Developing high-quality software is tough. ECLAIR is designed to help development, QA, and safety teams reach their quality goals.

Coverage of ISO 26262:2018 Objectives

1 Introduction to ISO 26262:2018

ISO 26262:2018, "Road vehicles — Functional safety", is a series of international functional-safety standards for the automotive industry. It adapts the IEC 61508 series of standards to the functional safety of electrical and/or electronic systems within road vehicles. The first edition of ISO 26262 was published in 2011. The second edition, published in 2018, completely supersedes the previous versions, incorporates a general restructuring of all parts for improved clarity, and contains numerous changes, updates and extensions, among which:

- requirements for motorcycles, trucks, buses, trailers and semi-trailers;
- extension of the vocabulary;
- more detailed objectives and objective oriented confirmation measures;
- management of safety anomalies;
- references to cybersecurity;
- guidance on model based development and software safety analysis;
- guidance on fault tolerance, safety-related special characteristics and software tools.

ISO 26262 provides guidance for the production of *all* software embedded into automotive systems and equipment, whether or not they are safety critical. ISO 26262 approach to risk management is based on the determination of the *Automotive Safety Integrity Level* (ASIL) for each safety function assigned to each subsystem. There are four ASILs: A, B, C and D, with A being the lowest safety integrity level and D being the highest. ASIL D represents likely potential for severely life-threatening or fatal injury in the event of a malfunction and requires the highest level of assurance that the dependent safety goals are sufficient and have been achieved.

In order to determine the ASIL of a safety function, the risk of functional defects has to be evaluated, for each hazardous event, according to three attributes:

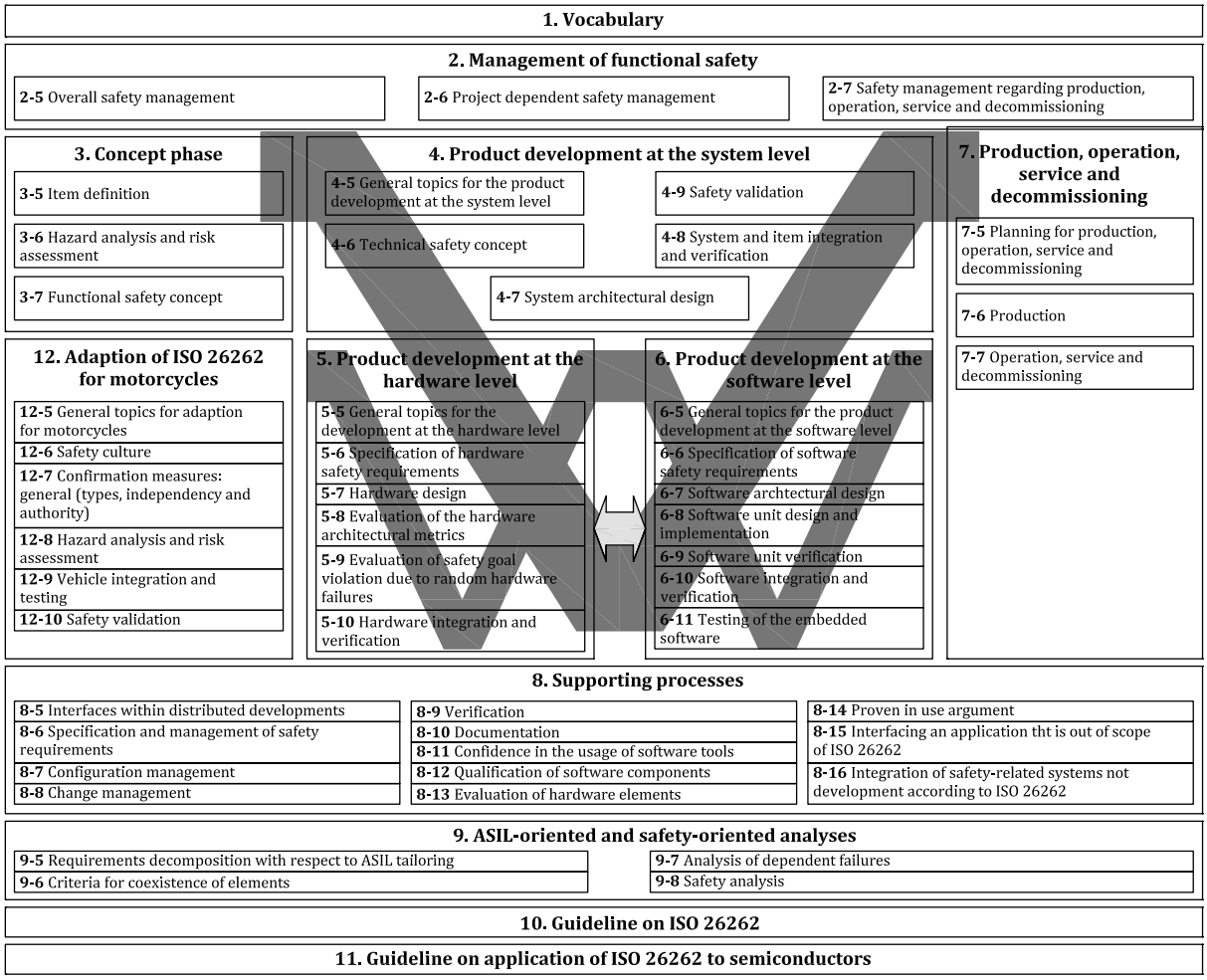
exposure a classification of the probability of the hazardous event (from “incredible” to “high probability”);

