network through access control lists (ACLs).	Comprehensive predefined alert thresholds and filters are used to alert a system administrator of only possible cybersecurity events via SMS or e-mail notifications on mine equipment and networks across all mines. Head office cybersecurity teams push event	Intrusion detection systems are deployed which can automatically detect suspicious events and respond by blocking the traffic associated with the event as the activity is taking place. Implement and integrate event detection generated by a third-party device into wider

	the cybersecurity team at head office. Local mining engineers would be responsible for handling security events and maintaining operations with clean-up operations performed by the head-office based cyber security teams.	Detect cybersecurity incidents from third party devices locally and push notification to head office.	notification and response plan to all mines autonomously including to third party IIoT devices	event detection mine network with appropriate response plans as indicated by vendors and internal cybersecurity teams.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Log list of security events is updated semi-regularly and attended to by security system admin.	Event detection logging is actioned against almost instantly with relevant event detection rules implemented.	Event detection rules can categorize severity of events allowing for hierarchical actioning of security events.	Event detection combined with an autonomous intrusion detection system that can detect and action on potentially malicious activity.

Table 3-17: Event detection and response plan.

3.18 Remediation, Recovery and Continuity of Operations Practice

Remediation, Recovery and Continuity of Operations Practice for a mining environment is closely linked with the supply chain management process due to the distance of the mine from possible suppliers and lead times imposed due to specialized equipment and repairs used in the mining process.

Mine collapses and fires are the two main physical threats to operational and IIOT remediation recovery, and continuity of operations for underground extraction processes. The physical distance and physical access limitations of the underground mining operation from the surface can result in a significant delay in replacing ICT equipment and re-establishing connectivity. On-site spares and sufficient redundancy for IIoT technology is thus a key requirement.

Safety critical systems must remain operational if connectivity with the control room is lost in contrast to non-critical systems which may remain offline. A degree of autonomous operation independent of the control room is thus required in an emergency.

Remediation, Recovery and Continuity of Operations				
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry-Specific Scope Considerations	Provide plans and means for emergency maintenance.	Formalized periodic service level agreement (SLA) based maintenance implement for all IIOT systems.	Redundant systems with automatic fail over in place for critical systems.	Redundant and control room independent functioning of all critical systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Mission critical infrastructure identified and maintained on a regular basis by either onsite or offsite maintenance teams.	Service level agreements in place for all critical IIoT infrastructure. Replacement units are available onsite and preconfigured for replacing critical infrastructure if required. Response and remediation prioritized by revenue and safety (e.g. processing operations). Priority for offline operations to be restored first if	Redundant IIoT infrastructure in place with automatic failover Implement firewalls, demilitarized zones security information and event management (SIEM), security operation centers (SOC) and CIC monitoring rooms at mine sites shall be used to monitor traffic in the network and dedicated 24/7	Fully redundant IIoT infrastructure for all in-mine activities with automatic failover and autonomous operation if control room connectivity is lost. Event detection systems fully integrated with security capabilities across mines with severity of security incidents are assessed through a formal, automated, cyber incident

		affected incident.	tracking of device uptime for faster event detection of cybersecurity incidents.	management process or generic risk management framework depending on the type of event, disruption caused, or financial impact to the mine.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	IIoT infrastructure is maintained, and records of maintenance activities are maintained with recovery strategies developed by mine engineers at individual mine sites.	Proof of service level agreements in place with equipment providers. Event recovery policies and strategies developed with indicated priority equipment and offline services that are to be restored to last backup state.	Redundant IIOT design architecture implemented. Dedicated monitoring systems implemented at individual mines sites for event detection and faster response for recovery.	Redundant IIOT design architecture implemented across all mine sites with formal, automated cyber incident management reports generated assessing risk, type of event, levels of disruption and financial impact.

Table 3-18: Remediation, recovery, and continuity of operations.

