TF-A-Tests Enhancements for Realm World Validation

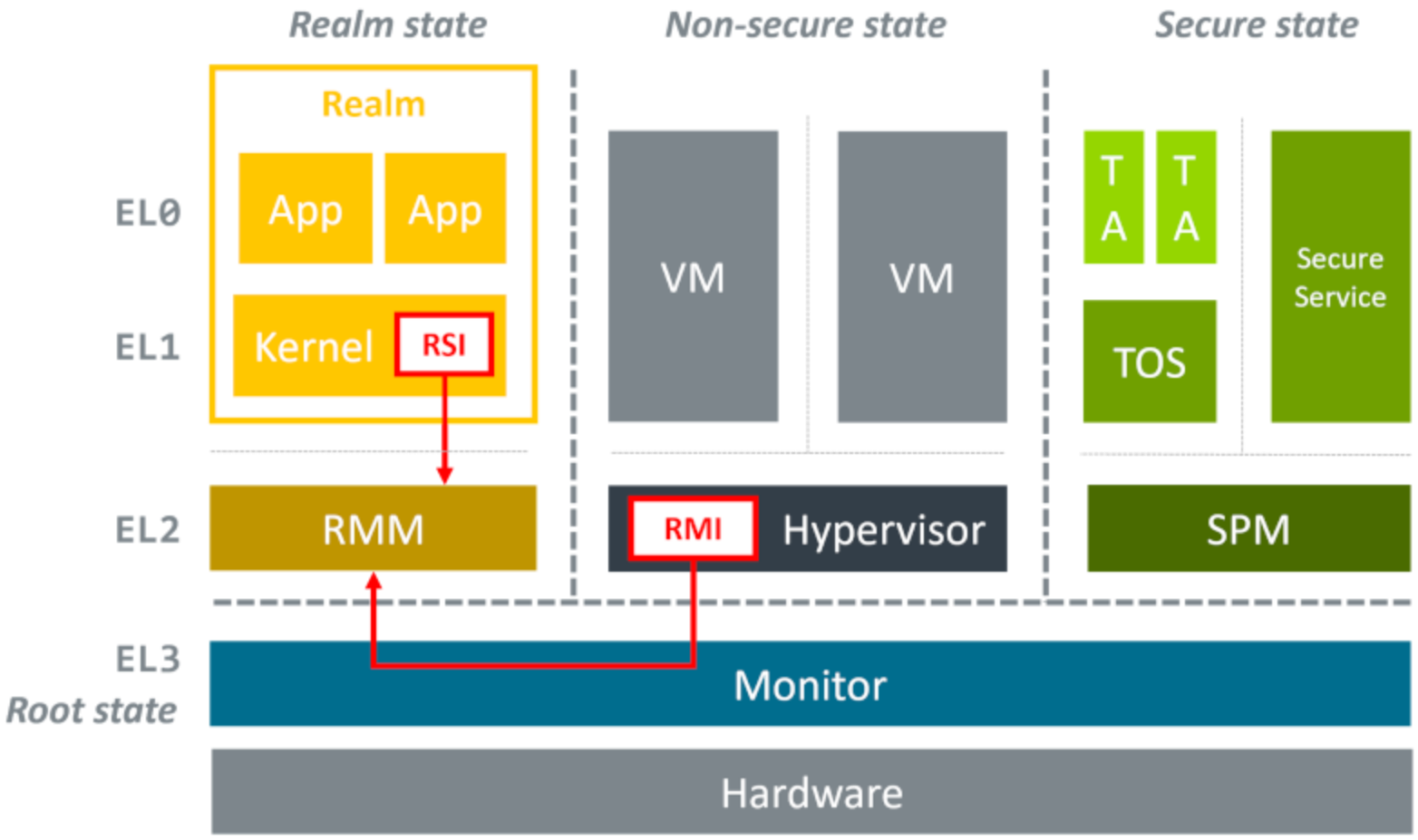
Shruti Gupta

02 May 2024

Agenda

- TF-A-Tests Baremetal tests for CCA SW Stack
- Build Command
- Realm Lifecycle
- PSCI Flow
- Misc Testcases
  - Realm Memory Management
  - Exception Model
  - Arch Feature – SVE/PMU/Timer
  - Security extension Pauth/BTI/DIT

