TECHNICAL BRIEF

Lone Worker Safety Systems

Technology Selection Framework

WHAT YOU WILL LEARN

- Regulatory landscape: OSHA General Duty Clause, 29 CFR 1910.269, and ISA 84 / IEC 61511 implications
- Four-layer technology architecture for connected lone worker protection
- Hazardous area classification and its impact on device selection (C1D1/C1D2, Zone 0/1/2)
- Connectivity options: Private 5G, Industrial Wi-Fi, LoRaWAN, and satellite backhaul
- A four-phase selection framework from risk assessment through pilot validation

Executive Summary

Lone workers in oil & gas and chemical manufacturing face a unique intersection of hazards: toxic gas exposure, high-energy equipment, confined spaces, and remote locations where emergency response times are measured in minutes, not seconds. Despite these elevated risks, many operators still rely on fragmented safety measures — a standalone gas detector here, a periodic radio check-in there — that provide incomplete visibility into worker status and leave dangerous gaps in emergency response capability.

The convergence of industrial IoT, private wireless networks, and cloud-based safety platforms has created an opportunity to fundamentally rethink how organizations protect their most vulnerable workers. Connected lone worker safety systems now integrate gas detection, man-down sensing, GPS location tracking, two-way communication, and automated alerting into unified platforms that provide continuous, real-time visibility from the field to the control room.

However, selecting the right technology stack requires more than evaluating product brochures. Organizations must navigate hazardous area classifications, connectivity constraints in remote environments, integration requirements with existing safety instrumented systems, and a regulatory landscape that — while lacking a single prescriptive lone worker standard — imposes clear obligations through OSHA's General Duty Clause, industry-specific standards like 29 CFR 1910.269, and process safety frameworks such as ISA 84 / IEC 61511.

> *This technical brief provides a vendor-agnostic framework for evaluating and selecting lone worker safety technologies. It is designed for HSE managers, operations directors, and IT/OT leaders who need to make defensible, field-credible technology decisions — not marketing-driven ones.*

Who Should Read This Document

Role	Key Concern	Relevant Sections
HSE Manager	Regulatory compliance, incident reduction	Sections 1, 2, 5
Operations Director	Operational continuity, ROI justification	Sections 3, 4, 6
IT/OT Manager	Network integration, cybersecurity	Sections 3, 4, 5
CIO / CISO	Enterprise risk, data governance	Sections 4, 5, 6

1. The Regulatory Landscape for Lone Worker Safety

A common misconception is that OSHA prescribes specific technology requirements for lone worker protection. It does not. The United States has no single, comprehensive lone worker regulation comparable to, for example, the UK's Health and Safety Executive guidance (INDG73). Instead, lone worker obligations emerge from a matrix of general duties, sector-specific standards, and process safety requirements.

1.1 OSHA's General Duty Clause — Section 5(a)(1)

The foundation of employer obligations toward lone workers is OSHA's General Duty Clause, which requires employers to furnish a workplace free from recognized hazards likely to cause death or serious physical harm. While the clause does not mention lone workers explicitly, OSHA has cited employers under this provision for failing to implement adequate monitoring and communication systems for isolated personnel. The absence of a specific lone worker standard does not relieve employers of their duty to assess and mitigate the unique risks these workers face.

1.2 Sector-Specific Standards

Certain OSHA standards contain direct provisions relevant to lone worker scenarios. 29 CFR 1915.84, governing shipyard employment, requires employers to account for each lone worker throughout the shift at regular intervals and at the end of each assignment, by sight or verbal communication. While specific to shipyards, this standard represents OSHA's clearest articulation of lone worker monitoring expectations and is widely referenced as a best-practice benchmark across industries.

29 CFR 1910.269, covering electric power generation, transmission, and distribution, requires that certain tasks be performed by at least two employees and mandates that lone workers be reachable within four minutes by a colleague trained in CPR and first aid. This four-minute reachability standard is one of the most specific time-bound requirements in OSHA's framework and has significant implications for communication system design.

1.3 Process Safety Management and ISA 84 / IEC 61511

For facilities operating under OSHA's Process Safety Management (PSM) standard (29 CFR 1910.119), safety instrumented systems — including those protecting lone workers — must comply with recognized and generally accepted good engineering practices. OSHA has endorsed ISA 84 / IEC 61511 as precisely such a standard. This means that safety-critical functions within a lone worker protection system, such as automated emergency shutdown triggers or gas detection alarm escalation, may need to meet specific Safety Integrity Level (SIL) requirements depending on the hazard scenario and layers of protection analysis (LOPA) findings.

