AEM
Association of Equipment Manufacturers

Automation & Autonomy Communications and Incident Response Framework



Industry Landscape, Case Studies, and Framework Considerations

AEM FUTURES COUNCIL

Nov. 9, 2026

Table of Contents

Executive Summary . . . 3
What This Paper Covers . . . 3
Why This Matters for the Non-Road Industry . . . 3

Part I - Industry Landscape Analysis . . . 4
Aviation Incident Response Model . . . 4
Step-by-Step Breakdown: How Aviation Handles a Significant Incident . . . 4
Communications Principles from Aviation . . . 4
Aviation SWOT Analysis . . . 5
On-Road Autonomous Vehicle Incident Response Model . . . 5
Step-by-Step Breakdown: How Autonomous Vehicle Incidents Are Typically Handled . . . 5
Autonomous Vehicle SWOT Analysis . . . 6
Aviation vs. Autonomous Vehicle Comparison . . . 6

Part II -Comparative Case Studies . . . 6
Case Study 1: Uber ATG Tempe Fatal Crash . . . 6
Incident Overview . . . 6
Response Analysis . . . 7
Lesson from Uber ATG . . . 7
Case Study 2: Cruise October 2023 Pedestrian Incident . . . 7
Incident Overview . . . 7
Response Analysis . . . 8
Direct Comparison: Uber ATG and Cruise Dimension . . . 8

Case Study Conclusion . . . 9

Internal Framework Considerations . . . 9
Recommended Framework Pillars . . . 9
Incident Response Framework Development Checklist . . . 10
Section 1: Governance & Organizational Readiness . . . 10
Section 2: Data Readiness & Evidence Preservation . . . 11
Section 3: Incident Classification & Escalation . . . 12
Section 4: Internal Coordination . . . 12
Section 5: Communications & Public Response . . . 12
Section 6: Regulatory & Government Engagement . . . 13
Section 7: Public Trust & Reputation Management . . . 13
Section 8: Learning & Continuous Improvement . . . 14

Framework Conclusion . . . 14

About the AEM Futures Council . . . 15



Executive Summary

This background paper provides companies with a practical understanding of how mature industries manage high-profile safety incidents and what lessons can be drawn from notable automation-related incidents. This document combines industry landscape analysis and comparative case study findings to help companies of different sizes and maturity levels understand the broader incident-response environment and inform their planning of a practical incident response framework.

The central conclusion is that effective incident response is not solely a communications exercise. It is an organizational capability built before an incident occurs through safety governance, clear decision rights, data readiness, internal coordination, regulator engagement, and disciplined external communications.

Companies should think about incident response in two connected phases: **readiness before an incident and response after an incident**. Two case studies from Uber and Cruise will be analyzed: Uber ATG illustrates the risk of weak pre-incident governance, while Cruise illustrates the risk of incomplete post-incident reporting and lost regulatory trust.

What This Paper Covers

- A step-by-step view of how aviation handles significant incidents through a mature investigation and communications model
- A step-by-step view of how the on-road autonomous vehicle sector handles incidents through data capture, reporting, technical reconstruction, and regulatory oversight
- A comparison of both models and what each offers companies
- SWOT analyses of aviation and autonomous vehicle incident-response approaches
- Detailed case studies of Uber ATG and Cruise, including response strengths, weaknesses, and implications for framework development
- Recommended framework building blocks and key considerations

Why This Matters for the Non-Road Industry

Agricultural and construction equipment manufacturers are entering a period where automation and autonomy will increasingly be deployed in complex, mixed human-machine environments. As adoption grows, so does the possibility of a highly visible incident that shapes public perception, customer confidence, policy debate, and regulatory action.

The purpose of this document is not to replace company-specific legal, safety, engineering, or communications plans. Instead, the opportunity is to provide helpful information, lessons learned, and a shared framework that supports better preparation, more consistent stakeholder engagement, and fact-based communications.