Annex A ACRONYMS

AIC	Availability, Integrity, Confidentiality
CAPEC	Common Attack Pattern Enumeration and Classification
CPS	Cyber-Physical Systems
DMR	Department of Mineral Resources
DWS	Department of Water and Sanitation
EA	Environmental Authorizations
EIAS	Environmental Impact Assessments
EMP	Environmental Management Plans
GPS	Global Positioning System
ICS	Industrial Control System
ICT	Information and Communications Technology
IIC	Industry IoT Consortium
IIRA	Industrial Internet Reference Architecture
IISF	Industrial Internet Security Framework
(I)IoT	(Industrial) Internet of Things
IT	Information Technology
ISO	International Standards Organization
LHD	Load Haul Dump
MHSA	Mine Health and Safety Act (Origin: South Africa)
MitM	Man-in-the-Middle
MPRDA	Mineral and Petroleum Resources Development Act (Origin: South Africa)
NEMA	National Environmental Management Act (Origin: South Africa)
OHSA	Occupational Health and Safety Act (Origin: United States of America)
OT	Operational Technology
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
POPIA	Protection of Personal Information Act

PPE	Personal Protective Equipment
SCADA	Supervisory Control and Data Acquisition
SHEQ	Safety, Health, Equipment and Quality
SLA	Service Level Agreement
TMM	Trackless Mobile Machine
WAN	Wide Area Network

Annex B DEFINITIONS

The following terms, specific to the context of the SMM, are defined here:

- *Security level* is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.
- *Security maturity* is a measure of an understanding of the current Security Level, its necessity, benefits, and cost of its support.
- *Domains* are the strategic-level priorities for security maturity. In the SMM, there are three domains: Governance, Enablement, and Hardening.
- *Subdomains* refer to the basic means to address a domain at the planning level. Each domain currently defines three subdomains.
- *Security practices* are the typical activities performed for a given subdomain; they provide the deeper detail necessary for planning. Each subdomain has a set of practices.
- *Comprehensiveness* is a measure of the completeness, consistency and assurance of the implementation of measures supporting the security maturity domain, subdomain or practice.
- *Scope* is a measure of the applicability to a specific vertical or system.
- *Security maturity target* is the desired “end state” for an organization or system. The security maturity target can apply to a new system under development or an existing brownfield system. The security maturity target is determined by the business objectives of the organization or group.

Annex C MINING REGULATIONS EXAMPLE: SOUTH AFRICAN MINING

The South Africa regulatory framework presented below is given as an example of a mature set of regulations that may be found within the mining industry. Other jurisdictions have similar regulatory environments, and these should be consulted for the relevant country.

The South African Mining Industry (SAMI) has several regulations and acts which govern how mining activities are to be conducted, including determining the ownership of ore, safety standards, environmental protection etc. Compliance with these regulations is needed to ensure the issuing and maintenance of a mining license within the country. Some of the main regulations include: Mineral and Petroleum Resources Royalty Act 2008,[20] Mineral and Petroleum Resources Development Act 28 2002 (MPRDA),[21] Mining Titles Registration Act 1967[22] Precious Metals Act 2005,[23] Diamonds Act 1986,[24] Mine Health and Safety Act 1996 (MHSA),[25] National Environmental Management Act 1998 (NEMA),[26] National Water Act 1998,[27] Spatial Planning and Land Use Management Act 2013,[28] Mine Qualifications Body (Legal appointments and Certifications). Other regulations affecting mining include Occupational Health and Safety Act 85 1993,[29] Basic Conditions of Employment and Labor Relations Act,[30] Driven Machinery Regulations DMR 18.1 to 18.10.[31]

The biggest overseeing compliance regulator is the Department of Mineral Resources (DMR) who are responsible for regulated matters relating to MPRDA, regulated matters relating to environmental impact assessments (EIAS), environmental management plans or programs

[20] *https://www.gov.za/documents/mineral-and-petroleum-resources-royalty-administration-act*

[21] *https://www.gov.za/documents/mineral-and-petroleum-resources-development-act*

[22] *https://www.gov.za/documents/mining-titles-registration-act-1-mar-1967-0000*