> ***Practical implication:*** *While lone worker wearables themselves are not classified as safety instrumented systems, the broader safety architecture into which they feed — alarm management, emergency response escalation, process shutdown logic — may be subject to SIL requirements. Technology selection must account for how lone worker data integrates with the facility's overall safety instrumented architecture.*

1.4 Regulatory Summary

Regulation / Standard	Applicability	Key Requirement
OSHA General Duty Clause Section 5(a)(1)	All employers	Workplace free from recognized hazards; cited for inadequate lone worker monitoring
29 CFR 1915.84	Shipyard employment (benchmark for all)	Account for lone workers at regular intervals by sight or verbal communication

29 CFR 1910.269	Electric power generation / T&D	Two-person rule for certain tasks; lone workers reachable within 4 minutes by CPR-trained colleague
29 CFR 1910.146	Permit-required confined spaces	Attendant required outside confined space; continuous communication with entrant
OSHA PSM (1910.119) + ISA 84 / IEC 61511	Highly hazardous chemical (HHC) process facilities	Safety-critical functions must meet SIL requirements per LOPA; applies to alarm escalation and ESD integration

2. Establishing the Risk-Based Foundation

Technology selection begins not with product evaluation, but with a rigorous understanding of the risk profile that the system must address. In oil & gas and chemical manufacturing, lone worker hazards span a spectrum from chronic low-severity exposures to acute, immediately life-threatening events.

2.1 Hazard Categories for Lone Workers

Hazard Category	Examples	Detection Method	Response Window
Toxic gas exposure	H_2S, CO, SO_2, VOCs	Electrochemical / PID sensors	Seconds to minutes
Combustible atmosphere	LEL (methane, propane)	Catalytic bead / IR sensors	Immediate
Man-down / incapacitation	Fall, loss of consciousness, heat stress	Accelerometer, no-motion timer	30s–90s (configurable)
Confined space entry	O_2 depletion, entrapment	Multi-gas + communication	Continuous monitoring
Workplace violence / intrusion	Unauthorized access, assault	SOS / panic button, geofencing	Immediate
Environmental exposure	Extreme heat, cold, radiation	Environmental sensors, biometrics	Minutes to hours

Table 1: Lone Worker Hazard Categories in O&G and Chemical Manufacturing

2.2 Applying LOPA to Lone Worker Scenarios

Layers of Protection Analysis (LOPA), as described in ISA 84 / IEC 61511, provides a structured method for determining the required risk reduction for each hazard scenario. While LOPA is traditionally applied to process safety events, the methodology is equally applicable to lone worker protection design. Each protection layer — from inherent safety measures to administrative controls to the lone worker monitoring system itself — contributes a quantifiable risk reduction factor.

For example, consider a lone worker performing valve maintenance on an H_2S-containing pipeline in a remote location. The initiating event is an uncontrolled release. Protection layers might include process design (inherent safety), pressure relief systems, gas detection and alarm, the lone worker's personal gas monitor with automatic escalation, and the emergency response team. LOPA determines whether the combined risk reduction from all layers meets the tolerable risk threshold — and if not, what additional capability the lone worker system must provide.

3. Lone Worker Safety System Architecture

A well-designed lone worker safety system is not a single device — it is an integrated architecture spanning four functional layers, from the wearable device on the worker's body to the cloud platform where safety data is aggregated, analyzed, and acted upon.

