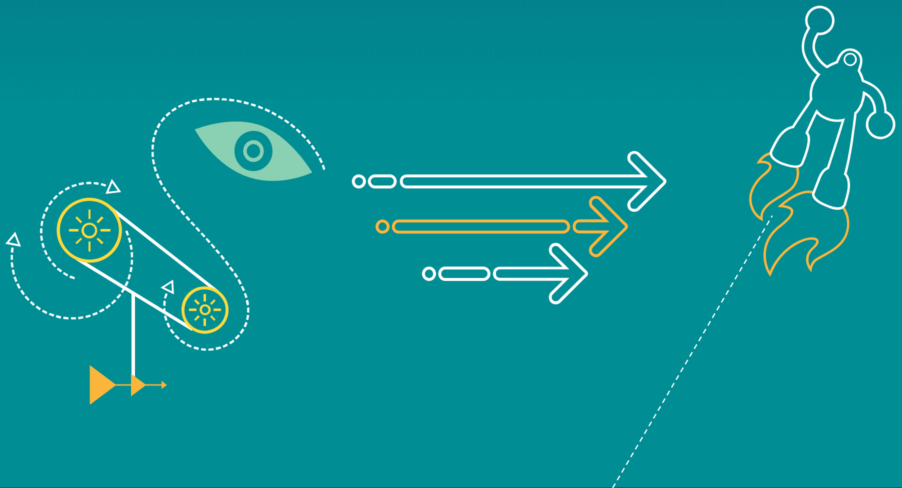
# Stability Issue First Triage

Qualcomm Technologies, Inc.



80-P7139-7 A

# Confidential and Proprietary – Qualcomm Technologies, Inc.

**NO PUBLIC DISCLOSURE PERMITTED:** Please report postings of this document on public servers or websites to: DocCtrlAgent@qualcomm.com.

Not to be used, copied, reproduced, or modified in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other product and brand names may be trademarks or registered trademarks of their respective owners.

This technical data may be subject to U.S. and international export, re-export, or transfer (“export”) laws. Diversion contrary to U.S. and international law is strictly prohibited.

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

# Revision History

| Revision | Date | Description |
|---|---|---|
| A | June 2016 | Initial release |

# Contents

- Quick Crash Classification
- Kernel Panic
- Non-Secure Watchdog Bark
- Non-Secure Watchdog Bite
- TrustZone Log Captured Errors
- RPM Log Captured Errors
- Hyperviser Errors
- Secure Watchdog Bite
- GCC_RESET_STATUS/PON_WARM_RESET_REASON Interpretation
- Others
- References
- Questions?

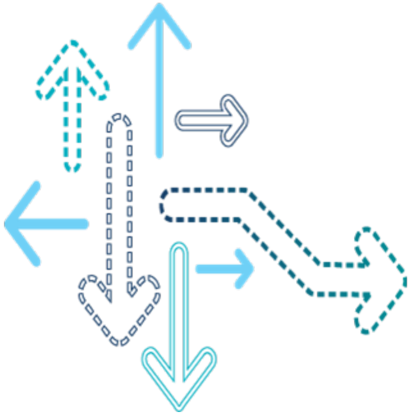
# Agenda

- Classify crash by logs (kernel log, TrustZone (TZ)/RPM logs, register)
- Panic errors shown in kernel log
  - BUG_ON
  - Prefetch abort
  - Unhandled page fault or NULL pointer access
  - Cache ECC error
  - Subsystem crash
  - Out-of-memory
- Non-secure watchdog bark
- Non-secure watchdog bite

# Agenda (cont.)

- TZ errors shown in TZ log
  - NOC error
  - SMMU error
  - XPU error
  - AHB timeout error
- RPM error fatal
- Hyperviser error
- Secure watchdog bite
- GCC_RESET_STATUS/PON_WARM_RESET_REASON Interpretation
  - Thermal reset
  - PMIC abnormal reset
  - PMIC watchdog

# Quick Crash Classification



# Tools

- Use QCAP (https://cap.qti.qualcomm.com/) to get an overview of the issues
- RAM parser to get HLOS details

