7th UCAAT User Conference on Advanced Automated Testing

ETSI

Bordeaux, 22-24 October 2019

Protocol Conformance Testing for 4G/5G soft-UEs

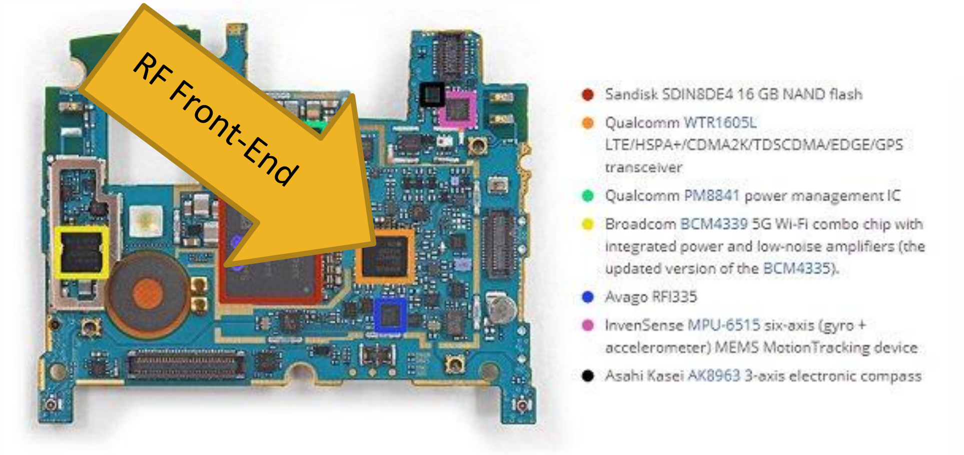
Andre Puschmann, Paul Sutton, Ismael Gomez