Part I - Industry Landscape Analysis

The two most useful reference points for the non-road industry are aviation and on-road autonomous vehicles. Aviation provides a mature model for independent investigation, communications discipline, and safety learning. The autonomous vehicle sector provides a closer technology analogue, with heavy reliance on sensor data, software logs, operational design domain assessments, reporting obligations, and rapid public narrative formation.

Aviation Incident Response Model

The aviation industry is widely viewed as a benchmark for incident investigation and post-incident communications. Its model relies on defined authority, clear investigative roles, structured access to technical expertise, and disciplined public communication. The NTSB party system allows organizations with relevant technical expertise to support the fact-finding phase while preserving the NTSB as the independent authority responsible for conclusions and recommendations.

Step-by-Step Breakdown: How Aviation Handles a Significant Incident

Phase	Description
1. Immediate life-safety response	Emergency response is activated, the scene is secured, affected individuals are supported, and immediate hazards are controlled.
2. Evidence preservation	Aircraft, equipment, maintenance records, flight records, event data, and other evidence are secured so investigators can reconstruct the event.
3. Authority notification and investigation activation	Relevant authorities are notified, and an independent investigation structure is established.
4. Party system/ technical expertise	Operators, manufacturers, regulators, and other technical experts may support fact-finding under the leadership of the investigating authority.
5. Communications coordination	Public information is tightly managed. Companies avoid speculation and focus on concern, cooperation, and facts that do not compromise the investigation.
6. Technical, human, organizational, and environmental analysis	The investigation considers systems, people, procedures, maintenance, training, weather, operations, and broader organizational factors.
7. Findings, recommendations, and learning	The final output emphasizes probable cause, contributing factors, safety recommendations, and prevention of future incidents.

Communications Principles from Aviation

- Acknowledge the event and express concern without speculating on cause.
- Coordinate with investigators before releasing information that could affect the investigation.
- Differentiate between factual background and technical or causal interpretation.

- Avoid statements that imply blame, exoneration, or conclusions before facts are established.
- Use the investigation as the primary path to public learning and future prevention.

Aviation SWOT Analysis

SWOT Element	Analysis
Strengths	Trusted investigation structure; independent authority; clear communications norms; strong safety-learning culture; high public credibility.
Weaknesses	Resource-intensive; formal processes can be slow; heavy regulatory complexity; difficult for smaller organizations to replicate fully; requires independent regulatory bodies.
Opportunities	Transferable principles around safety culture, independent fact-finding, evidence preservation, and disciplined communications.
Threats	Litigation pressure, political scrutiny, media demands for immediate answers, and increasing technology complexity can stress the model.

On-Road Autonomous Vehicle Incident Response Model

The autonomous vehicle sector is a younger and less settled model. It is highly relevant to the non-road industry because it involves software-enabled mobility, automation, operational design domains, sensor data, telemetry, public trust concerns, and rapidly evolving regulatory scrutiny. Unlike aviation, public narratives often form before formal investigations conclude.

Step-by-Step Breakdown: How Autonomous Vehicle Incidents Are Typically Handled

Phase	Description
1. Scene response and safety controls	The immediate priority is scene safety, emergency response, and determining whether operations should be paused or restricted.
2. Data preservation	Video, telemetry, sensor data, software version, diagnostics, operator inputs, and post-event behavior must be preserved quickly.
3. Technical reconstruction	Engineers assess what the system perceived, how it classified objects or hazards, what decision logic was used, whether the system was operating within its intended domain, and where human overrides may have occured.
4. Regulatory reporting	Regulators may require initial and updated reports describing pre-crash, crash, and post-crash details.
5. Public response and stakeholder communications	Companies must communicate before all facts are fully known while avoiding further speculation and ensuring that known material facts are not omitted.
6. Corrective actions and oversight	Responses may include software updates, operational changes, compliance reporting, independent review, or additional regulatory oversight.
7. Public trust recovery	The company must demonstrate that it understands the incident, has corrected deficiencies, and can continue operating safely or responsibly.