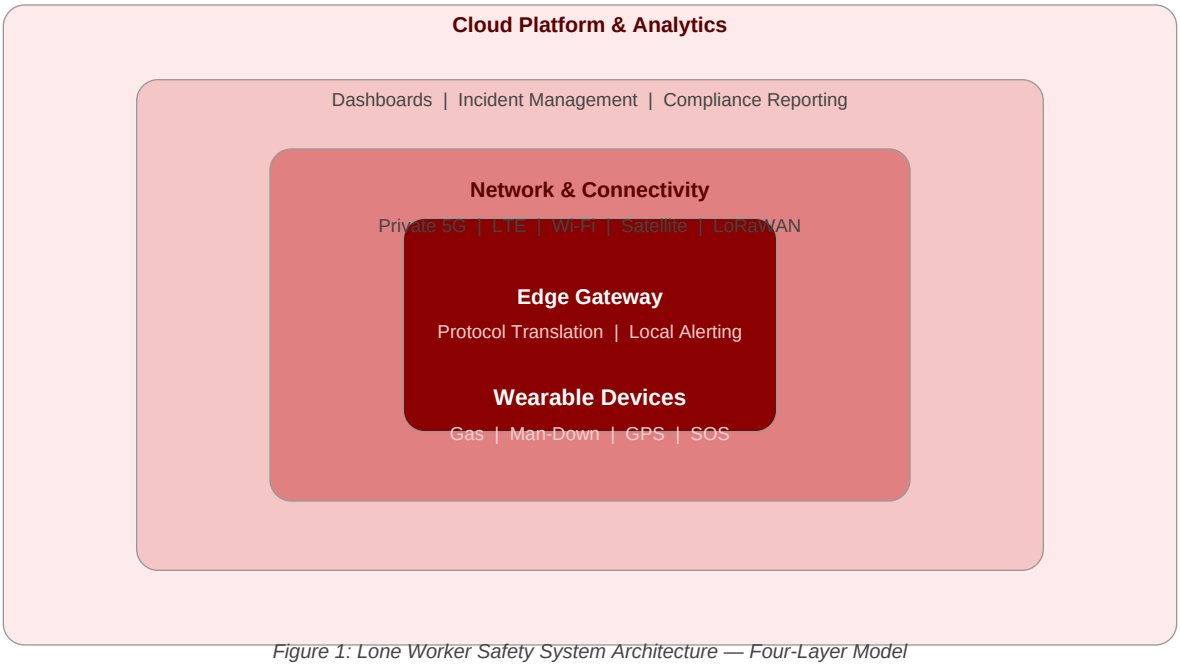

Figure 1: Lone Worker Safety System Architecture — Four-Layer Model

3.1 Layer 1 — Wearable Devices and Personal Sensors

The device layer is the foundation of the system and the primary interface with the worker. Modern lone worker wearables integrate multiple safety functions into a single form factor: multi-gas detection (typically H_2S, CO, O_2, and LEL at minimum), accelerometer-based man-down and fall detection, GPS location tracking, SOS/panic button, and two-way voice communication. The most capable devices support over-the-air configuration updates and can be reconfigured from single-gas to multi-gas as operational needs evolve.

Critical selection criteria at this layer include hazardous area certification (discussed in Section 4), battery life under continuous monitoring, sensor accuracy and cross-sensitivity characteristics, ergonomic wearability for extended shifts, and the ability to function as both a standalone safety device and a connected node in the broader system.

3.2 Layer 2 — Edge Gateway and Aggregation

The edge layer serves as the intermediary between field devices and the network. In vehicular deployments, a gateway installed in the worker's truck or service vehicle can aggregate data from the personal wearable and provide connectivity bridging — for example, using Bluetooth locally while backhauling over cellular or satellite. Edge gateways are particularly critical in environments where direct device-to-cloud connectivity is unreliable, such as remote wellheads, pipeline corridors, or large processing facilities with RF propagation challenges.

3.3 Layer 3 — Network and Connectivity

The connectivity layer determines whether the system can deliver on its promise of real-time monitoring. In industrial environments, this is often the weakest link. A lone worker device with sophisticated sensing capabilities is only as

useful as the network that carries its data. Connectivity options for lone worker systems span a range of technologies, each with distinct trade-offs.

Connectivity Technology Comparison for Lone Worker Systems

Private 5G/LTE	Industrial Wi-Fi	LoRaWAN	Satellite
Latency: <1s latency	**Latency:** Low latency	**Latency:** Seconds	**Latency:** High latency
Bandwidth: High BW	**Bandwidth:** Med BW	**Bandwidth:** Low BW	**Bandwidth:** Low BW
Range: Campus/site	**Range:** Building/area	**Range:** Wide area	**Range:** Global

Figure 3: Connectivity Technology Fit by Lone Worker Deployment Scenario

The choice of connectivity technology is highly site-dependent. A Gulf Coast refinery with dense infrastructure may be well served by Private 5G or industrial Wi-Fi. A Permian Basin operator with dispersed wellheads across hundreds of square miles will likely need a combination of cellular (where available) and satellite backhaul. Many deployments require a multi-bearer approach — with automatic failover between connectivity modes — to ensure that no worker is ever truly disconnected.