SRS LTE

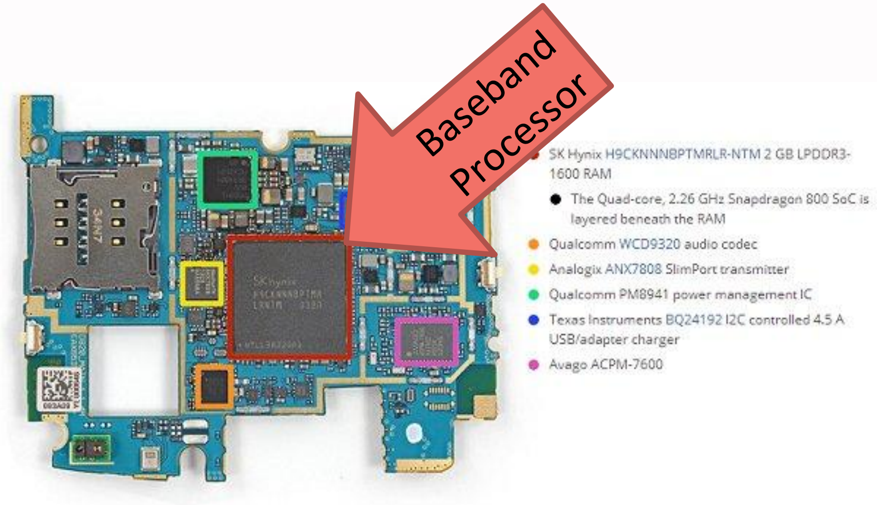
Agenda

- Introduction
- What’s srsLTE and srsUE?
- srsUE Protocol Conformance Testing

An off-the-shelf handset

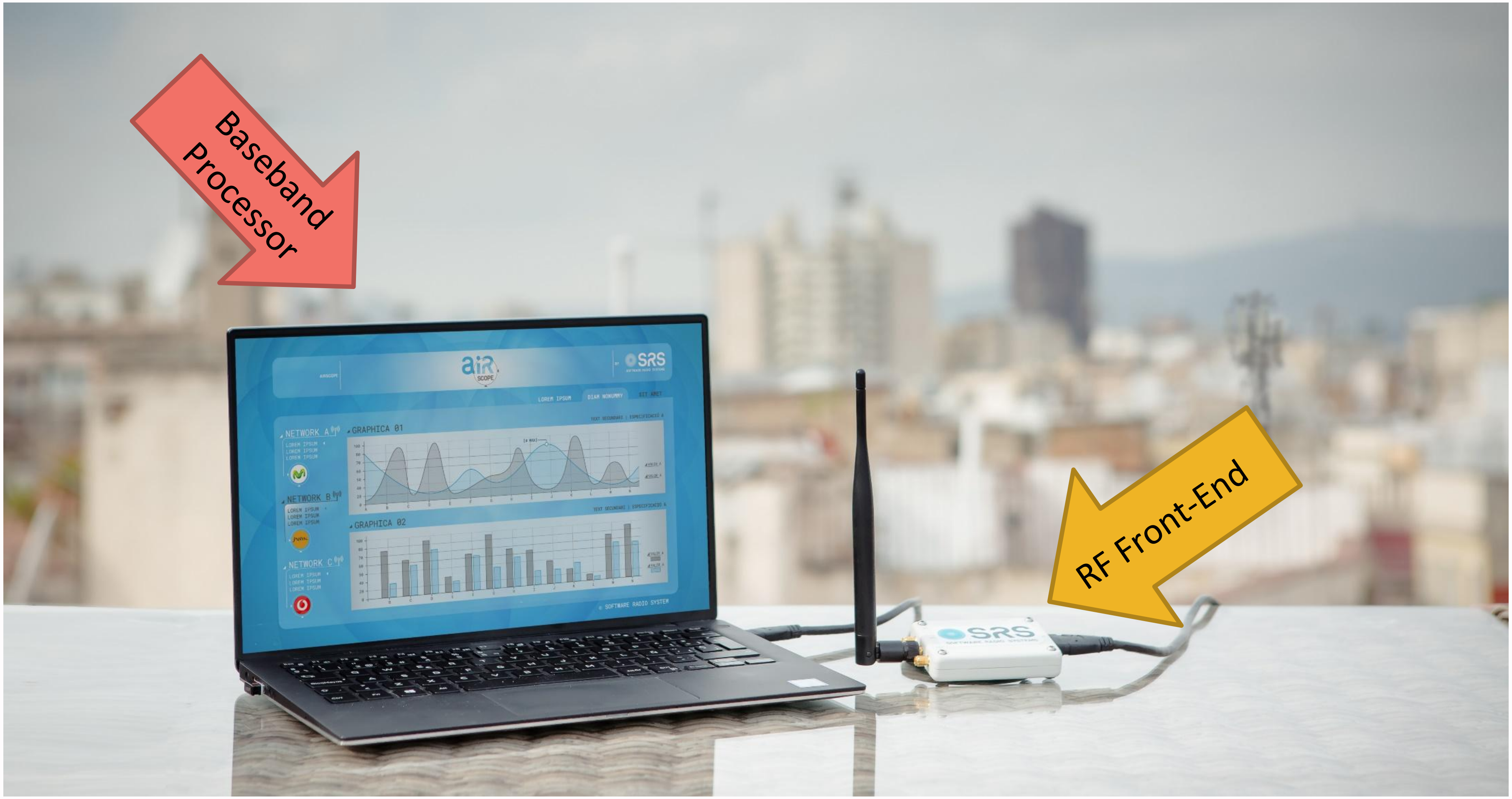


- 🔴 Sandisk SDIN8DE4 16 GB NAND flash
- 🟠 Qualcomm WTR1605L LTE/HSPA+/CDMA2K/TDSCDMA/EDGE/GPS transceiver
- 🟢 Qualcomm PM8841 power management IC
- 🟡 Broadcom BCM4339 5G Wi-Fi combo chip with integrated power and low-noise amplifiers (the updated version of the BCM4335).
- 🔵 Avago RFI335
- 🟣 InvenSense MPU-6515 six-axis (gyro + accelerometer) MEMS MotionTracking device
