Peacenik: Architecture Support for Not Failing under Fail-Stop Memory Consistency

Rui Zhang  Swarnendu Biswas  Vignesh Balaji
Ohio State University, USA  Indian Institute of Technology  Carnegie Mellon University, USA
zhang.5944@osu.edu  swarnendu@cse.iitk.ac.in  vigneshb@andrew.cmu.edu

Michael D. Bond
Ohio State University, USA
mikebond@cse.ohio-state.edu

Brandon Lucia
Carnegie Mellon University, USA
blucia@andrew.cmu.edu

Abstract
Modern shared-memory systems have erroneous, undefined behavior for programs that are not well synchronized. A promising solution is to provide fail-stop memory consistency, which ensures well-defined behavior for all programs. While fail-stop consistency avoids undefined behavior, it can lead to unexpected failures, imperiling performance or progress.

This paper presents architecture support called Peacenik that avoids failures in the context of fail-stop memory consistency. We demonstrate Peacenik by applying Peacenik’s general mechanisms to two existing architectures that provide fail-stop consistency. A simulation-based evaluation shows that Peacenik eliminates nearly all of the high costs of fail-stop behavior incurred by the baseline architectures, demonstrating how to get the benefits of fail-stop consistency without incurring most or all of its costs.

CCS Concepts: • Computer systems organization → Reliability; Availability; Processors and memory architectures; Multicore architectures; • Software and its engineering → Consistency.

Keywords. Data races, fail-stop memory consistency, conflict exceptions, failure avoidance

ACM Reference Format:


1 Introduction
To achieve high performance, today’s shared-memory systems use compiler and hardware optimizations that assume data-race-free (DRF) programs. The DRF assumption is codified in memory models including the C/C++ and Java memory models, which ascribe undefined or ill-defined semantics to programs with data races [3, 4, 13–15, 43]. Data races are not just erroneous in theory, but can cause serious problems in practice [36, 37, 48, 65]. Mature, widely used applications have data races, which are not easy to detect or eliminate fully [23, 27, 34–37, 40, 48, 65]. Production systems typically have different run-time characteristics than testing environments, making it difficult to catch all production-time data races during in-house testing.

Researchers have sought to provide stronger end-to-end (i.e., with respect to the source program) memory consistency by restricting compiler and hardware optimizations—notably by providing end-to-end SC [5, 58, 61, 64]. (Restricting only hardware [16, 20, 26, 38, 39, 52] or the compiler [45] fails to provide end-to-end SC.)

Alternatively, instead of restricting optimizations, a system can detect the conditions for weak or undefined semantics and treat them as fail-stop errors [9, 10, 21, 25, 41, 44, 53, 60, 67]. Under fail-stop memory consistency, all programs have well-defined behavior, and an execution stops if it might have undefined behavior due to a data race.

Fail-stop consistency solves one problem (undefined, erroneous behavior) but introduces another: data races can lead to unexpected production-time failures [23, 27, 35, 40]. If a system handles such failures by rebooting (i.e., terminating and restarting) a program or a component, fail-stop errors translate into more execution time.

This paper’s goal is to avoid failures due to fail-stop consistency as much as possible, with minimal cost and complexity while retaining strong consistency guarantees. To that end, we introduce Peacenik, a set of architecture mechanisms
that extend a baseline fail-stop consistency design to provide comprehensive, best-effort support for avoiding failures. Peacenik’s main components are support for (1) pausing a core’s execution to avoid conflicts that lead to failures, (2) restarting regions of code that would otherwise fail, and (3) cache replacement policy modifications that increase the chances of a region being eligible for restart. Peacenik cannot avoid all failures because its mechanisms are best-effort—in particular, a core cannot restart a region if the dirty data written by the region escapes from its private caches due to eviction or a remote coherence request—but Peacenik’s mechanisms are effective in practice. While Peacenik employs mechanisms borrowed from hardware transactional memory (HTM), its design differs from both best-effort and unbounded HTM (Section 2).

We show the generality and effectiveness of Peacenik by developing prototype implementations that extend ARC and Conflict Exceptions (CE), two architectures from prior work that provide fail-stop consistency [10, 41]. While ARC and CE—like any system that supports precise, unbounded region conflict detection—incur significant complexity on their own, Peacenik’s architecture support for avoiding failures is relatively simple and incurs low costs and complexity on top of any underlying system.

A simulation-based evaluation shows that, under fail-stop consistency semantics without Peacenik, several benchmarks and real-world programs suffer from fail-stop errors due to data races. Our experiments model these errors by rebooting the program, or by repeating a request in the case of server programs, leading to high performance costs from fail-stop errors. We also find that fail-stop errors incur significant costs even if the experiments model idealized process checkpointing. In contrast, Peacenik avoids nearly all fail-stop errors in our experiments, achieving essentially the same performance as data-race-free programs would achieve, while also providing strong behavior guarantees. These results show that simple, effective failure-avoidance mechanisms can overcome the primary obstacle to practical fail-stop memory consistency.

2 Background, Problem, and Related Work
This section overviews fail-stop consistency and its costs, and motivates the importance and challenge of avoiding failures.

2.1 Fail-Stop Memory Consistency
As Section 1 explained, data races are erroneous and lead to serious failures [3, 4, 13–15, 36, 37, 43, 48, 65]. Researchers have proposed systems that provide fail-stop semantics by generating a consistency exception upon a data race [19, 21, 24, 49, 53, 67]. Since sound and precise dynamic race detection is expensive [19, 24], efficient systems provide fail-stop consistency by detecting conflicts between concurrently executing synchronization-free regions (SFRs) [9, 10, 25, 41, 44, 60]. (An SFR is a sequence of per-thread dynamic instructions demarcated by synchronization operations.) In such systems—this paper’s focus—a conflict indicates a data race, while a conflict-free execution is equivalent to a serialization of executing SFRs. The rest of this paper uses the terms “SFR” and “region” interchangeably.

Lazy and eager conflicts. In this paper, an important distinction exists between conflicts that are detected lazily versus eagerly. We define a lazily detected conflict, or a lazy conflict, as a conflict detected when it is “too late” to ensure serializability of regions, i.e., if the continued execution cannot guarantee region serializability. In contrast, an eagerly detected conflict, or an eager conflict, is detected when it may still be possible for the execution to achieve region serializability. Note that, in contrast with typical definitions of eager conflict detection [29], our definition of an eagerly detected conflict permits both accesses to have already executed, so long as serializing the conflicting regions is still feasible. Our Peacenik design handles both lazy and eager conflicts.

