IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems

A Brief Introduction To The Evidence Base

Ken Wallace
krw@computer.org

***Abstract*—Use of an evidence base, derived from published literature, was one method employed to develop the IEEE 7009-2024 standard for fail-safe design of autonomous and semi-autonomous systems. To accompany publication of the standard, the evidence base has been released into the public domain. This Introduction is supplementary to that release and is provided to aid comprehension of the evidence base and the information contained within it.**

***Index Terms*—Evidence base, IEEE 7009, Standard, Safety, Synopsis.**

I. Introduction

IEEE 7009-2024 is one of a number of standards that form part of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Developed by the volunteers[1] of the IEEE P7009 Working Group on behalf of the Reliability, and Computer Societies of the IEEE, the standard establishes a requirement-based framework for the design of fail-safe autonomous and semi-autonomous systems. IEEE 7009-2024 [1] was published in July 2024 and is freely available through the IEEE GET Program for AI Ethics and Governance Standards[2]. Further information on the development of the standard can be found in [4].

IEEE Standards follow a defined process involving a six stage life cycle, based upon a set of principles. Use of an evidence base [5], derived from a corpus of published literature, was one of a number of methods employed by the P7009 Working Group to put the principles into practice during development of the standard. To coincide with publication of the standard, the evidence base is also made available[3] This Introduction supplements the release[4] to aid comprehension of the information contained within the evidence base.

II. The Evidence Base

The 7009X Evidence Base (EB) consists of a list of *Sources*. Each entry in the list comprises the following attributes:

1) The year of publication of the source
2) The title of the source
3) A hyperlink (DOI) to the source for the entry
4) The baseline for the source (see below)
5) The version of the EB in which the entry was first included.

Entries are listed in chronological order of publication, earliest year first, and alphabetically within a year, based upon attributed authorship. For a small number of entries that have no DOI an alternative URL is provided. The EB is available from Zenodo in searchable PDF format: the current version is V2.1. The EB does *not* include any source document[5]. Selection of a source title in the PDF document *should*[6] result in navigation to the source URL (DOI) via a browser.

The EB is compiled, principally, from an evolving corpus of published literature that was originally formulated as a tool to inform decision-making in industrial practice [7], [2], [8], [10][7]. The methods by which the originating corpus was derived have previously been reported [9]. These methods continue to provide a basis for development of the corpus, taking account of learning from experience (LfE) and academic research [3], [11]. Sources within the corpus are categorised according to an adapted '5S' information model [6]. The categories and information each provides, and the number of sources in each category[8] for the 505[9] entries in V2.1 of the EB are as follows:

Category	Type of Information	Population	%
Systems	Operational	6	1
Standards	Reference	44	9
Synopsis	Summary	20	4
Synthesis	Systematic	365	72
Studies	Empirical	70	14

As released, the EB is the product of merging two separate baselines (lists) of sources: the baseline utilised during the development of the 7009 standard (this baseline is labelled `B7009`) and a baseline being used for development of the first extension of the 7009 standard (the extension is labelled `X9.1`[10] and the associated baseline is `B9.1`).

Each baseline has an associated query consisting of the search terms used to identify sources in the corpus of possible relevance for the EB. Queries codify searches for purposes of repeatability, efficiency and verification: they do not impose any limits upon literature searches conducted when formulating individual baselines[11] (or upon the corpus itself). Reflecting the published status of IEEE 7009, the accompanying query (labelled `Q7009`) is stable (mature)[12]. In contract, the query (labelled `Q9.1`) for `X/B9.1` is itself in development and subject to change, as work on developing X9.1 progresses. Irrespective of the means of identification, all sources are reviewed prior to incorporation into the corpus. Sources identified by queries are subject to further review to determine whether or not inclusion in the EB is justified. The Q7009 and current Q9.1 queries are as below: the inclusion of a '.' in a term represents a single character wildcard.