- ⚫ Asahi Kasei AK8963 3-axis electronic compass



- 🔴 SK Hynix H9CKNNN8PTMRLR-NTM 2 GB LPDDR3-1600 RAM
  - ⚫ The Quad-core, 2.26 GHz Snapdragon 800 SoC is layered beneath the RAM
- 🟠 Qualcomm WCD9320 audio codec
- 🟡 Analogix ANX7808 SlimPort transmitter
- 🟢 Qualcomm PM8941 power management IC
- 🔵 Texas Instruments BQ24192 I2C controlled 4.5 A USB/adapter charger
- 🟣 Avago ACPM-7600

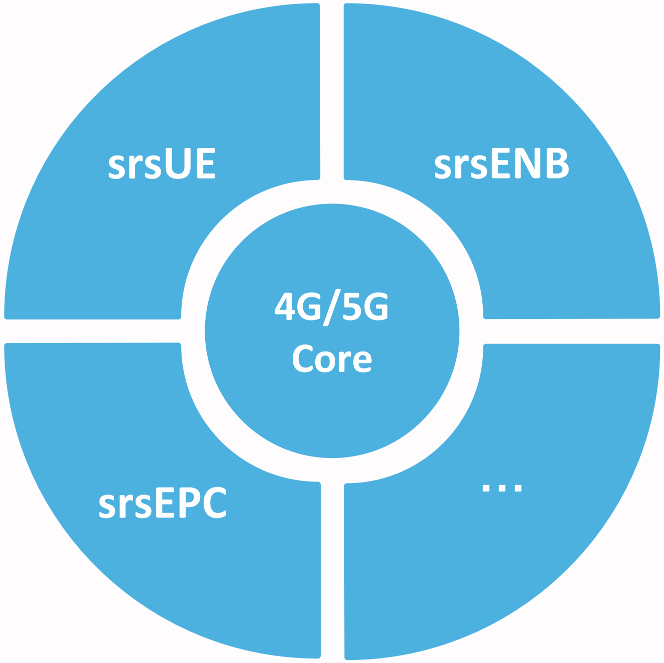
A Software Defined Radio



The srsLTE Eco-System

"Open-source 4G/5G software radio suite"