[23] *https://www.gov.za/documents/precious-metals-act*

[24] *https://www.gov.za/documents/diamonds-act-25-jun-1986-0000*

[25] *https://www.gov.za/documents/mine-health-and-safety-act*

[26] *https://www.gov.za/documents/national-environmental-management-act*

[27] *https://www.gov.za/documents/national-water-act*

[28] *https://www.gov.za/documents/spatial-planning-and-land-use-management-act*

[29] *https://www.gov.za/documents/occupational-health-and-safety-act*

[30] *https://www.gov.za/documents/basic-conditions-employment-act*

[31] *https://www.gov.za/documents/occupational-health-and-safety-act*

(EMPs) for new and existing mining activities, granting environmental authorizations (EAs) for prospecting, mining and related activities, approving prescribed financial provisions related to remediation and rehabilitation of environment from mining activities. Within the DMR, the compliance department is divided into the Mineral Regulation Branch/Mineral Regulation Management, Enforcement and Compliance Chief Directorate, Directorate Mineral and Petroleum Titles Registration Office.[32]

Another regulator is the Department of Water and Sanitation (DWS) whose focus is ensuring compliance with prescribed standards and water management practices according to the user pays and polluter pays principles.[33] This principle shifts portions of the treatment and clean-up costs back to polluters within the mining environment.

The two main mining regulations in South Africa are: Mine Health and Safety Act, Mineral and Petroleum Resources Development Act.

The use of legal appointments within the mining environment is in accordance with the structure and focus of the MHSA regarding the delegation of responsibility of Health and Safety. While the act determines that full responsibility lies with the employer, it also recognizes the impossibility of one person being responsible for all actions occurring on a day to day within a mine.[34]

A legal appointment is an act of formal acceptance of legal responsibility, with which a person accepts and is responsible for a certain portion of compliance management. Without a legal appointment, a job or operation could be deemed non-compliant in terms of the OHS Act. Legal appointments can be required for various operations within mining operations. For example, the figure below gives an example of the legal appointments required from the MHSA for exploration drilling operations.[35]

[32] *https://www.dmr.gov.za/mineral-regulation/overview*

[33] *https://www.dws.gov.za/*

[34] *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

[35] *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

Appointment	Reference	Who is responsible for the appointment
Chief Executive Officer	Not appointed but responsibility defined in MHSA Section 2A	
Manager	MHSA Section 3 (1) a	Employer
Employer representative	MHSA Section 4 (1)	Employer
Sub-ordinate Manager	Minerals Act Reg. 2.6.1	Manager
Person to assist	Minerals Act Reg. 2.9.2	Manager
Engineer	Minerals Act Reg. 2.13.1	Manager
Safety Officer	Minerals Act Reg. 2.17.1	Manager
Chief Safety Officer	Minerals Act Reg. 2.17.4	Manager
Health and Safety Representative (elected by employees)	MHSA Reg. 6.9 and Minerals Act Reg. 2.18.1	Manager

Example C-1: Examples of Legal Appointments that may be Present in the Mining Equipment.

Any person who is appointed responsibility through a legal appointment is required to understand the objectives of and requirements imposed by the MHSA. They are also required to have a certain level of competency prior to their appointment. This competency can either be certified competency, special competency or competency as defined by the Minerals Act, Regulation.[36]

With a legal appointment, an appointee needs to be very clear on the duties that are imposed upon them by the legal appointment, both in the day-to-day duties but also in keeping up to date with all changes that are made to the MHSA.[37]

[36] *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

[37] *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

Annex D REFERENCES

[1] D. McGinnis. (2023). What Is the Fourth Industrial Revolution? [Online]. Available: https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir/

McKinsey. (2022). What is industry 4.0 and the Fourth Industrial Revolution? | McKinsey [Online]. Available: *https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir*

[2] N. Huq. (Unknown). Cyber Threats to the Mining Industry [Online]. Available: *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

[3] Industry IoT Consortium: IoT Security Maturity Model: Practitioner's Guide, Version 1.2, 2020-05-05, retrieved 202-05-05 Available: *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

[4] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013. Available: *https://webstore.iec.ch/publication/7033*

[5] Not a URL.

