TraceMaster
CodeTrack

MACRO|4
A Division of UNICOM® Global

Code assurance for CICS

Improve the code quality, security and performance that underpins your business applications

TraceMaster CodeTrack is an effective solution offering CICS code path analysis and storage violation detection

TraceMaster CodeTrack is a key component of the TraceMaster family, offering advanced CICS code path analysis and storage violation detection. TraceMaster CodeTrack monitors the execution of every instruction performed by a targeted program, providing application developers with:

- More extensive pre-production application testing, supported by a variety of reports that present detailed testing results
- Greater understanding of code execution/non-execution, with clinical insight into the number of times specific instructions are executed throughout a program cycle
- Complete certainty that storage violations will not occur when application code is executed
- Fully audited test results which include verification that all code paths have been executed
- A pre-emptive testing process that aids improvements in application code quality, security and performance
- Reduced fault diagnosis costs

The code assurance solution

TraceMaster CodeTrack provides two valuable services:

- Code path analysis – monitoring every instruction issued by a targeted program
- Storage violation detection – tracking the execution paths of CICS applications

These services make TraceMaster CodeTrack an effective tool in the quality control process leading up to the promotion of applications to a production environment.

Code path analysis

Code path analysis enables the extent of testing carried out on new or enhanced applications to be determined.

TraceMaster CodeTrack monitors every instruction issued by the target program, accumulates a count of the number of times the instruction has been executed and can then produce reports that clearly outline:

- Executed code
- Code hotspots
- Poor code structure
- Redundant/non-executed code

TraceMaster
CodeTrack

Macro 4's integrated suite for z Systems fault analysis and testing:

DumpMaster
Fault analysis and recovery

InSync®
Data management and manipulation

TraceMaster
Interactive testing and debugging

TraceMaster CodeTrack
CICS code path analysis and storage violation detection

www.macro4.com

Storage violation detection

Storage violation detection tracks the execution path of CICS applications. When a monitored application is about to execute a store instruction that will update an area of storage, TraceMaster CodeTrack verifies that the targeted memory area is actually owned by the application.

If an application attempts to update storage lying outside of its ownership, the update is detected by TraceMaster CodeTrack, at which point the impending violation can be handled in a number of ways:

- LOG mode: A record is written to the TraceMaster CodeTrack log file, the violation is then permitted, and the program continues
- DUMP mode: A CICS transaction dump is taken, the violation is then permitted, and the program continues
- LOGDUMP mode: TraceMaster CodeTrack records an entry in the log file and takes a CICS transaction dump
- ABEND mode: TraceMaster CodeTrack prevents the violation by abending the transaction, creating a small diagnostic dump
- LOGABEND mode: TraceMaster CodeTrack records an entry in the log file and abends the transaction

Greater efficiency through pre-emptive processing

TraceMaster CodeTrack's pre-emptive process is more efficient, and safer than trying to detect a storage error after it has occurred – a considerable advantage over the standard CICS mechanisms.

The low-level interception approach enables monitoring to be applied in almost all circumstances, particularly to transactions that might preclude the use of standard CICS mechanisms.

Used in development or system testing environments, TraceMaster CodeTrack is the perfect tool for ensuring that none of the code going into the production environment will cause storage violations.

Easy upkeep

TraceMaster CodeTrack can be readily implemented in any number of CICS systems as there is minimal setup and maintenance required. This is valuable when monitoring for errors that occur rarely or under unusual circumstances. It also offers a significant advantage over the standard functions available through CICS.

When a program is started in a region where TraceMaster CodeTrack is active, TraceMaster CodeTrack determines whether it should be monitored by referencing the exclusion and inclusion lists.

Accurate reporting

When monitoring CICS applications for storage violations, TraceMaster CodeTrack creates a record in the log file that contains the session start and end time, as well as detailed information on each detected storage violation.

When performing code analysis, TraceMaster CodeTrack provides complete analysis reports that can be used for review and stored for auditing purposes. These reports enable testers to determine the level of testing carried out on new or updated applications.

TraceMaster CodeTrack analysis reports reveal leftover fragments of unused and potentially malicious code that need to be removed or corrected.

Please contact us for more information:

USA Tel: +1 973 526 3900 Email: market.usa@macro4.com
Europe Tel: +44 1293 872000 Email: market@macro4.com