ETSI TS 104 158-1 V1.1.1 (2026-03)

TECHNICAL SPECIFICATION

Securing Artificial Intelligence (SAI);
AI Incident Reporting;
Part 1: AI Common Incident Expression (AICIE)
Global Framework

Reference
DTS/SAI-0020

Keywords
artificial intelligence, cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Securing Artificial Intelligence (SAI).

The present document is part 1 of a multi-part deliverable covering AI Incident Reporting, as identified below:

Part 1: "AI Common Incident Expression (AICIE) Global Framework";

Part 2: "AI Common Incident Expression (AICIE) Common Container";

Part 3: "AI Common Incident Expression (AICIE) Security Container".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present technical specification establishes a design paradigm for openness, diversity, extensibility, and interoperability among AI reporting communities by creating a first part establishing a global decentralised, autonomous framework for sharing structured AI incident information. The objective is described as a framework designed to provide incentives to collaborate on AI incidents and exist as "connective tissue for sharing."

The preparation of the present document made clear that there were was a basic bifurcation existed between the needs of AI incident information for "AI safety" and for "AI security". It was also clear that the requirements would be constantly evolving and that three different user communities existed:

1) third-party incident information collectors;

2) sovereign repository instantiations by government authorities; and

3) companies with AI offerings dealing with vulnerabilities and security.

The common resource framework record described in Clause 5.2 is both extremely minimal and flexible as well as decentralised and self-replicating on any connected server. It enables any kind of AI incident related resources to be made known to others in almost any manner and basis of their choosing, including similar lists, specifications, and repositories of information "containers". This enables a dynamic and autonomous ensemble of multiple AI reporting standards, exchange mechanisms and repositories to emerge and communicate among different communities. The approach is derived from the newly emerged Global Common Vulnerability and Exposures (GCVE) community that is well-established and scales effectively.

A subsequent part of the present document provides a specification for a generic common incident reporting data record container derived from work of the OECD and other current providers of AI incident reporting.

Introduction

The OECD published in 2025 a significant report that summarized several years of study by itself and numerous other organizations urging a Common Framework for AI Incident Reporting. See [i.10] and in Annex C (Bibliography). The OECD structure is reflected in the container specification in ETSI TS 104 158-2 [i.33]. Implementing this capability is a matter of some substantial interest to the European Commission as its Artificial Intelligence AI Act requires several incident reporting actions. See [i.2]. Incident reporting requirements are also instantiated in NCSC AI security guides and Commonwealth legislative instruments and ETSI's own Baseline Cyber Security Requirements for AI Models and Systems [i.1].

The structured expression of cyber incidents was one of the earliest standards developed among incident reporting teams. Its evolution to exchange vulnerability information and mitigations was a significant next step. The present AI Common Incident Expression (AICIE) specification draws upon that work and intended to meet the requirements for a compatible and interoperable common framework that also supports government and industry compliance provisions.

The AI Common Incident Expression Framework in the present document is intended to support very diverse kinds of AI incident resources and communities of interest, threats, and threat actors that go well beyond the cybersecurity domain. It makes use of a decentralised open architecture pioneered by the Global CVE community supported by the CIRCL Computer Incident Response Center Luxembourg. See [i.8]. Specifying the present framework designs for openness, diversity, extensibility, and interoperability. This approach enables a dynamic and autonomous ensemble of other AI reporting standards, exchange mechanisms and repositories to emerge and communicate among different user communities.

ETSI TS 104 158-2 [i.33] provides an AI incident reporting information container. It consists of a generic common incident reporting data record container based on the OECD reporting model structure.

1 Scope

The present document provides a technical specification for an AI Common Incident Expression Framework for AI Incident Reporting.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI Collaborative tools for standardized technologies.

[2] JSON Schema: "Specification".

[3] IETF RFC 3986 (January 2005): "Uniform Resource Identifier (URI): Generic Syntax".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 104 223 (V1.1.1): "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

[i.2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[i.3] UK DSIT: "AI Cyber Security Code of Practice".

[i.4] UK NCSC: "Guidelines for secure AI system development".

[i.5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.6] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

[i.7] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[i.8] GCVE.EU: "GCVE: Global CVE Allocation System".

[i.9] Cornell University SarXiv:2503.16861v1 [cs.AI], Sean McGregor et al.: "In-House Evaluation Is Not Enough: Towards Robust Third-Party Flaw Disclosure for General-Purpose AI", 21 March 2025.

