सत्यमेव जयते

टीईसी का मानक दस्तावेज

टीईसी ५७०९०:२०२५

STANDARD DOCUMENT OF TEC

TEC 57090:2025

टेलीकम्युनिकेशन और महत्वपूर्ण डिजिटल अवसंरचना में ए आई घटना डेटा बेस की संरचना और वर्गीकरण

Schema and Taxonomy of an AI Incident Database in Telecommunications and Critical Digital Infrastructure

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली–110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 1: November,2025

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This Standard defines a standardized schema and comprehensive taxonomy for AI incident databases in telecommunications and related ICT. Artificial intelligence is increasingly being used across domains, offering significant benefits but also posing risks and harms when systems fail or are misused. The schema enables consistent and structured recording of incidents, while the taxonomy systematically categorizes and documents them. Together, they improve the understanding, prevention, and mitigation of AI-related harms.

CONTENTS

Clause **Particulars** **page No.**

HISTORY SHEET

S. No.	Standard document of TEC No.	Title	Remarks
1.	TEC 57090:2025	Standard for Schema and Taxonomy of an AI Incident Database in Telecommunications and Critical Digital Infrastructure	New Standard

REFERENCES

S.No.	Document No	Title/Document name
[1]	DOI ; 10.1109/CONECCT62155.2024.10677312	Agarwal, A., & Nene, M. J. (2024, July). Addressing AI Risks in Critical Infrastructure: Formalising the AI Incident Reporting Process. In 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT) (pp. 1-6). IEEE.
[2]	DOI ; 10.23919/ITUK62727.2024.10772925	Avinash, A., & Manisha, N. (2024, October). Advancing Trustworthy AI for Sustainable Development: Recommendations for Standardising AI Incident Reporting. In 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K) (pp. 1-8). IEEE.
[3]	DOI ; 10.1109/PuneCon63413.2024.10895867	Agarwal, A., & Nene, M. J. (2024, December). Standardised schema and taxonomy for AI incident databases in critical digital infrastructure. In 2024 IEEE Pune Section International Conference (PuneCon) (pp. 1-6). IEEE.

[4]	DOI ; 10.1609/aaai.v35i17.17817	McGregor, S. (2021, May). Preventing repeated real world AI failures by cataloging incidents: The AI incident database. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 35, No. 17, pp. 15458-15463).
[5]	DOI ; 10.3390/fire7030074	McNamara, D. J., & Mell, W. E. (2024). Examining exposure fires from the united states national fire incident reporting system between 2002 and 2020. Fire, 7(3), 74.
[6]	DOI ; 10.1145/3600211.3604700	Turri, V., &Dzombak, R. (2023, August). Why we need to know more: Exploring the state of AI incident documentation practices. In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (pp. 576-583).
[7]	DOI ; 10.5204/lthj.2682	Lupo, G. (2023). Risky artificial intelligence: The role of incidents in the path to AI regulation. Law, Technology and Humans, 5(1), 133-152.

1. Introduction

The rapid advancement and deployment of Artificial Intelligence(AI) technologies have transformed various sectors, including telecommunication, ICT and public services. AI systems are now instrumental in making decisions that affect individuals and society at large. Despite their numerous benefits, these systems are not without risks and challenges. Incidents of AI failure, biases, privacy violations, and unintended consequences have raised significant ethical, social, legal and technical concerns. These issues highlight the critical need for a structured approach to understand and manage the harms associated with AI.

There is a need to compile AI incidents occurring in telecommunications and critical digital infrastructure to build reliable datasets for analysis and to develop mitigation strategies that can help prevent recurrence of similar incidents [1][5]. A standardized schema enables structured compilation of incident data, while a standardized taxonomy ensures proper classification and meaningful analysis of reported incidents [2][4]. This standard defines a schema for AI incident databases in telecommunications and critical digital infrastructure. It also establishes a structured taxonomy for classifying AI incidents systematically. The schema ensures consistency in how incidents are recorded, making data collection and exchange more uniform across different systems. The taxonomy provides clear categories for classifying incidents based on their impact, improving transparency and accountability [3][7]. This standard supports regulatory compliance, helps in risk assessment, and enhances incident response by ensuring AI-related risks are documented in a structured and consistent manner [6].

2. Usage of the Standard

This standard defines structured data fields and classification criteria for AI incident databases in telecommunications and critical digital infrastructure[5]. It ensures consistency in documentation and enables interoperability across reporting frameworks, supporting data-driven policy decisions without prescribing specific mitigation strategies.