3.4 Layer 4 — Cloud Platform and Analytics

The cloud layer is where data from the field is transformed into actionable safety intelligence. Core platform capabilities include real-time dashboards showing worker location and status, configurable alert escalation workflows, incident management and documentation, compliance reporting (automated check-in logs, exposure records, response time tracking), and historical analytics for identifying patterns and driving continuous improvement.

Integration with existing systems is a key differentiator at this layer. The platform should be capable of feeding data into the facility's distributed control system (DCS), emergency management system, and enterprise safety management tools. API availability, support for standard industrial protocols (OPC-UA, MQTT), and data export capabilities are essential evaluation criteria.

4. Hazardous Area Classification and Device Selection

In oil & gas and chemical manufacturing, the operating environment dictates what equipment can be deployed. Hazardous area classification — the systematic identification of zones where explosive atmospheres may be present — directly constrains the selection of lone worker devices. Deploying a non-certified device in a classified area is not merely a compliance failure; it is a potential ignition source.

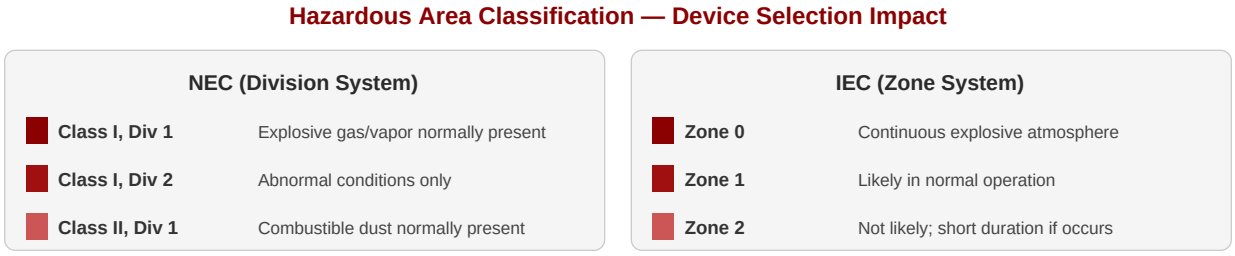

Figure 4: Hazardous Area Classification Systems — NEC vs. IEC

4.1 Understanding the Classification Systems

North America primarily uses the NEC Division system (Class I Division 1 and Division 2), while international standards follow the IEC Zone system (Zone 0, 1, and 2 for gases; Zone 20, 21, and 22 for dusts). In the NEC system, Division 1 indicates that ignitable concentrations of flammable gases or vapors can exist under normal operating conditions, while Division 2 indicates such concentrations arise only under abnormal conditions. The IEC Zone system provides a more granular, probability-based classification with three tiers. Most modern facilities are designed using the Zone system, though the Division system remains prevalent in legacy installations.

4.2 Device Certification Requirements

Area Classification	Required Protection	Certification Standard	Practical Impact
Class I, Division 1 (approx. Zone 0/1)	Intrinsically Safe (IS) or Explosion-Proof	UL 913, CSA C22.2 No. 60079-11, IECEx	Most restrictive; limits device power, battery size, and sensor options. Fewer products available.
Class I, Division 2 (Zone 2)	Non-incendive, Hermetically sealed	UL 121201, CSA C22.2 No. 213	Wider device selection; standard smartphones with certified cases may qualify.
Non-classified area	General purpose	Standard commercial certifications	Full device flexibility; consumer-grade devices acceptable.

Table 2: Hazardous Area Certifications and Their Impact on Device Selection

> ***Field note:*** *In practice, the most common mistake in lone worker technology deployment is specifying a device for the most hazardous zone on site and deploying it everywhere — including non-classified areas where a more capable, less restricted device would provide better protection. A risk-based approach matches device certification to actual zone requirements, area by area.*

4.3 The C1D1 Challenge

Class I Division 1 certification imposes significant constraints on device design. Intrinsic safety requirements limit the energy that can be stored or dissipated by the device, which directly affects battery capacity, display brightness, speaker volume, and processing power. This creates an inherent tension: the most hazardous environments demand the most capable safety monitoring, yet the certification requirements restrict the device capabilities that enable that monitoring.

Resolving this tension requires careful system architecture. In C1D1 environments, the wearable device may be deliberately constrained to core sensing and alerting functions, with data-intensive processing — analytics, video streaming, detailed location mapping — handled by edge gateways or cloud platforms outside the classified zone. This distributed approach preserves IS certification at the device level while maintaining full system functionality.

