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

The ECLAIR Bug Finder

The *ECLAIR Bug Finder* is a general-purpose static analysis application for C and C++ that runs on top of ECLAIR, a powerful platform for the automatic analysis, verification, testing and transformation of C and C++ programs. The package includes a very fast static analyzer able to detect and report bugs and weaknesses that can lead to crashes, misbehaviors, and security vulnerabilities.

1 Highlights

- Very fast: can be run on the developer's desktop, for early detection of a number of software defects.
- Extremely high signal-to-noise ratio.
- No need to write compiler personality files (time-consuming and often of questionable correctness).
- Automatically produces accurate and detailed reports.
- Reports optionally available to the entire development team and management using web-based technology.
- No stress: free consultancy services for the initial configuration. This includes full assistance to help your company make the transition to the *ECLAIR Bug Finder* package.

2 Features

The *ECLAIR Bug Finder* is a tool designed to run on the developer's desktop as well as on integration servers. It enables the early detection of a number of software defects.

Avoid shipping defects to customers (with disastrous consequences and high remediation costs) and lower the cost of development by drastically reducing the resources spent in reworking and retesting.

Unlike other systems, the *ECLAIR Bug Finder* does not require compiler- and target-dependent configurations (which are often error-prone) and presents accurate results that make it easy to identify "culprit" pieces of code and the correct remediations.

ECLAIR Bug Finder identifies security vulnerabilities, dead code, API misuses and other errors in C and C++ source code, including:

- buffer overflows
- dereferences of null pointers
- pointer arithmetic errors
- use of uninitialized variables
- uninitialized or invalid return values
- divisions by zero
- undefined operations
- dead stores
- leaks of stack memory addresses
- memory leaks
- unreachable code
- double-free
- use-after-free
- other dynamic memory allocation issues (e.g., taint analysis)
- lossy implicit conversions
- excessive padding (memory waste)
- vararg functions mistakes
- string manipulation errors
- library API violations
- insecure use of library functions
- multithreading issues
- dynamic type errors
- other common programming mistakes

3 Proper Integration with the Toolchain

ECLAIR Bug Finder, like all packages that run on ECLAIR, intercepts every invocation of the toolchain components (compilers, linker, assembler, archive manager) and it automatically extracts and interprets the options that the build system has passed to them. This allows for the seamless integration with any build system.

Moreover, you do not need to engage in error-prone activities such as (a) specifying which files make up the application, and where the right header files are located; (b) configuring the static analyzer so that the analysis parameters match the options given to the compilers (several options *do* affect the program semantics); (c) writing down predefined macros and the architectural parameters such as sizes, alignment constraints, address spaces and so forth. All this is automatic and supports build processes that involve the automatic generation of source files that depend on the configuration, without the need to develop and maintain a separate analysis procedure: with ECLAIR the existing build procedure can be used verbatim.

ECLAIR is available on most modern flavors of UNIX®, Linux, macOS®and Windows®, including Cygwin and MinGW, and can be used with just about any development environment. ECLAIR supports parallel and distributed program analysis, to leverage available computing resources. Most popular C/C++ compilers and cross compilers are supported, including AMD Xilinx™, Andes, ARM®, CAES™, CodeWarrior™, Cosmic Software, CrossWorks™, Emscripten, Espressif™, Freescale™, GCC and its derivatives, Green Hills®, HighTec, IAR™, Infineon™, Intel®, Keil Software®, Melexis™, Microsoft®, MPLAB®, NXP™, QNX™, Renesas Electronics, SOFTUNE™, TASKING®, Texas Instruments™, xPack, Wind River®, as well as clang/LLVM and its derivatives.

4 The Bigger Picture

ECLAIR is very flexible and highly configurable: it supports all kinds of software development workflows and environments.

ECLAIR is fit for use in mission- and safety-critical software projects: it has been designed from the outset 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, and is thus recognized as a partner who can reliably support their customers with industry leading functional safety products and services.

The *ECLAIR Bug Finder* is incorporated in many ECLAIR packages, such as B, MC and MP.

For More Information

BUGSENG srl
Via Fiorentina 214/C
I-56121 Pisa, Italy
Email: info@bugseng.com
Web: http://bugseng.com

bugseng

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