Arm CCA software stack

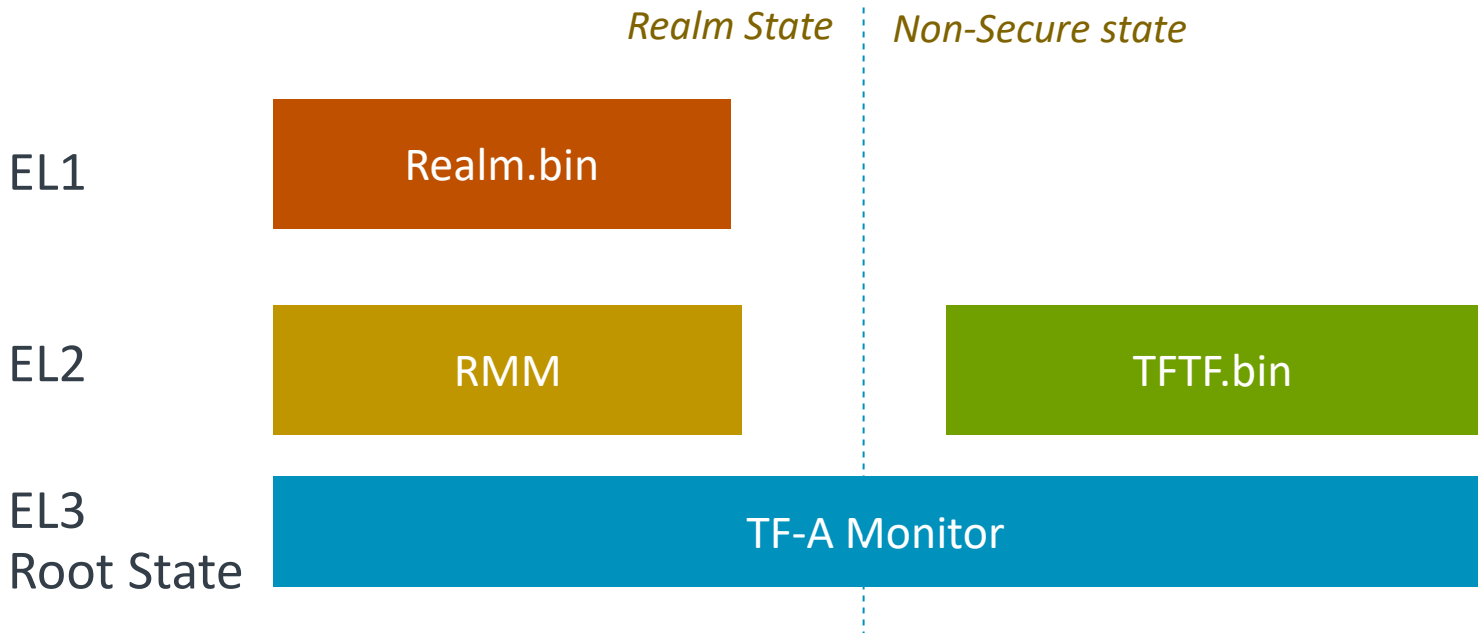


arm

TF-A-Tests for Realm Tests

TFTF Capabilities

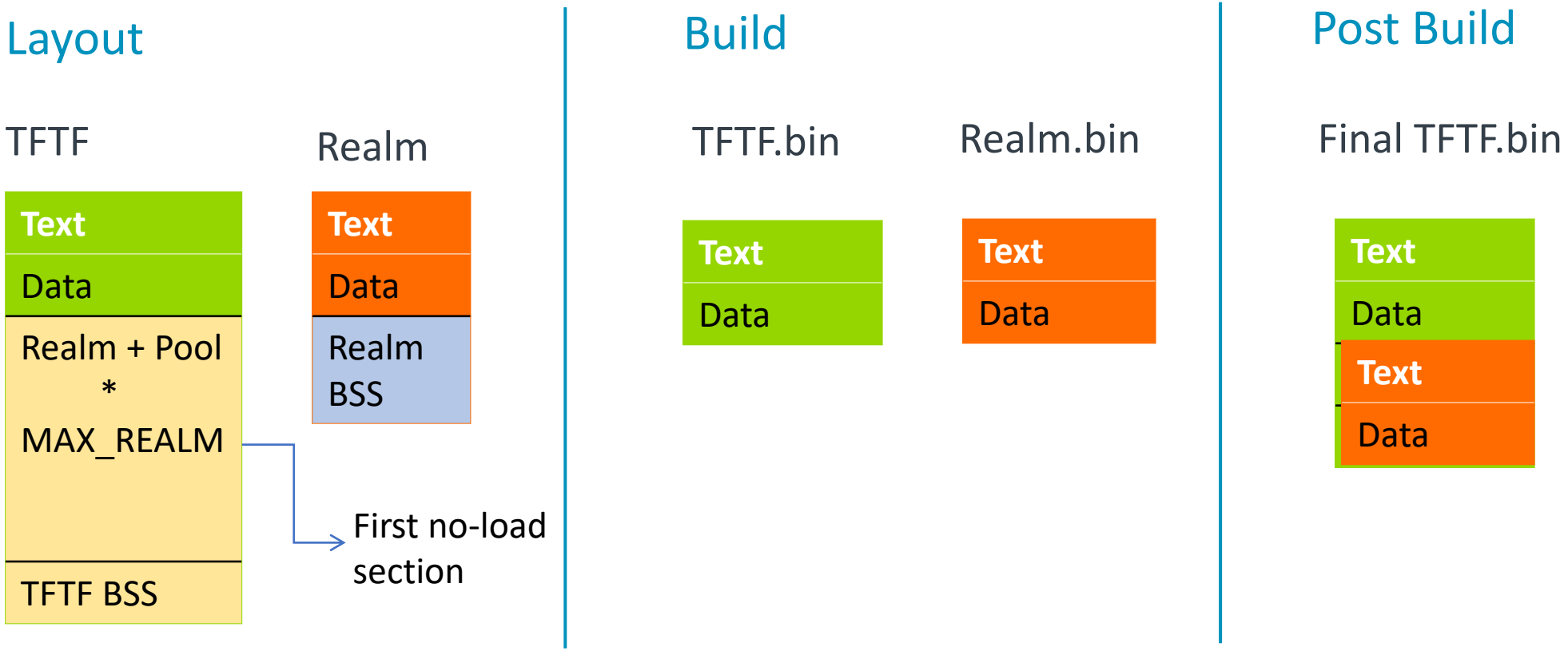
- Supports creation of 2 Realms, up to 8 REC per Realm
- Supports scheduling of multiple Rec on multiple Physical CPU
- Realm Payload is Platform independent



Build Command & Memory Layout

- Three World Execution Instruction
- *Make PLAT=fvp ENABLE_REALM_PAYLOAD_TESTS=1 all*

Generates realm.bin, tftf.bin. Realm.bin is appended at end of tftf.bin



Realm Management Interface

Discovery

- RMI_VERSION
- RMI_FEATURES

Memory delegation

- RMI_GRANULE_DELEGATE
- RMI_GRANULE_UNDELEGATE

Realm lifecycle

- RMI_REALM_CREATE
- RMI_REALM_DESTROY
- RMI_REALM_ACTIVATE

Stage 2 table management

- RMI_RTT_CREATE
- RMI_RTT_DESTROY
- RMI_RTT_FOLD
- RMI_RTT_READ_ENTRY
- RMI_RTT_INIT_RIPAS
- RMI_RTT_SET_RIPAS
- RMI_RTT_MAP_UNPROTECTED
- RMI_RTT_UNMAP_UNPROTECTED