severity a classification of its impact on safety (from “No injuries” to “Life-threatening injuries (survival uncertain), fatal injuries”);

controllability a classification of the possibility of the driver and other persons involved in the event, to deal with it (from “Controllable in general” to “Difficult to control or uncontrollable”).

The combination of these attributes determines the ASIL, or that the function is not safety related and thus that there are no requirements to comply with ISO 26262, in which case it is assigned class QM (Quality Management).

ISO 26262 is constituted by 12 parts, which are organized and structured as shown in the following figure:



Overview of the ISO 26262 series of standards

1.1 Role of ECLAIR in Ensuring Compliance with ISO 26262:2018

The ECLAIR static analyzer[1] can be used to comply with several of the objectives of ISO 26262:2018 Part 6 “Product development at the software level” [6] and Part 9 “Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses” [8]. In addition, ECLAIR Qualification Kits greatly

[1] This paper refers to packages of ECLAIR 3.9.0 and subsequent versions.

simplify compliance with the prescription of Section 11 “Confidence in the use of software tools” of ISO 26262:2018 Part 8 “Supporting processes” [7].

2 ECLAIR Coverage of ISO 26262:2018 Part 6 Objectives

For automotive applications, Part 6 of ISO 26262:2018 specifies the requirements for product development at the software level [6]. In particular it includes:

- general topics for product development at the software level;
- specification of the software safety requirements;
- software architectural design;
- software unit design and implementation;
- software unit verification;
- software integration and verification; and
- testing of the embedded software.

ISO 26262:2018 Part 6 features several tables defining topics and methods that must be considered in order to comply with the standard. The different topics and methods listed in each table contribute to the level of confidence in achieving compliance with the corresponding requirement. Topics and methods are listed in each table either as *consecutive entries*, numbered with 1, 2, 3, ... in the leftmost table column, or as *alternative entries*, labeled with 1a, 1b, 1c, ... in the same column.

The degree of recommendation to use each topic and method depends on the ASIL, and is symbolically encoded as follows:

++ indicates that the method is highly recommended for the identified ASIL;

+ indicates that the method is recommended for the identified ASIL;

o indicates that the method has no recommendation for or against its usage for the identified ASIL.

For consecutive entries, all listed as highly recommended and recommended topics and methods, in accordance with the ASIL, do apply. For alternative entries, an appropriate combination of topics and methods shall be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation should be preferred. A rationale shall be given that the selected combination of methods complies with the corresponding requirement.

The following tables have been obtained by extending the corresponding tables in ISO 26262:2018 Part 6 with a column indicating where ECLAIR, suitably instantiated with the appropriate package, can be used to ensure compliance or to facilitate the achievement of compliance. Note that, in the sequel, every reference to MISRA C:2012 should be interpreted as referring to [9] as amended by [10], whereas MISRA C++ is [11].

