
RRS mutability model as a template for 5G longevity

How mutable end-devices will impact 5G security

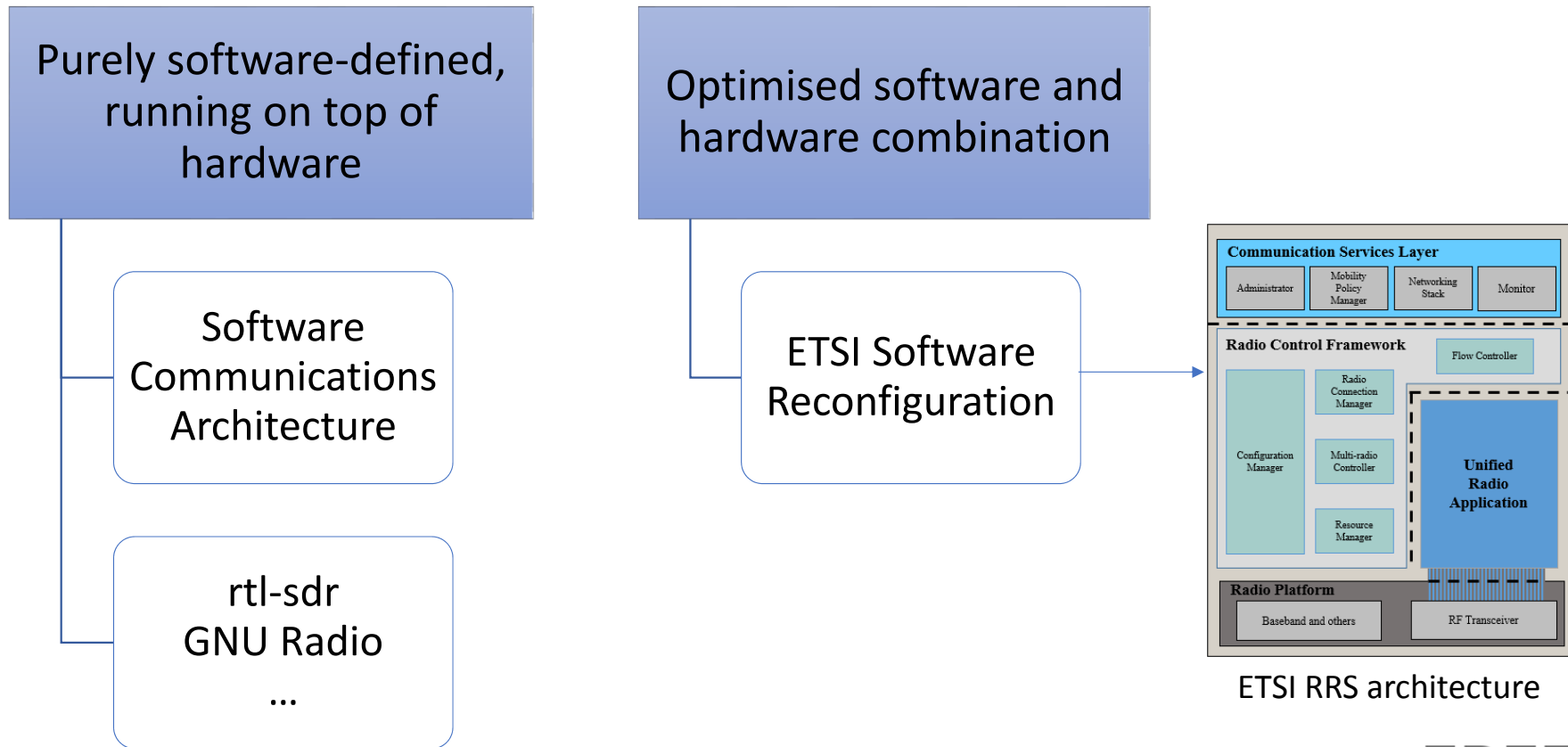
François Ambrosini

Outline

- Reconfigurable Radio Systems
- From radio to device virtualisation in 5G and beyond
- Consequences to the 5G trust model
- Addressing the new model
- One example: application of language-theoretic security
- Final note