Realm memory management

- RMI_DATA_CREATE
- RMI_DATA_CREATE_UNKNOWN
- RMI_DATA_DESTROY

Realm VCPU lifecycle

- RMI_REC_CREATE
- RMI_REC_DESTROY
- RMI_REC_AUX_COUNT
- RMI_PSCI_COMPLETE

Realm VCPU scheduling

- RMI_REC_ENTER

arm

Realm Services Interface

Discovery

RSI_VERSION

RSI_REALM_CONFIG

Measurement

RSI_MEASUREMENT_EXTEND

RSI_MEASUREMENT_READ

IPA state management

RSI_IPA_STATE_GET

RSI_IPA_STATE_SET

Attestation

RSI_ATTESTATION_TOKEN_INIT

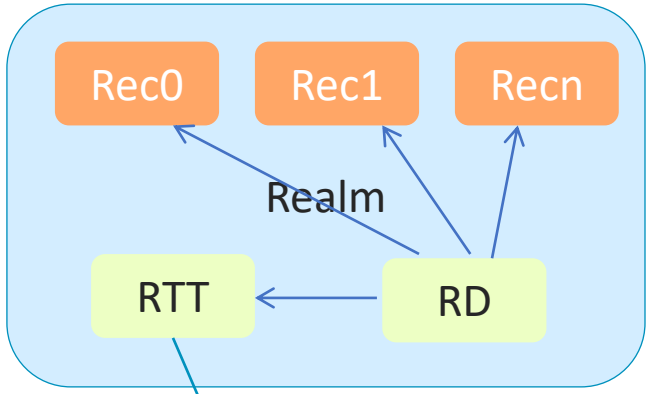
RSI_ATTESTATION_TOKEN_CONTINUE

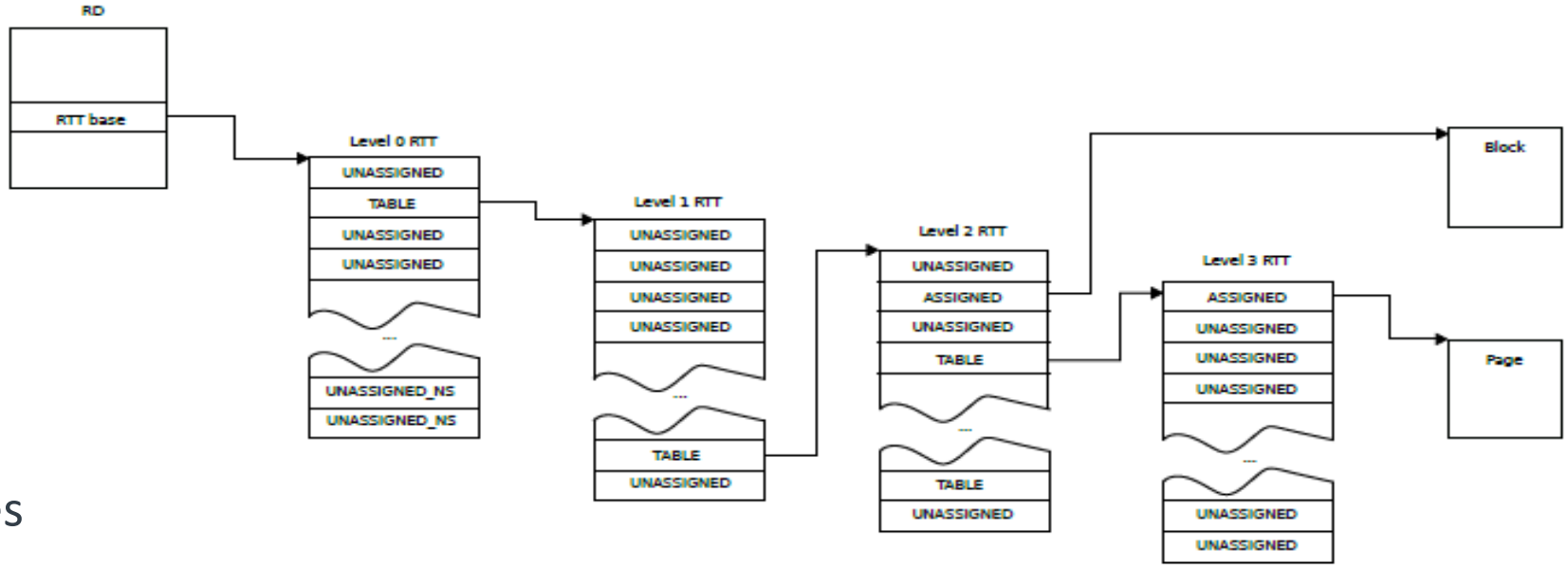
Communication

RSI_HOST_CALL

PSCI

Realm, Rec, RTT

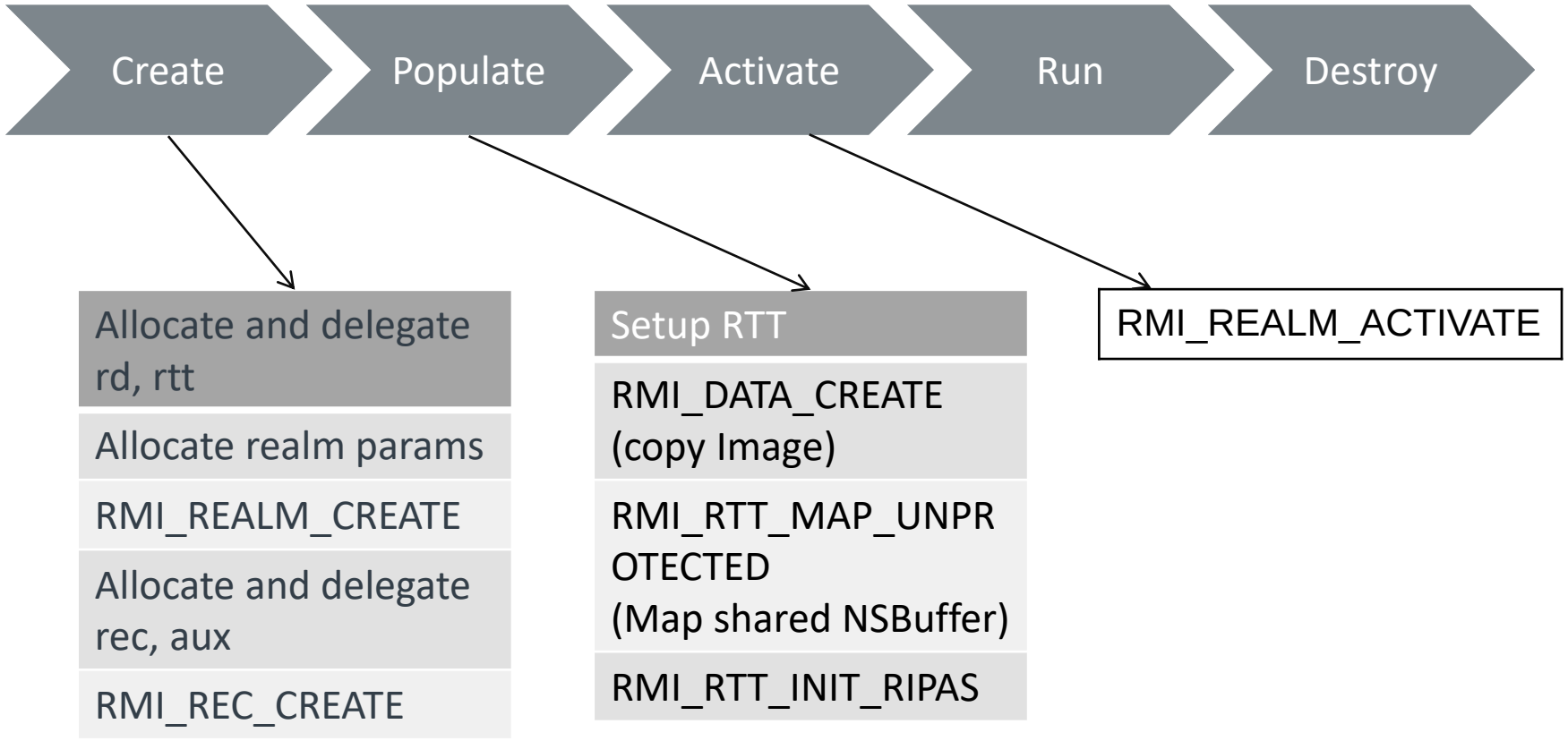




RTT base

Stage 2 tables

Realm Payload lifecycle



host_create_activate_realm_payload()

TFTF Framework

Host APIs

- Helpers
  - host_create_activate_realm_payload
  - host_enter_realm_execute
  - ..
- RMI Calls
  - host_rmi_rtt_readentry
  - host_rmi_rtt_set_ripas
  - …

