Industrial Emergencies Need a Well Defined "Crisis Communication System" A practitioner-informed exploratory study and framework for high-hazard facilities

G. S. Baveja

Former Corporate Head – HSSE, Bharat Petroleum Corporation Ltd.

DOI: https://doi.org/10.51244/IJRSI.2026.1310000212

Received: 24 September 2026; Accepted: 29 September 2026; Published: 15 November 2026

ABSTRACT

Industrial emergencies in refineries, petroleum terminals, chemical plants, and other high-hazard facilities require more than effective firefighting, process isolation, and rescue operations. They also demand timely, accurate, coordinated and stakeholder-specific communication. When information is delayed, inconsistent or inaccessible, operational response may be impeded, families may experience avoidable distress, emergency access may be obstructed, and confidence in the organization may be weakened. This paper examines three practitioner-observed industrial fire emergencies: a refinery fire/explosion in 1988, a fire at Jawahar Dweep in 2017, and a fire emergency encountered during an occupational health, safety, and environment audit. The cases are used as retrospective practitioner illustrations rather than as a statistically representative or conventionally documented qualitative dataset. The paper distinguishes direct observations and recollections from interpretations informed by emergency-communication literature and from the managerial framework proposed by the author. It develops an Industrial Crisis Communication Framework covering preparedness, detection and notification, command and information verification, stakeholder-specific dissemination, monitoring and feedback, and post-emergency learning. Attention is given to family information arrangements, communication redundancy, the separation of operational command channels from public-facing communication, vulnerable stakeholders, misinformation, cyber resilience, and measurable readiness. A preliminary readiness scorecard is proposed for pilot testing in tabletop and full-scale exercises. The framework is intended as a practical, auditable aid for plant-specific emergency preparedness; its effectiveness requires prospective validation.

Keywords: industrial emergency; crisis communication; emergency response; ERDMP; stakeholder communication; family assistance; information verification; high-hazard industry; emergency preparedness.

INTRODUCTION AND BACKGROUND

Industrial facilities are designed and operated to maintain stable production, but no plant can be assumed to remain indefinitely in normal operating conditions. Equipment failures, process deviations, fires, explosions, natural events, utility failures, and other unexpected situations may require rapid intervention. In process industries, an emergency can have consequences beyond the immediate unit because interconnected processes, inventories, utilities and upstream or downstream operations may be affected.

This paper focuses on communication during major or significant industrial emergencies, particularly fire-related events, rather than routine operational upsets. The central argument is that communication is not an auxiliary public-relations function. It is an enabling component of emergency management. Information about the nature and location of the incident, personnel accountability, evacuation or shelter-in-place instructions, hazards, emergency access, medical support, regulatory notifications, and family enquiries can influence the quality and speed of the overall response.

The author draws on professional experience associated with three industrial fire emergencies and observations made during occupational health, safety, and environment (OHSE) work. These experiences

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

prompted reflection on recurring communication vulnerabilities. They are presented here as practitioner evidence with explicit limitations, not as proof that the same deficiencies occur in every facility.

Purpose, Scope, and Research Questions

The purpose is to examine how communication weaknesses may complicate industrial emergency response and to propose a practical framework that organizations can incorporate into their Emergency Response and Disaster Management Preparedness Plan (ERDMP) or equivalent site emergency plan.

The paper addresses four exploratory questions:

- Which communication vulnerabilities were apparent in the three practitioner-observed incidents?
- How might delayed, inconsistent or inaccessible information affect operational coordination, family enquiries and stakeholder understanding?
- What organizational arrangements can improve communication before, during and after an industrial emergency?
- How can communication readiness be assessed through exercises and auditable performance indicators?

The paper does not claim to measure causal effects on emergency outcomes or stakeholder confidence. It identifies plausible mechanisms and practical lessons that warrant testing in future exercises and research.

APPROACH AND METHODOLOGICAL POSITION

Study design

The manuscript is positioned as a practitioner-informed exploratory multiple-case reflection and framework-development paper. The three cases were selected purposively because they were within the author's professional experience or direct professional connection and illustrated different communication challenges: family enquiries and crowd management; coordination of safety assurance and operational restart priorities across organizations; and inadequate information flow to a plant gate during an emergency.