Existing fail-stop consistency systems. DRFx is a system that provides fail-stop consistency by checking for conflicts between regions that are bounded (statically limited to a fixed number of memory accesses) [44, 60]. Bounded regions reduce DRFx’s hardware requirements but require compiler modifications that limit cross-region optimization. DRFx detects conflicts lazily by broadcasting an ending region’s read and write sets to other cores, which check for conflicts.

Valor, Conflict Exceptions (CE), and ARC detect conflicts between (unbounded) SFRs, i.e., regions bounded only at synchronization operations [9, 10, 41]. The resulting memory consistency model, called SFRSx, ensures that every execution is SFR serializable or generates a consistency exception due to a data race. Software or architecture support alone is sufficient to provide end-to-end SFRSx: hardware and compilers already restrict optimizations across SFR boundaries and thus require no complementary modifications.

Valor provides SFRSx in software only, slowing programs by almost 2× on average [9]. CE and ARC are architectures that provide SFRSx [10, 41]. CE detects all conflicts eagerly, while ARC detects some conflicts eagerly and others lazily.

By adding simple hardware components, Peacenik’s mechanisms (Section 3) and architecture design (Section 4) can extend any system that provides fail-stop behavior for conflicting regions, including DRFx, Valor, CE, and ARC. Our prototype implementations of Peacenik extend CE and ARC (Section 4).

2.2 Failures Impact Performance
Fail-stop consistency semantics provide a solid theoretical foundation for memory consistency [3]. But what are the practical implications of fail-stop consistency? What happens when a program encounters a consistency exception?
Although a program could potentially catch and handle a consistency exception using language or library support, we envision two major problems with that approach:

- Like memory errors and null pointer exceptions, consistency exceptions are unexpected. Writing handlers for every potentially shared access would be a huge programming burden.
- Existing systems that provide fail-stop semantics attain efficiency by detecting some or all conflicts after both conflicting accesses have already executed [9, 10, 44, 60], making precise exceptions infeasible.¹

Instead, we envision systems handling a consistency exception as a termination signal, by rebooting (i.e., terminating and restarting) the program.

Fail-stop behavior essentially trades one problem for another, avoiding the subtle failure modes of data races, but causing systems to stop executing and repeat some or all of their work upon encountering a data race. Consequently, consistency exceptions represent a threat to performance: a program that generates consistency exceptions will take longer to produce results or handle requests, wasting time and other resources. In this work, we seek to limit such costs, while still providing well-defined behavior for all program executions.

### 2.3 Avoiding Failure under Fail-Stop Semantics

Failure-avoidance mechanisms arguably should be implemented in hardware. Supporting failure avoidance architecturally permits the failure avoidance mechanism access to microarchitectural state such as the access metadata associated with private and shared cache lines used by existing fail-stop systems [10, 41, 44, 60].

Some prior work avoids failures with software support. **Avalon** extends software-based SFRSx support to avoid consistency exceptions by pausing threads that detect conflicts [71]. **SOFRITAS** enforces conflict serializability using two-phase locking, effectively pausing conflicting threads [18]. Both approaches rely on software only and do not introduce architecture support for pausing or resuming cores, nor can they support restarting regions.

#### Comparison with HTM

Architecture support for failure avoidance under fail-stop consistency is related to hardware transactional memory (HTM) [6, 11, 12, 28, 29, 31, 66, 69]. While our Peacenik design borrows and adapts some mechanisms from HTM, Peacenik differs from both best-effort and unbounded HTM as a consequence of targeting the fail-stop consistency context. Table 1 compares Peacenik’s requirements with those of best-effort and unbounded HTM.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Best-effort HTM</th>
<th>Unbounded HTM</th>
<th>Failure avoidance-mechanisms under fail-stop consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A conflict is a(n)…</td>
<td>Misspeculation</td>
<td>Misspeculation</td>
<td>Error</td>
</tr>
<tr>
<td>Conflict detection…</td>
<td>May be imprecise</td>
<td>May be imprecise</td>
<td>Must be precise</td>
</tr>
<tr>
<td>Pause execution at conflicts?</td>
<td>No, typically</td>
<td>Yes, for bounded time</td>
<td>Yes, indefinitely</td>
</tr>
<tr>
<td>Regions may become ineligible for restart?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Action when regions become ineligible for restart</td>
<td>Abort</td>
<td>N/A</td>
<td>Continue execution</td>
</tr>
</tbody>
</table>

Table 1. Comparison between the requirements of HTM and failure-avoidance mechanisms.

**Comparison with HTM.** Architecture support for failure avoidance under fail-stop consistency is related to hardware transactional memory (HTM) [6, 11, 12, 28, 29, 31, 66, 69].

While our Peacenik design borrows and adapts some mechanisms from HTM, Peacenik differs from both best-effort and unbounded HTM as a consequence of targeting the fail-stop consistency context. Table 1 compares Peacenik’s requirements with those of best-effort and unbounded HTM. HTM conflict detection is generally imprecise because a conflict is only a misspeculation, while failure avoidance must be precise since conflicts are errors. Some HTMs support detecting conflicts before one of the conflicting accesses has executed [9, 10, 44, 60], making precise exceptions infeasible.

Both best-effort and unbounded HTM have limitations as potential failure-avoidance mechanisms. Best-effort HTM provides no progress guarantee and in practice cannot complete long transactions or transactions with irrevocable operations. Unbounded HTM adds significant complexity and cost compared with this paper’s Peacenik mechanisms.

#### Other related work

Some prior work applies HTM or HTM-like mechanisms to enforce serializability of SFRs, incurring the complexity of unbounded HTM [5, 28, 47, 55, 56].

**Wait-n-GoTM** and **BulkSMT** use pausing to avoid conflicts [32, 50]. Like Peacenik, BulkSMT supports pausing in a non-speculative setting, but provides a consistency guarantee only with respect to the compiled program (serializability of bounded chunks), not an end-to-end guarantee [50]. **SC-safe** detects dependency cycles due to SC violations or false sharing, in order to enforce SC and log violations of SC [20]. In contrast, Peacenik detects deadlocks that it has introduced by pausing at detected region conflicts. **ConAir** and **BugTM**

¹A precise exception is generated immediately before a conflicting access executes. Note that the conditions for a precise exception (detecting a conflict before one of the conflicting accesses has executed) are stricter than the conditions for an eagerly detected conflict (as defined in Section 2.1).
Figure 1. Three examples showing how Peacenik’s mechanisms avoid consistency exceptions. For (a) and (c), we assume the conflicts are detected eagerly, while (b) assumes the conflicts are detected lazily. In all examples, shared variables x and y are initially 0. Boxes demarcate synchronization-free regions (SFRs); dashed boxes indicate restarted regions. Gray text indicates instructions delayed due to pausing. Gray dashed arrows indicate eager conflicts.

re-execute code regions to recover from concurrency bug failures such as atomicity violations [17, 72].