Autonomous Vehicle SWOT Analysis

SWOT Element	Analysis
Strengths	Rich operational data; strong technical visibility; rapid software learning cycles; ability to reconstruct event sequences using sensor and telemetry records.
Weaknesses	Less mature norms than aviation; inconsistent public trust; fragmented regulatory structures; tension between legal risk and transparency.
Opportunities	Ability to build proactive best practices before regulation hardens; potential to use data to demonstrate safety performance and continuous improvement.
Threats	High-profile incidents can quickly drive negative public narratives, regulatory overreaction, litigation, and loss of operating permissions.

Aviation vs. Autonomous Vehicle Comparison

Dimension	Aviation	Autonomous Vehicles
Investigation model	Independent, mature, formalized, global	Varies by event; often regulator/ company-driven, local
Communications model	Centralized and disciplined	Decentralized and fast-moving
Data model	Event recorders, maintenance records, operations data, simulation software	Video, telemetry, software logs, sensor data, ODD context, cloud data
Public trust	Generally high due to established process	Developing and vulnerable to high-profile events
Learning mechanism	Formal findings and safety recommendations	Corrective actions, software updates, oversight, and litigation-driven learning

Ultimately, the non-road equipment industry should not try to replicate aviation or on-road vehicle regulation. Instead, it can borrow aviation's discipline and autonomous vehicles' data-readiness lessons to inform a practical framework for non-road equipment manufacturers.

Part II - Comparative Case Studies

The Uber ATG and Cruise incidents are useful case studies because they highlight different failure modes. Uber ATG is best understood as a readiness failure involving safety governance and operator oversight. Cruise is best understood as a response failure involving completeness, transparency, and regulatory trust.

Case Study 1: Uber ATG Tempe Fatal Crash

Incident Overview

In March 2018, an Uber ATG developmental autonomous vehicle struck and killed a pedestrian in Tempe, Arizona. The automated driving system detected the pedestrian before impact but failed to properly classify the hazard or respond effectively. The human operator was distracted and did not intervene in

time. The NTSB identified deficiencies related to safety risk assessment, operator oversight, automation complacency controls, and safety culture.

Response Analysis

Response Area	Strength / Weakness	Detailed Analysis
Investigation cooperation	Strength	Uber ATG participated in the NTSB investigation, allowing the incident to be analyzed through technical, human factors, and organizational lenses.
Corrective action posture	Partial strength	Post-crash changes were documented in technical, operational, and organizational areas. This helped transition the response toward learning and improvement.
Transparency posture	Relative strength	The public record reviewed here focuses on safety governance and testing deficiencies rather than allegations of incomplete or intentionally misleading reporting to regulators.
Safety governance	Major weakness	The company entered the incident with inadequate safety risk assessment procedures, ineffective operator oversight, insufficient automation-complacency controls, and broader safety-culture weaknesses.
Human-machine supervision	Major weakness	The incident exposed the risk of relying on human supervision without adequate monitoring, training, engagement assurance, and escalation protocols.
Crisis readiness	Major weakness	Because weaknesses existed before the crash, the post-incident response was forced to address not only the event itself but also the company's broader readiness and safety management systems.

Lesson from Uber ATG

Uber ATG should be used as the readiness case. The lesson for companies is that incident response begins before deployment. Documented safety governance, operator oversight, risk management, and data readiness (both on-machine and in the cloud) must exist before an incident occurs.

Case Study 2: Cruise October 2023 Pedestrian Incident

Incident Overview

In October 2023, a pedestrian who had been struck by another vehicle entered the path of a driverless Cruise autonomous vehicle. The Cruise vehicle subsequently dragged the individual while executing a pull-over maneuver. The central public and regulatory issue became not only the vehicle behavior but also whether the company fully and accurately disclosed post-crash details to regulators.

