Quantification and Comparison of the Energy Impact of SAST within Continuous Integration (CI) in Large-Scale Projects

Rafael Petouris Rodríguez de Paterna, supervised by Xutong Liu & Carolin Brandt

1) Introduction

CI is essential in software development. Static Analysis Security Tools (SAST) help detect vulnerabilities ASAP. Vulnerabilities are rife. More code = more commits, costly review.

Pipeline runs a lot. This is not good for the environment. Elasticsearch builds alone ≈ 10% of the yearly avg. household electricity cons. Aggregate costs are known, but not per tool.

How do different SpotBugs configurations affect energy consumption?
What configurations optimize the energy-security tradeoff?

2) Methodology

Use Energibridge to measure energy consumption. Employ same environment. Minimize external processes, connect to wall socket.
1 Minute cooldown between tests to avoid aberrations. Warm up CPU before tests. 3 Spotbugs+FSB Configurations (Baseline/High Effort/Low Threshold), 7 Projects (from Zaidman's research), 30 tests per configuration and project. Automated through a click-and-run Batch file with supervision. Configurations benchmarked and compared. Data obtained is normalized and plotted with violin plots for analysis.

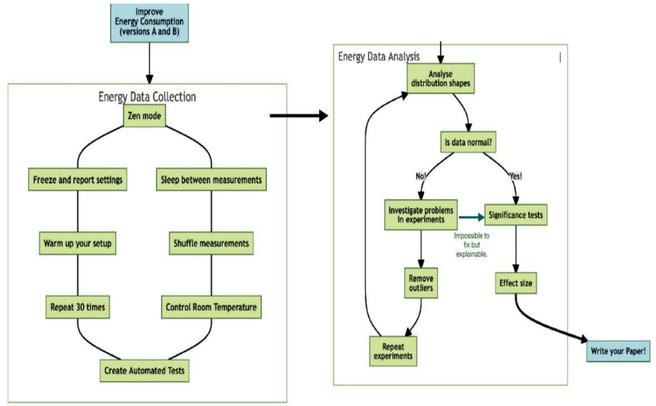

Fig. 1: Methodology

3) Results and Discussion

Configuration B (High Effort) provides no security benefit, it detected identical bug counts as baseline despite +7.44% energy cost for **large Gradle projects** (Elasticsearch).

Configuration C (Low Threshold) is valuable only for **Maven**: reported 146% more bugs (1,923 vs 781) with minimal energy increase (+1.07% for Maven, +0.65% for Guava). **No benefit for Gradle projects. Otherwise it does not matter.**

Maven consumes ~100x more energy than Gradle due to redundant rebuilding vs Gradle's incremental compilation caching.

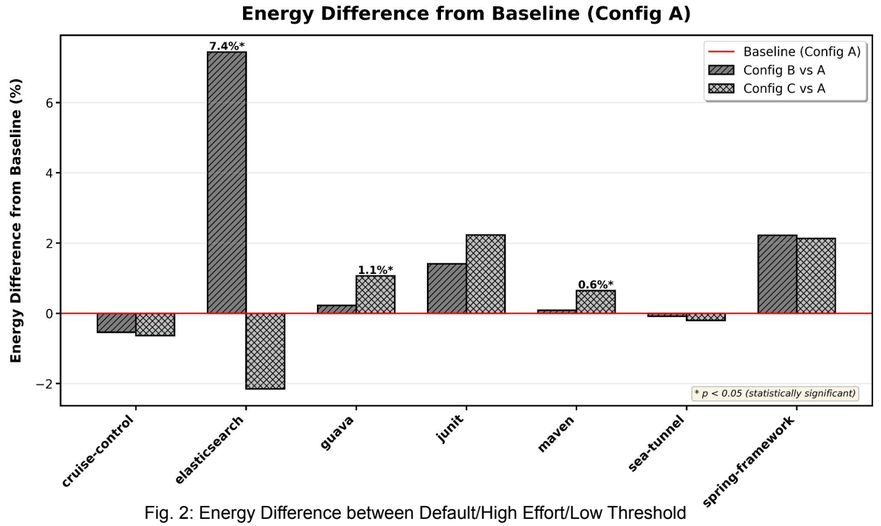

Fig. 2: Energy Difference between Default/High Effort/Low Threshold

4) Conclusions and Future Work

Configuration B (High Effort) not recommended It provides zero security benefit while increasing energy costs for large projects.

Configuration C (Low Threshold) recommended for small-to-medium Maven projects (<500MB). It provides 146% more bug detection with negligible energy cost. Else, it **does not matter** which configuration to use.

Maven consumes x100 more than Gradle.

Impact of project size on energy consumption and build tool across more diverse projects must be analyzed.
Test additional SpotBugs configurations beyond the 3.