How should failure-avoidance mechanisms be used? In testing, it is counterproductive to hide errors, so developers should disable failure-avoidance mechanisms. However, complete testing is infeasible. Even after fixing known data races (e.g., races detected during testing), large concurrent programs are likely to have unknown data races that manifest rarely and unexpectedly on production systems. Production systems should enable failure-avoidance mechanisms to avoid or reduce real costs from fail-stop errors. To aid debugging, a failure-avoidance mechanism such as Peacenik can log conflicts avoided in production and report them to developers.

3 Peacenik Design Overview

This section overviews the design of Peacenik, a set of architecture mechanisms for avoiding consistency exceptions. Section 4 describes Peacenik at an architectural level and studies two prototype implementations of Peacenik by extending existing fail-stop systems.

Pausing at region conflicts. Existing fail-stop systems generate a consistency exception when they detect or infer a region conflict between executing cores, which occurs when one core’s memory access conflicts with a memory access made in another core’s concurrent region [9, 10, 41, 44, 60]. Figure 1(a) shows an example of a region conflict. In the example, the system eagerly detects a write–read conflict at Core 2’s read of x with Core 1’s write to x. A system that ensures region serializability must not allow Core 2 to continue execution, at least until Core 1’s region completes; if Core 2 were to read y immediately after reading x (and see 0), the execution would become unserializable.

Peacenik avoids the region conflict by pausing Core 2’s execution until Core 1’s ongoing region completes, when Core 2’s access can then proceed without any conflict. Peacenik pauses Core 2 at the conflicting access until Core 1 finishes its ongoing region, serializing Core 2’s region after Core 1’s.

Pausing is not a panacea for avoiding consistency exceptions, for two reasons. First, Peacenik cannot usefully pause a core at a conflict detected lazily because it is too late for pausing to ensure region serializability (Section 2.1). In Figure 1(b), the system detects a conflict on x lazily at the end of Core 2’s region: the core has read an out-of-date value for x, and it is too late to pause to avoid violating serializability.

Second, pause can lead to a pausing deadlock when multiple cores are involved in a cycle of wait-for dependencies. Figure 1(c) shows that two eagerly detected read–write conflicts lead to a pausing deadlock when both cores try to avoid the conflicts by pausing. Peacenik detects a pausing deadlock by detecting a cycle of wait-for dependencies, and selects one core involved in the deadlock to generate a consistency exception (or to restart its region if eligible, as discussed next).

Restarting regions. Peacenik further avoids consistency exceptions by restarting eligible regions that would otherwise generate a consistency exception (due to a lazily detected conflict or a pausing deadlock). By restarting a region R, Peacenik tries to serialize R after any other core’s region with which R conflicted. Region restart is best effort; a region is eligible to restart if no data written by the region has become conflicted. Region restarting is best effort; a region is eligible to restart if no data written by the region has become conflicted.
visible to reads by other cores (e.g., through a cache eviction or remote coherence request).

Figures 1(b) and 1(c) show how restarting a region avoids a consistency exception due to a lazily detected conflict and a pausing deadlock, respectively. In both examples, Peacenik avoids the consistency exception by restarting Core 2’s ongoing region (the dashed box) and invalidating privately cached data, serializing it after Core 1’s completed region. Both examples assume that the regions are eligible for restart.

Regions can repeatedly restart (e.g., by repeatedly conflicting with each other), leading to livelock. As a simple extension to the above design, Peacenik could avoid livelock by using exponential backoff and by restarting only the youngest eligible region.

**Enhancing best-effort region restart.** To improve the odds that a region will be eligible to restart, Peacenik modifies the replacement policy of cores’ private caches. The modified policy avoids evicting lines written by the current region and instead favors evicting other lines in the same associativity set.

**Fallback.** In the case of a pausing deadlock or lazy conflict in which no region is eligible to restart, Peacenik falls back to a consistency exception.

### 4 Peacenik Architecture Design

This section introduces a Peacenik architecture design that generally applies to any baseline architecture that provides fail-stop consistency. We describe how to apply the Peacenik architecture design to two existing fail-stop architectures, ARC and CE [10, 41]. The resulting designs are called ARC+Peacenik and CE+Peacenik. This section assumes cores with two-level private caches, i.e., L1 and L2. We describe quantitatively how Peacenik adds minimal complexity on top of an underlying system that provides fail-stop consistency.

#### 4.1 Background: ARC and CE Details

Both ARC and CE are architecture designs that provide SFRSx (Section 2.1) by detecting conflicts between concurrently executing regions [10, 41]. ARC detects conflicts both eagerly and lazily, while CE detects all conflicts eagerly.

**ARC.** In ARC, cores execute synchronization-free regions (SFRs) mostly independently. At a high level, when a region completes, ARC uses a region commit protocol to ensure that the region’s memory accesses did not conflict with accesses in a region executed by another concurrently executing core, and that the region read consistent memory state. The protocol consists of three steps: (1) pre-commit, which writes back access metadata about privately cached dirty lines to the LLC, detecting eager conflicts in the process; (2) read validation, which compares privately cached read-from lines with the LLC’s versions, detecting lazy conflicts for inconsistent lines and eager write–read conflicts; and (3) post-commit, which writes back privately cached dirty lines to the LLC and clears access metadata for the core. When a core evicts a private cache line read and/or written by its ongoing region, ARC immediately performs read validation and/or pre-commit for the evicted line only.

For all detected conflicts, ARC delivers a consistency exception to the involved core, which handles the exception as a termination signal. Before performing an externally visible operation such as a system call, ARC (and other fail-stop systems that detect conflicts lazily) must provide timely exceptions. In particular, ARC preemptively performs read validation to check for conflicts before an externally visible operation.

Architecturally, ARC has three main components, illustrated by Figure 2 (excluding the shaded components, which Peacenik adds): (1) per-line metadata in each core’s private L1 and L2 caches, (2) an access information memory (AIM), and (3) distributed consistency controllers (CCs). The metadata added to private cache lines consists of two bits per byte that record whether the core has read and written each byte in the line. The AIM is a banked cache (banking not shown in Figure 2) of each core’s access metadata for each line resident in the LLC. A core’s core-side and AIM-side CCs manage the movement of data and metadata between the core, LLC, and AIM.