- Core 4G/5G library
  - Modular and portable, high-performance library for PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, NGAP, SDAP and GW
  - All bandwidths up to 20 MHz, TM1-4
  - Highly optimized Turbo decoder for Intel SSE4.1/AVX (+150Mbps in TM3/4)
- Applications
  - srsUE: First open-source SDR LTE UE
  - srsENB: A complete SDR LTE eNodeB application
  - srsEPC: A light-weight LTE core network
  - airScope: passive air-interface analyzer (not FOSS)



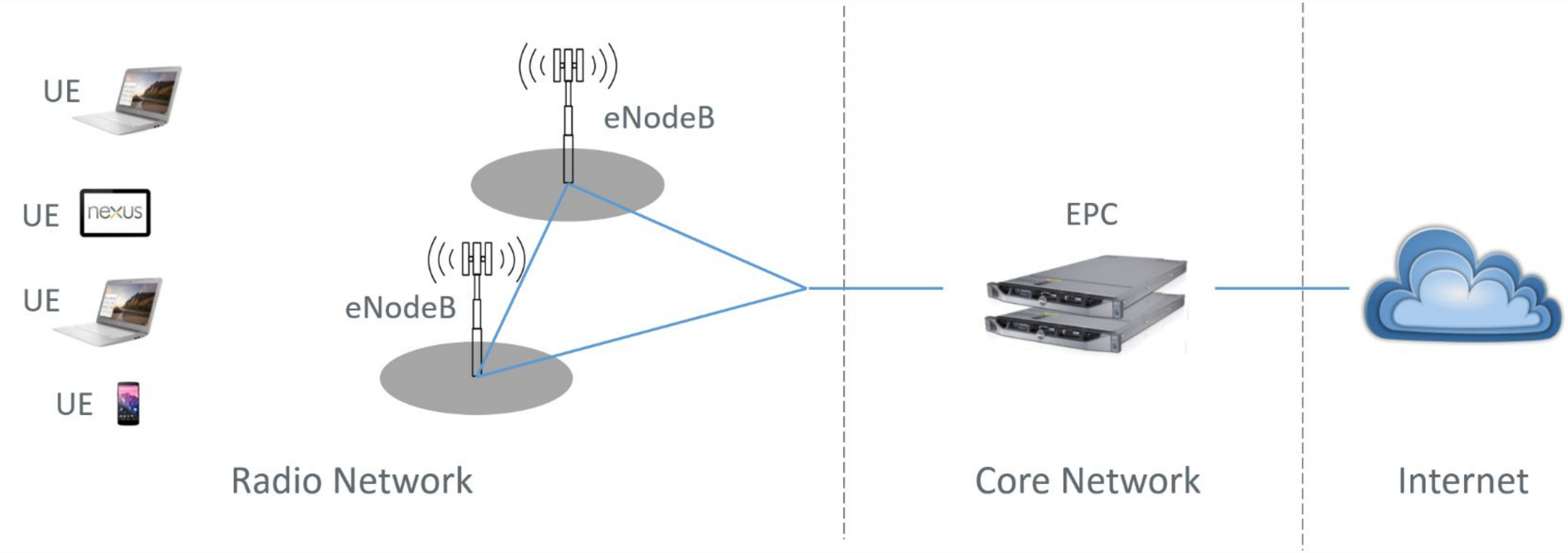
www.srslte.com

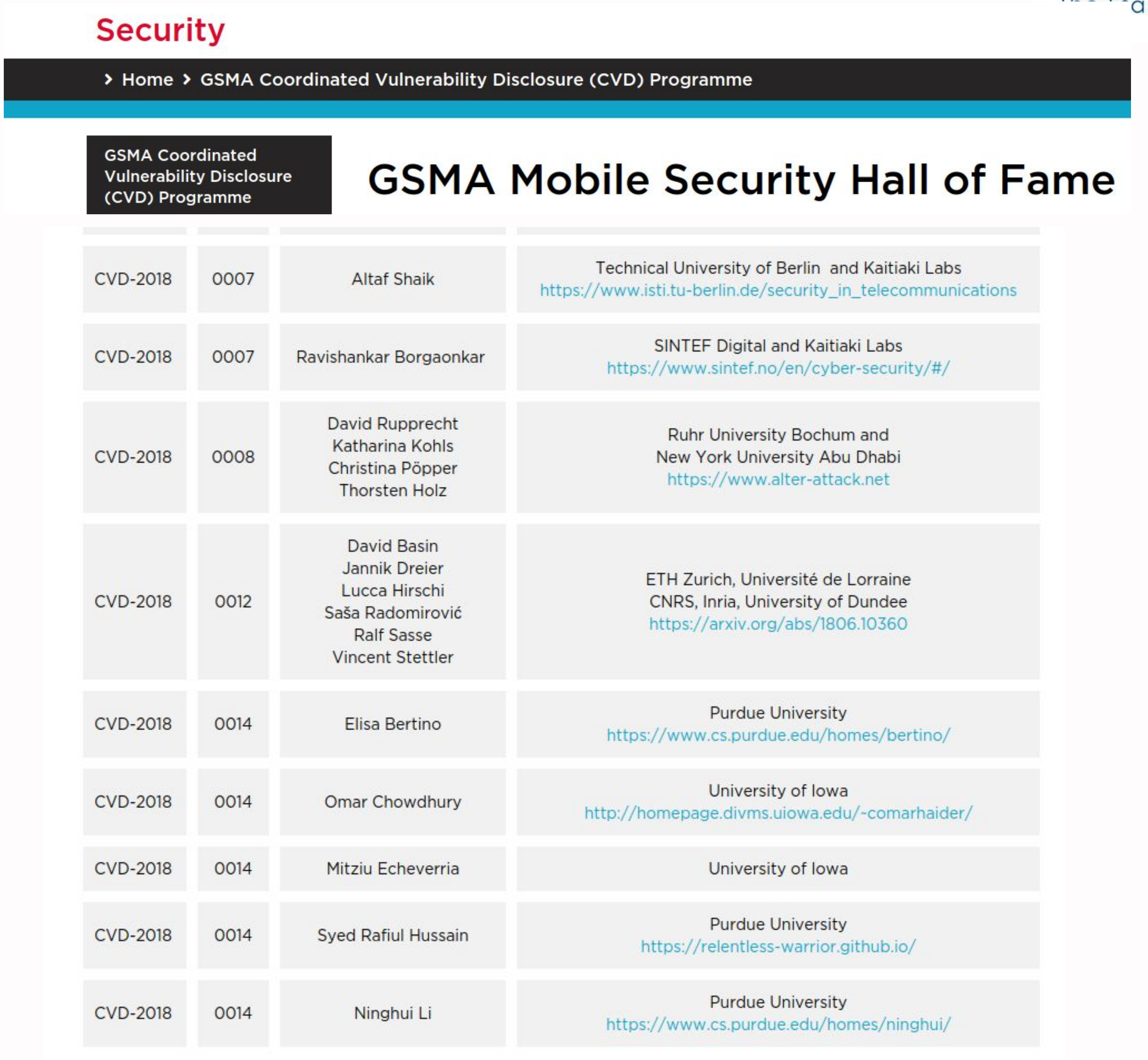
A Full E2E Open-Source Open LTE Solution