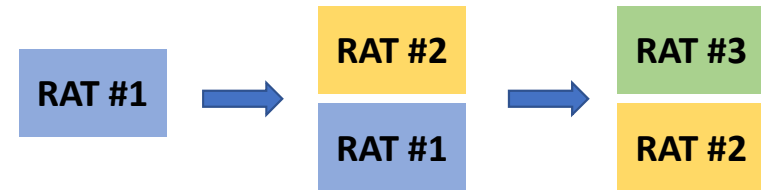
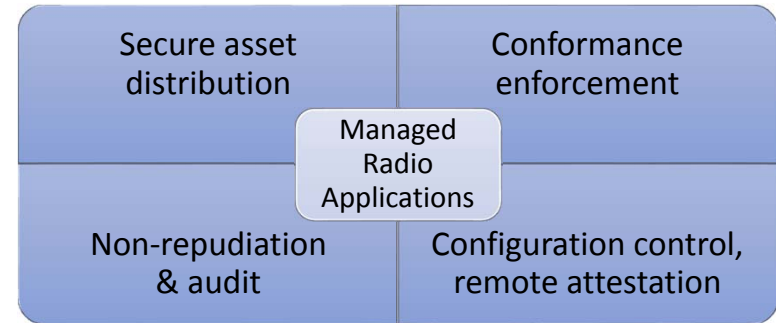
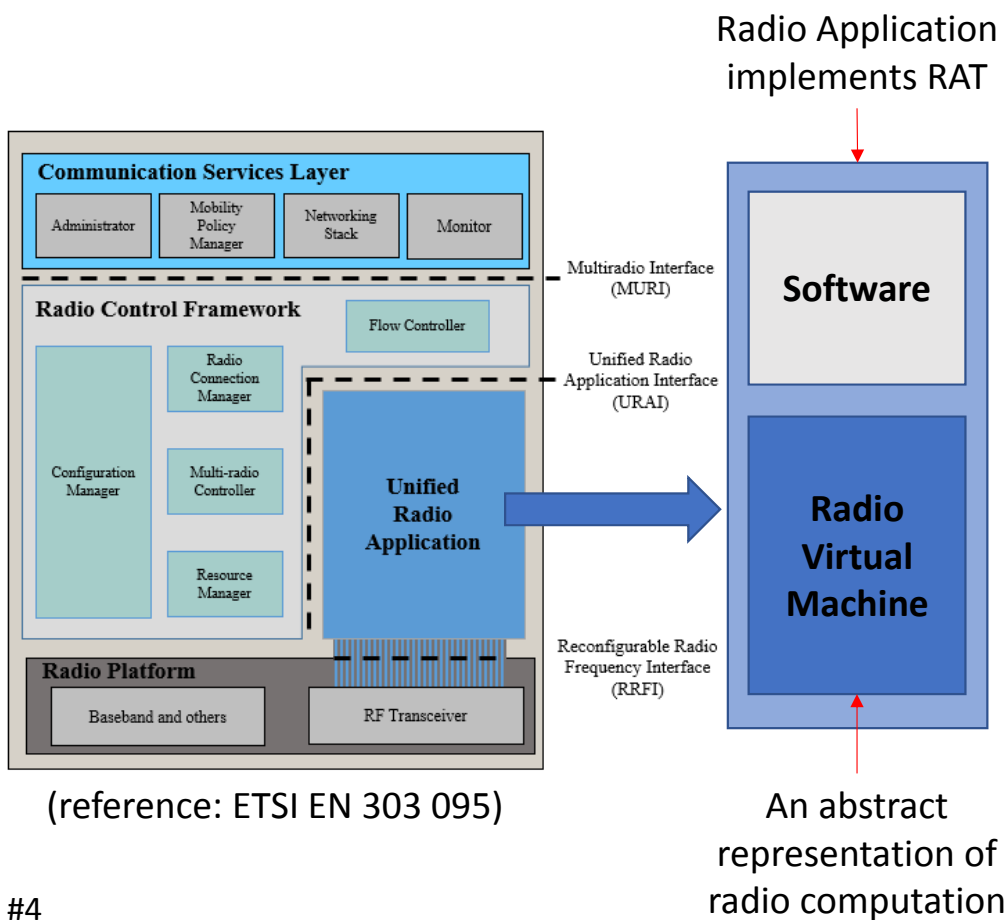
RRS: Reconfigurable Radio Systems