**CE.** CE introduces per-byte local and remote access bits to each privately cached line to keep track of bytes accessed by the ongoing region of the local core and remote cores, respectively. It piggybacks on MESI coherence messages to communicate access information indicated by the access bits between cores, and checks for region conflicts before performing any access by comparing the local access and remote access bits. For any conflict detected, CE generates
To implement support for pausing in ARC and CE, it is straightforward to add a centralized pausing controller to them, as shown in Figure 2 for ARC. The pausing controller could instead be distributed; however, it is an unlikely bottleneck since it is signaled rarely: when a conflict is detected or a wait-for core ends a region. Arbitration at the pausing controller is simple because of the rarity of these events. At small core counts, a bus connecting all cores to the pausing controller may be sufficient. At larger core counts, an ordered buffer at the pausing controller that NACKs signals on overflow is sufficient. After such a NACK, a core could try again, or eventually give up on pausing and terminate with an exception.

**Pausing in ARC+Peacenik.** When a core’s AIM-side CC detects a conflict eagerly, it signals the pausing controller to set the paused core’s pause bit. When the wait-for core completes post-commit for its ongoing region, it signals the pausing controller, which clears the paused core’s pause bit, allowing the core to resume.

In ARC, there are two situations in which a core may detect a conflict eagerly and consequently pause: during region commit and on an eviction from a core’s L2 cache. During region commit, a core’s CC may detect an eager conflict when performing pre-commit or read validation, in which case the core’s CC pauses the core; it restarts the commit protocol when the core resumes. Read validation may detect a lazy conflict, which is unavoidable by pausing, triggering a region restart if eligible. Likewise, a core’s CC may detect a conflict when performing pre-commit or read validation on a single line evicted from the private L2; it handles the conflict similarly to the commit protocol’s handling, except there is no need to restart the protocol.

**Pausing in CE+Peacenik.** When a core’s private cache detects a conflict before accessing a cache line, it signals the pausing controller to pause the core. The pausing controller then checks the line’s local bits in each of the other cores’ private caches (or the global table if the line was evicted by a core) and identifies a core as the wait-for core if the core has conflicting local bits set with the pause core. When the wait-for core ends its ongoing region, clearing its local access bits and receiving all acknowledgments from other cores (a paused core still acknowledges another core’s end-of-region message), the wait-for core signals the pausing controller to clear the paused core’s pause bit, allowing the core to resume.

**4.3 Architecture Support for Region Restart**

When the baseline fail-stop architecture detects a conflict lazily or when two or more cores enter into a pausing deadlock, Peacenik tries to avoid a consistency exception by restarting the execution of a relevant core’s ongoing region that is eligible to restart. A core’s region is eligible to restart if, during the region’s execution, the core has not written

---

3 Each core could have a bit indicating whether it is a wait-for core. To avoid a race between setting the wait-for bit and the relevant region ending, the design could identify regions uniquely (e.g., with per-core counters). Alternatively, instead of using per-core wait-for bits, the pausing controller could periodically wake up each paused core, which would recheck the conflict and the wait-for relationship.
back any line updated by the region from its private cache(s) to the LLC or any private cache of another core. A core becomes ineligible to restart when it writes back such a line, making it visible to other cores in the system.

Peacenik introduces a per-core restart-forbidden bit that indicates whether a core’s region is eligible to restart (Figure 2). Whenever a core writes back a private line that was updated by the current region to the LLC or any private cache of another core, the core sets its restart-forbidden bit. I/O operations, other system calls, and interrupts, which make a region irrevocable because their effects may be visible to the external world, also trigger setting the restart-forbidden bit.

When a core begins a region, it clears its restart-forbidden bit and saves a shadow copy of its current execution context, which is the same architecture state that the core normally saves on a context switch (i.e., register state, but not cache or memory contents). The core uses this shadow copy to initiate the re-execution of a region by restoring its execution context.

To handle a lazily detected conflict, Peacenik restarts a region involved in the conflict if it is eligible for restart (i.e., its restart-forbidden bit is cleared). To handle a pausing deadlock, the pausing controller selects an arbitrary core that has its restart-forbidden bit cleared, and signals the core to restart its region.

A core takes several steps to restart an eligible, ongoing region. To preserve atomicity, Peacenik needs to revert the updates performed by the restarting region. The core rolls back the region’s writes by invalidating the private cache lines updated by the region, relying on a lower-level cache (or memory) to contain values corresponding to the region’s start. Next the core restores its execution context (i.e., register file) from the shadow copy saved at region start, and starts executing again from the first instruction of the restarting region. The baseline fail-stop system may need to perform additional system-specific actions to handle the region restart, such as clearing access metadata used for conflict detection. Finally, the core prompts the pausing controller to reset the pause bits for any cores that are waiting for the restarting core.

Peacenik relies on the baseline fail-stop system having a mechanism for differentiating lines written by the restarting region from other dirty lines (i.e., lines written by the core’s previous regions). Furthermore, the system must ensure that a dirty line is backed up in the cache hierarchy before being written by a new region; otherwise values that correspond to the region’s start will be lost, thwarting region restart.

Peacenik cannot tolerate a lazy conflict or pausing deadlock if no involved core is eligible to restart. In such a case, Peacenik generates a consistency exception that terminates the program’s execution. A feature of Peacenik is that it does not modify the baseline fail-stop architecture’s consistency exception delivery mechanism. We assume the underlying architecture raises a dedicated per-core signal via a non-maskable interrupt to the executing core that, by default, is handled by operating system code that terminates program execution.

Region restart in ARC+Peacenik. In ARC+Peacenik, when a region restarts, the core clears its access information in the AIM, and clears access information for each read or written line in its private caches and then invalidates those lines. The core invalidates lines not only written by the restarting region, but also lines read by the region, in order to fetch up-to-date copies of them during re-execution of the region.

ARC already differentiates lines written by the restarting region from previously written lines. And it can generally invalidate a region’s written lines without losing writes by previous regions—except in the presence of ARC’s deferred write-back optimization, which defers writing back a region’s written-to lines until another core accesses them [10]. Briefly, ARC+Peacenik ensures that such lines from a previous region are not overwritten by writes in the current region, by backing up the lines’ values in the L2 when the lines are deferred during post-commit. ARC+Peacenik introduces a per-line deferred-write bit in the L2 to indicate such lines (Figure 2). If the L1 evicts a line for which the same line in the L2 has its deferred-write bit set, the L2 writes back its dirty values to the LLC and clears the deferred-write bit.

Region restart in CE+Peacenik. In CE+Peacenik, when a region restarts, it clears local access bits, sending end-of-region messages to other cores, and waiting for acknowledgments. To support region restart, CE+Peacenik must differentiate lines written by the current region from previously written lines, and preserve values of data from region start time. Briefly, CE+Peacenik extends CE so that when a dirty line is written to for the first time by a region (i.e., no access bits have been set), the line is first written back to the next lowest level of the cache/memory hierarchy. Then invalidating a region’s written-to lines restores the region start state.