Q7009: "accept." OR "ALARP" OR "anomal." OR "assuran." OR "autono." OR "aware." OR "consequ." OR "critical." OR "decid." OR "decisi." OR "defec." OR "depend." OR "detect." OR "deviat." OR "diagno." OR "error" OR "ethi." OR "event" OR "fail." OR "fail.safe" OR "harm" OR "incident" OR "inhibi." OR "intolerabl." OR "lear." OR "moderat." OR "monitor" OR "norm." OR "predict." OR "preser." OR "recover." OR "regulat." OR "reliab." OR "risk." OR "robust." OR "safe" OR "self." OR "tolerabl." OR "unaccept." OR "viol."

Q9.1: "accident" OR "adverse.event" OR "alert" OR "authenti." OR "chain.of.event" OR "close.call" OR "domino" OR "hazard" OR "hazardous.event" OR "hazardous.situation" OR "incident" OR "initiating.event" OR "knowledge" OR "learn.from.experience" OR "learn.from.incident" OR "learning.point." OR "LFE" OR "LFI" OR "near.hit" OR "near.miss"OR "never.event" OR "root.cause.analy." OR "safety.management.system" OR "sentinel.event" OR "SMS"

III. Version History

Versioning of the EB utilises a `MAJOR.MINOR` scheme[13] for numbering. The correspondence of versions to baselines is as follows:

B7009	B9.1	MAJOR	MINOR
●	○	1	0,1,2,3
●	●	2	0,1

where:

- ● denotes the inclusion of the baseline in the EB
- ○ denotes the lack of such inclusion.

The EB was formalised to assist Working Group review of drafts of the 7009 standard[14]. Prior to V2.1 each version of the EB was

The author is the current Chair of the IEEE P7009 Working Group and the individual to whom any errors or inconsistencies in the Evidence Base can be reported. The subject of the email should include: `7009X EB deficiency`.

allocated a P7009 Unique Identifier (UID): with the release of the EB this practice has been discontinued. Compilation of the current version of the EB identified a number of sources that were available to the Working Group prior to formalisation of the EB, but which were not included in preceding versions of the EB. For completeness these sources, mainly studies, have now been incorporated into the EB. The table below provides the history for versions prior to V2.1: these versions are not part of the EB release.

P7009 UID	Version	Date	Sources
P7009-20221222-A	1.0	December 2022	263
P7009-20230226-A	1.1	February 2023	295
P7009-20230522-A	1.2	May 2023	303
P7009-20230624-A	1.3	June 2023	322
P7009-20240704-A	2.0	July 2024	467

Future major versions of the EB will reflect the needs of any initiatives additional to X9.1 that might be developed by the P7009 Working Group. The extent of minor version updates will, in the first instance, be determined by the needs of the P7009 Working Group when developing X9.1, or maintaining the 7009 standard.

IV. Evidence Base or Based?

The inclusion of a source in the EB does not indicate, nor imply that the source necessarily influenced or contributed directly or indirectly to the development of the 7009 standard or the ongoing development of X9.1. When considering the EB and the sources identified therein, every care should be taken to avoid confusing correlation with causation.

V. Disclaimers

No attribution of either the EB or this Introduction, or both these work products to the IEEE, IEEE Standards Association, sponsoring societies, the IEEE P7009 Working Group, or any combinations thereof is permitted. Neither work product reflects an official position of the IEEE, IEEE Standards Association, sponsoring societies, the IEEE P7009 Working Group, or any combination thereof. No warranty is expressed or implied for either the Evidence Base or this Introduction: the user of either, or both, accepts all risk.

References

[1] "IEEE standard for fail-safe design of autonomous and semi-autonomous systems," *IEEE Std 7009-2024*, pp. 1–45, 2024. [Online]. Available: https://doi.org/10.1109/IEEESTD.2024.10582898

[2] S. Anderson, P. Sagar, B. Smith, and K. Wallace, "What we have learnt adopting evidence-based software engineering for industrial practice," in *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering*, ser. EASE '16. New York, NY, USA: ACM, 2016, p. 199. [Online]. Available: http://doi.acm.org/10.1145/2915970.2915981

[3] D. Budgen, P. Brereton, S. Drummond, and N. Williams, "Reporting systematic reviews: Some lessons from a tertiary study," *Information and Software Technology*, vol. 95, pp. 62–74, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584916303548

[4] M. Farrell, M. Luckcuck, L. Pullum, M. Fisher, A. Hessami, D. Gal, Z. Murahwi, and K. Wallace, "Evolution of the IEEE P7009 standard: Towards fail-safe design of autonomous systems," in *2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2021, pp. 401–406. [Online]. Available: https://doi.org/10.1109/ISSREW53611.2021.00109

[5] T. Greenhalgh, *How to read a paper: The basics of evidence-based medicine*. John Wiley & Sons, 2014.