The cases are heterogeneous in date, setting and the author's proximity to the events. They are not treated as equivalent units of observation, nor are they intended to support statistical generalisation. The 1988 case relies substantially on retrospective recollection and subsequent discussions with colleagues. The 2017 case draws on the author's participation in a third-party inspection assignment after the fire and on the account recorded in the original practitioner material. The third case is based on observations made in the context of an OHSE audit; the original account does not provide the plant name, exact date, or contemporaneous records.

Evidence boundaries and analysis

For analytical transparency, the paper separates three evidence layers:

- Case-based material: events and observations described by the author, including the limits of recollection and documentary corroboration.
- Literature-informed interpretation: established emergency-communication principles such as timely notification, empathy, credibility, message consistency, stakeholder differentiation, redundancy, and learning.
- Author-proposed framework: the Industrial Crisis Communication Cycle and the preliminary readiness scorecard presented in this paper. These are proposals for application and evaluation, not validated instruments.

The cases were reviewed comparatively by identifying recurring communication topics in the original narratives: notification and timeliness; access to reliable information; family and community enquiries; coordination between organizations and role-holders; competing operational priorities; and communication arrangements at the site boundary. These topics were then grouped into practical themes and mapped to the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

proposed framework. This is a descriptive thematic synthesis, not a formal qualitative coding study. No formal codebook, independent second coder, inter-coder reliability test or systematic interview protocol was used. Contradictory evidence could not be systematically sought because the underlying records and informants were not available for this revision.

Accordingly, statements about the cases are phrased as the author's observations or recollections. Broader claims are framed as risks or plausible implications unless supported by the cited guidance. Future research should strengthen the evidence base through contemporaneous records, interviews with multiple stakeholder groups, peer review of coding and prospective exercise data.

Case-evidence summary

Case	Year / setting	Author's relationship	Evidence described	Communication issue illustrated	Interpretive value	Limitations
I	1988; refinery fire/explosion	Present at the refinery and involved in emergency-support activities; subsequent discussions with colleagues	Retrospective personal recollection; later discussions; newspaper clipping reproduced in source article	Families had difficulty obtaining dependable personnel-status information; crowd and media presence at the gate	Shows the importance of family information, personnel accountability, and controlled access	Long recall interval; no contemporaneous internal incident report or family interviews presented; public clipping does not verify all communication observations
II	7 October 2017; Jawahar Dweep oil terminal fire	Member of third-party inspection team engaged after the fire to assess safe restart conditions	Professional participation in post-incident inspection; press reports reproduced in source article; discussions with facility officials	Different priorities between operational restart expectations and safety assurance; need for clear coordination between organizations	Illustrates communication across organizational boundaries and the need to distinguish operational urgency from verified safety clearance	The author's role was post-fire, not incident command; no full communication log or independent stakeholder interviews presented
III	Date and facility not specified; industrial fire during OHSE audit	Member of an OHSE audit team; observed events around the facility gate after learning of the fire	Retrospective practitioner observation recorded in the source article	Families and others gathered at the gate; information did not appear to reach gate control adequately; emergency vehicle access was obstructed	Highlights the site-boundary interface, family enquiries, crowd management, and emergency access	Exact date, facility, incident records, and contemporaneous audit notes are not supplied; details are intentionally limited in the source account

What the Three Cases Illustrate

Case I: refinery fire/explosion, 1988

The author recalls a major refinery fire/explosion on the day of Deepawali. Employees and other personnel supported firefighting, medical assistance, logistics, gate control, and relief of fire crews. The fire chief led the response with support from local management, and senior management subsequently arrived. The author's principal communication observation concerns families seeking information about employees and contractors inside the refinery. In the absence of a clearly functioning family-information arrangement, relatives relied on informal sightings and verbal assurances. Some employees were unable to contact their families for several hours.

The case therefore points to the need for a designated family-information point, a dependable personnel-accountability process, and a controlled method of communicating confirmed information. The recollection is valuable as practitioner experience, but the precise sequence and scale of the communication gaps should not be treated as independently verified in the absence of contemporaneous internal records or interviews with affected families.

Case II: Jawahar Dweep fire, 7 October 2017

The author describes a fire at Jawahar Dweep, an oil terminal managed by the then Mumbai Port Trust, serving crude-oil tanker operations associated with refineries. After the fire was extinguished, a third-party inspection team was engaged to assess conditions for a safe resumption of berthing operations. The author participated in that inspection. The account records an apparent difference in emphasis: refinery-side personnel were concerned about restoring crude supply and operations, while the terminal-side officials emphasised verification of fire and safety conditions, including isolation of relevant vents, drains, and interconnecting lines.

