

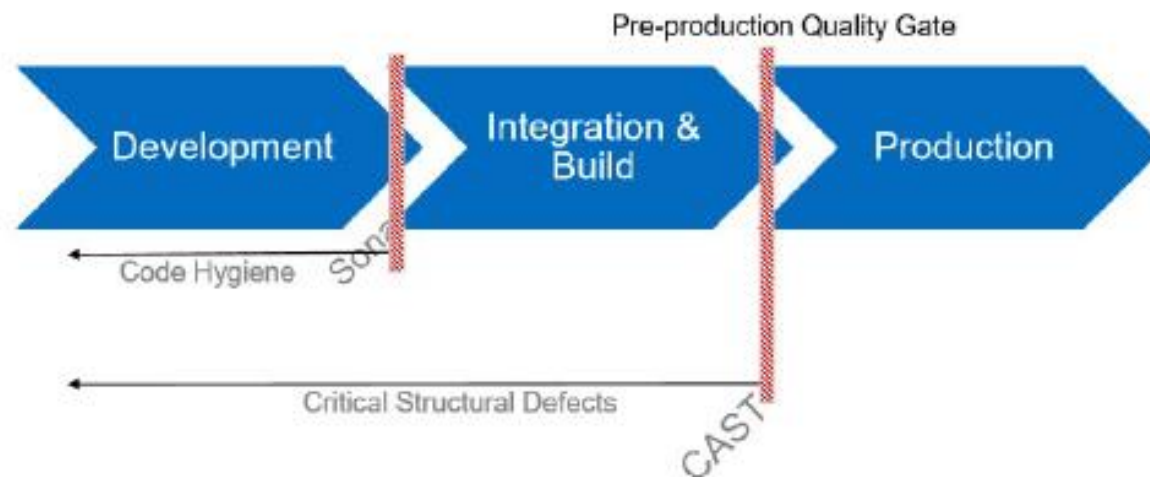
CAST Vs Sonar

CAST and SONAR are Complimentary



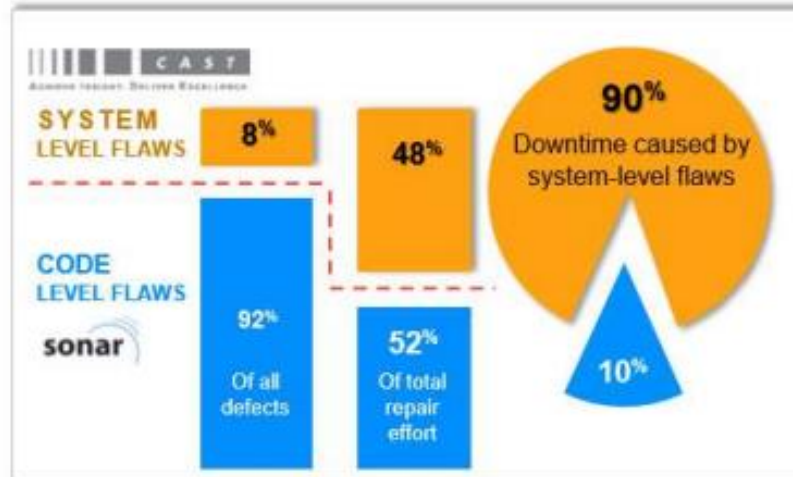
- A vast majority of CAST clients are also Sonar users
- Often client's consider the two solutions to be competitors, but actually they serve very different purposes in the software development life cycle.
- Sonar is a code hygiene tool used by developers which focuses on maintainability and changeability. It is not meant to identify risks that could cause security breaches, slow performance, or critical failures in production.
- CAST acts as a pre-production quality gate, specifically focusing on finding critical structural defects to address software risk.

Example of Customer Deployment of CAST with Sonar in Dev Cycle



CAST Vs Sonar

Quality Model Evolution – from Lines of Code to Systems



Trends and What CIOs Tell Us

- Sonar used early as developer tool for first move towards quality. Focus is on developer code hygiene.
- CAST added as quality programs matured to support four key uses:
 - System-level flaw detection
 - Robust pre-production quality gates
 - Accurate measurement including function points to enable decision-making
 - Technology coverage to address vast majority of application components

Nascent

Quality Model Evolution

Mature



























Sonar

- File-level analysis provides entry-level insight for developer
- Rules focus on code hygiene versus detecting critical defects
- No calculation of productivity measurements (automated function points)
- Limited supported technology coverage
- No scope control (can create spotty app coverage)

CAST AIP

- System-level view finds the most critical and hardest to detect defects
- System-level delivers accurate and repeatable measurements of technical debt, function points, and application quality
- Breadth of technology coverage delivers analytics for all of your applications from user interface to database

CAST Vs Sonar

Features	CAST	Sonar	Comments
System Level Analysis			AIP performs inter-tier/ inter-technology analyses. SONAR performs one technology at a time
Application Blueprinting			CAST has a unique capability to image an entire multi -tier application - Imaging System
Sizing & Estimation – Function Points			CAST provides AFP and AEP metrics using Function Points – IPFUG standards
Support for multiple technologies			SONAR – 25(Among them many are supported by the open source community) CAST – 50+ including older languages, frameworks, middleware, ERPs, mainframe, etc. + 30 additional technologies provided by CAST Extend
Support for industry Quality and Security Standards			CAST gives a System level perspective starting from the UI to End points(like Database, Webservices etc). It supports the CISQ standards along with others such as OWASP Top 10, CWE, NIST, STIG, OMG
Architecture Rules			Native architecture rules can be augmented with Architecture Checker Architects can monitor compliance using the checker. Custom rules can be added.
Quality Benchmarking			CAST AppMarq DB has a unique application benchmarking capability, across industries, apps type, technologies. The details are available in the Health Dashboards.
Portfolio level assessment and Reporting			Sonar has limited flexibility into arranging applications as portfolios for Senior Management/Executive level
DevOps Integration			Seamless integration to the DevOps pipeline
IDE integration			SONAR provides IDE plugins.
Cross-technology Transaction Mapping/ Tagging Sensitive Data			CAST can map a transaction path from user input to database. This is crucial to ensure application security
Remediation plans management & prioritization			CAST provides an Action Plan Optimizer along with risk metrics. Continuous Improvement graphs can be accessed by the teams.
Compares versions			Snapshot comparison can be done with CAST where added/modified and deleted violations and code can be identified.