2.1 MISRA C:2012

MISRA C:2012 [9] with Amendment 2 [10] is the latest software development C subset developed by MISRA, which is now a de facto standard for safety-, life-, security-, and mission-critical embedded applications in many industries, including of course the automotive industry where MISRA was born. MISRA C:2012 Amendment 2 allows coding MISRA-compliant applications in subsets of C11 and C18, in addition to C90 and C99. MISRA C:2012 is supported by the ECLAIR package called “MC3”.

2.2 MISRA C++:2008

MISRA C++:2008 [11] is the software development C++ subset developed by MISRA for the motor industry, which is now a de facto standard for safety-, life-, and mission-critical embedded applications also in many other industries. It is currently undergoing a quite deep revision: the structure is being made similar to that in MISRA C:2012, add support for C++17, and merge the AUTOSAR guidelines. MISRA C++:2008 is supported by the ECLAIR package called "MP1".

2.3 BARR-C:2018

The *Barr Group's Embedded C Coding Standard*, BARR-C:2018, [3], is, for coding standards used by the embedded system industry, second only in popularity to MISRA C. BARR-C:2018 guidelines include 64 guidelines dealing with language subsetting and project management as well as 79 guidelines concerning programming style. For projects in which a MISRA C compliance requirement is not (yet) present, the adoption of BARR-C:2018 is a major improvement with respect to the situation where no coding standards and no static analysis are used. Moreover, complying with BARR-C:2018, besides avoiding many dangerous bugs, entails compliance with a non-negligible subset of MISRA C:2012 [2]. ECLAIR support for BARR-C:2018 has no equals on the market: it is included in all ECLAIR packages, including the affordable package "B".

Table 1 — Topics to be covered by modelling and coding guidelines

Topics		ASIL				ECLAIR
		A	B	C	D	
1a	Enforcement of low complexity	++	++	++	++	✓[a]
1b	Use of language subsets	++	++	++	++	✓[b]
1c	Enforcement of strong typing	++	++	++	++	✓[c]
1d	Use of defensive implementation techniques	+	+	++	++	✓[d]
1e	Use of well-trusted design principles	+	+	++	++	✓[e]
1f	Use of unambiguous graphical representation	+	++	++	++	–
1g	Use of style guides	+	++	++	++	✓[f]
1h	Use of naming conventions	++	++	++	++	✓[g]
1i	Concurrency aspects	+	+	+	+	–

[a] HIS [4] and other metrics related to program complexity. ECLAIR allows associating thresholds to each metric.

[b] MISRA C/C++ and BARR-C:2018 define language subsets where the potential of committing possibly dangerous mistakes is reduced.

[c] MISRA C/C++ enforce strong typing on the respective languages. E.g., for MISRA C:2012, Rules 9.1–9.5, 10.1–10.8, 11.1–11.9, and 14.4.

[d] The MISRA C/C++ guidelines promote the use of several defensive programming techniques. E.g., for MISRA C:2012, Directive 4.1, Rules 2.1–2.7, Rule 14.2, Rule 15.7, and Rule 16.4.

[e] The MISRA C/C++ guidelines and thresholds on HIS metrics embody well-trusted design principles.

[f] More than half of the guidelines in BARR-C:2018 [3] concern coding style [2]. MISRA C:2012 Rules 7.3 and 16.5 are also stylistic.

[g] The MISRA C/C++ guidelines provide some minimal naming advice. E.g., for MISRA C:2012, Directives 4.5 and 4.6, and Rule 8.3. More extensive naming advice is included in BARR-C:2018: Rules 4.1.a–d concern module and file names; Rules 5.1.a–c concern type names; Rules 6.1.e–i, 6.4.a and 6.5.b concern function names; Rules 7.1.e–o concern variable names. Two naming rules are also contained in AUTOSAR-C:2009 [1]. In addition, ECLAIR provides configurable naming rules for maximum flexibility.