The communication lesson is not that one priority was inherently improper. Continuity of supply and safe restart are both legitimate concerns, but they must be reconciled through a transparent decision process, documented evidence, and clearly assigned authority.

The case illustrates the importance of inter-organizational communication, agreed acceptance criteria and avoiding pressure for operational resumption before safety verification is complete. Since the author's involvement was in the post-fire inspection, the case does not provide direct evidence about the quality of communications during the firefighting phase.

Case III: fire observed during an OHSE audit

The author recalls being part of a third-party OHSE audit team at a major industrial plant. During an evening meeting, members of the client organization received telephone calls and subsequently informed the group that a fire emergency had occurred at the plant. On approaching the facility, the audit team observed a large crowd near the main gate.

The crowd was concerned about the well-being of relatives working inside the plant. The author observed that the gathering obstructed the gate and affected the movement of emergency vehicles, while security personnel and police attempted to manage the situation.

The case highlights the need for a pre-planned interface between the emergency control structure, security, gate control, police, and a family-information function. It also illustrates how an information vacuum can contribute to crowding and potentially compromise emergency access. The account does not establish the cause of the fire or quantify any operational delay. The facility and date are not identified in the source material, and no contemporaneous gate log or audit record is presented.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Cross-case synthesis

Across the three accounts, five recurring managerial concerns emerge: (i) timely and verified information for people directly affected; (ii) a designated route for family enquiries and personnel-status updates; (iii) clear coordination across departments and external organizations; (iv) controlled access and protection of emergency routes; and (v) explicit separation of safety decisions from production or business-continuity pressure. These are practitioner-derived themes. They are not frequency estimates and should not be interpreted as a ranking of the most common failures across industry.

Distinguishing Communication Functions

The term ‘crisis communication’ is often used broadly. For industrial emergency planning, it is useful to distinguish three connected functions:

- Operational emergency communication: real-time information exchanged by control rooms, incident controllers, firefighting teams, medical teams, security, maintenance and external responders to direct protective and response actions. It must be rapid, resilient, and governed by the incident-command structure.
- Emergency and risk communication: information provided to employees, contractors, families, nearby communities and other affected groups about hazards, protective actions, uncertainty, available assistance, and changing conditions. It should be timely, understandable, actionable and audience specific.
- Reputation- and accountability-oriented crisis communication: communication with media, regulators, investors, customers and the wider public about organizational actions, responsibility, investigation, recovery, and corrective measures. It must be accurate, appropriately authorized, and consistent with legal and regulatory obligations.

These functions overlap but should not be collapsed into one approval chain. A single verified information picture is essential, but centralization must not delay urgent operational instructions. Technical responders should retain established command and peer-to-peer channels within the emergency organization. Public-facing statements and stakeholder updates should use an authorized verification and release process.

Principles for Effective Industrial Crisis Communication

Timeliness with verification

Communicate early enough to support protective action but distinguish confirmed facts from information still being checked. State what is known, what is not yet known, what is being done to verify it and when the next update is expected.

Empathy and respect

Acknowledge fear, injury, loss, disruption and uncertainty without speculation or exaggerated reassurance. Families and affected communities should be treated as people requiring assistance, not merely as audiences.

Credibility and competence

Identify the responsible incident authority and provide clear, factual explanations of the response. Demonstrate competence through actions, accurate updates, and coordination rather than unsupported claims.

Consistency with audience relevance

Maintain one verified incident picture while tailoring the content, language, channel, and level of detail to the stakeholder group. Different audiences may need different actions and details.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Openness within legal and ethical limits

Do not conceal material facts or make premature claims. Protect personal information, casualty identities pending family notification, investigation integrity, security-sensitive details, and legally protected information.

Accountability and learning

Record significant messages, decisions, approvals, recipients, and update times. Explain corrective actions after the event and close identified gaps.

The Industrial Crisis Communication Framework

The following six-stage cycle is proposed as a practical architecture for integration into a site ERDMP. It is a framework for implementation and testing, not a validated model.

Stage 1 – Preparedness and stakeholder mapping

Identify credible emergency scenarios and affected groups; map information needs, preferred languages, accessibility needs, communication channels, and responsible role-holders. Prepare contact lists, message templates, escalation criteria, and fallback arrangements.

Stage 2 – Detection and initial notification

Define who can raise an alarm, who receives it, how the control room confirms the location and nature of the event, and how the incident-command structure is activated. Issue protective instructions without waiting for a media statement.