4.4 Reducing Dirty Evictions to Shared Cache

To avoid dirty evictions to a shared cache, which render a core’s region ineligible for restart, Peacenik modifies the last-level private cache (e.g., the L2 in Figure 2) replacement policy to prefer clean lines over dirty ones as eviction candidates. Peacenik adds this constraint to a baseline pseudo-LRU replacement policy, modeled after the one used in the Intel Core i7 memory hierarchy [30]. Baseline pseudo-LRU uses one most recently used (MRU) bit per line that the core sets each time it accesses the line, indicating that the line was recently accessed. When the MRU bits of all lines in a cache set become set, pseudo-LRU clears all of the set’s MRU bits, except for the most recently set bit. Pseudo-LRU implements eviction by selecting an arbitrary line that has its MRU bit cleared.
To reduce the frequency of evictions of dirty lines, Peacenik modifies the replacement policy’s behavior when clearing MRU bits: instead of clearing all MRU bits (except for the most recently set one), Peacenik sets each line’s MRU bit equal to the value of the line’s dirty bit. To select a line for eviction, Peacenik’s modified pseudo-LRU evicts a line with its MRU bit cleared, which will be a clean line if any line is clean. If all of a set’s MRU bits are set, then all of the lines in the set are dirty. If all of the lines in the set are dirty, Peacenik’s replacement policy behaves like a normal pseudo-LRU policy, and chooses an arbitrary line to evict. The core sets its restart-forbidden bit if it evicts a dirty line in this case.

Due to inclusion, when a core evicts a line from L2, the corresponding line in L1 must be recalled and evicted. To avoid evicting a line that is clean in L2 but dirty in L1—which would make the region ineligible to restart—a core sets the dirty bit for a line in both L1 and L2 when the L1 line first becomes dirty in a region, making Peacenik’s modified pseudo-LRU less likely to evict it.

Prior research on high-performance cache replacement policies shows that the effects of replacement decisions are significant only for the shared LLC, and modifying the replacement policy of the L2 cache is unlikely to have a significant impact on performance [33, 68].

ARC+Peacenik and CE+Peacenik use the modified L2 eviction policy exactly as described above.

4.5 Hardware Complexity

The hardware components added by Peacenik on top of the underlying systems that provide fail-stop consistency have low complexity and do not contribute significantly to area or static power. Per-core pause and restart-forbidden bits contribute negligibly to complexity. Peacenik adds a per-line deferred-write bit to the L2 cache, which amounts to only 0.1% of the L2 cache. The wait list in the pausing controller contains one entry per core, and each entry identifies a wait-for core. With c cores, the overhead of the wait list is $c \times \log_2(c)$ bits, which is just 20 bytes of storage for 32 cores. The logic to check for pausing is not on the critical path of cache data or tag accesses and will not impact cycle time. This checking logic relies on simple table lookups and single-bit comparators (for checking pause and restart-forbidden bits) and does not contribute significantly to complexity. Peacenik’s additions on top of existing support for fail-stop consistency increase complexity only negligibly and are not likely to significantly impact power, area, or performance.

4.6 Thread Migration and Context Switches

The discussion so far has assumed that each core executes a single, pinned thread. Here, we discuss how Peacenik supports thread switching and migration.

Peacenik assumes that the underlying fail-stop system (e.g., ARC or CE) already supports migrating and switching threads. Peacenik additionally must virtualize per-thread pausing and restart state. Each thread must include a pause bit and a wait-for entry in its execution context that is saved with the rest of the context through switches and migration, and used to set a core’s pause bit and waiting-for status when the thread is scheduled or migrated to the core. A paused core can switch threads; it is likely advantageous to switch to a non-paused thread.

Although each thread could add a restart-forbidden bit to its execution context, it seems difficult to support restart for a migrated or switched thread. A straightforward option is to simply set a core’s restart-forbidden bit whenever it switches to a different thread.

It is straightforward to extend Peacenik to support simultaneous multithreading (SMT), by adding pause and restart-forbidden bits and a wait-for entry in the wait list for each logical core, and applying Peacenik’s mechanisms to logical cores.

Pausing interacts with I/O and interrupts similarly to how pausing responds to thread context switches. We argue that a system that provides fail-stop semantics should avoid detecting conflicts when executing privileged code such as system calls.

5 Evaluation

This section evaluates Peacenik’s ability to avoid consistency exceptions and the resulting impact on performance.

5.1 Evaluation Methodology

We implemented the two Peacenik prototypes, ARC+Peacenik and CE+Peacenik, by extending simulators for ARC and CE [10, 41] that we implemented for the ARC paper [10].

We have made our ARC+Peacenik and CE+Peacenik implementations publicly available. The simulators consume a trace of instructions generated by a Pin-based front end [42] and model a simple, in-order core architecture with 8–32 cores. Table 2 shows the main parameters used for the modeling. We report execution time as the maximum cycles of any core. The ARC and ARC+Peacenik simulators model a non-inclusive LLC, while the CE and CE+Peacenik simulators model an inclusive LLC to support an inclusive directory cache embedded in the LLC [62].

Workloads. Our experiments run the PARSEC 3.0 benchmarks [7] with simsmall inputs, except we use simmedium workload because its simsmall workload does not support >16 threads. We exclude facesim and raytrace, which fail to finish executing with the simulators, and freqmine.
which uses OpenMP instead of pthreads. The simulators only compute cycles for each PARSEC program’s “region of interest” (ROI), which includes the whole parallel phase of each program.

The experiments also execute two real server programs: Apache HTTP Server 2.4.23 (httpd) and MySQL Server 5.7.16 (mysqld) [1, 2]. We configure both programs to create a single child process with \(n\) worker threads, where \(n\) is the number of cores in the simulated architecture. We launch \(n\) client processes that repeatedly and concurrently perform simple requests using a methodology documented by prior work [70].\(^3\) In our experiments, client processes executing natively send 128K HTTP requests (httpd) or 256 SQL queries (mysqld) to the server, distributed evenly over the client processes.

We compiled the PARSEC benchmarks without optimizations (i.e., gcc -O0) and mysqld with -O1, for two reasons. First, our Pintool front end identifies synchronization operations according to specific pthreads function names. At higher optimization levels, these names can be optimized away, leading to missing synchronization boundaries and thus false conflicts. Second, with higher optimization levels our Pintool is unable to consistently get the source locations involved in conflicts, which we need to report, analyze, and understand the conflicts reported in Section 5.5. We performed a separate evaluation and found no significant difference between the unoptimized and optimized experiments in terms of the relative performance differences between configurations. We compiled httpd at its default optimization level (-O2) because the default optimizations did not lead to missing synchronization functions or inconsistent source locations in our experiments.