SRS UE

SRS ENB

SRS EPC





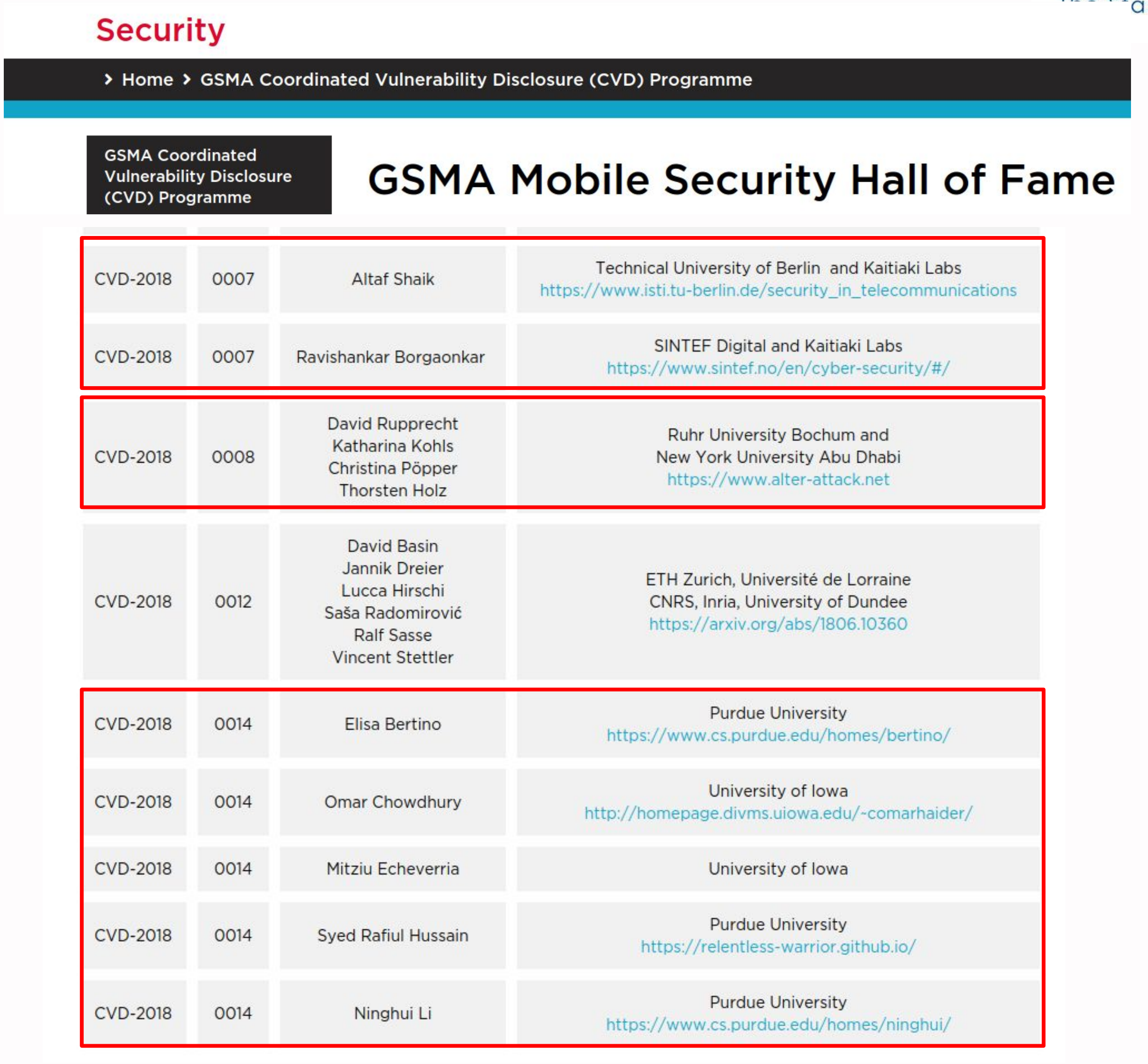
Security

› Home › GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2018	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2018	0007	Ravishankar Borgaonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	0012	David Basin Jannik Dreier Lucca Hirschi Saša Radomirović Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omar Chowdhury	University of Iowa http://homepage.divms.uiowa.edu/~comarhaider/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/



Security

› Home › GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Coordinated Vulnerability Disclosure (CVD) Programme

GSMA Mobile Security Hall of Fame

CVD-2018	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
CVD-2018	0007	Ravishankar Borgaonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/
CVD-2018	0008	David Rupprecht Katharina Kohls Christina Pöpper Thorsten Holz	Ruhr University Bochum and New York University Abu Dhabi https://www.alter-attack.net
CVD-2018	0012	David Basin Jannik Dreier Lucca Hirschi Saša Radomirović Ralf Sasse Vincent Stettler	ETH Zurich, Université de Lorraine CNRS, Inria, University of Dundee https://arxiv.org/abs/1806.10360
CVD-2018	0014	Elisa Bertino	Purdue University https://www.cs.purdue.edu/homes/bertino/
CVD-2018	0014	Omar Chowdhury	University of Iowa http://homepage.divms.uiowa.edu/~comarhaider/
CVD-2018	0014	Mitziu Echeverria	University of Iowa
CVD-2018	0014	Syed Rafiul Hussain	Purdue University https://relentless-warrior.github.io/
CVD-2018	0014	Ninghui Li	Purdue University https://www.cs.purdue.edu/homes/ninghui/

Towards srsUE Protocol Conformance Testing

- Motivation
  - Protocol and signaling conformance to 3GPP specifications
  - Interoperability
  - Regression testing
  - Extend current in-house testing

- Challenges
  - Very dynamic code base
  - Only interested in L2/L3 testing (full UE is out of scope here)
  - Integration into CI is a must

Typical Test Systems Don’t Fit

ME7873L
LTE RF Conformance Test System

- Too big, expensive, heavy and noisy
- No protocol-only testing
- Bad support for older devices

Eclipse TITAN

- Complete, full-featured TTCN-3 toolset developed by and widely used within Ericsson
- Released under Eclipse Public License (EPL) 1.0 in 2014
- Command line tools for compiling, executing and analysing functional and performance tests (generates native C++ code for GCC)
- Built-in codec generators for ASN.1 BER, JSON, XML, RAW
- GUI plugin for Eclipse with Executer and LogViewer
- Many testports also available under EPL 1.0 (e.g. TCP/UDP, telnet, SCTP, PCAP, SIP)
- 1.6 MLoC C++, 3kLoC in Java

Solution: Port 3GPP UE Testsuite to TITAN (+srsLTE)