Stage 3 – Command, verification, and information management

Establish an incident information function or designated information manager. Maintain a time-stamped incident log separating confirmed facts, unverified reports, decisions, and information gaps. Resolve discrepancies through the incident-command structure.

Stage 4 – Stakeholder-specific dissemination

Issue appropriate updates to employees, contractors, responders, families, nearby communities, regulators, local authorities, customers, and media. Use approved spokespersons for external statements, while operational teams communicate directly through their command channels.

Stage 5 – Monitoring, feedback, and correction

Monitor enquiries, channel performance, social-media and media reports, rumours, and stakeholder feedback. Correct materially false information promptly, explain uncertainty and adapt messages as the situation changes.

Stage 6 – Recovery, review, and learning

Provide verified updates on all-clear or continuing restrictions, welfare support, business continuity, and investigation arrangements. Conduct a structured debrief, preserve records, and assign corrective actions with owners and deadlines.

Organization, Roles, and Information Governance

Each facility should define a site-specific communication organization linked to its incident-command and ERDMP arrangements. A generic structure may include:

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

- Incident Controller / Site Incident Controller: directs the site response and establishes operational priorities.
- Emergency Control Centre / Control Room: receives alarms, records initial information, activates the plan and maintains communication with field teams.
- Information Manager / Crisis Communication Lead: maintains the verified incident picture, coordinates stakeholder messages and records releases.
- Family Information Cell: receives enquiries, coordinates with personnel accountability and medical/HR functions, and provides confirmed information through a controlled process.
- Security and Gate Control: protects emergency access, manages assembly and visitor control, and routes family enquiries to the designated information point.
- Authorized Spokesperson(s): provide external updates, with trained primary and alternate personnel available across shifts.
- Regulatory and Liaison Coordinator: manages notifications and coordination with statutory authorities, district administration, police, fire services, and mutual-aid partners.
- IT / Telecom Support: maintains communication systems, cyber-resilience arrangements, and alternative channels.

Role names should be aligned with the terminology and statutory requirements applicable to the facility. A role-holder should never be assumed to be available solely because the person is named in a plan. Primary and alternate personnel, shift coverage, delegated authority, and escalation routes must be explicit.

Family information and personnel accountability

A family-information mechanism should be activated early when personnel may be missing, injured, evacuated, or otherwise affected. It should be physically separate from emergency vehicle routes and, where practicable, away from the main operational gate. The process should include:

- A designated telephone number and staffed information point, with a documented handover between shifts.
- A reliable method for reconciling employee, contractor, visitor, and emergency-responder accountability information.
- Verification before communicating an individual's status; casualty identities should be released in accordance with law, privacy requirements, and family-notification protocols.
- Multilingual support and a process for people who cannot use digital channels.
- Referral arrangements for medical, welfare, counselling, transport, and other immediate family needs.
- An enquiry log that records the caller, relationship, question, response, time, and follow-up commitment.

Communication redundancy and cyber resilience

Critical alerts should not depend on a single channel. Depending on site risk and infrastructure, the facility should evaluate combinations of public-address systems, sirens, radios, telephone trees, SMS/cell broadcast, approved messaging platforms, email, satellite, or other independent communications. Redundancy means more than having several applications: power supplies, network routes, devices, user access, contact data, and trained operators must also be considered.

The plan should address loss or compromise of digital communication systems, including ransomware, telecom outages, power failure, false alerts, account takeover, and manipulation of online information. Maintain offline contact lists, paper message forms, radio protocols, backup power, access controls, and an agreed method to authenticate official messages.

Stakeholder Mapping and Message Design

Stakeholder mapping should identify both priority and information need. A typical matrix is provided below; each site should adapt it to its hazard profile and local context.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Stakeholder group	Priority information	Likely channel(s)	Key safeguard
Employees and contractors	Alarm meaning, evacuation/shelter instructions, muster points, safe routes, accountability, and return-to-work status	Sirens/PA, radios, SMS, supervisors, notice boards	Include contract labour, visitors, shift workers, and workers with disabilities
Families	How to make enquiries, where to obtain verified updates, personnel status when confirmed, welfare support	Dedicated helpline, family centre, SMS/voice updates	No speculation or release of identities before authorized notification
Emergency responders and authorities	Hazard inventory, incident location, access routes, isolation status, resources, casualties, and changing risks	Dedicated radio/command channels, control centre, liaison officers	Use common terminology, clear command, and time-stamped updates
Nearby communities	Protective actions, affected area, shelter/evacuation advice, health precautions, and update timing	Sirens, local authority channels, public address, SMS, community representatives	Accessible, multilingual, and non-digital options
Regulators / district administration	Required notifications, verified incident facts, response status, and statutory reports	Designated liaison, prescribed reporting systems	Meet applicable notification timelines and preserve records
Media / public	Confirmed facts, actions taken, known impacts, uncertainties, and next update	Authorized spokesperson, briefing, official digital channels	Correct errors; avoid speculation, blame or premature assurances
Customers / suppliers / business partners	Supply disruption, continuity arrangements, safety restrictions, and expected update cadence	Account managers, formal notices, approved portals	Do not allow commercial pressure to override safety decisions