**Handling synchronization.** All simulators identify calls to pthreads functions (and mysqld’s PolicyMutex.enter() and PolicyMutex.exit()) as lock operations. At a lock operation, ARC and ARC+Peacenik execute a distributed queue-based locking protocol [10, 63] and end the current synchronization-free region (SFR) by performing the region commit protocol, while CE and CE+Peacenik end the current SFR by performing end-of-region actions.

ARC treats non-pthreads atomic instructions (e.g., inlined assembly or C++ atomic accesses [14]) as synchronization but not region boundaries. To implement that behavior, the ARC and ARC+Peacenik simulators treat non-pthreads atomic instructions (i.e., instructions with the x86 LOCK prefix and fence instructions; the evaluated programs do not use C++ atomic variables; atomic instructions in the experiments originate from inlined assembly in the source code) as lock operations but not region boundaries. CE and CE+Peacenik treat non-pthreads atomic instructions as regular memory accesses but do not detect conflicts on the instructions. As a result, the simulators do not detect conflicts on atomic instructions, but they may detect false conflicts on accesses to other variables happens-before-ordered by the atomic instructions. The simulators detected such false conflicts in several low-level library functions: malloc, start_thread, dlinfo, and seekoff. We modified the simulators to ignore these conflicts. A deployed system using ARC and CE should identify such atomic-instruction-ordered accesses in library functions as atomic.

**Modeling of pausing, region restarts, consistency exceptions, and reboots.** The simulated cost of Peacenik pausing a core \(C\) is the cycles executed by the wait-for core \(C_w\) while \(C\) is paused, transitively including any cycles that core \(C_w\) spent in a paused state while waiting for other cores. To achieve realistic thread interleavings with pausing, the simulator backend “pauses” the application thread by signaling back to the Pintool front end, which stops executing the thread until signaled to continue by the simulator backend.

The simulators model the cost of region restart by re-executing the region’s instructions in the simulator, but not in the actual application. To support re-execution, the simulator buffers each core’s region’s instructions until commit. Our evaluation faithfully counts the performance cost no matter how many times a region restarts.

For PARSEC, we assume that ARC, CE, and Peacenik handle a consistency exception by rebooting the application, i.e., restarting it from the beginning. The simulators model the cost of rebooting by adding the total cycles incurred so far (not including prior reboots) to the overall computed

---

\(^3\)We reuse methodology from https://github.com/jiexi/concurrency-bugs, but use more recent versions of httpd and mysqld, which still have data races that manifest as region conflicts.
Table 3. Behaviors of each simulated configuration, characterized by actions taken on eagerly and lazily detected conflicts and on pausing deadlocks, and whether using the modified pseudo-LRU replacement policy in the L2 cache. *CE and CE+Peacenik do not detect any conflicts lazily. † If a region is ineligible to restart, Peacenik generates a consistency exception.

<table>
<thead>
<tr>
<th>Config</th>
<th>eager conflict</th>
<th>lazy conflict†</th>
<th>pausing deadlock</th>
<th>L2 replacement policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARC or CE</td>
<td>Consistency exception</td>
<td>Consistency exception</td>
<td>N/A</td>
<td>Default pseudo-LRU</td>
</tr>
<tr>
<td>PNP</td>
<td>Pause core</td>
<td>Restart region†</td>
<td>Restart region†</td>
<td>Default pseudo-LRU</td>
</tr>
<tr>
<td>PNpr</td>
<td>Pause core</td>
<td>Restart region†</td>
<td>Restart region†</td>
<td>Default pseudo-LRU</td>
</tr>
<tr>
<td>PN</td>
<td>Pause core</td>
<td>Restart region†</td>
<td>Restart region†</td>
<td>Modified pseudo-LRU</td>
</tr>
</tbody>
</table>

5.2 Peacenik’s Run-Time Impact

This section evaluates Peacenik’s ability to avoid consistency exceptions and thus reduce execution costs compared with ARC and CE. To break down the benefit of Peacenik’s mechanisms, we use the following configurations, which extend the baseline system (ARC or CE):

- **PNP** is a partial Peacenik configuration that pauses at eager conflicts, but does not restart regions.
- **PNpr** extends PNP to restart eligible regions that encounter a lazy conflict (if applicable) or pausing deadlock.
- **PN** is the full, default Peacenik configuration. It extends PNpr by modifying pseudo-LRU to avoid dirty L2 evictions.

The PN configuration faithfully performs Peacenik’s modified pseudo-LRU algorithm and thus incurs any performance effects resulting from potentially suboptimal eviction decisions. Other Peacenik and non-Peacenik configurations faithfully perform unmodified pseudo-LRU.

Table 3 summarizes the behavior of each configuration.

Table 4 and Figure 3 present the main results of the evaluation. They show results for the four programs for which ARC and CE detect conflicts for 32 cores: canneal, streamcluster, httplib, and mysqld. For each program, all ARC and ARC+Peacenik configurations process the same execution trace generated by the Pintool front end; similarly, CE and CE+Peacenik configurations process the same trace. We run ARC and CE experiments separately because ARC and CE use different conflict detection mechanisms, and hence their pausing behavior differs and leads to different traces.

In Table 4, the *Ordinary regions (cycles)* column is each program’s total executed SFRs and executed cycles, excluding extra regions and cycles executed due to pausing and restarting. The *Regions w/* columns count regions with at least one eagerly detected conflict (EC), lazily detected conflict (LC), and pausing deadlock (PDL), respectively. Peacenik’s pausing inherently avoids eagerly detected conflicts, so EC actually represents conflicts avoided by pausing for all Peacenik configurations. The *Region restarts* column counts eligible regions restarted by Peacenik. The *Retried requests (avg. cycles)* column counts retried requests and reports average cycle cost of each retried request (applicable to server programs only). *App reboots (avg. cycles)* counts application reboots and shows average cycle cost of each reboot.

Figure 3 shows run time for the same configurations and programs as Table 4. The graphs break down run time into multiple components. All configurations incur costs due to *ordinary execution* and *handling exceptions*. Each program’s bars are normalized to the *ordinary execution* cost of the baseline (ARC or CE alone). Peacenik includes costs for *pausing and restarting regions*, although costs are small in the experiments and not visible in most cases.