Response Analysis

Response Area	Strength / Weakness	Detailed Analysis
Data availability	**Strength**	Video and operational data existed and ultimately enabled reconstruction of the event sequence.
Corrective action process	**Reactive strength**	Cruise ultimately entered formal corrective and compliance processes, including corrective action planning and expanded reporting obligations.
Independent/ internal review	**Partial strength**	Extensive review activity examined internal coordination, leadership decisions, and response failures after the incident.
Initial disclosure completeness	**Major weakness**	Regulators stated that post-crash details were omitted from reports, shifting focus from the technical event to the company's reporting practices.
Regulatory trust	**Major weakness**	Incomplete reporting damaged credibility and contributed to a broader regulatory and public trust crisis.
Internal coordination	**Major weakness**	Public reporting on review findings identified poor leadership, mistakes in judgment, lack of coordination, and misunderstanding of regulatory requirements.
Narrative control	**Major weakness**	The response became part of the story and overshadowed technical analysis, corrective actions, and broader safety claims.

Lesson from Cruise

Cruise should be used as the response case. The lesson for companies is that incomplete disclosure, poor coordination, and delayed correction can become as damaging as the incident itself.

Direct Comparison: Uber ATG and Cruise Dimension

Uber ATG	Cruise
Primary failure mode	Readiness failure	Response failure
Most significant weakness	Safety governance and testing oversight	Transparency, completeness, and regulator trust
Most useful lesson	Prepare before deployment	Coordinate and communicate accurately after an incident
Data role	Reconstructed technical and operator factors	Revealed post-crash behavior and reporting omissions
Public issue	Can the company safely test/ deploy?	Can the company be trusted to report accurately?
Framework implication	Pre-incident governance pillar	Post-incident communications and regulatory engagement pillar

Case Study Conclusion

Aviation and autonomous vehicles offer complementary lessons for companies. Aviation demonstrates the value of independent fact-finding, disciplined communications, and safety learning. Autonomous vehicles demonstrate the importance of data preservation, software and sensor reconstruction, regulatory reporting, and transparency in the face of rapidly forming public narratives.

Uber ATG and Cruise illustrate two different but connected risks. Uber ATG shows that weak safety governance and operator oversight can undermine the response before an incident occurs. Cruise shows that incomplete reporting and poor coordination can turn the response itself into a separate crisis. Companies should use both examples to inform a framework that emphasizes readiness, evidence preservation, coordinated decision-making, factual communications, prompt correction, and continuous improvement.

Internal Framework Considerations

The combined landscape analysis and case studies suggest that any framework should be organized around practical company readiness, and their framework should help companies ask the right questions before an incident and coordinate the right actions after one.

Recommended Framework Pillars

Framework Pillar	Purpose
1. Governance and safety culture	Define who owns autonomy safety, who can pause deployment, how risk is escalated, and how safety decisions are documented and decided.
2. Data readiness	Identify what logs, sensor data, video, telemetry, software versions, operator inputs, warnings, and pre- and post-incident records exist and how they are preserved.
3. Incident management	Create an internal coordination structure linking legal, engineering, safety, communications, customer support, regulatory, and executive decision-makers.
4. Stakeholder communications	Develop holding statements, escalation criteria, customer/dealer scripts, employee communications, media protocols, and policymaker engagement principles.
5. Regulatory engagement	Determine which authorities may need notification, how facts are verified before submission, and how updates or corrections are handled.
6. Continuous improvement	Document lessons learned, corrective actions, internal training needs, and anonymized insights that may inform broader industry safety practices.

Initial Company Readiness Checklist

Every organization developing a framework should be able to confidently answer the following 10 questions:

1. *Who is in charge if an incident occurs?*
2. *What data will we immediately preserve?*
3. *How quickly can we reconstruct what happened?*
4. *How will we coordinate technical, legal, and communications teams?*
5. *What will we say publicly in the first 24 hours?*
6. *What regulators may need to be contacted?*
7. *How will we ensure transparency without speculation?*
8. *How will we demonstrate that safety remains the top priority?*
9. *How will we determine and communicate corrective actions?*
10. *How will we learn from the event and improve?*

Incident Response Framework Development Checklist

The checklist below is designed as a practical self-assessment tool for companies developing their own incident response framework. The framework concepts emphasize governance, data readiness, internal incident management coordination, stakeholder communications, regulatory engagement, and continuous improvement.