Holding statements

Pre-approved holding statements can help an organization acknowledge an incident while facts are being verified. They must be adapted to the actual situation and should never imply that all relevant facts are known.

“We are responding to an incident at [location]. The safety of employees, contractors, responders, and the surrounding community is our immediate priority. Emergency procedures have been activated, and the relevant authorities are being informed. We are verifying the details and will provide the next update through

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

[official channel] at [time]. Anyone in the affected area should follow instructions issued by [designated authority]."

Every update should carry a time, source or issuing authority, geographic relevance where appropriate, action required, and the expected time or channel for the next update. If information changes, explain the correction rather than silently replacing the earlier message.

Contemporary Communication Risks

Misinformation and rumours

Monitor public and employee channels for consequential false claims. Correct information promptly through trusted channels, explain the verified basis and avoid amplifying trivial rumours.

Unofficial photographs and posts

Employees and contractors may share images or comments before facts are established. Provide clear guidance on privacy, safety, confidentiality and the need not to obstruct response activities; do not rely solely on punitive controls.

AI-generated or manipulated content

Deepfake audio/video, fabricated notices, and synthetic images can imitate officials or depict events inaccurately. Establish authenticated official channels, verification contacts, digital evidence preservation, and a rapid correction protocol.

Language and accessibility

Prepare messages in relevant local languages and accessible formats. Consider hearing or visual impairment, literacy, age, disability, temporary workers, migrant labour and people without smartphones or reliable connectivity.

Cyber or infrastructure disruption

Plan for communication systems to fail or be compromised. Evaluate manual fallback, independent power, alternate radio frequencies, and authentication of instructions.

Training, Exercises and Performance Evaluation

A crisis communication plan should be assessed as an operating capability, not treated as a document-completion exercise. Tabletop exercises can evaluate decision-making and message approval; functional exercises can evaluate control-room, family-cell, and stakeholder-notification processes; and full-scale drills can assess communications under realistic noise, time pressure, and channel failure.

Exercise scenarios should include, as relevant, a major fire or explosion, missing personnel, contractor accountability, family gathering at the gate, loss of mobile networks, conflicting reports, a social-media rumour, a request for media comment, an off-site impact and pressure to restart operations. Exercise observers should record timestamps, decisions, failed channels, message accuracy, stakeholder reach and corrective actions.

Preliminary Crisis Communication Readiness Scorecard

The following scorecard is proposed as a starting point. It is not a validated benchmark. Each organization should establish site-specific target values after baseline testing, considering hazard severity, workforce size, geography, regulatory obligations, and available infrastructure.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Indicator	Operational definition	Evidence / data source	Owner	Suggested review
Time to first verified alert	Elapsed time from first credible detection to first authenticated alert to the defined response group	Alarm/control-room log; radio and alert-system timestamps	Control Room / Incident Controller	Every drill and incident
Emergency team activation time	Elapsed time from emergency declaration to acknowledgement by required primary/alternate role-holders	Call-out log; acknowledgement records	Emergency Coordinator	Every drill and incident
Contact-list currency	Percentage of sampled critical contacts confirmed accurate and reachable	Quarterly sample verification; HR/contractor records	HR / Emergency Planning	Quarterly
Critical-channel availability	Percentage of tested primary and alternate channels that function under the exercise conditions	Channel test sheets; telecom/IT logs	IT / Telecom	Monthly and during drills
Initial holding statement readiness	Elapsed time from authorization to issue of a factual initial public/stakeholder statement, where required	Approved statement and release timestamps	Crisis Communication Lead	Every relevant exercise
Personnel-accountability status	Percentage of persons in the defined affected population whose status is reconciled within the site's exercise target	Muster records; contractor and visitor registers	HR / Area Wardens	Every drill and incident
Family enquiry handling	Percentage of enquiries logged, acknowledged, and followed up within the site-	Family-cell enquiry register	Family Information Lead	Every drill and incident