5. The Technology Selection Framework

With the regulatory context, risk foundation, system architecture, and hazardous area constraints established, the following four-phase framework provides a structured approach to selecting and validating the right technology stack.

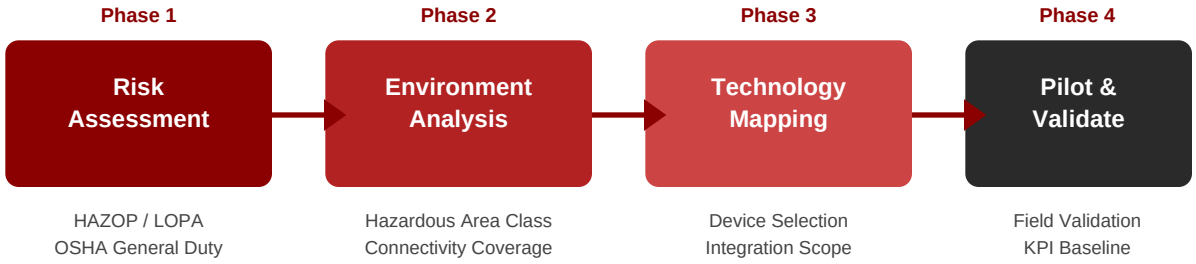

Figure 2: Technology Selection Framework — Four-Phase Approach

1

Phase 1: Risk Assessment and Requirements Definition

Begin with a formal risk assessment for each lone worker scenario, using HAZOP, LOPA, or an equivalent methodology appropriate to the facility's process safety management framework. Document the hazard profile for each work type (routine rounds, maintenance, confined space entry, emergency response), the required detection capabilities (gas species, man-down sensitivity, location accuracy), the mandated response times (from detection to control room notification to emergency team dispatch), and the regulatory requirements applicable to the specific facility and jurisdiction.

2

Phase 2: Environment Analysis and Constraints Mapping

Map the physical and electromagnetic environment across all areas where lone workers operate. This includes hazardous area classification zone-by-zone (determining which device certifications are required where), a connectivity survey covering existing cellular coverage, Wi-Fi infrastructure, and RF propagation characteristics, and identification of GPS-denied areas such as indoor process units, underground facilities, and dense metallic structures where alternative positioning technologies (UWB, BLE beacons) may be needed.

3

Phase 3: Technology Mapping and Vendor Evaluation

With requirements and constraints defined, evaluate candidate technologies against a structured matrix. Critical evaluation dimensions include: device capabilities vs. hazardous area certification requirements, connectivity architecture and failover design, platform integration capabilities (API, OPC-UA, MQTT, DCS/SCADA connectivity), data residency and cybersecurity posture (particularly relevant for OT environments where IT/OT convergence introduces risk), total cost of ownership including devices, connectivity, platform licensing, and ongoing calibration/maintenance, and vendor viability and support infrastructure.

4

Phase 4: Pilot Deployment and Validation

Before committing to enterprise-wide deployment, conduct a structured pilot in a representative operating environment. The pilot should validate device performance under actual field conditions (temperature, humidity, vibration, chemical exposure), test connectivity reliability across all coverage zones including edge-of-coverage scenarios, exercise the full alert escalation chain from device alarm through control room notification to emergency response dispatch, measure actual response times against requirements, and validate user acceptance — because the most sophisticated safety device is useless if workers find it too cumbersome to wear or too complex to operate.

5.1 Technology Evaluation Matrix

The following matrix provides a structured framework for scoring candidate solutions against weighted criteria. Weights should be adjusted based on the specific risk profile and operational constraints identified in Phases 1 and 2.