✓ Section 1: Governance & Organizational Readiness

Leadership and Accountability

- Have we designated an executive responsible for incident response oversight?
- Have we identified a single incident commander or response leader?
- Are decision making authorities clearly documented?
- Is there a defined process for addressing identified issues within testing, deployment, or operation following a significant incident?
- Are legal, engineering, safety, communications, and executive responsibilities clearly assigned?

Safety Governance

- Do we have a documented safety management process?
- Do we periodically review autonomy related risks?
- Are escalation thresholds clearly defined?
- Have we identified foreseeable misuse scenarios?
- Do we review operator supervision requirements regularly?

Crisis Preparedness

- Have we conducted incident response tabletop exercises?
- Have we tested executive response procedures?
- Have we identified external advisors and subject matter experts before an incident occurs?
- Have we established communication protocols for weekends, holidays, and after-hours incidents?

✓ Section 2: Data Readiness & Evidence Preservation

Data Availability

- Can we determine the machine's operating mode?
- Can we identify who was operating, supervising, or monitoring the system?
- Can we determine whether the machine was operating within its intended conditions?
- Can we identify software versions running at the time?
- Can we identify configuration settings in use?

Data Capture

- Do we retain operational logs?
- Do we collect diagnostic information?
- Do we capture sensor data?
- Do we capture video imagery?
- Do we retain operator interaction records?
- Do we retain remote command history (if applicable)?
- Do we capture warning or alert information?
- Do we retain maintenance history?

Data Preservation

- Is there a documented data preservation procedure?
- Is responsibility for preserving data assigned?
- Is data captured immediately before the incident?
- Are retention periods defined?
- Can data be secured immediately after an incident?
- Are chain of custody procedures documented?

✓ Section 3: Incident Classification & Escalation

Incident Categories

- Have we established incident severity levels?
- Are trigger criteria defined for each level?
- Do employees know when incidents must be escalated?
- Have we defined "near-miss" events?
- Have we defined public reportable incidents?

Escalation Process

- Is there a documented notification tree?
- Are escalation timelines established?
- Are backup contacts identified?
- Have we identified situations requiring immediate executive involvement?

✓ Section 4: Internal Coordination

Response Team Structure

- Legal representative identified
- Safety representative identified
- Engineering representative identified
- Communications representative identified
- Regulatory representative identified
- Customer support representative identified
- Executive representative identified

Shared Fact Base

- Is there a process for creating a single verified timeline?
- Do all teams work from the same approved information?
- Is information validated before release externally?
- Is responsibility for fact verification assigned?

✓ Section 5: Communications & Public Response

Initial Communications

- Do we have a pre-approved holding statement?
- Does the holding statement avoid speculation?
- Does it express concern and commitment to safety?
- Does it acknowledge active fact gathering?
- Does it acknowledge cooperation with authorities when appropriate?

Stakeholder Communication Plans

- Customer communications prepared
- Dealer/distributor communications prepared
- Employee communications prepared
- Media communications prepared
- Regulator communications prepared
- Policymaker communications prepared
- Investor communications prepared (if applicable)

Messaging Principles

- Avoid speculation
- Avoid assigning fault prematurely
- Avoid releasing unverified information
- Avoid conflicting messages between departments
- Define approval processes for external statements

✓ Section 6: Regulatory & Government Engagement

Regulatory Readiness

- Have we identified potentially relevant regulators?
- Do we understand applicable reporting requirements?
- Have we identified required reporting timelines?
- Have we assigned reporting responsibilities?

Government Relations

- Have we identified potential policy sensitivities?
- Do we have a process for legislative inquiries?
- Do we have a process for agency outreach?
- Have we identified when other industry stakeholders should be informed or engaged?

✓ Section 7: Public Trust & Reputation Management

Reputation Considerations

- Can we explain the purpose and safety value of the technology?
- Can we explain the human role in system operation?
- Can we explain limitations of the system?
- Can we explain corrective actions clearly?
- Can we demonstrate commitment to continuous improvement?