**PARSEC programs.** The simulators report hundreds of conflicts in canneal and streamcluster. ARC and CE generate consistency exceptions at these conflicts and incur high slowdowns (76–240 × for canneal and 240–670 × for streamcluster) from substantial re-execution of the program from the start. For example, as Table 4 shows, ARC’s consistency exceptions in canneal incur 20 million cycles per reboot in an execution of only 47 million cycles. ARC and CE detect different numbers of conflicts (and in general, CE detects more conflicts than ARC) because (1) CE detects all conflicts eagerly and (2) ARC and CE detect conflicts at different points (which explains why ARC detects a different number of conflicts than CE for canneal, despite detecting no lazy conflicts).

In contrast, Peacenik avoids much or even all of the cost of consistency exceptions. For canneal, ARC+Peacenik pauses at all 189 eagerly detected conflicts (more than the 173 conflicts reported by ARC because pausing leads to different timing and thus different region conflicts), instead introducing...
Table 4. Run-time characteristics of programs for which ARC and CE detect conflicts, on 32 cores. A blank entry (–) indicates an inapplicable case for the configuration or program. The table reports cycles in thousands (K) or millions (M), rounded to two significant figures. EC: eager conflicts, LC: lazy conflicts, PDL: pausing deadlocks.
ellegant to restart, which substantially improves run time. By modifying pseudo-LRU, PN enables one region to restart that would otherwise be ineligible to restart, avoiding consistency exceptions entirely. CE+Peacenik detects all conflicts eagerly and thus pausing avoids all consistency exceptions, without incurring any pausing deadlocks.

**Server programs.** For httpd, ARC generates 6 consistency exceptions: 2 occur when processing a request, allowing retrying the request; the other 4 occur outside of request processing, requiring a server reboot. Reboots incur a relatively low cost: rebooting takes only 5% of httpd’s ordinary cycles. PNp detects 9 conflicts, again a few more than ARC due to pausing’s impact on region timing. PNp does not reduce consistency exceptions for httpd because PNp has extra conflicts and pausing causes 2 pausing deadlocks. For the PNpr and PN configurations, all regions with lazily detected conflicts or pausing deadlocks are eligible for restart, and ARC+Peacenik avoids all consistency exceptions. CE detects 8 eager conflicts; pausing avoids all conflicts without any pausing deadlocks.

For mysqld, ARC generates consistency exceptions due to 13 regions with conflicts, 9 of which occur in requests. Booting mysqld is costly (790M cycles), and ARC incurs a 3–4× slowdown to reboot 4 times. Pausing alone (i.e., PNp) avoids 2 consistency exceptions from eagerly detected conflicts, but pausing-related timing differences lead to extra lazy conflicts, resulting in modest net reductions in run time. Peacenik configurations that support restarting regions (PNpr and PN) detect no conflicts eagerly, as a result of execution differences caused by restarting regions and modifying ARC’s deferred write-back optimization (Section 4.3). The support for restarting regions helps avoid all consistency exceptions by restarting eligible regions with lazily detected conflicts, whether using modified pseudo-LRU or not. CE generates 19 consistency exceptions, all of which occur outside of request processing and lead to server reboots. Pausing leads to no pausing deadlocks and thus avoids all consistency exceptions with minimal cost.

In summary, the results in this section show that when applied to a system that provides fail-stop semantics by detecting conflicts both eagerly and lazily, all of Peacenik’s components—pausing, region restart, and modified pseudo-LRU—are collectively important for avoiding consistency exceptions, together eliminating nearly all of the performance impact of fail-stop semantics for data races. Region restart and modified pseudo-LRU are particularly important for a system like ARC that detects conflicts lazily, while an eager-conflicts-only system like CE gets by with pausing alone. The results thus show the effectiveness and generality of Peacenik applied to systems that provide fail-stop behavior for data races.

### 5.3 Scalability

Figure 4 evaluates Peacenik on 8-, 16-, and 32-core systems. The results include a *weak memory model* (WMM) configuration, which models a typical multiprocessor architecture that ignores data race errors, to compare with the current state of practice. We implemented the WMM configuration by disabling CE’s components in the CE simulator. WMM does not detect conflicts or generate consistency exceptions. As in Section 5.2, the ARC (Figure 4(a)) and CE (Figure 4(b)) results are each from a separate set of runs.

We note that for vips with 8 and 16 cores, CE detects conflicts that are not detected with 32 cores because of different timing and data contention patterns. Conversely, with 8 cores CE misses all conflicts detected in mysqld with 16 and 32 cores.

Overall, the data show that across core counts, Peacenik not only avoids nearly all consistency exceptions in our experiments, eliminating performance degradation, but it negligibly impacts conflict-free programs relative to the underlying fail-stop system (ARC or CE).

### 5.4 Idealized Checkpointing as a Rebooting Alternative

The evaluation so far has assumed that ARC and CE handle a consistency exception by rebooting the program—a high price to pay. Instead, programs executing under fail-stop memory consistency could periodically record a *process checkpoint*, in order to return the execution’s state to the most recent checkpoint if a core encounters a failure.

Here we evaluate a highly *idealized* checkpointing implementation that incurs *no cost* for taking checkpoints. The actual cost of creating and maintaining process checkpoints would increase costs, making Peacenik by contrast look even more favorable. We emphasize that checkpointing is distinct from Peacenik’s support for best-effort region restart: checkpointing must record a process’s memory contents, whereas region restart only requires recording a shadow copy of the execution context at region start (Section 4.3).

Figure 5 shows the run time of unmodified ARC and ARC+Peacenik (for simplicity this experiment excludes CE and CE+Peacenik), compared to ARC configurations that perform idealized checkpointing (labeled $ARC$-$cp[k,1,...,1000]$ and $ARC$-$noreboot$) running on 32 cores.

For canneal and streamcluster, the system checkpoints at global synchronization barriers that demarcate the programs’ outer-loop iterations. For each ARC-ckp configuration, the system checkpoints every $k$ iterations (e.g., ARC-ckp10 checkpoints every 10 iterations). At a consistency exception, the simulator adds run time assuming re-execution from the last checkpoint, instead of a full reboot. These ARC-ckp configurations improve run time compared with ARC: 6–27× for canneal and 3–170× for streamcluster. However, even checkpointing at every barrier (i.e., ARC-ckp1) slows both
programs by several times. In contrast, Peacenik eliminates all costs due to re-execution, by avoiding consistency exceptions altogether.

For httpd and mysqld, the ARC-noreboot configuration takes a checkpoint immediately after booting, to avoid the cost of rebooting. By avoiding rebooting through checkpointing, ARC-noreboot avoids virtually all of the cost of ARC’s consistency exceptions, although a realistic checkpointing scheme would incur costs from checkpointing.