Evaluation Criterion	Weight	Scoring Guidance
Hazardous area certification coverage	Critical	Pass/fail. Device must hold valid certification for every classified zone where it will be deployed.
Gas detection capability	High	Number of gas sensors, species coverage, sensor accuracy, cross-sensitivity characteristics, bump test / calibration requirements.
Man-down / fall detection	High	Sensitivity / specificity trade-off; configurable thresholds; false positive rate under actual field conditions.
Connectivity reliability	High	Coverage footprint, automatic failover between bearers, latency from alarm to platform receipt.
Location accuracy	Medium–High	Outdoor GPS accuracy; indoor positioning capability (UWB, BLE); vertical positioning (floor/level).
Battery life	Medium	Runtime under continuous monitoring with all sensors active; charging time; hot-swap capability.
Platform integration	Medium	API availability, OPC-UA/MQTT support, DCS/SCADA integration, SIEM/SOC feed capability.
Ergonomics and wearability	Medium	Weight, form factor, clip/harness options, compatibility with PPE, ease of use with gloves.
Total cost of ownership	Medium	Device cost, connectivity fees, platform licensing, calibration consumables, replacement cycle.
Cybersecurity posture	Medium	Data encryption (at rest and in transit), authentication, SOC 2 / ISO 27001 compliance, OT network segmentation.

Table 3: Weighted Evaluation Matrix for Lone Worker Safety Technology Selection

6. Implementation Considerations

6.1 Integration with Existing Safety Architecture

A lone worker safety system does not operate in isolation. Its value is maximized when it is integrated into the facility's broader safety and operational infrastructure. Key integration points include the plant's DCS or SCADA system for process context (e.g., correlating a gas alarm from a worker's personal monitor with readings from the fixed gas detection network), the emergency management system for coordinated response, the enterprise safety management platform for compliance documentation and trend analysis, and the IT/OT security operations center for monitoring the health and integrity of the safety system itself.

6.2 Cybersecurity in OT-Connected Safety Systems

Any system that connects field devices to cloud platforms through the facility's network introduces potential attack vectors. This is especially sensitive when the system touches OT networks. Cybersecurity considerations include network segmentation (the lone worker system should operate on a dedicated VLAN or network segment, isolated from process control traffic), device authentication and encryption (TLS 1.2+ for data in transit, AES-256 for data at rest), cloud platform security (SOC 2 Type II compliance at minimum; evaluate data residency for sensitive operational data), and vulnerability management and patching processes for all system components including firmware on edge devices.

6.3 Change Management and Worker Adoption

Technology deployments fail most often not because of technical shortcomings, but because of inadequate change management. Workers who perceive the system as surveillance rather than protection will resist adoption — and a safety device that sits in a locker instead of on a worker's belt provides zero protection. Successful adoption requires involving frontline workers in the evaluation process (their input on wearability and usability is invaluable), framing the system as a safety lifeline rather than a tracking tool, providing thorough hands-on training that includes simulated emergency scenarios, establishing clear data governance policies that define what data is collected, who can access it, and how it is used, and demonstrating responsiveness — when the system generates an alert, the response must be swift and visible.

6.4 Maintenance and Lifecycle Management

Connected safety devices require ongoing maintenance that goes beyond traditional gas detector calibration. A comprehensive lifecycle management program should address bump testing and calibration schedules per manufacturer specifications and site-specific gas exposure profiles, firmware and software update management (including OTA update capability and rollback procedures), battery health monitoring and replacement scheduling, sensor degradation tracking and proactive replacement before end-of-life, and device assignment management for shift changes, contractor onboarding, and multi-user deployments.

> ***Key metric:*** *Track system availability — the percentage of time each lone worker is actively connected and monitored during their shift. Industry benchmarks for connected safety systems target 98%+ availability. Anything below 95% indicates systematic connectivity or device management issues that must be addressed.*

7. Conclusion and Next Steps

Lone worker safety in oil & gas and chemical manufacturing is not a single-product problem. It is a systems engineering challenge that requires integrating the right devices, the right connectivity, and the right platform into a facility's existing safety and operational architecture — all within the constraints imposed by hazardous area classification, regulatory requirements, and the practical realities of field operations.

The four-phase framework presented in this brief — risk assessment, environment analysis, technology mapping, and pilot validation — provides a structured, defensible approach to technology selection that prioritizes field credibility over marketing claims. By beginning with the hazard profile and working outward to the technology solution, organizations can make investment decisions that are grounded in actual operational risk rather than vendor promises.

The technology landscape for connected worker safety is evolving rapidly. Private 5G networks are extending reliable connectivity to previously unreachable areas. Wearable devices are becoming more capable while maintaining intrinsic safety certification. Cloud platforms are delivering analytics that move safety management from reactive incident response to proactive risk prevention. Organizations that establish a solid technology selection foundation now will be best positioned to adopt these advances as they mature.

Document Reference: CIQ-TB-LW-2025-001 | Published: 2025 | Clover IQ | sales@cloveriq.com | www.cloveriq.com