Table 3 — Principles for software architectural design

Methods		ASIL				ECLAIR
		A	B	C	D	
1a	Appropriate hierarchical structure of software components	++	++	++	++	✓[a]
1b	Restricted size and complexity of software components	++	++	++	++	✓[b]
1c	Restricted size of interfaces	+	+	+	++	✓[c]
1d	Strong cohesion within each software component	+	++	++	++	✓[d]
1e	Loose coupling between software components	+	++	++	++	✓[d]
1f	Appropriate scheduling properties	++	++	++	++	–
1g	Restricted use of interrupts	+	+	+	++	–
1h	Appropriate spatial isolation of the software components	+	+	+	++	–
1i	Appropriate management of shared resources	++	++	++	++	✓[e]

[a] ECLAIR provides service `B.PROJORG` to enforce constraints about layering and to prevent bypassing of software interfaces.

[b] HIS and other metrics related to the size and complexity of software components. ECLAIR allows associating thresholds to each metric.

[c] HIS metrics counting function parameters and MISRA C/C++ guidelines on reduction of variables' scope.

[d] ECLAIR specific metric.

[e] Management of shared resources is addressed by some MISRA C/C++ guidelines and ECLAIR Bug Finder checks. E.g., for MISRA C:2012, Rules 22.1–22.10.

Table 4 — Methods for the verification of the software architectural design

Methods		ASIL				ECLAIR
		A	B	C	D	
1a	Walk-through of the design	++	+	o	o	✓[a]
1b	Inspection of the design	+	++	++	++	✓[a]
1c	Simulation of dynamic behaviour of the design	+	+	+	++	–
1d	Prototype generation	o	o	+	++	–
1e	Formal verification	o	o	+	+	–
1f	Control flow analysis	+	+	++	++	✓[b]
1g	Data flow analysis	+	+	++	++	✓[c]
1h	Scheduling analysis	+	+	++	++	–

[a] ECLAIR analyses of the implemented designs can highlight design defects and facilitate walk-through and inspection.

[b] ECLAIR builds accurate control flow graphs to reason on (feasible and unfeasible) execution paths.

[c] ECLAIR performs a number of data flow analyses to reason about, e.g., pointers, values and dead stores.

2.4 HIS and Other Source Code Metrics

Source code metrics are recognized by many software process standards (and from MISRA) as providing an objective foundation to efficient project and quality management. One of the most well known set of metrics has been defined by HIS (Herstellerinitiative Software, an interest group set up by Audi, BMW, Daimler, Porsche and Volkswagen).

The *HIS source code metrics* [4], while well established, include some metrics that are obsolete and miss others that are required or recommended by software process standards, such as those that allow

estimating function coupling. For this reason, ECLAIR supplements HIS source code metrics with numerous other metrics that allow software quality to be assessed in terms of complexity, testability, readability, maintainability and so forth. Keeping track of these metrics also provides an effective and objective method to assess the quality of the software development process. The full set of metrics is available in all ECLAIR packages.

Table 6 — Design principles for software unit design and implementation

Methods		ASIL				ECLAIR
		A	B	C	D	
1a	One entry and one exit point in subprograms and functions	++	++	++	++	✓[a]
1b	No dynamic objects or variables, or else online test during their creation	+	++	++	++	✓[b]
1c	Initialization of variables	++	++	++	++	✓[c]
1d	No multiple use of variable names	++	++	++	++	✓[d]
1e	Avoid global variables or else justify their usage	+	+	++	++	✓[e]
1f	Limited use of pointers	+	++	++	++	✓[f]
1g	No implicit type conversions	+	++	++	++	✓[g]
1h	No hidden data flow or control flow	+	++	++	++	✓[h]
1i	No unconditional jumps	++	++	++	++	✓[i]
1j	No recursions	+	+	++	++	✓[j]

[a] MISRA C:2012 Rule 15.5, MISRA C++ Rule 6-6-5. Metric `HIS.RETURN`.

[b] The MISRA C/C++ guidelines include prescriptions limiting the use of dynamic memory allocation. E.g., for MISRA C:2012, Directive 4.12 and Rules 18.7, 21.3, 22.1 and 22.2.

[c] The MISRA C/C++ guidelines include rules mandating the proper initialization of variables. E.g., for MISRA C:2012, Rules 9.1–9.5.