A type of software defined radio (SDR) for mobile devices



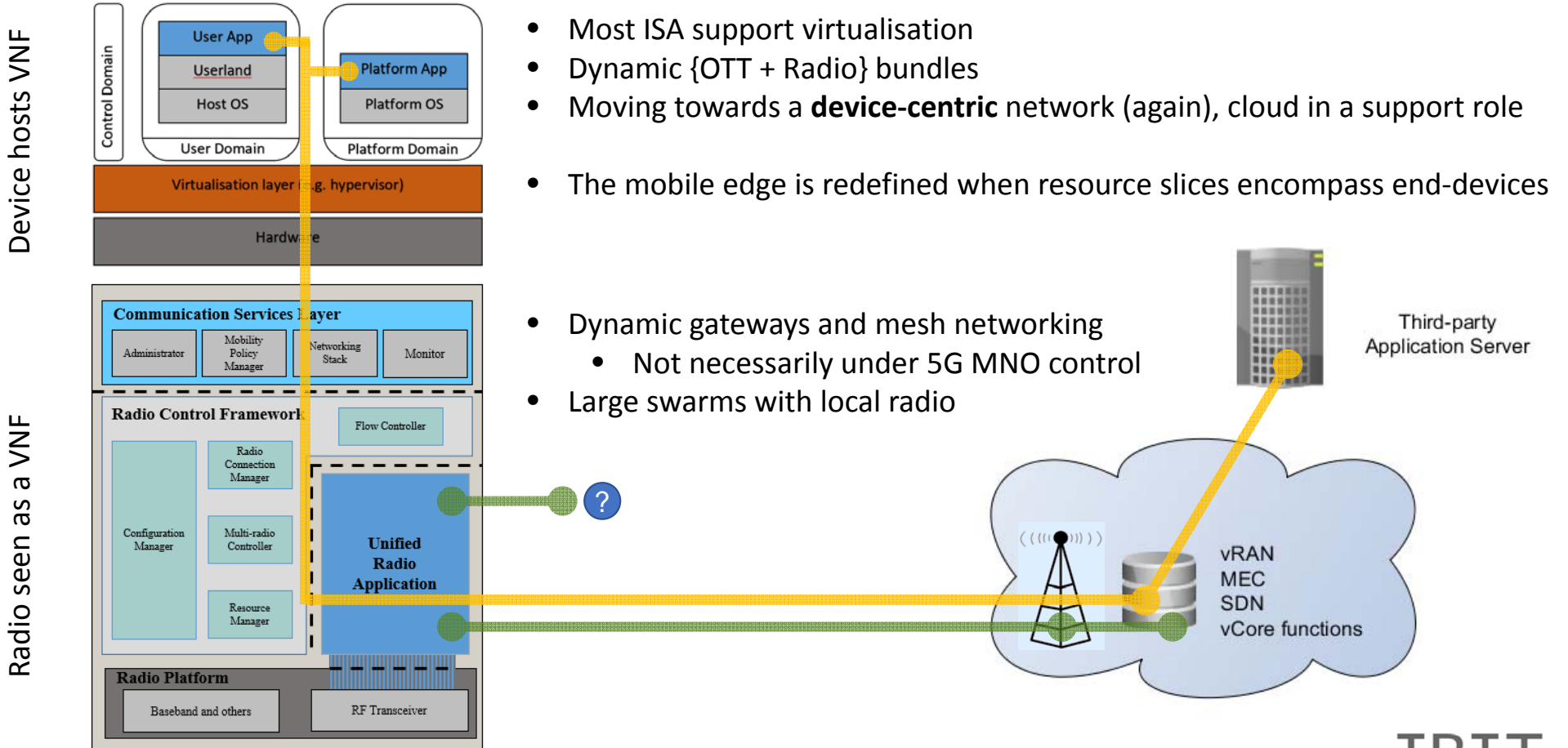
RRS: Reconfigurable Radio Systems

A control framework for radio devices



Benefits	network agility, radio upgrade on both ends
	less legacy, long-term management
Example	from DSCR update to 3GPP in the vehicular domain

From radio to device virtualisation in 5G and beyond



- Most ISA support virtualisation
- Dynamic {OTT + Radio} bundles
- Moving towards a **device-centric** network (again), cloud in a support role
- The mobile edge is redefined when resource slices encompass end-devices
- Dynamic gateways and mesh networking
 - Not necessarily under 5G MNO control
- Large swarms with local radio

Consequences to the 5G+ trust model

A more active role for end-devices

- To flexible network access, add devices of flexible type
- From potential threat to network component (more than simple tethering)
- How can one **trust** and **certify** a mutable device?