[i.10] OECD: "Towards a Common Reporting Framework for AI Incidents", OECD Artificial Intelligence Papers, February 2025, No. 34.

[i.11] OECD: "AIM: AI Incidents and Hazards Monitor".

[i.12] OECD: "Defining AI Incidents and Related Terms", OECD Artificial Intelligence Papers, May 2024, No. 16.

[i.13] McGregor, S. (2021): "Preventing Repeated Real World AI Failures by Cataloging Incidents: The AI Incident Database", Proceedings of the AAAI Conference on Artificial Intelligence, 35(17), 15458-15463.

[i.14] OECD Framework for the Classification of AI Systems, February 2022, No. 323.

[i.15] NCSC: "Where to Report a Cyber Incident".

[i.16] NCSC: "Responding to a cyber incident - a guide for CEOs".

[i.17] Confédération Suisse Federal Office for Cybersecurity BACS: "Information on the reporting obligation".

[i.18] CSET: H. Frase & R.B. L. Dixon: "AI Incidents, Key Components for a Mandatory Reporting Regime", January 2025.

[i.19] OWASP Gen AI Incident/Exploit Round-up Submission.

[i.20] Recommendation ITU-T X.1500: "Overview of cybersecurity information exchange".

[i.21] ETSI TR 104 003: "Cyber Security (CYBER); The vulnerability disclosure ecosystem".

[i.22] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.23] CISA: "Cybersecurity Incident & Vulnerability Response Playbooks".

[i.24] NIST AI600-1: "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile".

[i.25] AIID: "AI Incident Database".

[i.26] MIT: "MIT AI Risk Repository".

[i.27] AVID: "AI Vulnerability Database".

[i.28] OECD: "Overview and methodology of the AI Incidents and Hazards Monitor".

[i.29] MIT: "MIT AI Risk Repository".

[i.30] Kaggle: "AI Incident Database".

[i.31] JSON-LD.org: "JSON for Linking Data".

[i.32] IEEE™ CSR: Sharkov: "Unveiling the invisible: Knowledge Graph-Driven Discovery of Hidden Cascade Risks in Critical Infrastructure Supply Chains".

[i.33] ETSI TS 104 158-2: "Securing Artificial Intelligence (SAI); AI Incident Reporting; Part 2: AI Common Incident Expression (AICIE) Common Container".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Additional Data Publication (ADP): set of additional structured information that enriches existing AICIE records

AI common incident expression identifier: alphanumeric string that uniquely identifies an AI Incident using the present document

AI disaster: serious AI incident that disrupts the functioning of a community or a society and that may test or exceed its capacity to cope, using its own resources. The effect of an AI disaster can be immediate and localized, or widespread and lasting for a long period of time

NOTE: More details available in [i.12].

AI hazard: event, circumstance or series of events where the development, use or malfunction of one or more AI systems could plausibly lead to an AI incident, i.e. any of the following harms:

a) injury or harm to the health of a person or groups of people

b) disruption of the management and operation of critical infrastructure

c) violations to human rights or a breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights

d) harm to property, communities or the environment

NOTE: More details available in [i.12].

incident: event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms:

a) injury or harm to the health of a person or groups of people

b) disruption of the management and operation of critical infrastructure

c) violations of human rights or a breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights

d) harm to property, communities or the environment

NOTE: More details available in [i.12].

serious AI hazard: event, circumstance or series of events where the development, use or malfunction of one or more AI systems could plausibly lead to a serious AI incident or AI disaster, i.e. any of the following harms:

a) the death of a person or serious harm to the health of a person or groups of people

b) a serious and irreversible disruption of the management and operation of critical infrastructure

c) a serious violation of human rights or a serious breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights

d) serious harm to property, communities or the environment

e) the disruption of the functioning of a community or a society and which may test or exceed its capacity to cope using its own resources

NOTE: More details available in [i.12].

serious incident: incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

a) the death of a person, or serious harm to a person's health

b) a serious and irreversible disruption of the management or operation of critical infrastructure

c) the infringement of obligations under Union law intended to protect fundamental rights

d) serious harm to property or the environment

NOTE: More details available in [i.2] and [i.12].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
AICIE	AI Common Incident Expression
AIID	AI Incident Database
CSET	Center for Security and Emerging Technology
CVE	Common Vulnerabilities and Exposures
DSIT	Department for Science, Innovation & Technology (UK)
FAS	Federation of American Scientists
GCVE	Global Common Vulnerabilities and Exposures
NCSC	National Cyber Security Centre (UK) (Switzerland)
OECD	Organisation for Economic Co-operation and Development
URI	Uniform Resource Identifier