# Kernel Panic

# Prefetch Abort

```
14603.036095:   <6> Unhandled prefetch abort: unknown 1 (0x001) at
0xc03c6a36
14603.036098:   <6> Internal error: : 1 [#1] PREEMPT SMP ARM5
14603.036101:   <6> amd2771_ioctl, clear ps enable bit here
14603.036103:   <6> Modules linked in:      CPU: 1 PID: 0 Comm:
swapper/1 Tainted: G        W    3.10.28-svn446 #1
14603.036105:   <6> Task: ee863480 ti: eea08000 task.ti: eea08000
14603.036108:   <6> PC is at msm_spm_drv_set_spm_enable+0x6/0x48
14603.036110:   <6> LR is at uncached_logk_pc+0x14/0x178
14603.036113:   <6> pc : [<c03c6a36>]    lr : [<c019c980>]    psr:
200f0093
14603.036115:   <6> sp : eea09ea0  ip : 00000000  fp : 00000000
r10: 00000001  r9 : ed4ef500  r8 : 00000001
14603.036117:   <6> r7 : 00000000  r6 : 00000003  r5 : c10e1910  r4 :
f01bc030
```

- Possible reasons:
  - DDR corruption − use data.list to check the value
  - Cache corruption − use data.list to check the value
  - CPU misbehavior
  - Software bug − check the LR register

# Unable to Handle Kernel Paging Request

```
5664.261287:   <6> Unable to handle kernel paging request at virtual address
ffffff8004a3d088
5664.261368:   <6> CPU: 7 PID: 24000 Comm: VosRXThread Tainted: P        W  O 3.10.73-
perf-g3e27d8e-00337-g6e3f732 #1
5664.261632:   <2> PC is at dphLookupHashEntry+0x2c/0xb0 [wlan]
5664.261931:   <2> LR is at dphLookupHashEntry+0x20/0xb0 [wlan]
5664.261940:   <2> pc : [<ffffffbffc0d3e24>] lr : [<ffffffbffc0d3e18>] pstate: 60000145
5664.261952:   <2> x29: ffffffc017ba7a30 x28: ffffffc01950c000
5664.262105:   <2> x3 : ffffff8003211158 x2 : 0000000000000029
5664.262114:   <2> x1 : ffffff8004a3d000 x0 : 0000000000000088
5664.262359:   <2> Call trace:
5664.262596:   <2> [<ffffffbffc0d3e24>] dphLookupHashEntry+0x2c/0xb0 [wlan]
5664.262841:   <2> [<ffffffbffc0d762c>] limIsDeauthDiassocForDrop+0x48/0xc4 [wlan]
5664.263124:   <2> [<ffffffbffc1962e4>] sysBbtProcessMessageCore+0xac/0x138 [wlan]
5664.263347:   <2> [<ffffffbffc0d5948>] $x+0x1a8/0x200 [wlan]
5664.263620:   <2> [<ffffffbffc1c06c0>] WLANTL_RxFrames+0x258/0x760 [wlan]
5664.263890:   <2> [<ffffffbffc218a3c>] $x+0x2d4/0x378 [wlan]
5664.264081:   <2> [<ffffffbffc07066c>] dxeRXFrameRouteUpperLayer+0x108/0x128 [wlan]
5664.264278:   <2> [<ffffffbffc071ae8>] dxeRXFrameReady+0x6c/0x2e0 [wlan]
5664.264459:   <2> [<ffffffbffc072870>] dxeRXEventHandler+0x2f0/0x824 [wlan]
5664.264731:   <2> [<ffffffbffc1d0af8>] $x+0x4/0x78 [wlan]
5664.264752:   <2> [<ffffffc0000bdef4>] kthread+0xac/0xb8
5664.264762:   <6> Code: 97ffffed d37d3c00 f94017a3 f9400061 (f8606820)
```

- Possible reasons: such issues need restoring stack for detail analysis
  - If the address looks valid, it is a possible software issue, such as a race condition
  - If the address seems abnormal, DDR issues are very likely