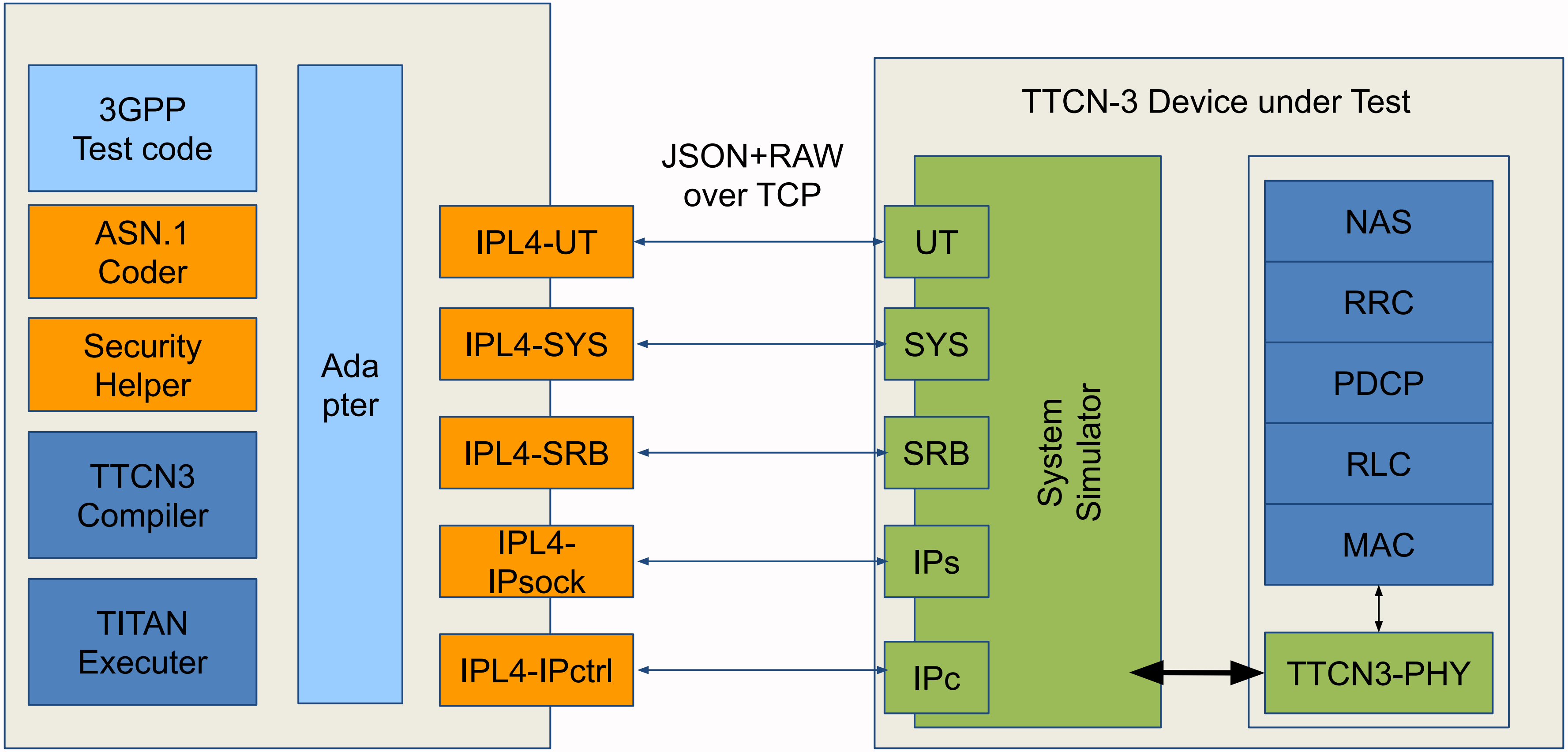
Goals:

- Develop SW to use 3GPP tests to test higher protocol layers of srsUE
- Full CI/CD integration to execute with every pull-request

Steps:

1. Declare testports (TTCN-3 to SS to DUT)
2. Implement codecs (e.g. ASN1 BER to PER converter, decorate type definitions for RAW codec)
3. Implement external function (e.g. security)
4. Design+Implement SS and soft-PHY for DUT

System Architecture



Minor Modification	Major Modification	From Scratch	Unmodified

The NAS Codec Dilemma

- Titan (<= 6.3) incapable of decoding NAS PDUs (from ETSI test suites)
- RAW codec cannot generate unpacker for mandatory fields in, e.g., ATTACH_REQUEST, with format LV (length and value but no type)

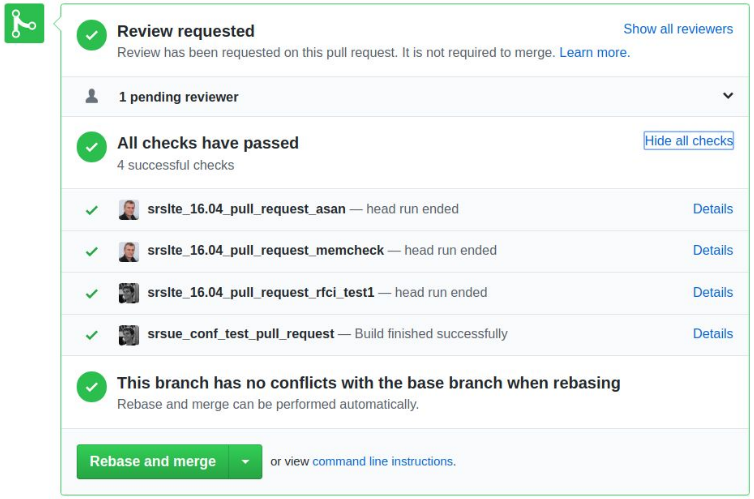
```
type record ESM_MessageContainer {               /* 24.301 cl. 9.9.3.15 */
  IEI8_Type                   iei      optional, /* present in case of TLV; omit in case of LV */
  INT16b                      iel,
  octetstring                 esmPdu   optional  /* ESM PDU without NAS security header;       */
} with {
  encode "RAW"
  variant (iel) "LENGTHTO(esmPdu)";
};
```

- Ericsson provided internal EPS-NAS Definitions as 1st solution (now FOSS)
- Dilemma: Use those new types or make code generator work
- SRS filed bug, sketched possible solution and provided working hack
- Ericsson provided fix for RAW codec with new FORCEOMIT keyword

CI/CD Integration

- Pull-request hook in Github

- Executed in Jenkins
  - Podman containers running TITAN and srsUE
  - Result collection with per-TC TITAN log and srsUE log and PCAP



Review requested Show all reviewers
Review has been requested on this pull request. It is not required to merge. Learn more.