2.1 Users of the Standard

2.1.1 Organisations/ Individuals developing and deploying AI systems:

Developers and deployers can utilise the incident taxonomy to capture and document incidents during the development and testing phases of AI systems [5]. This will help in identifying patterns of failure or risk, thereby informing the design of safer and more reliable AI technologies.

2.1.2 Policy Makers and Regulators:

While developing policies and regulations related to AI services and technologies, policy makers and regulators can benefit from comprehensive and systematically gathered data in line with this standard. This will promote the development of fair and safe AI systems.

2.1.3 Researchers and Academia:

Researchers and academia can also use the rich datasets of captured and documented incidents, along with incident taxonomy for advancing research in AI ethics, safety and performance, thereby contributing to academic knowledge and innovation.

2.1.4 Incident Reporters:

Incident reporters, such as individuals, employees, users, or whistleblowers, will benefit from a simplified and comprehensive reporting through a well-structured schema, which will be highly useful for subsequent analysis and action.

3. Database Schema for Capturing AI Incidents

This standard defines a database structure for systematically capturing AI incidents, ensuring thorough documentation for analysis and improvement of AI systems. It specifies key data fields essential for incident reporting, along with optional fields for additional context as follows [3]:

1. **Incident ID:** A unique identifier assigned to each incident.
2. **Incident Title:** A concise title that encapsulates the incident.
3. **Incident Summary:** A detailed overview of the incident, up to 250 words.
4. **Incident Date:** The exact date (and time, if applicable) when the incident took place.
5. **Incident Location(s):** The geographical area(s) where the incident occurred.
6. **Affected Party(ies):** The individuals, organizations, or entities impacted by the incident.
7. **Sector(s) Impacted:** The industry or sector affected by the incident.
8. **Incident Issue(s):** The specific concerns related to the system, governance, technology, or third-party actions.
9. **AI Application Name(s):** The name of the AI system or application involved in the incident.
10. **Application Version:** The specific version of the AI application in use.
11. **Application Technology(ies):** The technologies employed within the AI application/system.
12. **Application Purpose(s):** The intended function or goal of the AI application.
13. **Application Deployer:** The organization or entity responsible for deploying the AI system.
14. **Application Developer:** The organization or entity that created the AI system.
15. **Application Transparency:** The level of clarity, accessibility, and accountability of the AI system to users and stakeholders, including the ability to challenge it.

16. **Incident severity:** The level of impact or seriousness of the incident.
17. **Incident Cause(s):** The root causes or contributing factors leading to the AI incident.
18. **Physical Harm:** Any form of injury, damage, or adverse impact on the physical well-being of an individual or a group.
19. **Environmental Harm:** Any adverse impact or damage on the natural and built environment, affecting ecosystems, wildlife, quality of air, water or soil.
20. **Property Harm:** Damaging or destroying property of an individual, group or organisation.
21. **Psychological Harm:** Damage to mental health and well-being of an individual or a group.
22. **Reputational Harm:** Damage of reputation to an individual, group or organisation.
23. **Financial Harm:** Impairment of financial assets of an individual, group or organisation.
24. **Legal/regulatory Harm:** Any form of violation of legal/regulatory matters.
25. **Fundamental Rights/ Human Rights Harm:** Damage to fundamental rights or human rights to an individual.
26. **Link to incident description/ news article:** A URL directing to external sources for detailed information or news coverage of the incident.
27. **Name of submitter:** The full name of the individual or organization submitting the incident report.
28. **Email of submitter:** The contact email address of the submitter for follow-up and verification purposes.
29. **Incident news source(s):** The sources, such as news articles or reports, from which information about the incident was obtained.
30. **Extra information shared by the submitter:** Additional details or context provided by the submitter that may enhance the understanding of the incident.

Note: Serial numbers 26 to 29 are redacted fields as they pertain to details of the submitter.

The schema would have the following structure [3]:

S.	Field Name	Data	Description	Constraints

No.		Type		
1.	**Incident ID**	Integer	A unique identifier assigned to each incident.	Primary Key, Auto-Increment
2.	**Incident Title**	Varchar (255)	A concise title that encapsulates the incident.	Not Null
3.	**Incident Summary**	Text	A detailed overview of the incident, up to 250 words.	Not Null
4.	**Incident Date**	DateTime	The exact date and time when the incident occurred.	Not Null
5.	**Incident Location(s)**	Varchar (255)	The geographical area(s) where the incident occurred.	
6.	**Affected Party(ies)**	Varchar (255)	Individuals, organizations, or entities impacted.	
7.	**Sector(s) Impacted**	Varchar (255)	The industry or sector affected by the incident.	
8.	**Incident Issue(s)**	Text	Specific concerns related to the system or third-parties.	
9.	**AI Application Name(s)**	Varchar (255)	Name of the AI system involved in the incident.	Not Null
10.	**Application Version**	Varchar (50)	Specific version of the AI application in use.	Not Null
11.	**Application Technology(ies)**	Varchar (255)	Technologies employed within the AI system.	
12.	**Application Purpose(s)**	Varchar (255)	Intended function or goal of the AI application.	
13.	**Application Deployer**	Varchar (255)	Organization responsible for deploying the AI system.	
14.	**Application Developer**	Varchar (255)	Organization that created the AI system.	
15.	**Application Transparency**	Varchar (255)	Level of clarity and accountability of the AI system.	
16.	**Incident Severity**	Varchar (50)	Degree of impact or seriousness of the incident.	Not Null
17.	**Incident Cause(s)**	Varchar (255)	The root causes or contributing factors leading to the AI incident	Not Null
18.	**Physical Harm**	Boolean	Indicates if there was physical	

			harm caused.	
19.	**Environmental Harm**	Boolean	Indicates if there was environmental harm caused.	
20.	**Property Harm**	Boolean	Indicates if there was property damage or destruction.	
21.	**Psychological Harm**	Boolean	Indicates if there was psychological harm caused.	
22.	**Reputational Harm**	Boolean	Indicates if there was reputational damage.	
23.	**Financial Harm**	Boolean	Indicates if there was financial impairment.	
24	**Legal/Regulatory Harm**	Boolean	Indicates if there was a violation of Legal/Regulatory matters.	
25.	**Fundamental Rights/Human Rights Harm**	Boolean	Indicates if there was a violation of human rights.	
26.	**Link to Incident Description/News Article**	URL	Hyperlinks to external sources detailing the incident.	
Redacted fields (submitter details):				
27.	**Name of submitter**	Varchar (50)	Name of the submitter	Not Null
28.	**Email of submitter**	Varchar (255)	Email of the submitter	Not Null
29.	**Incident news source(s)**	URL	Hyperlinks to external sources detailing the incident.	Not Null
30.	**Extra information shared by the submitter**	Text	Provide additional context, comments, or observations, which may support incident analysis or provide relevant background information not covered in standard fields.	

4. Taxonomy

The proposed taxonomy categorizes AI incidents in critical digital infrastructure, addressing sector-specific challenges in telecommunications and energy. It classifies incidents based on type, affected systems, severity, failure cause, and harm, with subcategories for detailed analysis [3].

Category	Subcategory	Examples
Incident type	Network Disruption	Telecom network outages, power grid failures.
	Service Quality Degradation	Slower internet speeds, voltage fluctuations.
	Security Breach	Data breaches, unauthorized access.
	AI Mismanagement	Incorrect resource allocation, faulty AI decisions.
	Operational Failure	Trading system errors, logistics failures.
	Predictive Maintenance Failure	Unpredicted power outages, hardware failures.
Affected system	Core Network	Failure in central telecom switches, energy grid control centres.
	Edge/Access Networks	Base station disruptions, edge server issues.
	Data Transmission Systems	Data link failures, fiber optic congestion.
	Virtualized/Cloud Infrastructure	Cloud service outages, virtual network issues.
	IoT Components	Faulty smart meters, IoT sensor failures.
	Physical Infrastructure	Security system malfunctions, HVAC failures.
Incident severity	Critical	Major nationwide outages, complete system failures.
	High	Significant disruptions, major service

		degradation.
	Moderate	Regional outages, partial service degradation.
	Low	Minor interruptions, brief service slowdowns.
Cause of failure	Al Misconfiguration	Misconfigured resource settings, faulty automation.
	Predictive Maintenance Error	Missed maintenance alerts, undetected failures.
	Security Vulnerability	Exploited Al weaknesses, data breach vulnerabilities.
	Human-Related AI Errors	Design flaws, oversight errors.
Type of harm	Physical Harm	Injuries from machinery failures, infrastructure damage.
	Environmental Harm	Increased emissions, environmental damage.
	Property Harm	Damage to telecom towers, power substations.
	Psychological Harm	Public anxiety from outages, distress from service disruptions.
	Reputational Harm	Loss of trust in service providers, damaged corporate credibility.
	Economic Harm	Revenue loss from outages, penalties for non-compliance.
	Legal/Regulatory Harm	Fines for GDPR breaches, regulatory sanctions.
	Human Rights Harm	Privacy violations, restricted freedoms from surveillance.

5. Abbreviations

Abbreviation	Full Form
AI	Artificial Intelligence
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information Communication Technology
IoT	Internet of Things
URL	Uniform Resource Locator

****End of Standard****