4 Existing Ecosystem

4.1 Cybersecurity information exchange models

The contemporary period of cybersecurity information exchange emerged in the 1990 timeframe and consisted of the exchange of combinations of incident, vulnerability, and threat information via repositories among a complex global community of product and service vendors, end users, and industry and government cyber security organizations. See [i.20], [i.21] and [i.22]. The actual sharing of information together with a broad array of related protocols consists of five activities. [i.20]:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishment of trust and policy agreement between exchanging entities;
- requesting and responding with cybersecurity information;
- assuring the integrity of the cybersecurity information exchange.

The incident response component has been formalized in cybersecurity models or playbooks and includes information sharing as part of the model. See [i.23]. See Figure 4.1-2. For AI specifically, disclosing incident information is included as part of 25 distinct GOVERN, MAP, MEASURE, and MANAGE tasks in the NIST AI Risk Management Framework. See [i.24].

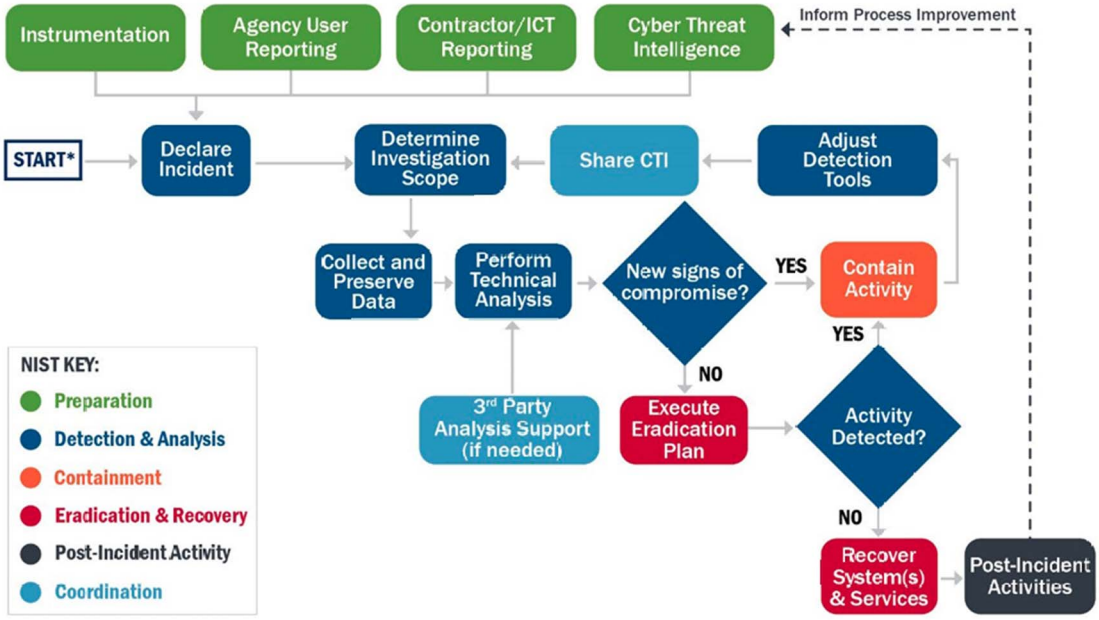

Figure 4.1-2: Incident Response Process [i.23]

4.2 AI incident information exchange implementations

During the past several years, several well-known, different AI incident repository implementations have emerged that provide different collections with varying record structures to serve a kind of emerging marketplace. See [i.11], [i.25], [i.26], [i.27], [i.28], [i.29] and [i.30]. The implementations lack a common discovery mechanism and interoperability. These insufficiencies combined with the emerging obligations articulated in clause 4.3, led to the OECD report on a common incident reporting and classification frameworks, see [i.10] and [i.14].

The rapid growth of AI implementations for all manner of use cases is certain is producing a rapidly expanding array of AI incident reporting needs and implementations. The situation makes compelling the need for a common framework for identifying, discovering and expressing incident information that is global, open, extensible, interoperable, scalable, and capable of accommodating the diversity of potential implementations. See [i.9], [i.13], [i.18] and [i.19].