Realm APIs

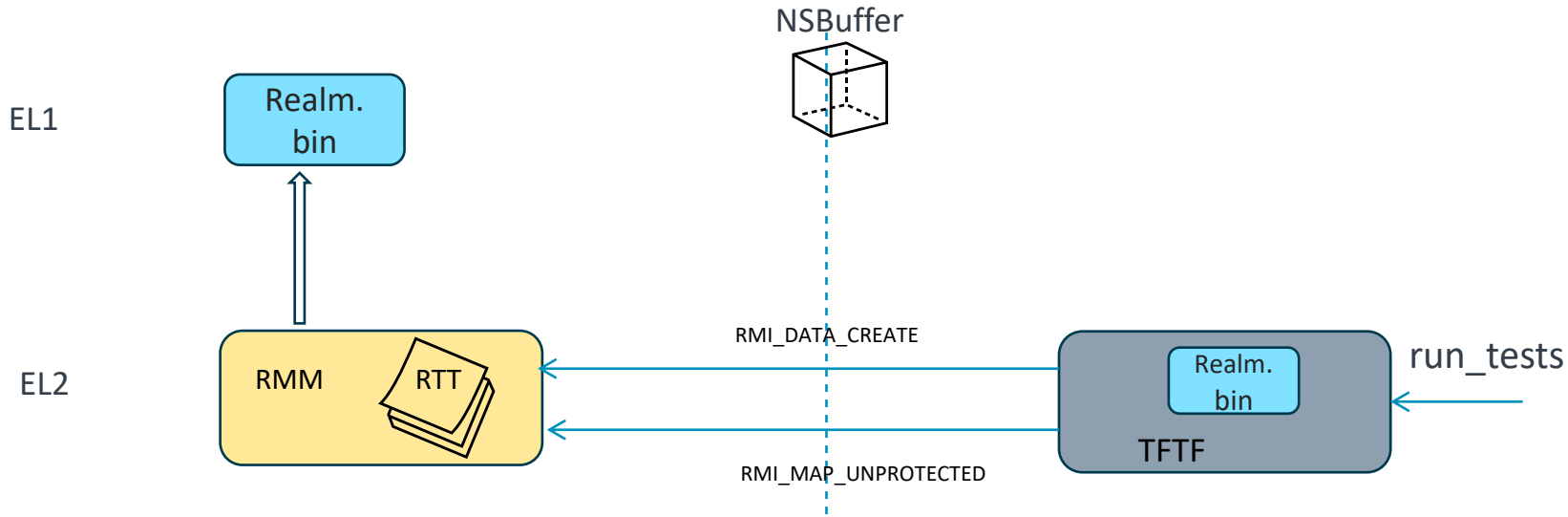
- Helpers
  - realm_cpu_on
  - realm_printf
  - ..
- RSI Calls
  - rsi_ipa_state_get
  - rsi_exit_to_host
  - ..
- PSCI

Common lib pauth_test_lib_fill_regs_and_template, ..

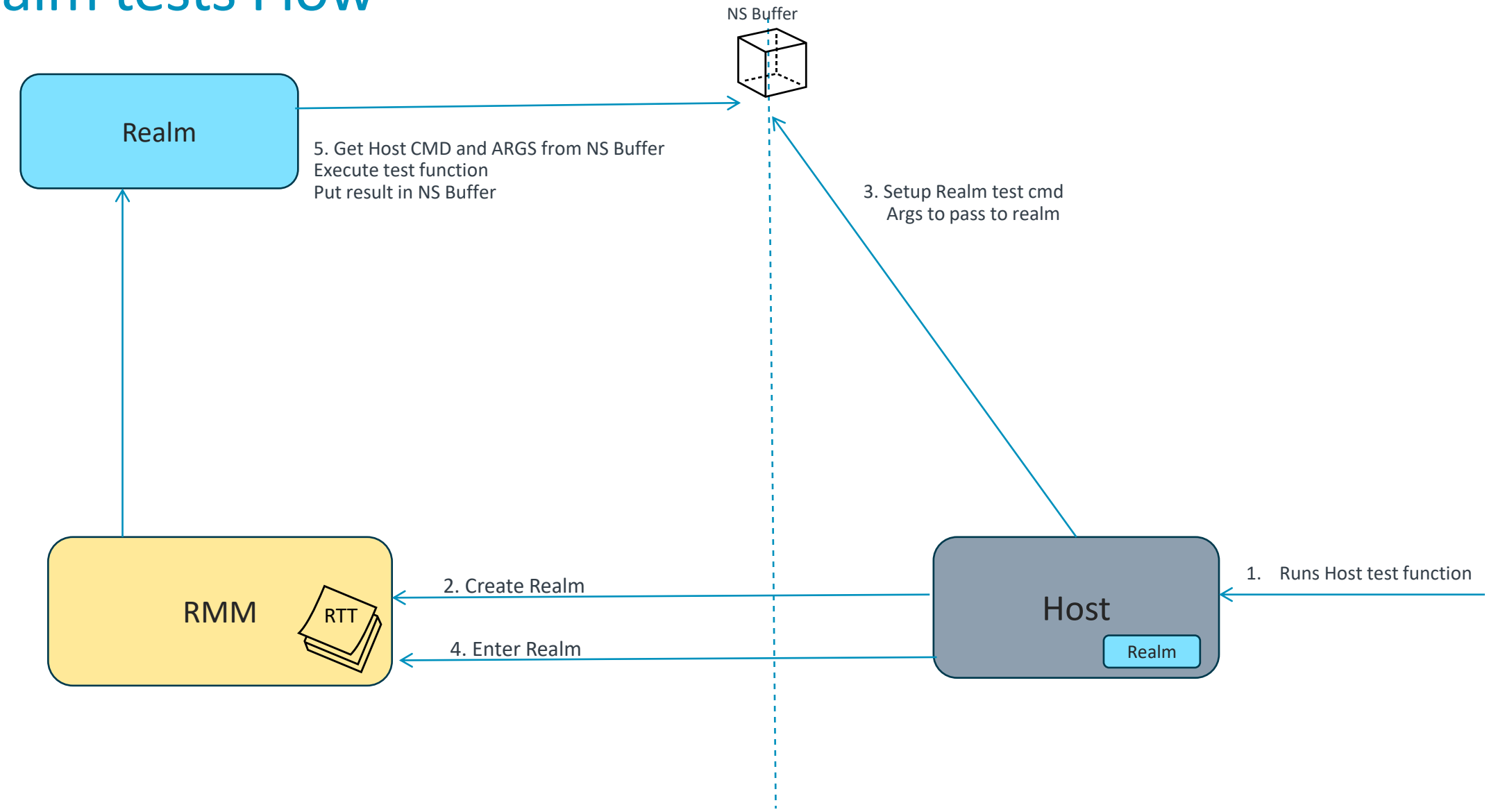
TFTF RTT Setup

- Host loads realm.bin to a new region (protected IPA), sets up RTT
  - Helper - host_realm_delegate_map_protected_data
    - § RMI_DATA_CREATE
    - § RMI_RTT_CREATE

- Host maps shared NS buffer in Realm memory (unprotected IPA), sets up RTT
  - Helper - host_realm_map_unprotected