[d] The MISRA C/C++ guidelines include prescriptions against the multiple use of variable names. E.g., for MISRA C:2012, Rules 5.3, 5.5–5.9 and 21.2.

[e] The MISRA C/C++ guidelines include prescriptions against the use of unnecessary global variables. E.g., for MISRA C:2012, Rules 8.7 and 8.9. The specific ECLAIR service `B.GLOBALVAR` allows fine control of allowed global variables.

[f] The MISRA C/C++ guidelines include rules restricting the use of pointers. E.g., for MISRA C:2012, Rules 8.13, 11.1–11.8, and 18.1–18.5. The specific ECLAIR services `B.PTRDECL` and `B.PTRUSE` allows fine control of pointers' use.

[g] The MISRA C/C++ guidelines include several rules restricting the use of implicit conversions. E.g., for MISRA C:2012, Rules 10.1, 10.3–10.7, 11.1, 11.2, 11.4, and 11.5.

[h] The MISRA C/C++ guidelines include prescriptions about hidden control flow and data flow. E.g., for MISRA C:2012, Directive 4.9, Rules 2.1, 5.3, 13.2, 15.1–15.7, 20.7, 20.9, 21.4.

[i] The MISRA C/C++ guidelines include limits on the use of non-structured control-flow constructs as well as other unconditional jumps. E.g., for MISRA C:2012, Rules 14.3, 15.1–15.4, and 21.4. A threshold on metric `HIS.GOTO` allows limiting the use of `goto`.

[j] MISRA C Rule 17.2 and MISRA C++ Rule 7-5-4 forbid recursion. A threshold on metric `HIS.ap_cg_cycle` also allows ruling out recursion.

Table 7 — Methods for software unit verification

Methods		ASIL				ECLAIR
		A	B	C	D	
1a	Walk-through	++	+	o	o	✓[a]
1b	Pair-programming	+	+	+	+	✓[a]
1c	Inspection	+	++	++	++	✓[a]
1d	Semi-formal verification	+	+	++	++	✓[b]
1e	Formal verification	o	o	+	+	–
1f	Control flow analysis	+	+	++	++	✓[c]
1g	Data flow analysis	+	+	++	++	✓[d]
1h	Static code analysis	++	++	++	++	✓[e]
1i	Static analyses based on abstract interpretation	+	+	+	+	✓[f]
1j	Requirements-based test	++	++	++	++	–
1k	Interface test	++	++	++	++	–
1l	Fault injection test	+	+	+	++	–
1m	Resource usage evaluation	+	+	+	++	–
1n	Back-to-back comparison test between model and code, if applicable	+	+	++	++	–

[a] Compliance to the MISRA C/C++ and the BARR-C:2018 guidelines greatly increases code readability and understandability, thereby facilitating verification activities by walk-through, pair-programming and inspection.
[b] ECLAIR implements numerous verification algorithms based on semi-formal notation.
[c] ECLAIR builds accurate control flow graphs to reason on (feasible and unfeasible) execution paths.
[d] ECLAIR performs a number of data flow analyses to reason about, e.g., pointers, values and dead stores.
[e] All ECLAIR verification algorithms are based on static code analysis.
[f] Several verification algorithms implemented by ECLAIR are formalized in terms of abstract interpretation.

Table 10 — Methods for verification of software integration

Methods		ASIL				ECLAIR
		A	B	C	D	
1a	Requirements-based test	++	++	++	++	–
1b	Interface test	++	++	++	++	–
1c	Fault injection test	+	+	++	++	–
1d	Resource usage evaluation	++	++	++	++	–
1e	Back-to-back comparison test between model and code, if applicable	+	+	++	++	–
1f	Verification of control and data flow	+	+	++	++	✓[a]
1g	Static code analysis	++	++	++	++	✓[b]
1h	Static analyses based on abstract interpretation	+	+	+	+	✓[c]

[a] ECLAIR executes a number of control flow and data flow analyses.
[b] All ECLAIR verification algorithms are based on static code analysis.
[c] Several verification algorithms implemented by ECLAIR are formalized in terms of abstract interpretation.