Device entrusted with new classes of decisions

- E.g. traffic characterisation, slice selection, routing, RAT & radio topology selection

Flexible device roles influence network access control

- And a device may start performing access control on behalf of the network

Working assumptions on the device similar to NFV

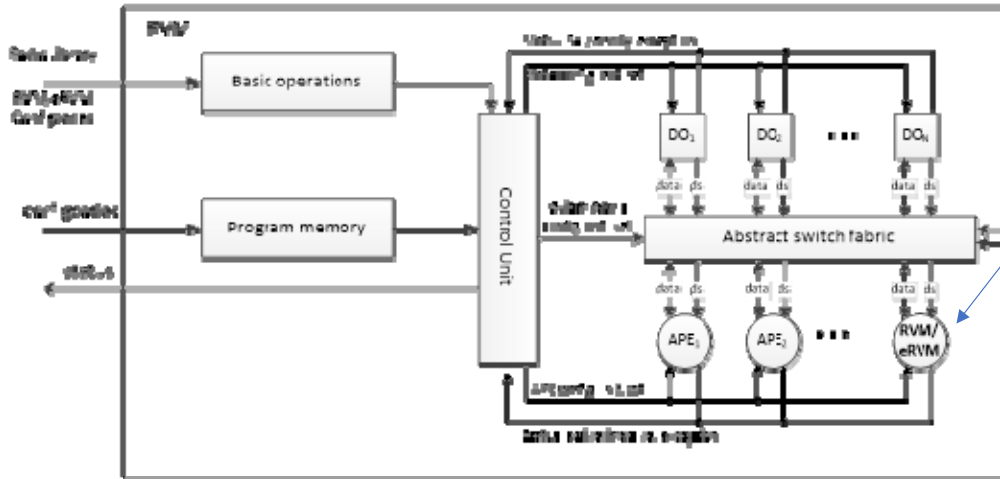
- Multi-tenant model with more challenging physical security

Addressing the new model

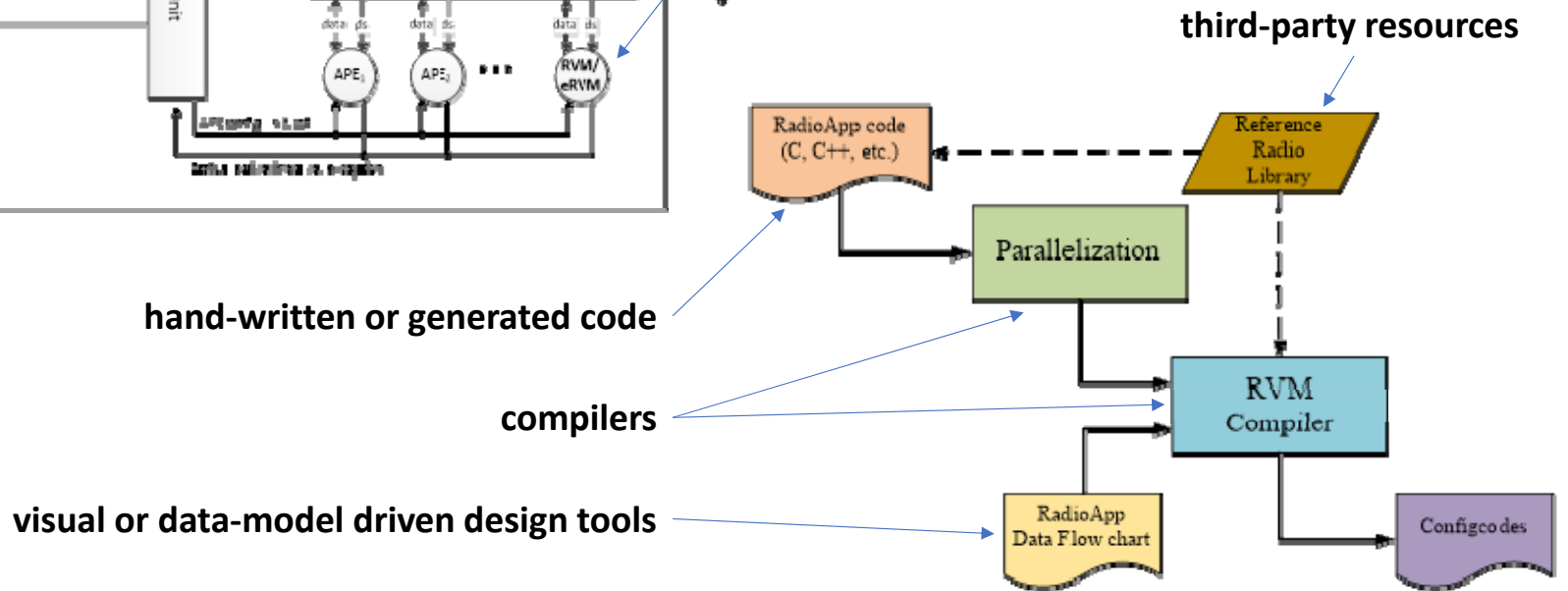
An outlook on future standardisation and research