Transparency Considerations

- Do we have a process for correcting inaccurate statements?
- Do we have a process for updating regulators if facts change?
- Do we have a process for updating customers if facts change?
- Have we established principles for transparency?

✓ Section 8: Learning & Continuous Improvement

Incident Review

- Do we conduct formal post-incident reviews?
- Do we identify root causes?
- Do we identify contributing factors?
- Do we identify organizational lessons?
- Do we identify process improvements?

Corrective Actions

- Are corrective actions assigned?
- Are owners identified?
- Are deadlines assigned?
- Are corrective actions tracked to completion?
- Are lessons incorporated into future development and deployment?

Industry Learning

- Should lessons be shared internally?
- Should lessons be shared with customers?
- Should lessons be shared through outside industry forums?
- Can lessons contribute to industry-wide best practices?

Framework Conclusion

The above accompanying checklist is intended as a practical starting point for organizations developing their own incident response frameworks. It is not intended to prescribe a single approach, but rather to help companies identify potential gaps, establish internal alignment, and ensure they have the foundational capabilities necessary to respond to an incident in a manner that protects people, preserves facts, maintains trust, and supports continuous improvement. Areas such as governance, data preservation, incident management, stakeholder communications, regulatory engagement, and organizational learning should be considered core components of any response framework.

Ultimately, the objective is not simply to manage a crisis, but to foster confidence in the safe and responsible deployment of automation and autonomy technologies. By proactively developing incident response capabilities today, organizations can strengthen resilience, support industry credibility, and help ensure that a future incident does not define public perception of these technologies.

About the AEM Futures Council

"Without disruption and innovation, progress isn't possible."

The global impact of non-road equipment manufacturing on our communities and our economy is well known. Taking that knowledge and the strong commitment of our 1,000-plus member companies to make a difference in our world, our AEM Futures Council has worked to tackle the disruptive trends poised to shape the industry of tomorrow.

Chaired by Dr. Ray Gallant of Volvo Construction Equipment North America, the AEM Futures Council brings together industry leaders and subject matter experts to identify disruptive trends and help members prepare for future challenges and opportunities.

Supported by AEM's Industry Sector leadership teams, the Council delivers value through thought leadership, strategic initiatives, industry insights, and member engagement opportunities designed to strengthen the industry's long-term success. For more information, visit aem.org/futurescouncil

AEM FUTURES COUNCIL

AEM Futures Council Chair:
Ray Gallant – *Volvo CE*

Erol Ahmed – *Built Robotics*

Brad Arnold – *AGCO*

Andy Black – *Husco*

Christian Bryzinski – *CNH Industrial*

Ann Davis – *John Deere*

Ryne DeBoer – *Morey*

Doug Griffin – *Kearney*

Emilie Hitch – *broadhead*

Rhett Hawkins – *RR46*

Colin Hurd – *Mach*

Joe Michaels – *Kubota North America*

Jeff Osterman – *Parker Hannifn*

Vijay Palanisamy – *Dynapac North America*

Darren Siekman – *Valley Global Irrigation*

Marcus Suess – *First Green Industries*

Alka Upadhyay – *Caterpillar*

Alicia VanDuyse – *Sherwin-Williams*

Jaime Wines – *Ditch Witch*

Staff Liaison–
John Rozum – *AEM*

AUTONOMY & AUTOMATION VISION TEAM

Erol Ahmed – *Built Robotics*

Xavier Drake – *Lely North America*

Grant Good – *AGCO*

Colin Hurd – *Mach*

Erik Klosinksi – *HCC*

Jason Looman – *Scanreco*

Jeff Osterman – *Parker Hannifn*

Kendal Quandahl – *Case IH*

Corey Quinnell – *Husco*

Byron Sheroan – *Link-Belt Cranes*

Joe Wieciek – *Agtonomy*

Patrick Wiltzius – *DeLaval*

Staff Liaison –
Austin Gellings – *AEM*

AEM
Association of Equipment Manufacturers

6737 W. Washington Street, Suite 2400 | Milwaukee, WI 53214-5650 | aem.org