# Kernel NULL pointer access

```
[ 13.723273] Unable to handle kernel paging request at virtual address
ffffffc0002271b8
[ 13.723288] pgd = ffffffc0b5734000
[ 13.723294] [ffffffc0002271b8] *pgd=0000000000000000
[ 13.723305] Internal error: Oops: 9600004e [#1] PREEMPT SMP
[ 13.723311] Modules linked in: qdrbg_module(O) qcrypto_module(O)
[ 13.723330] CPU: 2 PID: 663 Comm: netmgrd Tainted: G W O 3.10.49-
perf-g67c73a8 #1
[ 13.723337] task: ffffffc0b5632b00 ti: ffffffc0b576c000 task.ti:
ffffffc0b576c000
[ 13.723349] PC is at run_timer_softirq+0x430/0x4d4
[ 13.723355] LR is at run_timer_softirq+0x2d0/0x4d4
```

- Possible reasons: such issues need to restore stack for detail analysis
  - If the address looks valid, it is possibly a software issue, such as race condition
  - If the address seems abnormal, very likely DDR issues

# Kernel Bug – If CONFIG_DEBUG_BUGVERBOSE is Not Defined

```
[  341.650326] qcom,qpnp-wled qpnp-wled-f6e91000: backlight enabled
[  342.389185] ------------[ cut here ]------------
[  342.389211] Kernel BUG at c015bbe8 [verbose debug info unavailable]
[  342.389221] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP ARM
[  342.389230] Modules linked in: core_ctl(PO) wlan(O) qdrbg_module(O)
qcrypto_module(O)
[  342.389272] CPU: 1 PID: 0 Comm: swapper/1 Tainted: P        W  O
3.10.84-gbd86dbb #1
[  342.389286] task: f798be80 ti: f7b2c000 task.ti: f7b2c000
[  342.389316] PC is at dec_hmp_sched_stats_fair+0x8c/0x9c
[  342.389335] LR is at sched_upmigrate_min_nice+0x0/0x4
[  342.389347] pc : [<c015bbe8>]    lr : [<c131c4d8>]    psr: a00001d3
[  342.389347] sp : f7b2dc48  ip : c131c4d8  fp : ce996ac0
[  342.389359] r10: ce996ac0  r9 : 00000004  r8 : ce996b08
[  342.389369] r7 : 0000004f  r6 : f2940c80  r5 : c131c4d8  r4 :
ce997010
[  342.389381] r3 : ffffffff  r2 : fff48387  r1 : 00179626  r0 :
ce997008
[  342.389394] Flags: NzCv  IRQs off  FIQs off  Mode SVC_32  ISA ARM
Segment kernel
[  342.389405] Control: 10c0383d  Table: b0cd406a  DAC: 00000015
```

# Kernel BUG – If CONFIG_DEBUG_BUGVERBOSE is Defined

```
0.000000: <2>[07-01 11:41:11.041] kernel BUG at
/home/android/kernel/kernel/timer.c:896!
0.000000: <0>[07-01 11:41:11.049] Internal error: Oops - BUG: 0 [#1]
PREEMPT SMP ARM
0.000000: <6>[07-01 11:41:11.056] Modules linked in: [last unloaded:
wlan]
0.000000: <6>[07-01 11:41:11.061] CPU: 0 Tainted: G W O (3.4.0+ #1)
0.000000: <6>[07-01 11:41:11.067] PC is at add_timer+0x14/0x18
0.000000: <6>[07-01 11:41:11.072] LR is at
breath_leds_write+0xe4/0x13c
0.000000: <6>[07-01 11:41:11.077] pc : [<c01997b8>] lr : [<c06317dc>]
psr: a0000013
0.000000: <6>[07-01 11:41:11.077] sp : f2753f50 ip : 00000000 fp :
5ff9cc84
0.000000: <6>[07-01 11:41:11.089] r10: 00000000 r9 : f2752000 r8 :
00000001
0.000000: <6>[07-01 11:41:11.095] r7 : f2753f88 r6 : 00000001 r5 :
00000003 r4 : c0fd1470
0.000000: <6>[07-01 11:41:11.102] r3 : 0000dae8 r2 : c0f6a844 r1 :
00000000 r0 : c0fd1528
0.000000: <6>[07-01 11:41:11.109] Flags: NzCv IRQs on FIQs on Mode
SVC_32 ISA ARM Segment user
0.000000: <6>[07-01 11:41:11.117] Control: 10c5387d Table: 3266c06a
DAC: 00000015
```

- For such issues, check the code logic to see why a Bug is triggered and then analyze the stack