- Roots of trust on end-devices to be fully leveraged
 - Ensure persistent device identity and parameters while having non-persistent RATs
 - Vertical coordination: cover the whole application stack and extend to third-parties
 - Horizontal coordination
- Expand on certification and protocols to determine conformance
- Large scale hierarchical and distributed remote attestation
 - to support large swarms
- Ontologies for mutable systems
- Temporary authentication in mesh networks
- Expand on strongly secure building blocks
 - Bootstrapping trust in compilers
 - Language-theoretic security & formal proofs

Applying language-theoretic security to RRS



hierarchical structure
the RVM is an input-driven directed graph



hand-written or generated code

compilers

visual or data-model driven design tools

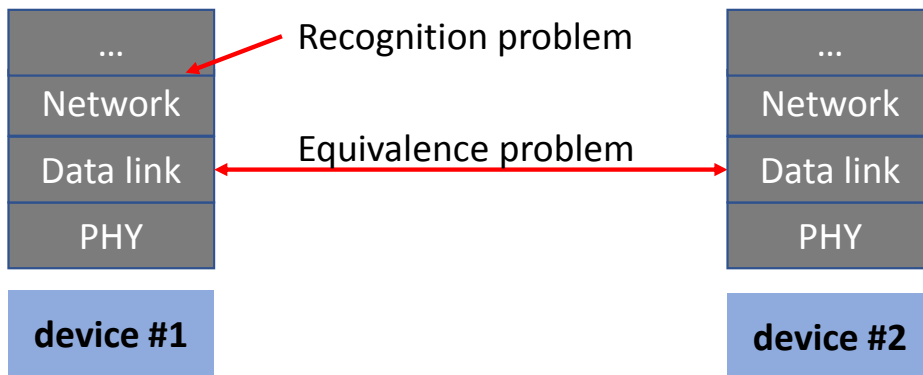
(reference: ETSI EN 303 146-4)

Applying language-theoretic security to the stack

Solvability of the recognition and equivalence problems

At the RVM:

- Ensure isolation of all Data Objects and Abstract Processing Elements
- Avoid processing loops between eRVMs
- RVM becomes a simple (acyclic) directed graph with a finite set of known state
 - Lower complexity than Turing Machine
 - formal proof of security possible



- Push LangSec up the stack
 - At least reduce interface complexity
 - Orthogonal to message security
 - Deter fuzzing at lower layers
- Leverage composition

Final note

The technology is available to allow full virtualisation on end-devices and this transformation will be driven by real usage scenarios. Radio reconfiguration will enable a smooth transition towards 5G but this will in turn result in permanent uncertainty regarding the nature of end-devices, even though such end-device may transform into an infrastructure component. This is part of the problem space we need to address.



Thank you!

Annex: references

- ETSI EN 303 095
 - “Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices ”
- ETSI TS 103 146-4
 - “Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 4: Radio Programming Interface (RPI)”
- Vladimir Ivanov, Seungwon Choi, Markus Mueck,
 - “Radio Virtual Machine, Virtual machine for reconfigurable radio”, ETSI workshop on future radio technologies – air interfaces, January 27-28 2016
- ETSI TR 103 502
 - “Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks; Security aspects”