Formula 1

Content placeholder

Formula 2

Content placeholder

Related Content

Title	Type	Slug
Blast Design Excel Template v4.2	resource	blast-design-excel-template
Drill Rig Maintenance Inspection Checklist	resource	drill-rig-maintenance-checklist
Rock Mass Rating (RMR) Field Survey Sheet	resource	rmr-field-survey-sheet
Drilling Energy Benchmarking Dashboard (Power BI)	resource	drilling-energy-dashboard
TBM Advance Rate Prediction Curve Library	resource	tbm-advance-rate-library

Detailed Explanation

NIST SP 800-82 provides foundational guidance for securing Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments—systems that share architectural similarities with AHS, such as distributed sensors, real-time controllers, wireless vehicle-to-infrastructure (V2I) links, and centralized dispatch systems. The AHS Cybersecurity Architecture Reference Design extends this guidance by modeling AHS-specific assets—including autonomous haul trucks, onboard perception/decision systems, GNSS/RTK positioning infrastructure, edge compute gateways, fleet management software, and mine-wide OT/IT convergence points—into a hierarchical, zone-based architecture aligned with the ISA/IEC 62443 standard. Key principles include segregation of safety-critical control traffic from non-critical IT traffic, zero-trust enforcement at zone boundaries (e.g., between truck ECU networks and the operations center), cryptographic authentication of firmware updates and

remote commands, and continuous monitoring via embedded security agents compliant with IEC 62443-3-3 SL2 requirements. Applications span threat modeling (e.g., spoofing GNSS signals or injecting false obstacle data), secure over-the-air (OTA) update mechanisms, and integration with Security Information and Event Management (SIEM) platforms using standardized logging formats (e.g., RFC 5424). Crucially, the design mandates co-engineering of cybersecurity and functional safety (per ISO 26262 and IEC 61508), recognizing that cyber compromises can directly induce hazardous motion or control failures—requiring joint hazard analysis (JHA) and security assurance levels (SAL) mapped to safety integrity levels (SIL).

Key Components

#	Component
1	Zoned Network Architecture (e.g., Vehicle Zone, Edge Gateway Zone, Operations Center Zone)
2	Secure Communication Protocols (TLS 1.3, DTLS, IEEE 1609.2 for V2X)
3	Runtime Integrity Monitoring & Secure Boot for ECUs

Applications

#	Application
1	Securing autonomous truck platooning and dynamic path planning against adversarial manipulation
2	Enabling compliant OT/IT convergence in brownfield mining sites with legacy SCADA integration
3	Supporting regulatory audits and third-party certification (e.g., UL 2900-2-2, IEC 62443-3-3) for AHS deployments

Related Concepts

#	Concept

1	ISA/IEC 62443
2	Zero Trust Architecture (ZTA) for OT
3	Functional Safety–Cybersecurity Co-Engineering

Tags

> autonomous vehicles, industrial control systems, mining cybersecurity