Realm tests Flow



NS Buffer

- Used to share information across NS Host and Recs.
- Realm does not have UART, print buffer is transferred to Host via HOST_CALL

```
/*
 * This structure maps the shared memory to be used between the Host and Realm
 * payload
 */
typedef struct host_shared_data {
        /* Buffer used from Realm for logging */
        uint8_t log_buffer[MAX_BUF_SIZE];

        /* Command set from Host and used by Realm */
        uint8_t realm_cmd;

        /* array of params passed from Host to Realm */
        u_register_t host_param_val[MAX_DATA_SIZE];

        /* array of output results passed from Realm to Host */
        u_register_t realm_out_val[MAX_DATA_SIZE];

        /* Buffer to save Realm command results */
        uint8_t realm_cmd_output_buffer[REALM_CMD_BUFFER_SIZE];
} host_shared_data_t;
```

REC entry and exit

RMI_REC_ENTER(rec, run)

RmiRecEntry
“MMIO emulated” flag
“Inject SEA” flag
“Trap WFx” flags
GPRs
GIC HCR, LRs

RmiRecExit
REC exit reason
ESR_EL2, FAR_EL2, HPFAR_EL2
GPRs
GIC HCR, LRs, MISR, VMCR
Virt + phys timer control, compare
RIPAS change values
Host call immediate value
PMU overflow, interrupt enable, counter enable

Exit reasons

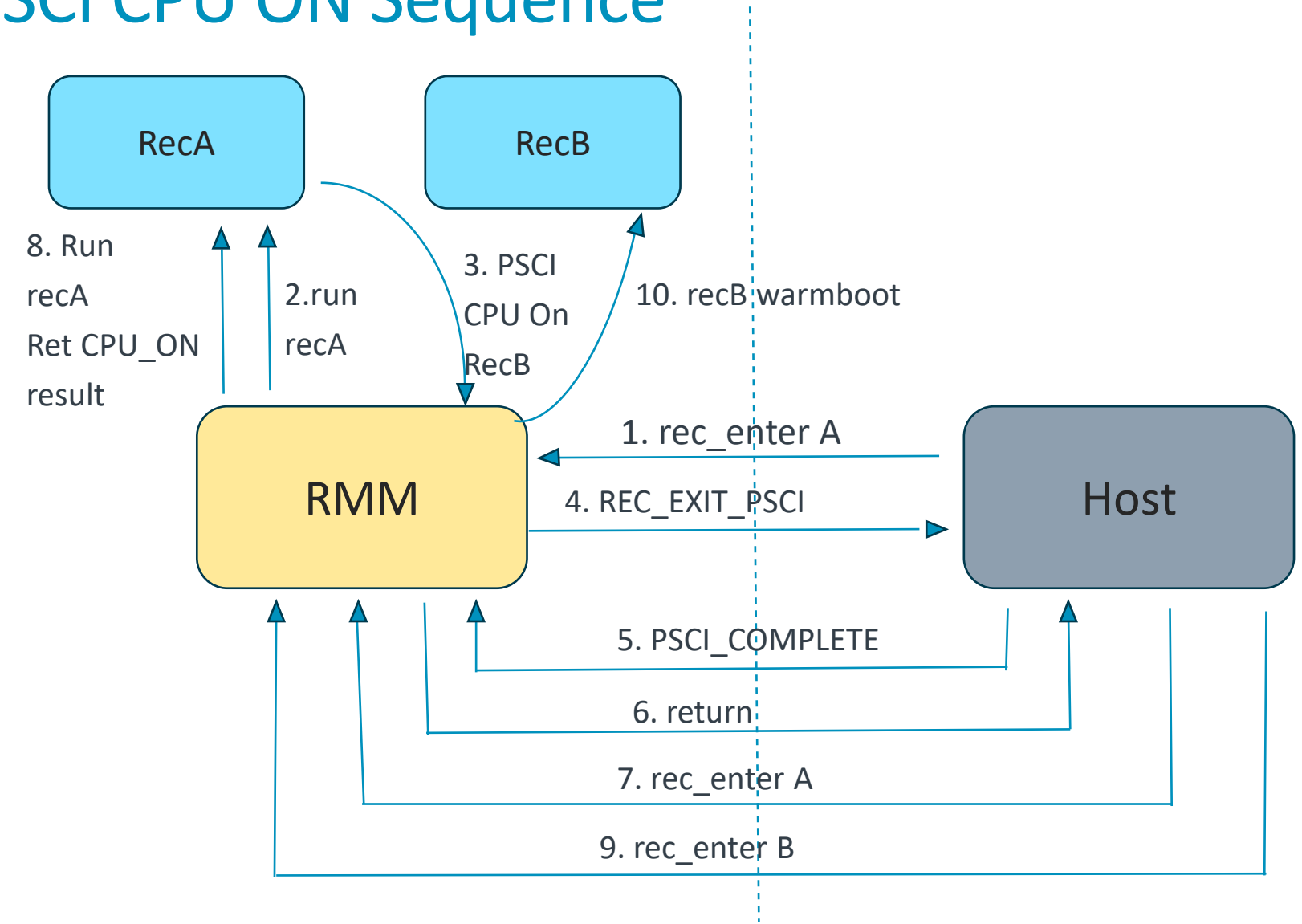
- Emulatable Data Abort
- Non-emulatable Data Abort
- Instruction Abort
- Sysreg emulation (ICC_SGI*R_EL1 and ICC_DIR_EL1 writes only)
- WFx
- IRQ
- FIQ
- PSCI
- RIPAS change
- Host call
- SError