4.3 AI Incident information exchange obligations

4.3.1 The exchange obligation ecosystem

AI information exchange obligations arise somewhat autonomously from multiple sources. Organic legislative instruments and implementing regulations by regional and national authorities constitute obligations that incur penalties for non-compliance. See [i.4], [i.5], [i.6] and [i.7]. Government security agency and industry body technical standards constitute another source of implied obligation of "best practice" - sometimes coupled in juridical law with potential civil law liability exposure. See [i.15], [i.16] and [i.17]. The obligations can also arise by contractual agreement among parties in the provision of services.

4.3.2 EU Artificial Intelligence Act

One of the most prominent contemporary legislative instruments is the EU Artificial Intelligence Act [i.2]. In five of its Articles, there are provisions that impose the below information sharing obligations.

*"**Art. 17: Quality management system***
1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation.

…

(i) procedures related to the reporting of a serious incident in accordance with Article 73;

Art. 26(5): Obligations of deployers of high-risk AI systems
…

5. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, Article 73 shall apply mutatis mutandis.

Art. 60: Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes
…

7. Any serious incident identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 73.

Section 2 - Sharing of information on serious incidents

Art. 73: Reporting of serious incidents

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

2. The report referred to in paragraph l shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident.

The period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the event of a widespread infringement or a serious incident as defined in Article 3, point (49)(b), the report referred to in paragraph 1 of this Article shall be provided immediately, and not later than two days after the provider or, where applicable, the deployer becomes aware of that incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report.

6. Following the reporting of a serious incident pursuant to paragraph 1, the provider shall, without delay, perform the necessary investigations in relation to the serious incident and the AI system concerned. This shall include a risk assessment of the incident, and corrective action. The provider shall cooperate with the competent authorities, and where relevant with the notified body concerned, during the investigations referred to in the first subparagraph, and shall not perform any investigation which involves altering the AI system concerned in a way which may

affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

7. Upon receiving a notification related to a serious incident referred to in Article 3, point (49)(c), the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be issued by 2 August 2025, and shall be assessed regularly.

8. The market surveillance authority shall take appropriate measures, as provided for in Article 19 of Regulation (EU) 2019/1020, within seven days from the date it received the notification referred

to in paragraph 1 of this Article, and shall follow the notification procedures as provided in that Regulation.

9. For high-risk AI systems referred to in Annex ill that are placed on the market or put into service by providers that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this Regulation, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c).

10. For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 [Medical Device Regulation] and (EU) 2017/746 [In-vitro Medical Device Regulation], the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c) of this Regulation, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred.

11. National competent authorities shall immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of Regulation (EU) 2019/1020.

Art. 76: Supervision of testing in real world conditions by market surveillance authorities

…

3. Where a market surveillance authority has been informed by the prospective provider, the provider or any third party of a serious incident or has other grounds for considering that the conditions set out in Articles 60 and 61 are not met, it may take either of the following decisions on its territory, as appropriate:

(a) to suspend or terminate the testing in real world conditions;

(b) to require the provider or prospective provider and the deployer or prospective deployer to modify any aspect of the testing in real world conditions."

4.3.3 ETSI TS 104 223, UK DSIT Code of Practice

The United Kingdom's National Centre for Cyber Security (NCSC) developed a set of AI best practices [i.3] which were codified into regulator provisions by the regulatory body the Department for Science, Innovation and Technology (DSIT). The provisions were largely transposed into ETSI TS 104 223 [i.1] and contain five clauses impose information sharing obligations enumerated below:

- **Provision 5.1.2-3** To support the process of preparing data, security auditing and incident response for an AI system, Developers shall document and create an audit trail in relation to the AI system. This shall include the operation, and lifecycle management of models, datasets and prompts incorporated into the system.
- **Provision 5.2.2-5** Developers and System Operators shall create, test and maintain an AI system incident management plan and an AI system recovery plan. (DSIT Principle 6.4).
- **Provision 5.3.1-3** Developers and System Operators should support End-users and Affected Entities during and following a cyber security incident to contain and mitigate the impacts of an incident. The process for undertaking this should be documented and agreed in contracts with End-users. (DSIT Principle 10.2).
- **Provision 5.4.2-1** System Operators shall log system and user actions to support security compliance, incident investigations, and vulnerability remediation.