[6] Industry IoT Consortium: IoT Security Maturity Model: Practitioner's Guide, Version 1.2, 2020-05-05, retrieved 202-05-05 Available: *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

[7] B. Byrne and C. Engdahl. (2021). Mining 4.0: How innovation is shaping mines of the future [Online]. Available: *https://miningdigital.com/smart-mining/mining-40-how-innovation-shaping-mines-future*

[8] Cisco. (2021). Cisco Industrial Automation Solution – Mining [Online]. Available: *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

[9] Cisco. (2021). Cisco Industrial Automation Solution – Mining [Online]. Available: *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

[10] Mining Industry Occupational Safety and Health. (2023). Summary - Mining Industry Occupational Safety & Health [Online].
Available: *https://www.mosh.co.za/falls-of-ground/summary*

V. Netshilaphala and T. Zvarivadza, "Fall of Ground Management Through Underground Joint Mapping: Shallow Chrome Mining Case Study," Geotechnical and Geological Engineering, vol. 40, no. 2022, pp.2231-2254, Nov 27, 2021.
Available: *https://link.springer.com/article/10.1007/s10706-021-02023-3*

[11] N. Huq. (Unknown). Cyber Threats to the Mining Industry [Online].
Available: *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

[12] Cisco. (2021). Cisco Industrial Automation Solution – Mining [Online]. Available: *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Verticals/Mining/AAG/Industrial_Automation_in_Mining_AAG.pdf*

[13] N. Huq. (Unknown). Cyber Threats to the Mining Industry [Online].
Available: *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

PWC. (2021). Threat digest- Emerging cyber threats in the manufacturing and mining sectors [Online].
Available: *https://www.pwc.co.za/en/assets/pdf/threat-advisory-manufacturing-mining-sector.pdf*

British Standards Institute. (2021). Embracing digital transformation in the Mining Industry [Online]. Available: *https://www.bsigroup.com/globalassets/localfiles/en-za/mining/mining-cyber.pdf?utm_source=website&utm_medium=AfricaMining&utm_content=PDF&utm_campaign=ZA-Information-Security-Mining-2021*

S. Verma, A. Deas, A. Douglas, and A. Davidse. (Unknown). An integrated approach to combat cyber risk: Securing industrial operations in mining [Online]. Available: *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/cyber-risk-in-mining.pdf*

[14] N. Huq. (Unknown). Cyber Threats to the Mining Industry [Online].
Available: *https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf*

[15] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. (2015). NIST Risk Management Framework- Industrial Control Systems [Online]. Available: *https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/overlay-repository/nist-developed-overlay-submissions/industrial-control-systems*

[16] Deloitte. (2011). How secure is your supply? A guide to effective supply risk management in the mining industry [Online]. Available: *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/dttl-er-mining-how-secure-is-your-supply.pdf*

EY Limited. (2022). Top 10 business risks and opportunities for mining and metals in 2023 [Online]. Available: *https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/mining-metals/ey-top-10-business-risks-and-opportunities-for-mining-and-metals-in-2023.pdf*

[17] EY Limited. (2022). Top 10 business risks and opportunities for mining and metals in 2023 [Online]. Available: *https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/mining-metals/ey-top-10-business-risks-and-opportunities-for-mining-and-metals-in-2023.pdf*

[18] Deloitte. (2011). How secure is your supply? A guide to effective supply risk management in the mining industry [Online]. Available: *https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/dttl-er-mining-how-secure-is-your-supply.pdf*

[19] South African Government. (2019). POPIA ACT [Online]. Available: *https://popia.co.za/act/*

[20] South African Government. Mineral and Petroleum Resources Royalty (Administration) Act 29 of 2008 | South African Government [Online]. Available: *https://www.gov.za/documents/mineral-and-petroleum-resources-royalty-administration-act*

[21] South African Government. Mineral and Petroleum Resources Development Act 28 of 2002 | South African Government [Online]. Available: *https://www.gov.za/documents/mineral-and-petroleum-resources-development-act*