2.5 ISO 26262:2018 *Freedom from Interference*, *Independence*, and *Interference*

ISO 26262:2018 defines *freedom from interference* (FFI) as "absence of *cascading failures* between two or more *elements* that could lead to the violation of a *safety* requirement" [5, Clause 3.65]. Simply put, a *cascading failure* (CF) is a failure that causes an element to fail, which in turn causes a failure in another element [5, Clause 3.17], whereas a *common cause failure* (CCF) is the failure of two or more elements resulting directly from a single specific event (root cause) [5, Clause 3.18]. The union of CFs and CCFs gives what ISO 26262:2018 calls *dependent failures* (DFs), namely, failures that are not statistically independent [5, Clause 3.29].

The notion of DF comes into play in the definition of one aspect of *independence*: "absence of dependent failures between two or more elements that could lead to the violation of a safety requirement" [5, Clause 3.78].[2] As CFs are a subset of DFs, FFI is instrumental in achieving independence. In turn, achievement of independence or freedom from interference between the software architectural elements can be required because of: (a) the application of an ASIL decomposition at the software level; (b) the implementation of software safety requirements;[3] or (c) required coexistence of the software architectural elements [6, Annex E]. Concerning the last point, criteria for coexistence of elements are given in [8, Clause 6]. When coexistence is required there are two options: (1) all coexisting sub-elements are developed in accordance to the highest ASIL applicable to the sub-elements; (2) the guidance provided in [8, Clause 6] is used to determine whether sub-elements with different ASILs can coexist within the same element. Such guidance is based on the analysis of *interference* of each sub-element with other sub-elements: evidence has to be provided to the effect that there are no CFs from a sub-element with no ASIL assigned (QM), or a lower ASIL assigned, to a sub-element with a higher ASIL assigned, such that these CFs lead to the violation of a safety requirement of the element.[4]

Software partitioning is one of the possibilities for implementing freedom of interference, which must be developed and evaluated taking into account faults concerning *timing and execution*, *memory*, and *exchange of information* [6, Annex D]. ISO 26262:2018 prescribes that software partitioning must be supported, for ASIL D, by dedicated hardware features or equivalent [6, Clause 7.4.9]. A memory protection unit (MPU) is typically used for this purpose; however, as these devices can only enforce partitioning of memory areas and system-on-chip peripherals, other measures are required in order to ensure freedom of interference.

ECLAIR Support for *Freedom from Interference*, *Independence*, and *Interference*

ECLAIR provides crucial support to provide evidence ensuring *freedom of interference*, *independence*, and absence of *interference*. Compliance to the MISRA guidelines reduces the risk of execution blocking due to unexpected excessive loop iterations (one of the issues in the *timing and execution* category) as well as of stack overflow (in the *memory* category). Most importantly, ECLAIR provides a very general service to detect and check, by control and data flow static analyses, all interactions between user-defined software elements occurring via read or write accesses to shared memory, function calls, passing and returning of data, and so on. This ECLAIR service can be used:

1. In the context of ASIL decomposition applied at the software level, to verify whether the elements implementing the decomposed requirements are sufficiently *independent*.
2. In the implementation of software safety requirements that rely on *freedom from interference* or sufficient *independence* between software components.

[2] This is the technical aspect of *independence*, the other aspect being the organizational one.

[3] E.g., to provide evidence for the effectiveness of monitoring safety mechanisms by showing independence between the monitored element and the monitor.

[4] It is important to realize that "absence of *interference*" and "*freedom of interference*" are distinct concepts in ISO 26262:2018. The latter concept does not depend on ASILs or lack thereof, so that "*freedom of interference*" implies "absence of *interference*," but not the other way around.

3. To determine whether sub-elements with different ASILs can coexist within the same element by verifying absence of *interference* between the sub-elements.

For applications 1 and 2, the user configures the software components by specifying the program elements (functions, variables, ...) that are assumed to be private to each component or shared between components. With this information, ECLAIR can produce output detailing the actual interactions between the software components, both in textual and in graphic form. If the user further specifies the allowed interactions between components, ECLAIR will produce a violation message for each unwanted interaction. For application 3, the user configures the ASIL (or QM) of the sub-elements, and the service will flag all program actions whereby a CF might exist from a sub-element with no ASIL assigned (QM), or a lower ASIL assigned, to a sub-element with a higher ASIL assigned. All this greatly simplify the work to be done in order to ensure compliance with the objectives of related to Clause 7 and Annex E of ISO 26262:2018 Part 6, and Clause 6 of ISO 26262:2018 Part 9.