5 AI Common Incident Expression (AICIE) Framework

5.1 The AICIE Framework architecture

The present technical specification facilitates the AI information exchange ecosystem described in Clause 4, above, using a framework that establishes a design architecture for openness, diversity, extensibility, and interoperability among AI reporting communities. This global decentralised, autonomous framework architecture enables widespread sharing structured AI incident information via multiple common distributed directories that enable users to discover and access AI incident reporting resources in the form of other directory lists, specifications, incident repositories, or any other kind of related enrichment information. It is modelled after the Global CVE framework architecture. See [i.8].

The structure for the framework record format is set forth in Clause 5.2. The JSON representation is in Annex A. See [1], [2], [3] and [i.31].

An example of the ETSI implementation of the framework list is in Annex B.

5.2 AICIE Framework Resource Record Format and Values

5.2.0 Introduction

The AICIE Framework resource record format is depicted in Figure 5.2-1 and captures the minimum essential information concerning an AI incident reporting resource. Bold field names are mandatory and "…" indicates free-form content. Resources include not only AICIE incident report containers described in other parts of the present document in repositories, but also any other existing or potential new AI incident-related resource including other AICIE compliant framework listings, technical specifications, repositories, or enrichment information including AI BOMs and knowledge graphs. See [i.32].

The inclusion of AICIE framework compliant lists as a resource enables directory instantiations to be autonomously created, replicated, and synchronized among any accessible network servers - including among a closed communities using any desired medium.

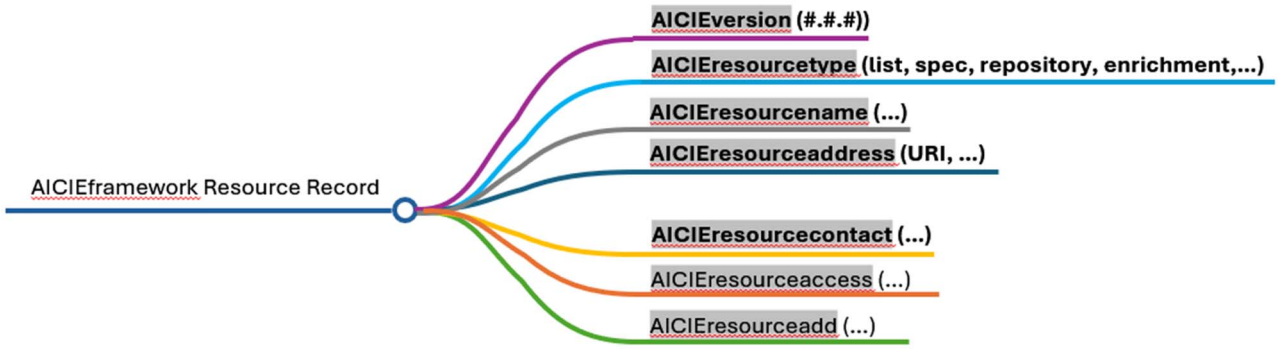

Figure 5.2-1: Mindmap of the AICIE Framework Resource Record

5.2.1 AICIEverison

This required value describes the AICIE Framework Resource Record specification version being used and expressed as three numbers separated by periods and set initially to 1.0.0.

5.2.2 AICIEresourcetype

This required value describes the AI incident reporting resource type in the following non-case-sensitive enumeration:

Table 5.2.2-1

list	Another AICIE Framework Resource list directory based on the present document
spec	Any technical specification for AI incident information reporting
repository	Any repository for AI incident information reporting
enrichment	Any information providing AI incident enrichment information including AI BOMs and knowledge graphs
…	A one word description of any other resource

5.2.3 AICIEresourcename

This required value describes the name of the resource without any constraints - prefaced by any related identifier associated with the name.

EXAMPLE: "ETSI TS 104 158-1 V1.1.1, Securing Artificial Intelligence (SAI); AI Incident Reporting; Part 1: AI Common Incident Expression (AICIE) Global Framework".

5.2.4 AICIEresourceaddress

This required value describes the resource address location without any constraints - preferably as a persistent, precise, accessible Uniform Resource Identifier (URI) or a link capable of providing the resource.

EXAMPLE: https://www.etsi.org/deliver/etsi_ts/104100_104199/10415801.

5.2.5 AICIEresourcecontact

This required value describes the contact information without any constraints for the entity maintaining and accessing the resource preferably including physical and location and useable email address.

EXAMPLE: "ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia Antipolis FRANCE, secretariat@etsi.org".