# Cache Errors

- If the cache ECC checking function is available on the platform or Kernel, then the config of cache error panic is enabled (e.g., CONFIG_MSM_CACHE_M4M_ERP64 related to the 8996 platform)

```
<1>[ 141.961268] I[3: servicemanager: 642] msm_cache_erp64: CPU3: D-cache error detected
<1>[ 141.961389] I[2: cfinteractive: 362] msm_cache_erp64: CPU2: D-cache error detected
<1>[ 141.961556] I[2: cfinteractive: 362] msm_cache_erp64: CPU2: L1 DCESR 0x80000001, DCESYNR0 0x0, DCESYNR1 0x42, DCEAR0 0xecbefac0, DCEAR1 0x8001ffc0
```

- For such errors, it is mainly related to voltage.
- If a cache error of other kind occurs (such as master port decode error, non-parity errors), verify the TrustZone logs to check whether XPU or NOC error is caused.

# Subsystem Crash

- This is due to restart level set to RESET_SOC for debugging subsystem issues

```
[33325.177128] subsys-restart: subsystem_restart_dev(): Restart
sequence requested for modem, restart_level = SYSTEM.
[33325.177184] M-Notify: General: 8
[33325.177197] Kernel panic - not syncing: subsys-restart: Resetting
the SoC - modem crashed.
```

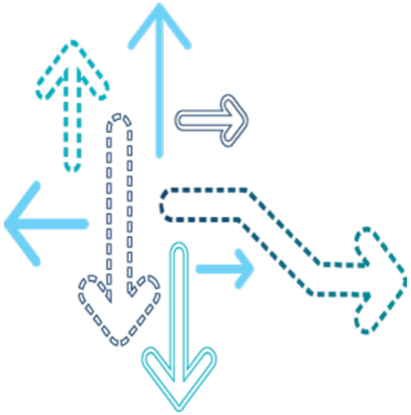
- For such errors, check each subsystem to verify the err_fatal or dog bite.

# Out Of Memory (OOM)

```
<4>[54062.495330] android.browser invoked oom-killer: gfp_mask=0xc0d0,
order=2, oom_adj=0, oom_score_adj=0
<4>[54062.502349] Mem-info:
<4>[54062.502471] Normal per-cpu:
<4>[54062.502655] CPU 0: hi: 90, btch: 15 usd: 0
<4>[54062.502777] CPU 1: hi: 90, btch: 15 usd: 0
<4>[54062.502868] HighMem per-cpu:
<4>[54062.503082] CPU 0: hi: 186, btch: 31 usd: 0
<4>[54062.503173] CPU 1: hi: 186, btch: 31 usd: 60
<4>[54062.503387] active_anon:87251 inactive_anon:624 isolated_anon:1
<4>[54062.503387] active_file:11946 inactive_file:12064
isolated_file:0
<4>[54062.503387] unevictable:3936 dirty:3 writeback:0 unstable:0
<4>[54062.503387] free:4209 slab_reclaimable:2750
slab_unreclaimable:5916
```

- OOM is a mechanism when Linux system meets memory shortage. After this error is printed, the kernel log also prints the memory usage in the system. Sometimes it happens due to memory leak and sometimes it is just because of the memory allocation being too much. For the memory leakage, refer to kernel/Documentation/kmemleak.txt for further debugging. For the whole system memory usage tuning, adjust the low memory killer parameters to make it work efficiently before OOM is triggered.