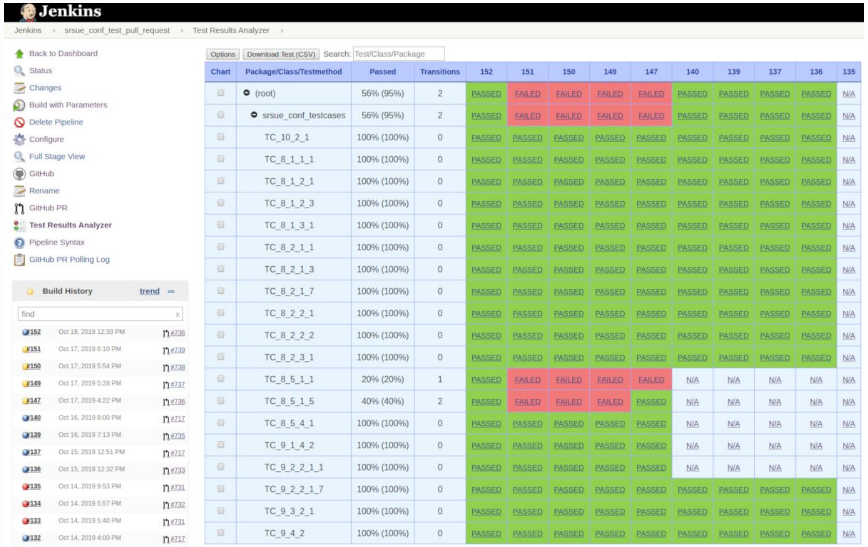
1 pending reviewer

All checks have passed Hide all checks
4 successful checks

✓	**srslte_16.04_pull_request_asan** — head run ended	Details
✓	**srslte_16.04_pull_request_memcheck** — head run ended	Details
✓	**srslte_16.04_pull_request_rfci_test1** — head run ended	Details
✓	**srsue_conf_test_pull_request** — Build finished successfully	Details

This branch has no conflicts with the base branch when rebasing
Rebase and merge can be performed automatically.

Rebase and merge ▾ or view command line instructions.



Jenkins

Jenkins › srsue_conf_test_pull_request › Test Results Analyzer ›

Build History trend

find

#152	Oct 18, 2019 12:33 PM	#736
#151	Oct 17, 2019 6:10 PM	#739
#150	Oct 17, 2019 5:54 PM	#738
#149	Oct 17, 2019 5:28 PM	#737
#147	Oct 17, 2019 4:22 PM	#736
#140	Oct 16, 2019 8:00 PM	#717
#139	Oct 16, 2019 7:13 PM	#735
#137	Oct 15, 2019 12:51 PM	#717
#136	Oct 15, 2019 12:32 PM	#733
#135	Oct 14, 2019 9:53 PM	#731
#134	Oct 14, 2019 5:57 PM	#732
#133	Oct 14, 2019 5:40 PM	#731
#132	Oct 14, 2019 4:00 PM	#717

Options | Download Test (CSV) | Search: Test/Class/Package

Chart	Package/Class/Testmethod	Passed	Transitions	152	151	150	149	147	140	139	137	136	135
☐	(root)	56% (95%)	2	PASSED	FAILED	FAILED	FAILED	FAILED	PASSED	PASSED	PASSED	PASSED	N/A
☐	srsue_conf_testcases	56% (95%)	2	PASSED	FAILED	FAILED	FAILED	FAILED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_10_2_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_1_1_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_1_2_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_1_2_3	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_1_3_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_1_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_1_3	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_1_7	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_2_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_2_2	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_2_3_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_8_5_1_1	20% (20%)	1	PASSED	FAILED	FAILED	FAILED	FAILED	N/A	N/A	N/A	N/A	N/A
☐	TC_8_5_1_5	40% (40%)	2	PASSED	FAILED	FAILED	FAILED	PASSED	N/A	N/A	N/A	N/A	N/A
☐	TC_8_5_4_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	N/A	N/A	N/A	N/A	N/A
☐	TC_9_1_4_2	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	N/A	N/A	N/A	N/A	N/A
☐	TC_9_2_2_1_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	N/A	N/A	N/A	N/A	N/A
☐	TC_9_2_2_1_7	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_9_3_2_1	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A
☐	TC_9_4_2	100% (100%)	0	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	PASSED	N/A

Conclusion and Results

- Basic SS and DUT under AGPLv3 in srsLTE 19.09
  - Unmodified srsUE upper layers
  - Complete RRC/NAS test model
  - MAC/RLC/PDCP model work-in-progress
  - 5GNR EN-DC Inter RAT work-in-progress
- Full CI/CD integration
- TTCN-3 tester/testports, protocol codecs, security helpers, 3GPP testsuite patch for TITAN not FOSS (License for ETSI code?)