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

	defined service target			
Message accuracy and consistency	Proportion of sampled messages free of material factual inconsistency and containing required action/update information	Message audit against incident log	Information Manager	Every drill and incident
Stakeholders reach and accessibility	Percentage of sampled target recipients reached through an accessible channel; record unmet groups	Delivery receipts; observer checks; feedback	Communication Lead	Every drill
Corrective-action closure	Percentage of communication-related corrective actions closed by due date and verified for effectiveness	Action tracker and closure evidence	ERDMP Owner / HSE	Monthly / quarterly

Scoring approach for pilot use: rate each indicator from 0 to 4—0 = absent; 1 = documented but not tested; 2 = tested with major gaps; 3 = tested and meets the site's provisional target; 4 = repeatedly demonstrated, including under degraded conditions. Record evidence and comments for every rating. Do not rely on an aggregate score alone: a serious weakness in personnel accountability, protective alerts or emergency access should trigger corrective action even if the overall score appears satisfactory.

Targets should be set only after baseline exercises. For example, the site may define acceptable notification and acknowledgement times by scenario and stakeholder group, rather than adopting a universal number that may be inappropriate for different facilities. The scorecard should be reviewed after each exercise and incident.

Integration with ERDMP and Emergency Command

The site ERDMP or equivalent emergency plan should contain, or clearly cross-reference, the following communication arrangements:

- Site-specific emergency scenarios and communication consequences, including on-site and off-site cases.
- Emergency organization chart showing command, communication, family assistance, liaison, and alternate role-holders.
- Separate operational communication and external/public communication protocols, with defined interfaces.
- Communication flow chart showing who receives, verifies, authorizes, and disseminates each class of information.

- Stakeholder register, contact directory, language/accessibility provisions, and update requirements.
- Family-information and personnel-accountability procedure, including contractor and visitor records.
- Primary and alternate channels, power backup, cyber-resilience, and manual fallback arrangements.
- Regulatory notification matrix and coordination arrangements with district authorities, police, fire services, hospitals, and mutual-aid partners.
- Approved holding statements, spokesperson protocol, media arrangements, and misinformation response.
- Message logs, document control, training records, exercise evaluation, and corrective-action tracking.

A typical flow is field detection or alarm → emergency control centre → incident controller and emergency organization → verification and incident information log → operational instructions through command channels and stakeholder-specific information through authorized routes → feedback and update → recovery communication and post-incident review. The flow must be adapted to the statutory ERDMP requirements and command terminology applicable to the facility. The ERDMP diagram reproduced in the earlier manuscript may be retained as a reference illustration only if its source, permission status, legibility, and regulatory currency are confirmed.

Ethical, Legal and Confidentiality Considerations

The cases are presented as professional recollections and observations from the author's work. The source material does not document a formal institutional ethics review, participant interviews, or written organizational permissions. Before publication in a journal or other formal research outlet, the author should confirm whether institutional or publisher ethics review is required and obtain any permissions necessary for use of organizational records, photographs, diagrams, and third-party material.

The present revision avoids naming the facility in Case III because the source account does not identify it. No personal casualty details are added. Where an incident is publicly identifiable, factual claims should be checked against reliable public records and clearly distinguished from the author's own observations. Confidential, proprietary, security-sensitive, and personal information should not be disclosed.

Transparency does not mean unrestricted disclosure. Communication must respect casualty-notification protocols, privacy and data-protection requirements, regulatory reporting duties, law-enforcement requests, investigation integrity, insurance processes, and legal proceedings. The organization should explain what can be shared, what cannot yet be confirmed and when further information is expected, without using legal constraints as a pretext for avoidable silence.

Limitations and Future Validation

This paper has several limitations. First, it relies on three heterogeneous practitioner cases, not a representative sample. Second, the 1988 account is retrospective and may be affected by recall and reconstruction. Third, the third case lacks a date, facility identity and supporting contemporaneous documentation in the source material. Fourth, the author's relationship to each event differs, limiting direct comparison. Fifth, no systematic interviews, formal coding protocol, independent coding, stakeholder-confidence measures, or communication logs were available for this revision. Sixth, the framework and scorecard have not been prospectively tested or validated.