5.2.6 AICIEresourceaccess

This optional value without any constraints describes any resource access controls.

EXAMPLE: "Members only". The default when leaving blank is publicly available without constraints.

5.2.7 AICIEresourceadd

This optional value without any constraints describes any useful additional attributes of the resource.

Annex A (normative): AICIE Framework Resource Record JSON Format V1.0.1

```
{
    "$schema": "tbd",
    "$id": "tbd2",
    "properties": {

"AICIEversion": {
            "description": "AICIE Framework Resource Record specification version being used and
expressed as three numbers separated by periods and set initially to 1.0.1",
            "type": "string"

        },
"AICIEresourcetype": {
            "description": "value describing AI incident reporting resource type",
            "type": "string"
          "enum": [
                "list",
                "spec",
                "repository",
                "enrichment"
            ]

"AICIEresourcename": {
            "description": "name of the resource prefaced by any related identifier associated with
the name",
            "type": "string"

        },
        "AICIEresourceaddress": {
            "description": "The resource address location without any constraints - preferably as a
persistent, precise, accessible Uniform Resource Identifier (URI) or a link capable of providing the
resource",
            "type": "string"

        },
        "AICIEresourcecontact": {
            "description": "The contact information without any constraints for the entity
maintaining and accessing the resource preferably including physical location and useable email
address",
            "type": "string"

        },
        "AICIEresourceaccess": {
            "description": "describes any resource access controls",
            "type": "string"

        },
        "AICIEresourceadd": {
            "description": "any useful additional attributes of the resources",
            "type": "string"

        }
    },
    "required": [
                 "AICIEversion",
                 "AICIEresourcetype",
                 "AICIEresourcename",
                 "AICIEresourceaddress",
                 "AICIEresourcecontact"
     ]
}
```

Annex B (informative): ETSI AICIE Framework Resource Record Example

```
AICIEversion    1.0.1
AICIEresourcetype   spec
AICIEresourcename   ETSI TS 104 158-1 V1.0.1, Securing Artificial Intelligence (SAI); AI Incident
Reporting; Part 1: AI Common Incident Expression (AICIE) Global Framework
AICIEresourceaddress    https://www.etsi.org/deliver/etsi_ts/104100_104199/10415801
AICIEresourcecontact    ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia
Antipolis FRANCE, secretariat@etsi.org
AICIEresourceaccess
AICIEresourceadd    ETSI implementation specification for AICIE resource records
=====
AICIEversion    1.0.1
AICIEresourcetype   spec
AICIEresourcename   ETSI TS 104 158-2 V1.0.1, Securing Artificial Intelligence (SAI); AI Incident
Reporting; Part 2: AI Common Incident Expression (AICIE) Container
AICIEresourceaddress    https://www.etsi.org/deliver/etsi_ts/104100_104199/10415802
AICIEresourcecontact    ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia
Antipolis FRANCE, secretariat@etsi.org
AICIEresourceaccess
AICIEresourceadd    ETSI implementation specification for AICIE resource records
=====
AICIEversion    1.0.1
AICIEresourcetype   repository
AICIEresourcename   AICIE Framework Resources Known to ETSI
AICIEresourceaddress    https://forge.etsi.org/rep/explore/projects [TBD]
AICIEresourcecontact    ETSI Secretariat, ETSI 650, Route des Lucioles 06560 Valbonne - Sophia
Antipolis FRANCE, secretariat@etsi.org
AICIEresourceaccess
AICIEresourceadd    ETSI implementation of AICIE resource record framework
=====
AICIEversion    1.0.1
…..
```

Annex C (informative): Bibliography

- CSET, Ren Bin Lee Dixon and Heather Frase: "An Argument for Hybrid AI Incident Reporting", Center for Security and Emerging Technology, March 2024.
- Georgetown-CSET GitHub: "CSET-AIID-harm-taxonomy", June 2024.
- Federation of American Scientists (FAS), John Croxton et al.: "Message Incoming: Establish an AI Incident Reporting System", 25 Jun 2024.
- MIT, Peter Slattery et al.: "The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks From Artificial Intelligence".
- MITRE: "AI Assurance - Challenges, Maturity, and Paths Forward", June 2024.
- Frontier Model Forum: "FMF Announces First-Of-Its-Kind Information-Sharing Agreement", March 2025.

History

Version	Date	Status
V1.1.1	March 2026	Publication