# Non-Secure Watchdog Bark

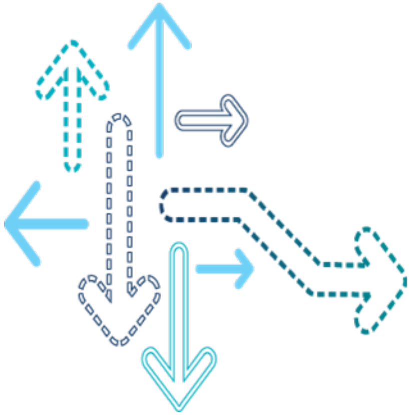


# Bark due to Non-Secure Watchdog not Pet in Time

```
<2>[87433.537697] Apps Watchdog bark received - Calling Panic
<0>[87433.537728] Kernel panic - not syncing: Apps Watchdog Bark
received
<0>[87433.537728]
<4>[87433.537819] [<c003c6b0>] (unwind_backtrace+0x0/0x11c) from
[<c03f1d98>] (panic+0x6c/0x190)
<4>[87433.537850] [<c03f1d98>] (panic+0x6c/0x190) from [<c006835c>]
(msm_wdog_bark_fin+0x20/0x2c)
<4>[87433.537911] [<c006835c>] (msm_wdog_bark_fin+0x20/0x2c) from
[<ffff00c0>] (0xffff00c0)
<0>[87433.637590] Rebooting in 5 seconds..
<5>[87438.620072] Going down for restart now
```

- Possible reasons:
  - Excessive logging
  - Work queue
  - Timer
  - Run queues
  - Pet-time/bark-time configuration
  - Other hardware issues (crystal/CPU)

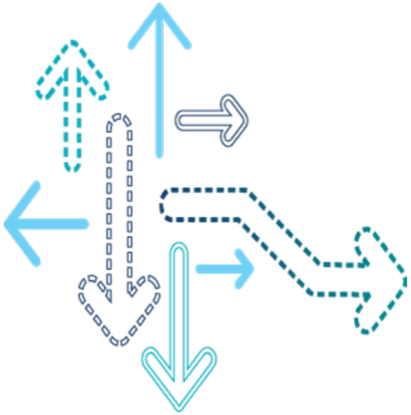
# Non-Secure Watchdog Bite



# This Log is Shown in the TrustZone Part

- bits_per_word=8<br>
  bits_per_word=8<br>
  Fatal Error: NON_SECURE_WDT<br>
  L2 SPM is BAD for CPU 3, No of CPU On in CL 2
- This is non-secure watchdog bite that can occur and is grasped in the TrustZone module.
- Possible reasons
  - This is similar analysis as the non-secure watchdog bark issue
  - Gather the CPU context to get more information

# TrustZone Log Captured Errors



# AHB timeout

```
ABT SNOC_2 ID: 0x00004300
ABT SNOC_2 ADDR0: 0x0c051004
ABT SNOC_2 ADDR1: 0x00000000
ABT SNOC_2 HREADY: 0xfffffffe
ABT SNOC_2 Slaves: 1
Fatal Error: AHB_TIMEOUT
```

```
BID = 0x2
PID = 0x3
MID = 0x0
BID/PID/MID = BIMC CPUSS

Slave = lpass

Address offset = 0x0c051004
```

- AHB timeout is due to a slave not responding, it maybe due to the non-clock access or wrong access.

# XPU Violation

```
xpu:>>> [2] XPU error dump, XPU id IMC_MPU1)<<<
xpu: uErrorFlags: 00000002
xpu:  HAL_XPU2_ERROR_F_CLIENT_PORT
uBusFlags: 000205a1
xpu:  HAL_XPU2_BUS_F_ERROR_AC
xpu:  HAL_XPU2_BUS_F_APROTNS
xpu:  HAL_XPU2_BUS_F_AWRITE
xpu:  HAL_XPU2_BUS_F_AOOO
xpu:  HAL_XPU2_BUS_F_ABURST
xpu:  HAL_XPU2_BUS_F_MSA_RG_MATCH
xpu: uPhysicalAddress: f5232400
xpu: uMasterId: 00000006, uAVMID    : 00000000
xpu: uATID    : 00000002, uABID     : 00000002
xpu: uAPID    : 00000000, uALen     : 00000007
xpu: uASize   : 00000004, uAPReqPriority   : 00000000
xpu: uAMemType: 00000000
Fatal Error: NOC_ERROR
```

- This is due to the TrustZone XPU configuration. Submit the cases to QTI.