[22] South African Government. Mining Titles Registration Act 16 of 1967 | South African Government [Online]. Available: *https://www.gov.za/documents/mining-titles-registration-act-1-mar-1967-0000*

[23] South African Government. Precious Metals Act 37 of 2005 | South African Government [Online]. Available: *https://www.gov.za/documents/precious-metals-act*

[24] South African Government. Diamonds Act 56 of 1986 | South African Government [Online]. Available: *https://www.gov.za/documents/diamonds-act-25-jun-1986-0000*

[25] South African Government. Mine Health and Safety Act 29 of 1996 | South African Government [Online]. Available: *https://www.gov.za/documents/mine-health-and-safety-act*

[26] South African Government. National Environmental Management Act 107 of 1998 | South African Government [Online]. Available: *https://www.gov.za/documents/national-environmental-management-act*

[27] South African Government. National Water Act 36 of 1998 | South African Government [Online]. Available: *https://www.gov.za/documents/national-water-act*

[28] South African Government. Spatial Planning and Land Use Management Act 16 of 2013 | South African Government [Online]. Available: *https://www.gov.za/documents/spatial-planning-and-land-use-management-act*

[29] South African Government. Occupational Health and Safety Act 85 of 1993 | South African Government [Online]. Available: *https://www.gov.za/documents/occupational-health-and-safety-act*

[30] South African Government. Basic Conditions of Employment Act 75 of 1997 | South African Government [Online]. Available: *https://www.gov.za/documents/basic-conditions-employment-act*

[31] South African Government. Occupational Health and Safety Act 85 of 1993 | South African Government [Online]. Available: *https://www.gov.za/documents/occupational-health-and-safety-act*

[32] South African Government. Mineral Regulation Overview | Department of Mineral Resource [Online]. Available: *https://www.dmr.gov.za/mineral-regulation/overview*

[33] South African Government. DWS Home [Online]. Available: *https://www.dws.gov.za/*

[34] C. Rice. (2017). Legal Appointments and Liability [Online]. Available: *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

[35] C. Rice. (2017). Legal Appointments and Liability [Online]. Available: *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

[36] C. Rice. (2017). Legal Appointments and Liability [Online]. Available: *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

[37] C. Rice. (2017). Legal Appointments and Liability [Online]. Available: *https://www.drillsafe.co.za/drillsafe-articles/legal-appointments-and-liability?format=amp*

Annex E FURTHER READING

Industry IoT Consortium: The Industrial Internet, Volume G1: Reference Architecture Technical Report, version 1.9, 2019-06-19, retrieved 2020-04-29, *https://www.iiconsortium.org/IIRA.htm*

Industry IoT Consortium: The Industrial Internet of Things Volume G4: Security Framework Version 1.0, 2016-September-26 *http://www.iiconsortium.org/IISF.htm*

Industry IoT Consortium: The Industrial Internet, Volume G8: Vocabulary Technical Report, version 2.2, 2019-11-06, retrieved 2020-01-24, *https://www.iiconsortium.org/vocab/index.htm*

Industry IoT Consortium: IoT Security Maturity Model: Description and Intended Use, version 1.2, 2020-05-05, retrieved 2020-05-05 *https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf*

S. Brander. IETF. "Key Words for Use in RFCs To Indicate Requirement Levels." March 1997. Best Current Practice. *https://ietf.org/rfc/rfc2119.txt*

ACKNOWLEDGEMENTS

This publication is a work product of the IIC’s IoT SMM Mining Profile Tiger Team, chaired by Frederick Hirsch (Upham Security) and Jean-Jacques Verhaeghe (Mandela Mining Precinct).

Authors: The following people contributed substantial written content to this document: Lehlogonolo Ledwaba (Mandela Mining Precinct), Frederick Hirsch (Upham Security), Carel Kruger (Mandela Mining Precinct), and Ron Zahavi (Auron Technologies).

Technical Editor: Chuck Byers (IIC staff) oversaw the process of organizing the contributions of the above Authors into an integrated document.