Overall, checkpointing reduces the impact of consistency exceptions, but even idealized checkpointing cannot outperform Peacenik in our evaluation. Peacenik and process checkpointing are complementary and could be deployed together.

### 5.5 Analysis of Detected Conflicts

This section analyzes the conflicts detected in the experiments (by ARC only, for simplicity), which we have confirmed as true data races using existing race detection tools. These conflicts are directly representative of data races that exist in mature legacy code, despite being erroneous under the C/C++ memory model [3, 14], and will lead to consistency exceptions when deployed on an SFRSx system.

We extended the ARC simulator to report the source locations of each conflict, including files and line numbers, by tracking the instruction that last accessed each byte in each cache line. Table 5 shows conflicting sites reported by ARC with 32 cores. Table 5 reports more dynamic conflicts than Table 4 because ARC may report multiple conflicting sites for a conflicting region.

We confirmed that the conflicts correspond to true data races using ThreadSanitizer (TSan) [57] and our own Pintool implementation of collision analysis, which pauses threads.
Table 5. Conflicts detected by ARC in the evaluated programs, on 32 cores. \textit{Variable name} shows the source name of each variable involved in a conflict; Point* and PFS\_single\_stat\_* indicate structs with multiple conflicting fields. \textit{Conflicting sites} shows the static source file(s) and line number(s) in one conflict; the table abbreviates pfs\_setup\_actor\_cc as actor\_cc. \textit{Dyn} is dynamic occurrences of conflicts for each variable. The last column shows if the conflict was confirmed by TSan \((TS)\), collision analysis \((CA)\), or prior work \([59]\), or is unconfirmed \((-)\). The text explains \(TS^*\) and \(TS^\dagger\).

6 Conclusion
Peacenik provides best-effort avoidance of failures on top of systems that provide fail-stop memory consistency. A simulation-based evaluation shows that Peacenik eliminates nearly all of the costs of fail-stop consistency while providing strong behavior guarantees for all programs. Peacenik shows how production systems can get the benefits of fail-stop consistency while minimizing the costs of failures.

Acknowledgments
We thank the anonymous reviewers for their insightful feedback. This work is supported by the National Science Foundation under Grants CAREER-1253703, CCF-1421612, and XPS-1629126 and by compute credits awarded by the Google Cloud Platform (GCP) Education Programs Team.
A Artifact Appendix

A.1 Abstract
This artifact provides a VirtualBox image that includes source code and x86-64 binaries of our simulators and evaluated PARSEC 3.0 benchmarks and real server programs.

We also provide scripts to build and run the simulators with the benchmarks and server programs and to generate the performance graphs in the paper.

A.2 Artifact check-list (meta-information)
- **Algorithm:** Simulated Peacenik architecture mechanisms based on the ARC and CE architectures.
- **Program:** The ARC and ARC+Peacenik, CE and CE+ Peacenik, and WMM simulators; a Pin-based front end; a framework to drive experiments; and 10 PARSEC benchmarks and two server programs.
- **Data set:** Test and simsmall workloads for the PARSEC benchmarks and custom workloads for the server programs as described in Section 5.1.
- **Run-time environment:** VirtualBox 5.2.34 or above.
- **Hardware:** Memory \(\geq 16\) GB and cores \(\geq 4\) for test workloads; memory \(\geq 104\) GB and cores \(\geq 16\) to reproduce results in the paper.
- **Output:** Execution cycles graphs and reports of detected region conflicts.
- **How much time is needed to complete experiments (approximately)?** Several weeks if all experiments are run sequentially. Using multiple VMs to run the experiments in parallel is highly recommended.
- **Publicly available?** Yes.
- **Archived?** https://doi.org/10.5281/zenodo.3603351

A.3 Description

A.3.1 How delivered:
VirtualBox image is publicly available on Zenodo: https://doi.org/10.5281/zenodo.3603351.

A.3.2 Hardware dependencies:
In order to reproduce the data for the graphs in the paper, the hardware should be able to host one or more VMs, each with \(\geq 16\) cores and 104 GB memory.

A.3.3 Software dependencies:
VirtualBox 5.2.34 or above on Ubuntu 18.04 or RHEL 7 is recommended.

A.4 Installation
The VirtualBox image can be imported into VMs with either the VirtualBox GUI or from the command line. Make sure your VirtualBox kernel module is correctly loaded using the following command for Ubuntu:

```bash
$ systemctl status virtualbox
```

Port 2200 of the host has been forwarded to port 22 of the VM/guest to enable ssh access. If the host's port 2200 has been assigned to another process (in which case the above command will fail), you may want to change the port forwarding. For example, to change to port 2222 instead, use the following commands.

```bash
(If VM is off) $ VBoxManage modifyvm "asplos20-ae-vm" --natpf1 "guestssh,tcp,,2222,,22"
(If VM is on) $ VBoxManage controlvm "asplos20-ae-vm" natpf1 "guestssh,tcp,,2222,,22"
```

Type the password "asplos20" when prompted.

A.5 Experiment workflow
In the VM, use the scripts to run simulation as follows.

```bash
$ cd /home/asplos20/scripts
$ test.sh output_dir
```

Go to /home/asplos20/exp-products/output_dir for the resulting data tables and graphs.

Use the exp-figX.sh scripts to run simulation to generate data for Figure X in the paper. For example, to reproduce Figure 3(a),

```bash
$ nohup ./exp-fig3a.sh output_dir > fig3a.out
```

A.6 Evaluation and expected result
After running the experiments, expect the following.
1) Graphs similar to those in the paper. All graphs are generated in /home/asplos20/exp-products in the VM.
2) Reports of detected conflicts as reported in Table 5, if ARC configurations are used. Reports are output directly to stdout.

A.7 Experiment customization
Users can change the scripts to customize experiments.

A.8 Notes
See /home/asplos20/scripts/README in the VM for more information about using the scripts, viewing results, and customizing experiments.

Check out source code of our experiment framework and simulators at the following locations in the VM ($HOME=/home/asplos20).

- **Experiment framework:** $HOME/viser-exp
- **Pin-based front end:** $HOME/intel-pintool/source/tools/ViserST
- **ARC and ARC+Peacenik simulators:** $HOME/visersim-backend
- **CE, CE+Peacenik, and WMM simulators:** $HOME/mesisim-backend

A.9 Methodology
Submission, reviewing, and badging methodology:
- [http://cTuning.org/ae/submission-20190109.html](http://cTuning.org/ae/submission-20190109.html)
- [http://cTuning.org/ae/reviewing-20190109.html](http://cTuning.org/ae/reviewing-20190109.html)
- [https://www.acm.org/publications/policies/artifact-review-badging](https://www.acm.org/publications/policies/artifact-review-badging)