Sources and Further Reading

- https://www.netdevconf.org/2.2/session.html?welte-ttcn3-talk
- http://www.ttcn-3.org/
- https://dl.cdn-anritsu.com/en-en/test-measurement/files/Product-Introductions/Product-Introduction/me7873l-el11300.pdf
- http://www.sharetechnote.com/html/LTE_Protocol_CT.html
- "Assessing Compliance of 5G Device Implementations To 3GPP Standards" by Olivier Genoud, ETSI (https://docbox.etsi.org/Workshop/2018/201812_ETSI_OAI/WORKSHOP/SESSION03/ETSI_GENOUD.PDF)
- https://www.3gpp.org/ftp/tsg_ran/WG5_Test_ex-T1/TTCN/Deliveries/TTCN3/

Thanks!

Backup slides

EUTRAN Test System Architecture

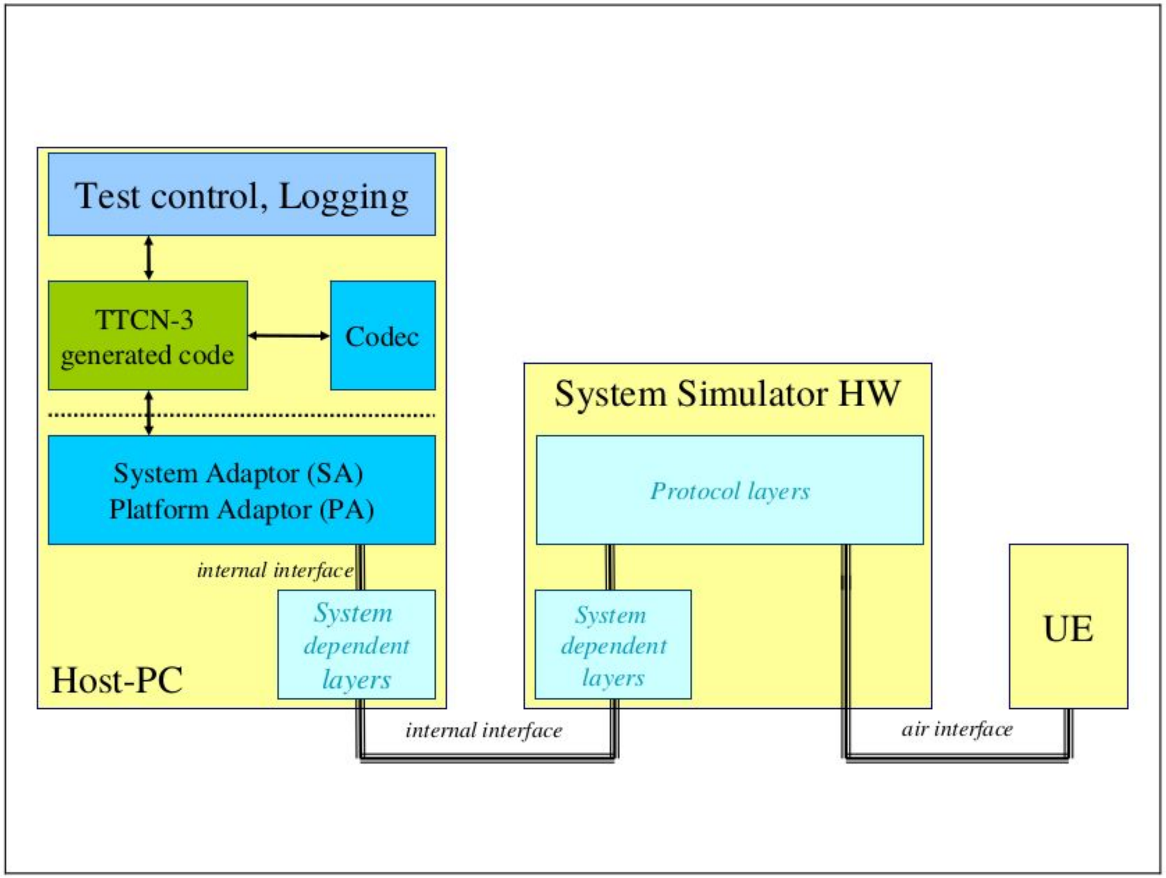


Figure 4.1.1-1: Architecture of system simulator

Source: TS 36.523 v8.6.0

srsLTE Testing (1)

- Static code analysis (SA)
  - Using Coverity and cppcheck
- Unit tests (UT)
  - Executed periodically in AWS Jenkins (i.e. make test)
  - Mostly PHY layer, and partly common (e.g. RLC)
  - Very limited for UE upper layers, (almost) non for eNB/EPC
  - Valgrind checks and address sanitizer runs (ctest memcheck)

srsLTE Testing (2)

- RF Conformance (TS 36.521)
- Protocol Conformance (TS 36.523)
  - 3GPP has defined entire conformance test architecture and conformance test cases based on TTCN3
- Pre-IOT Testing
  - RF continuous-integration (RF-CI)
  - Customer
- Interoperability Testing (IOT)
  - Carried out manually in the field in a live network