TFTF Testcase

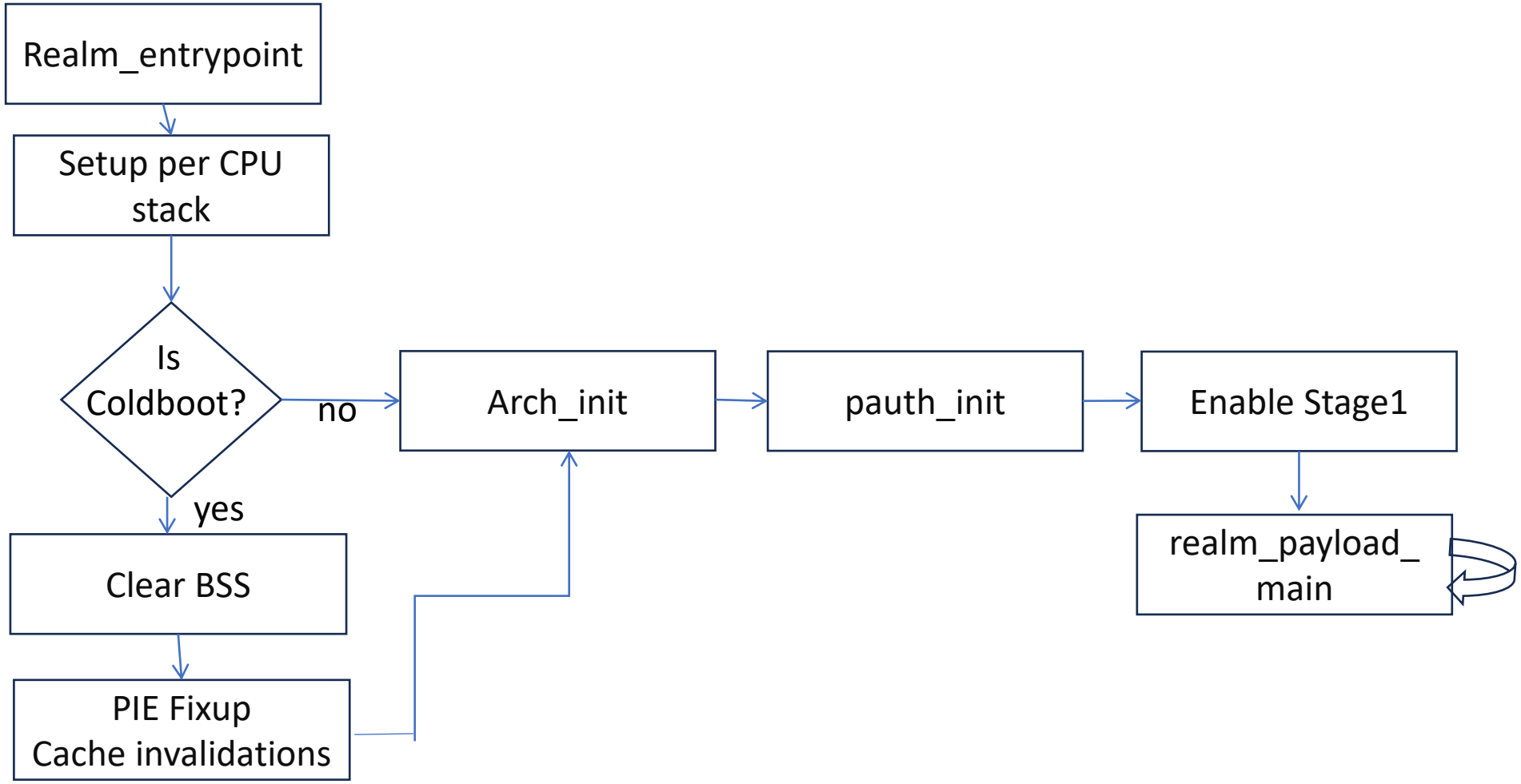
- <testcase name="Realm payload multi rec single cpu"
  - function="host_realm_multi_rec_single_cpu" />
- <testcase name="Multiple Realm EL1 creation and execution test“
  - function="host_test_multiple_realm_create_enter" />

Tests for PSCI Support

PSCI CPU ON Sequence



Boot Sequence Realm Payload



TFTF Testcase

<testcase name="Realm payload multi rec multiple cpu"

- function="host_realm_multi_rec_multiple_cpu" />

```
> Executing 'Realm payload multi rec multiple cpu'
INFO:    Realm start adr=0x8811a000
[VMID 7][Rec 0]: Realm: running on CPU = 0x0
INFO:    Booting
INFO:    Booting
INFO:    Booting
[VMID 7][Rec 1]: running on CPU = 0x1 cxt_id= 0x101
INFO:    Booting
[VMID 7][Rec 2]: running on CPU = 0x2 cxt_id= 0x102
INFO:    Booting
[VMID 7][Rec 3]: running on CPU = 0x3 cxt_id= 0x103
INFO:    Booting
[VMID 7][Rec 4]: running on CPU = 0x4 cxt_id= 0x104
INFO:    Booting
[VMID 7][Rec 5]: running on CPU = 0x5 cxt_id= 0x105
[VMID 7][Rec 6]: running on CPU = 0x6 cxt_id= 0x106
[VMID 7][Rec 7]: running on CPU = 0x7 cxt_id= 0x107
INFO:    Powering off
INFO:    Powering off
INFO:    Powering off
INFO:    Powering off
INFO:    Powering off
INFO:    Powering off
INFO:    Powering off
[VMID 7][Rec 0]: All CPU are off
  TEST COMPLETE                                                  Passed
```