# NOC Errors

```
CNOC ERROR: ERRLOG0 = 0x80030000
CNOC ERROR: ERRLOG1 = 0x22a01016
CNOC ERROR: ERRLOG3 = 0x00000030
CNOC ERROR: ERRLOG4 = 0x00000008
CNOC ERROR: ERRLOG5 = 0x00000000
```

| | |
|---|---|
| **InitFlow** | qxm_snoc/1/0 |
| **TargetFlow** | qhs6/T/qhs6_mss_cfg |
| **Address** | 0x02000030 |
| **Master ID** | HMSS |

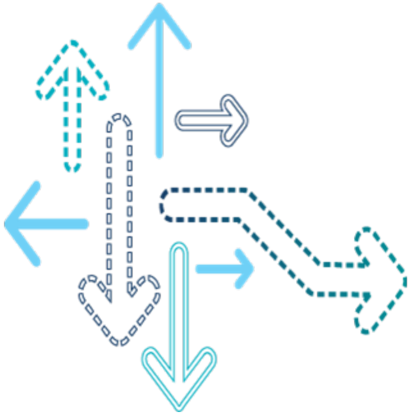
- Submit the cases to QTI.

# SMMU Errors

```
[770] SMMU:>> MDP CB2 Fault:
[770] FSR=0x40000402
[770] FAR=0x0000000004131000
[780] IPAFAR=0x0000000068211000
[780] FSYNR0=0x00000025
[780] FSYNR1=0x0803000a
[780] CBFRSYNRA2=0x00000000
[790] CR0=0x00000001
[790] NSCR0=0x00201e36
[790] CBAR2=0x00000003
[790] CBA2R2=0x00000001
[800] SCTLR=0x00df00e1
[800] TCR=0x8001005c
[800] TTBR0=0x000000017e45a000
[800] ***** ENHANCED SMMU DEBUG *****
[810] faultingSmmuBase = 0x d00000
[810] fsynr0 = 0x00000025 -- faultingStage1CB = 0x d08000
[820] faultingStage2CB = 0x d0a000
…
[880] Fatal Error: SMMU
```

- Please check the SMMU culprit component and submit cases to the concerned technical team.

# RPM Log Captured Errors

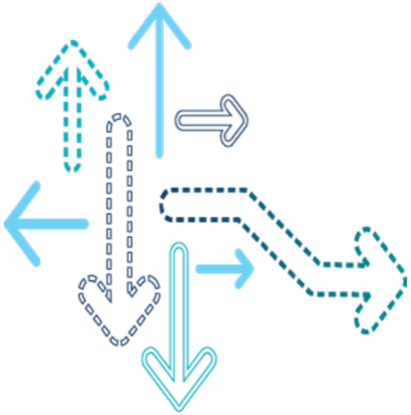


# RPM Error Fatal

```
0x0000000158BDBCC2:   railway_change_voltage: (rail: Mx) (new
microvolts: 1225000)
0x0000000158BDFBD6:   rpm_err_fatal (lr: 0x0000C397) (ipsr:
0x00000000)
```

- Submit the cases to the QTI RPM team for further analysis.

# Hyperviser Errors

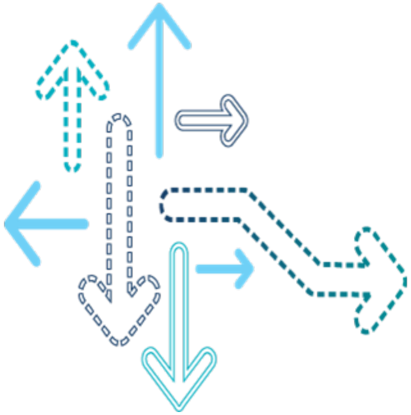


# Error in the Hyperviser Log (QCAP)

```
sec_img_tear_down_and_unmap [51]
hyp_pil_unlock_area [35]
Error shutting down subsystem [12]
Making SMC call with ID: TZ_SECURE_WDOG_TRIGGER_ID to ensure the fault
is handled
```

- First the SLPI crashes, and the SSR happens successfully and is bringing SLPI up. However, there is still a pending shutdown request by the peripheral manager to tear down SLPI. Then, HYP is unable to handle this case, and makes an SCM call to TZ and a non-secure dog bite occurs. The root cause is that the SLPI-related patches are missing.
- Hyperviser can capture the errors from EL1, so it is a possible HLOS error. Check whether other symptom happens at the same time and submit cases to the QTI team.