The cases therefore support practical reflection and framework development, not causal conclusions about the effect of communication on incident outcomes or measured stakeholder trust. The framework should be evaluated through a staged programme: (i) expert review by emergency managers, regulators, communication specialists, worker and contractor representatives; (ii) baseline tabletop exercises at multiple high-hazard facilities; (iii) implementation of selected interventions; and (iv) repeat exercises using comparable scenarios and predefined measures. Future studies should collect time-stamped records, interview employees, contractors, families, and responders where ethically appropriate, and examine both successful and unsuccessful communication episodes.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

CONCLUSIONS AND RECOMMENDATIONS

Industrial emergency response is strengthened when communication is planned as an integral operational capability. The three practitioner accounts in this paper illustrate different vulnerabilities: uncertainty for families seeking personnel-status information, competing priorities during post-fire safety clearance and restart planning and crowding at a facility gate when reliable information is not readily available. Although the cases cannot establish prevalence or causality, they identify practical issues that site emergency plans can address.

The central recommendation is that every high-hazard facility should develop and periodically test a location-specific crisis communication system integrated with its ERDMP. The system should preserve rapid operational communication while ensuring that public-facing information is verified, authorized, timely and tailored to stakeholder needs.

- Develop a site-specific communication plan and flow chart linked to the emergency command structure, with primary and alternate role-holders.
- Establish a family-information cell and dependable personnel-accountability process covering employees, contractors, visitors, and responders.
- Separate operational command channels from external/public communication approval, avoiding bottlenecks in urgent response instructions.
- Map stakeholders by priority, information need, language, accessibility, and channel availability.
- Provide tested communication redundancy, offline fallback, and cyber-resilience arrangements.
- Train primary and alternate spokespersons and all role-holders who communicate with employees, families, responders, authorities, and communities.
- Prepare adaptable holding statements and a protocol for misinformation, social-media content and AI-generated or manipulated material.
- Include communication performance in tabletop, functional and full-scale exercises, using defined indicators and documented corrective actions.
- Review the plan after organizational changes, contact changes, incidents, exercises and changes in technology or regulatory requirements.

A plan is effective only when people can use it under pressure. The ultimate test is not whether a communication procedure exists on paper, but whether accurate and actionable information reaches the right people, through functioning channels, at the time it is needed—without delaying operational response or compromising safety, privacy, and accountability.

References and Source Note

The following source list is retained from the original practitioner manuscript. Several entries do not contain complete publication details. They should be bibliographically verified and standardized before journal submission; no missing authors, dates, titles, or publication data have been invented.

- Developing Emergency Communication Strategies, National Institute of Standards and Technology (NIST), United States. Full report details to be verified.
- Effective Workplace Fire Prevention, Advanced Consulting & Training. Publication details to be verified.
- Manual of Emergency Planning, Pollution Control Board, Madhya Pradesh. Edition and date to be verified.
- Off-site Emergency Management Plan, District Dhenkanal, Odisha. Version/date to be verified.
- Off-Site Emergency Response Plan, District Administration, Karnal, Haryana. Version/date to be verified.
- Fire Emergency Evacuation Plan & The Fire Procedure, FireSafe (website cited in the original manuscript; page and access date to be verified).

- Codes of Practices for Emergency Response and Disaster Management Plan (ERDMP) Regulations, 2010. Verify the applicable official notification and current amendments.
- How to Plan for Workplace Emergencies and Evacuations, U.S. Department of Labor, Occupational Safety and Health Administration, OSHA 3088, revised edition (publication details to be checked).
- Guide for All-Hazard Emergency Operations Planning, State and Local Guide (SLG) 101, Federal Emergency Management Agency, United States. Edition to be verified.
- International Conference on Communication, Management, and Information Technology (ICCMIT 2015): Knowledge Management Process in Several Organizations—Analytical Study of Modeling and Several Processes. Full author and proceedings details to be verified.
- Bernstein, Jonathan. The 10 Steps of Crisis Communications. Full publication details to be verified.
- Crisis Communications Handbook. Author, publisher, and edition to be verified.
- Crisis Management: Using the Power of Communication to Maintain Business Continuity. Author, publisher, and date to be verified.
- Crisis and Emergency Risk Communication, Disaster Control & Prevention, Hong Kong. Full issuing-body and edition details to be verified.

Case-specific public reporting reproduced in the original article includes a newspaper clipping concerning the 1988 refinery incident and news reports concerning the 2017 Jawahar Dweep fire.