[6] B. Haynes, "Of studies, syntheses, synopses, summaries, and systems: the "5S" evolution of information services for evidence-based healthcare decisions," *Evidence Based Nursing*, vol. 10, no. 1, pp. 6–7, 2007. [Online]. Available: http://ebn.bmj.com/content/10/1/6.short

[7] B. A. Kitchenham, T. Dybå, and M. Jørgensen, "Evidence-based software engineering," in *Proceedings of the 26th International Conference on Software Engineering*, ser. ICSE '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 273–281. [Online]. Available: https://doi.org/10.1109/ICSE.2004.1317449

[8] K. R. Wallace, "Safe and secure: re-engineering a software process set for the challenges of the 21st century," in *System Safety and Cyber Security (2014), 9th IET International Conference on*, 2014, pp. 1–6. [Online]. Available: https://doi.org/10.1049/cp.2014.0987

[9] ——, "Can evidence-based software engineering contribute to safer software?" in *Engineering Systems For Safety: Proceedings of the 23rd Safety Critical Systems Symposium*, ser. SSS '15. Bristol, England, UK: Safety-Critical Systems Club, 2015, pp. 79 – 94. [Online]. Available: https://scsc.uk/scsc-129

[10] ——, "Safe software: A suitable case for an evidence-based treatment?" in *Proceedings of the 20th European Safety and Reliability*, ser. ESREL '16. Glasgow, Scotland, UK: ESREL, 2016, pp. 2403 – 2410. [Online]. Available: https://doi.org/10.1201/9781315374987

[11] C. Wohlin, E. Mendes, K. R. Felizardo, and M. Kalinowski, "Guidelines for the search strategy to update systematic literature reviews in software engineering," *Information and Software Technology*, vol. 127, p. 106366, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095058491930223X

Notes

1. The author acknowledges and thanks all who take the time to participate in, and contribute to, the work of the IEEE P7009 Working Group.

2. Other standards developed as part of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems are also available as part of the program.

3.

4. Information provided in this Introduction is current as at the time of writing. In contrast to the EB this document will not be maintained, except for purposes of addressing any deficiencies that are identified.

5. As such the EB is a list of references (pointers) to the sources.

6. YMMV in this regard, depending upon the environment within which interaction with the EB occurs.

7. Applications that utilise the corpus have subsequently expanded to encompass the development of other standards that were part of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, and accreditation of engineering and computing programs in accordance with international agreements, and policy and procedural considerations of accreditation. All applications contribute to the evolution of the corpus.

8. Percentages are given to the nearest integer.

9. The total number represents circa 20% of the sources in the corpus at the time of writing.

10. Development of the X9.1 extension by the IEEE P7009 Working Group is in progress at the time of writing. Participation in the P7009 Working Group is open to any interested party. The P7009 WG provides a public interest email reflector. To (un)subscribe to the reflector, please send an email to ListServ@ieee.org containing the following text in the body of the message: `(un)subscribe STDS-P7009 Your FirstName YourLastName`. The reflector does not support an e-mail address field so subscription requests that do not conform to the specified format are unlikely to meet with success.

11. A query represents but one starting point for identifying relevant sources.

12. The query evolved over a period of several years as a result the deliberations of the P7009 Working Group.

13. The EB is not patched: any errors or inconsistencies are addressed in a version of the EB subsequent to identification

14. The reviews were in preparation for the process of balloting the standard. This process commenced in November 2023 and completed in March 2024. The standard was approved by the IEEE Standards Association in May 2024.