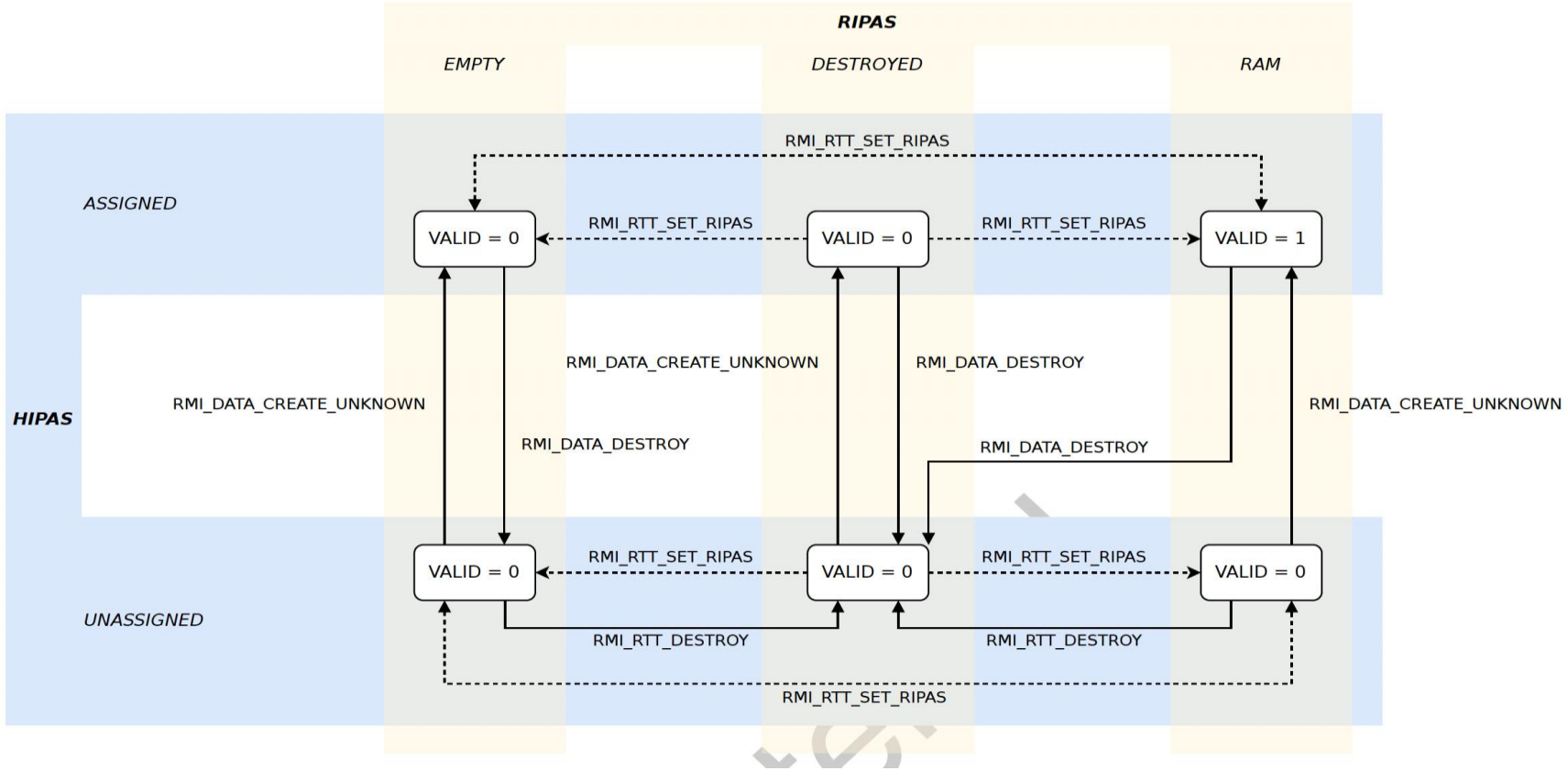
```
PSCI_c4000003              1 8811a000 101 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 1 8811a000 101
SMC_RMM_PSCI_COMPLETE      88223000 88235000 0 > RMI_SUCCESS
PSCI_c4000003              2 8811a000 102 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 2 8811a000 102
SMC_RMM_PSCI_COMPLETE      88223000 88247000 0 > RMI_SUCCESS
PSCI_c4000003              3 8811a000 103 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 3 8811a000 103
SMC_RMM_PSCI_COMPLETE      88223000 88259000 0 > RMI_SUCCESS
PSCI_c4000003              4 8811a000 104 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 4 8811a000 104
SMC_RMM_PSCI_COMPLETE      88223000 8826b000 0 > RMI_SUCCESS
PSCI_c4000003              5 8811a000 105 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 5 8811a000 105
SMC_RMM_PSCI_COMPLETE      88223000 8827d000 0 > RMI_SUCCESS
PSCI_c4000003              6 8811a000 106 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 6 8811a000 106
SMC_RMM_PSCI_COMPLETE      88223000 8828f000 0 > RMI_SUCCESS
PSCI_c4000003              7 8811a000 107 88131fa0 88131fa0 88131f60 ffffffc8 > c4000003 7 8811a000 107
SMC_RMM_PSCI_COMPLETE      88223000 882a1000 0 > RMI_SUCCESS
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_84000002              0 0 0 0 0 0 0 > 0 0 0 0
PSCI_c4000004              1 0 107 88131fa0 88131fa0 88131f60 ffffffc8 > c4000004 1 0 107
SMC_RMM_PSCI_COMPLETE      88223000 88235000 0 > RMI_SUCCESS
PSCI_c4000004              2 0 107 88131fa0 88131fa0 88131f60 ffffffc8 > c4000004 2 0 107
SMC_RMM_PSCI_COMPLETE      88223000 88247000 0 > RMI_SUCCESS
PSCI_c4000004              3 0 107 88131fa0 88131fa0 88131f60 ffffffc8 > c4000004 3 0 107
SMC_RMM_PSCI_COMPLETE      88223000 88259000 0 > RMI_SUCCESS
PSCI_c4000004              4 0 107 88131fa0 88131fa0 88131f60 ffffffc8 > c4000004 4 0 107
```

arm

Realm Memory Management

Realm IPA state (RIPAS) and Host IPA state (HIPAS)

- Realm and Host each have their own view of the Realm's Protected IPA space
- Each of the two can manipulate this view independently



TFTF Testcases

- <testcase name="New Realm PAS Validation"
  - function="host_realm_pas_validation_new" />
- <testcase name="Active Realm PAS validation"
  - function="host_realm_pas_validation_active" />

arm

Realm Memory Exception Model

Realm Memory Exception

I_{TPGKW} The following table summarizes the properties of Realm IPA space.

Realm IPA	Data access causes abort to Realm?	Data access causes REC exit due to Data Abort?	Instruction fetch causes abort to Realm?	Instruction fetch causes REC exit due to Instruction Abort?
Protected, RIPAS=EMPTY	Always (SEA)	Never	Always (SEA)	Never
Protected, RIPAS=RAM	Never	When HIPAS=UNASSIGNED	Never	When HIPAS=UNASSIGNED
Protected, RIPAS=DESTROYED	Never	Always	Never	Always
Unprotected	Host can inject SEA following REC exit due to Data Abort	When HIPAS=UNASSIGNED_NS	Always (SEA)	Never
Outside Realm IPA space	Always (Address Size Fault)	Never	Always (Address Size Fault)	Never

TFTF Testcases

- <testcase name="Realm SEA Unprotected"
  - function="host_realm_sea_unprotected" />
- <testcase name="Realm SEA Adr Fault“
  - function="host_realm_sea_adr_fault" />
- <testcase name="Realm Abort Unassigned RAM“
  - function="host_realm_abort_unassigned_ram" />
- <testcase name="Realm Abort Unassigned Destroyed“
  - function="host_realm_abort_unassigned_destroyed" />

```
> Executing 'Realm SEA Adr Fault'
INFO:    Realm start adr=0x8811a000
INFO:    base_ipa=0x200088000000
[VMID 14][Rec 0]: Initial ripas=0x0
[VMID 14][Rec 0]: Generate Data Abort
INFO:    Rec0 ESR=0x97c08210
[VMID 14][Rec 1]: Initial ripas=0x0
[VMID 14][Rec 1]: Generate Instruction Abort
INFO:    Rec1 ESR=0x86000210
INFO:    base_ipa=0x202000088000000
[VMID 14][Rec 2]: Initial ripas=0x0
[VMID 14][Rec 2]: Generate Data Abort
INFO:    Rec2 ESR=0x96000000
[VMID 14][Rec 3]: Initial ripas=0x0
[VMID 14][Rec 3]: Generate Instruction Abort
INFO:    Rec3 ESR=0x86000000
  TEST COMPLETE                                                 Passed

> Executing 'Realm Abort Unassigned RAM'
INFO:    Realm start adr=0x8811a000
INFO:    Initial state base = 0x8824a000 rtt.state=0x0 rtt.ripas=0x1
[VMID 15][Rec 0]: Initial ripas=0x1
[VMID 15][Rec 0]: Generate Instruction Abort
INFO:    IA FAR=0x0, HPFAR=0x8824a0 ESR=0x80000007
[VMID 15][Rec 1]: Initial ripas=0x1
[VMID 15][Rec 1]: Generate Data Abort
INFO:    DA FAR=0x0, HPFAR=0x8824a0 ESR=0x90000007
  TEST COMPLETE                                                 Passed

> Executing 'Realm Abort Unassigned Destroyed'
INFO:    Realm start adr=0x8811a000
INFO:    Initial state base = 0x8824a000 rtt.state=0x1 rtt.ripas=0x1
INFO:    New state4 base = 0x8824a000 rtt.state=0x0 rtt.ripas=0x2
[VMID 16][Rec 0]: Initial ripas=0x2
[VMID 16][Rec 0]: Generate Instruction Abort
INFO:    IA FAR=0x0, HPFAR=0x8824a0 ESR=0x80000007
[VMID 16][Rec 1]: Initial ripas=0x2
[VMID 16][Rec 1]: Generate Data Abort
INFO:    DA FAR=0x0, HPFAR=0x8824a0 ESR= 0x90000007
  TEST COMPLETE                                                 Passed
```