3 ECLAIR Coverage of ISO 26262:2018 Part 8 Objectives

For automotive applications, Part 8 of ISO 26262:2018 specifies the requirements for supporting processes [7, Section 11], including:

- the criteria to determine the required level of confidence in software tools;
- the means for the qualification of software tools, in order to create evidence that such tools are suitable to be used to support the activities and tasks required by ISO 26262.

ECLAIR qualification kits for ISO 26262 provide crucial help to safety teams in charge of qualifying ECLAIR for use in safety-related projects: the kits contain documents, test suites, procedures and automation facilities that can be used by the customer to obtain all the required confidence-building evidence.

4 The Bigger Picture

ECLAIR is very flexible and highly configurable. It can support your software development workflow and environment, whatever they are.

ECLAIR is fit for use in mission- and safety-critical software projects: it has been designed from the outset so as to exclude configuration errors that would undermine the significance of the obtained results.

ECLAIR is developed in a rigorous way and carefully checked with extensive internal test suites (tens of thousands of test cases) and industry-standard validation suites.

ECLAIR is based on solid scientific research results and on the best practices of software development.

ECLAIR's unique features and BUGSENG's strong commitment to the customer, allow for a smooth transition to ECLAIR from any other tool.

BUGSENG's quality system has been certified by TÜV Italia (TÜV SÜD Group) to comply with the requirements of UNI EN ISO 9001:2015 for the "Design, development, maintenance and support of tools for software verification and validation" (IAF 33).

BUGSENG is an Arm's Functional Safety Partner. Arm's Functional Safety Partnership Program promotes partners who can reliably support their customers with industry leading functional safety products and services.

References

[1] AUTOSAR. Specification of C implementation rules. Technical report, AUTOSAR, 2009.

[2] R. Bagnara, M. Barr, and P. M. Hill. BARR-C:2018 and MISRA C:2012: Synergy between the two most widely used C coding standards, 2020.

[3] M. Barr. *BARR-C:2018 — Embedded C Coding Standard*. Barr Group, www.barrgroup.com, 2018.

[4] H. Kuder et al. HIS source code metrics. Technical Report HIS-SC-Metriken.1.3.1-e, Herstellerinitiative Software, 2008. Version 1.3.1.

[5] ISO. *ISO 26262:2018: Road Vehicles — Functional Safety — Part 1: Vocabulary*. ISO, Geneva, Switzerland, 2018.

[6] ISO. *ISO 26262:2018: Road Vehicles — Functional Safety — Part 6: Product development at the software level*. ISO, Geneva, Switzerland, 2018.

[7] ISO. *ISO 26262:2018: Road Vehicles — Functional Safety — Part 8: Supporting processes*. ISO, Geneva, Switzerland, 2018.

[8] ISO. *ISO 26262:2018: Road Vehicles — Functional Safety — Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses*. ISO, Geneva, Switzerland, 2018.

[9] MISRA. *MISRA C:2012 — Guidelines for the use of the C language critical systems*. HORIBA MIRA Limited, Nuneaton, Warwickshire CV10 0TU, UK, 2019. Third edition, first revision.

[10] MISRA. *MISRA C:2012 Amendment 2 — Updates for ISO/IEC 9899:2011 Core functionality*. HORIBA MIRA Limited, Nuneaton, Warwickshire CV10 0TU, UK, 2020.

[11] MISRA. *MISRA C++:2008 — Guidelines for the use of the C++ language in critical systems*. MIRA Limited, Nuneaton, Warwickshire CV10 0TU, UK, 2008.

For More Information

BUGSENG srl
Parco Area delle Scienze 53/A
I-43124 Parma, Italy
Via Lenin 132/F
I-56017 San Giuliano Terme (PI), Italy
Email: info@bugseng.com
Web: http://bugseng.com

**no shortcuts,
no compromises,
no excuses:
software verification done right**