# Secure Watchdog Bite



# Secure Dog Bite

- No obvious error logs
- We can confirm this by GCC_RESET_STATUS and PON_WARM_RESET_REASON (T.B.D in next chapter)
- Check:
  - SDI captured CPU context is most valuable
  - Kernel/TZ/RPM logs to conclude which routine it is executing
  - RTB log is also useful
  - Sometimes, it is also useful to test multiple patches before arriving at the final conclusion

# GCC_RESET_STATUS/PON_WARM_RESET_REASON Interpretation

# GCC_RESET_STATUS Definition (check each platform SWI)

| Bits | Field Name | Field Values | Retention | Calculated Value |
|---|---|---|---|---|
| 5 | SECURE_WDOG_EXPIRE_STATUS | – | No | – |
| 4 | PMIC_ABNORMAL_RESIN_STATUS | – | No | – |
| 3 | TSENSE_RESET_STATUS | – | No | – |
| 2 | SRST_STATUS | – | No | – |
| 1:0 | DEBUG_RESET_STATUS | – | No | – |

# GCC_RESET_STATUS Definition (check each platform SWI) (cont.)

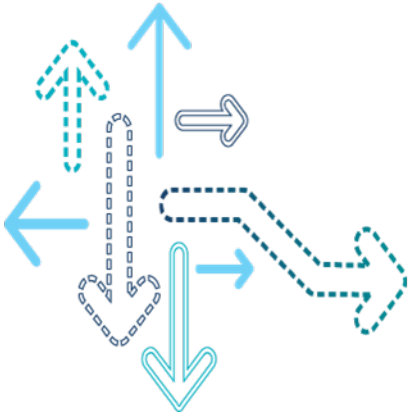
- For example:
  - GCC_RESET_STATUS = 0x23 → Secure Watchdog Bite
  - GCC_RESET_STATUS = 0x13 → PMIC Abnormal Reset
  - GCC_RESET_STATUS = 0x1B → TSENSE Reset (Temperature Sensor Triggered Reset)
  - GCC_RESET_STATUS = 0x0 → Non-MSM triggered Reset

# PON_WARM_RESET Status

```
7 KPDPWR_N Triggered from new KPDPWR press
0x1: TRIGGER_RECEIVED
6 CBLPWR_N Triggered from CBL_PWR1_N
0x1: TRIGGER_RECEIVED
5 PON1 Triggered from PON1
0x1: TRIGGER_RECEIVED
4 USB_CHG Triggered from USB charger
0x1: TRIGGER_RECEIVED
3 DC_CHG Triggered from DC charger
0x1: TRIGGER_RECEIVED
2 RTC Triggered from RTC
0x1: TRIGGER_RECEIVED
1 SMPL Triggered from SMPL
0x1: TRIGGER_RECEIVED
0 HARD_RESET Triggered from a Hard Reset event (check)
```

- PON_WARM_RESET_REASON1: 0x4 : Triggered by PMIC watchdog reset
- Also need to check PON_RESON and POFF_REASON

# Others



# Thermal Reset

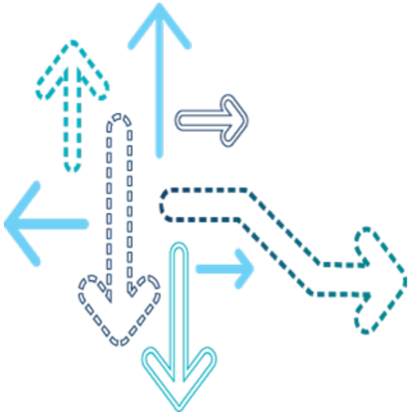
- For thermal reset, please check the thermal tuning.

# PMIC Abnormal Reset

- For PMIC abnormal reset, PMIC software and hardware team need monitor signals and check code/schematics

# References

| Acronym or term | Definition |
|---|---|
| TZ | TrustZone |
| QTI | Qualcomm Technologies, Inc. |
| PMIC | Power Management Integrated Circuit |
| NOC | Network of Connection |
| SMMU | System Memory Management Unit |
| XPU | External Protection Unit |
| AHB | Advanced High performance Bus |
| DDR | Double Data Rate sdram |
| HLOS | High Level Operation system |
| ECC | Error Correcting Code |
| OOM | Out of Memory |
| RPM | Resource Power Manager |
| SLPI | Serial Link Phy Interface |



# Questions?

**https://createpoint.qti.qualcomm.com**