

Liveness and Atomicity (Sec 3.3.5)

MMCSLockOp (HLkOp)

mcs_lock_init pass_lock [pass_hlock_spec] wait_lock [wait_hlock_spec] ...

Data Representation and Ghost State (Sec 3.3.4)

MQMCSLockOp (QLkOp)

mcs_lock_init pass_lock [pass_qlock_spec] wait_lock [wait_qlock_spec] ...

Low-level Functional Spec. (Sec 3.3.3)

MMCSLockOp (LkOp)

mcs_lock_init pass_lock [mcs_release_spec] wait_lock [mcs_acquire_spec] ...

Event Interleaving (Sec 3.3.2)

MMCSLockAbsIntro (AbsIntro)

mcs_lock_init

mcs_swap_tail mcs_set_next mcs_get_busy
mcs_cas_tail mcs_get_next mcs_set_busy

Memory Operation (Sec 3.3.1)

MMCSLockIntro (Intro)

bootloader_init mcs_init_node mcs_log

mcs_SWAP_TAIL mcs_SET_NEXT mcs_GET_BUSY
mcs_CAS_TAIL mcs_GET_NEXT mcs_SET_BUSY

Base Layer

MBoot (Boot)

bootloader_init mcs_init_node_log atomic_mcs_log atomic_mcs_CAS mcs_GET_NEXT_log mcs_SET_BUSY_log

Initialization Primitives Logical Primitives Passthrough Primitives

(a) Abstract memory operations into events

(b) Combine getter / setter primitives with logical interleaving primitive (mcs_log)

(c) Prove functional correctness

(d) Add ghost state

(e) Prove liveness and provide atomic specifications