REFRENCES

1. Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of Situational Crisis Communication Theory. Corporate Reputation Review, 10(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049
2. Coombs, W. T. (2015). The value of communication during a crisis: Insights from strategic communication research. Business Horizons, 58(2), 141–148. https://doi.org/10.1016/j.bushor.2014.10.003
3. Heath, R. L., & Lee, J. (2016). Chemical manufacturing and refining industry legitimacy: Reflective management, trust, precrisis communication to achieve community efficacy. Risk Analysis, 36(6), 1108–1124. https://doi.org/10.1111/risa.12504
4. Heinsberg, K. L., & Lamanna, A. J. (2024). Crisis communication in construction: Organizational strategies for worksite fatalities. Journal of Safety Research, 88, 145–160. https://doi.org/10.1016/j.jsr.2023.11.002
5. Jha, A., Lin, L., Short, S. M., Argentini, G., Gamhewage, G., & Savoia, E. (2018). Integrating emergency risk communication into the public health system response: Systematic review of literature to aid formulation of the 2017 WHO guideline for ERC policy and practice. PLOS ONE, 13(10), e0205555. https://doi.org/10.1371/journal.pone.0205555
6. Kasperson, R. E., Webler, T., Ram, B., & Sutton, J. (2022). The social amplification of risk framework: New perspectives. Risk Analysis, 42(7), 1367–1380. https://doi.org/10.1111/risa.13926
7. McLean, H., & Power, M. R. (2014). When minutes count: Tension and trust in the relationship between emergency managers and the media. Journalism, 15(3), 307–325. https://doi.org/10.1177/1464884913480873
8. Miller, A. N., Sellnow, T., Neuberger, L., Todd, A., Freihaut, R., Noyes, J., Allen, T., Alexander, N., Vanderford, M., & Gamhewage, G. (2017). A systematic review of literature on effectiveness of training in emergency risk communication. Journal of Health Communication, 22(7), 612–629. https://doi.org/10.1080/10810730.2017.1338802
9. Mohamad, B., Abdul Hamid, A. S., Adamu, A. A., & Wolf, K. (2025). Managerial roles in internal crisis communication across high-risk industries: Toward a comparative framework and measurement tool. Corporate Communications: An International Journal, 30(6), 1111–1129. https://doi.org/10.1108/CCIJ-05-2025-0111

10. Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. Academy of Management Review, 23(1), 59–76. https://doi.org/10.5465/amr.1998.192960
11. Reynolds, B., & Quinn, S. C. (2008). Effective communication during an influenza pandemic: The value of using a crisis and emergency risk communication framework. Health Promotion Practice, 9(4 Suppl.), 13S–17S. https://doi.org/10.1177/1524839908325267
12. Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. Journal of Health Communication, 10(1), 43–55. https://doi.org/10.1080/10810730590904571
13. Reddick, C. G., Chatfield, A. T., & Brajawidagda, U. (2016). Open government process and government transparency in crisis communication: The case of AirAsia QZ8501 crash. Information Polity, 21(3), 255–271. https://doi.org/10.3233/IP-160392
14. Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. Administrative Science Quarterly, 38(4), 628–652. https://doi.org/10.2307/2393339
15. Wray, R., Rivers, J., Whitworth, A., Jupka, K., & Clements, B. (2006). Public perceptions about trust in emergency risk communication: Qualitative research findings. International Journal of Mass Emergencies & Disasters, 24(1), 45–75. https://doi.org/10.1177/028072700602400102
16. Indian Express News Service. (2017, October 9). Butcher Island fire rages on for third consecutive day. The Indian Express.
17. Indian Express News Service. (2017, October 11). Butcher Island fire put out after four days. The Indian Express.

Appendix A – Minimum Exercise Observation Sheet

Observation item	What to record	Evidence	Finding / action
Detection and first alert	Detection time, alert time, recipient, and acknowledgement		
Command activation	Incident declaration, role activation, handover, and escalation times		
Information verification	Confirmed facts, unknowns, source, and time of verification		
Operational communication	Whether responders received timely, actionable instructions		
Family information	Activation time, enquiry handling, personnel-status verification		
Gate and access management	Crowd control, family routing, and unobstructed emergency access		
Channel resilience	Primary channel failure, fallback		

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

	activation, and delivery success		
External communication	Holding statement, approval, release time, and subsequent updates		
Misinformation response	Rumour detected, verification and correction time		
Learning and closure	Corrective action, owner, due date, and effectiveness check		