Misc Testcases

- SVE/FPU/SIMD – Verify Save restore registers across Exceptions
  - host_sve_realm_check_config_register
  - host_realm_fpu_access_in_rl_ns_se
- PMU – Access PMU counter from Realm, Tests PMU overflow ISR injection
  - host_realm_pmuv3_overflow_interrupt
- PAuth – Realms can enable Pauth, program keys, verify save/restore of keys, testcase to generate Pauth Fault in Realm
  - host_realm_pauth_fault

Future Work

- Add more tests for Increased Coverage
- Optimize Realm payload loading
- Tests for LPA2 Support
- Enable Stage 1 in Realms with LPA2 Support
- Framework for Planes & Device Assignment Testing

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు

CPPCheck in RMM for Misra Compliance

Shruti Gupta
02/05/2024

CPPCheck

CPPCheck is an open-source C/C++ static analyzer tool.

CPPCheck can detect bugs like

Undefined Behaviors

- Dead pointers
- Division by zero
- Integer overflows
- Invalid bit shift operands
- Invalid conversions
- Invalid usage of STL
- Memory management
- Null pointer dereferences
- Out of bounds checking
- Uninitialized variables
- Writing const data

Security Vulnerabilities

- Buffer Errors
- Improper Access Control
- Information Leak
- Permissions, Privileges, and Access Control
- Input Validation

Coding Standards

- Misra C 2012
- Cert C

Installing CPPCheck

- Recommended version 2.13.4
- To install CPPCheck from source –

- *git clone https://github.com/danmar/cppcheck.git -b 2.13.x*
- *mkdir build*
- *cd build*
- *cmake ..*
- *cmake --build .*
- *export PATH=$cppcheck_root/build/bin:$cppcheck_root/htmlreport:$PATH*
- *cppcheck --version*

Integrating CPPCheck in RMM Project

- *cmake -DRMM_CONFIG=fvp_defcfg -S . -B build -DCMAKE_EXPORT_COMPILE_COMMANDS=ON*

- *To run CPPCheck standalone*
  - *cmake --build build – cppcheck*
  - Generates cppcheck.xml in build/tools/cppcheck folder

- *To run CPPCheck + MISRA*
  - *cmake --build build -- cppcheck-misra*

    Generates cppcheck_misra.xml in build/tools/cppcheck folder

- Refer - https://cppcheck.sourceforge.io/manual.pdf

Misra Configuration

https://github.com/TF-RMM/tf-rmm/tree/main/tools/cppcheck

Misra.json

```
{
  "script": "misra.py",
    "args": [
            "--suppress-rules=1.2,2.5,3.1,5.7,8.5,8.6,8.9,8.12,8.13,9.5,10.5,10.8,11.3,11.4,
            11.5,11.6,12.3,13.3,15.1,15.4,15.5,15.7,16.1,16.2,16.3,16.5,16.6,17.1,17.8,
            17.12,19.2,20.6,20.10,20.12,21.1,21.2,21.6",
            "--rule-texts=./tools/cppcheck/misra.rules“   ← Replace Misra rule description
           ]
}
```

CPPCheck Suppression

- Inline Suppression
  - /* cppcheck-suppress uninitvar */
  - /* cppcheck-suppress [arrayIndexOutOfBounds, uninitvar] */
  - /* cppcheck-suppress-begin uninitvar */
  - /* cppcheck-suppress-end uninitvar */

- Suppression.txt
  - [error id]:[filename]:[line]
  - *:*/ext/*
  - [Uninitvar, arrayIndexOutOfBounds]:*/file.c:10

CPPCheck output

- Generates XML output

```
<errors>
   <error id="someError" severity="error" msg="short error text"
    verbose="long error text" inconclusive="true" cwe="312">
     <location file0="file.c" file="file.h" line="1"/>
</error>
```

- Cppcheck-htmlreport –
  - Takes XML input and generates user-friendly html report.
  - htmlreport/cppcheck-htmlreport --file=cppcheck_misra.xmlr.xml --report-dir=test --source-dir=.
  - Generated test/index.html

CI Job

- CPPCheck job is automated in internal RMM CI, CI+1

Cppcheck report - [project name]

error | warning | portability | performance | style | information | cppcheck | clang-tidy | File: | Filter:

Defect summary

Toggle all

Show #	Defect ID
11	misra-c2012-10.4
8	misra-c2012-10.6
5	misra-c2012-18.4
3	misra-c2012-10.1
3	misra-c2012-8.4
2	misra-c2012-10.7
2	misra-c2012-17.2
1	checkersReport
1	knownConditionTrueFalse
1	misra-c2012-10.3
1	misra-c2012-14.2
1	misra-c2012-17.3
39	total

Statistics

Line	Id	CWE	Severity	Message
	checkersReport		information	Active checkers: 4/637 (use --checkers-report=<filename> to see details)
/mnt/c/workspace/demo/tf-rmm/drivers/pl011/src/pl011.c				
72	misra-c2012-8.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/allocator/src/memory_alloc.c				
162	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
163	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
164	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
185	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
202	misra-c2012-10.1		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
206	misra-c2012-18.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
212	misra-c2012-18.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
245	misra-c2012-10.1		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
249	misra-c2012-18.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
274	misra-c2012-18.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
278	misra-c2012-18.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
283	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
352	misra-c2012-10.1		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
426	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
429	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
431	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
432	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
433	misra-c2012-10.3		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
434	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/gic/src/gic.c				
100	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/realm/include/rec.h				
233	misra-c2012-10.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/s2tt/src/s2tt.c				
606	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
1036	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
1058	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
1184	knownConditionTrueFalse	398	style	The comparison 's2tte&ns_attr_host_mask != ns_attrs' is always false because 's2tte&ns_attr_host_mask' and 'ns_attrs' represent the same value.
1274	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/xlat/src/xlat_contexts.c				
261	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/lib/xlat/src/xlat_tables_core.c				
313	misra-c2012-17.2		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
326	misra-c2012-17.2		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/runtime/core/handler.c				
234	misra-c2012-8.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
259	misra-c2012-17.3		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
450	misra-c2012-8.4		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/runtime/core/sysregs.c				
352	misra-c2012-14.2		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/runtime/rmi/realm.c				
114	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
116	misra-c2012-10.6		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
196	misra-c2012-10.7		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)
/mnt/c/workspace/demo/tf-rmm/runtime/rmi/run.c				
55	misra-c2012-10.7		style	misra violation (rule-texts-file not found: tools/cppcheck/misra.rules)

Future Work

- Add GitHub Action to run CPPCheck
- Maintain 0 CPPCheck MISRA errors on RMM Main

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు