NFV / SDN RAM* Standards Discussion

IEEE SRPSDVE Study Group
October 29, 2014

Rob Paterson

KerrNet Consulting Inc

Ottawa, Canada

**** RAM = Reliability, Availability, Maintainability***

Agenda

1. **NFV/SDN IEEE RAM Standards Scope**
2. **Drivers for Change**
3. **Areas for Standardization**

CSP: Communications Service Provider
DoS: Denial of Service
GR: General Requirement
HW: Hardware
ISV: Independent Software Vendors
M2M: Machine-to-Machine
NE: Network Element
NEP: Network Equipment Provider
NFV: Network Functions Virtualization
OAM: Operations, Administration, Management
PSTN: Public Switched Telephone Network
R/A: Reliability/Availability
SLA: Service Level Agreement
SW: Software
VNF: Virtualized Network Function

NFV/SDN RAM Standards Scope

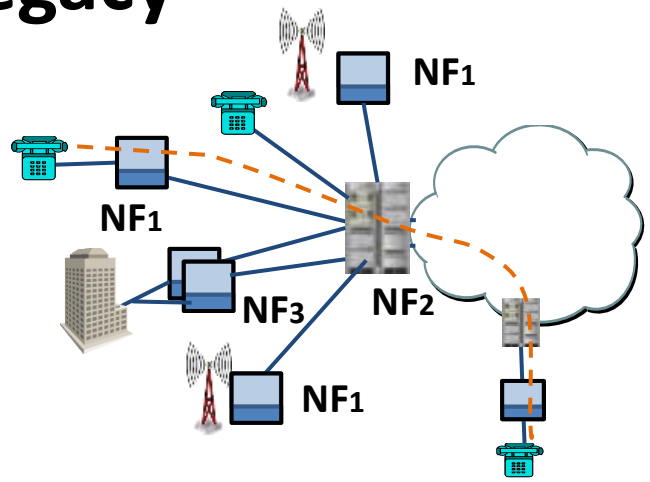
1. **Terminology:** to support consistent communicate of reliability-related NFV/SDN terms
2. **Metrics:** to set requirements/targets, define SLAs and verify compliance
3. **Metric Criteria:** to define service failure, service outage, OAM failure, OAM outage,…
4. **Metric Use Guidelines**: for consistent, repeatable use for setting targets, modeling, calculation, measurement,…
5. **Fault Management Features:** fault handling capabilities used to detect, contain, recovery, alarm, diagnose & repair systems from failures and errors required to implement RAM strategies (i.e. protocols, interfaces, ….)

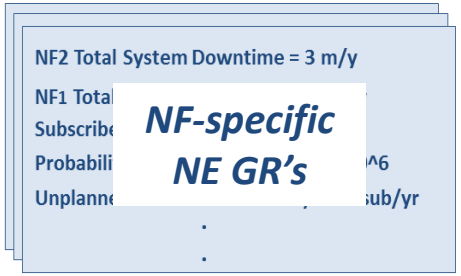
Requirements for new RAM standards depends on gaps between current state and NFV/SDN needs and IEEE SRPSDVE Study Group

KERRNET CONSULTING INC 2014

PSTN: Historical Legacy

- Voice-based services over TDM pre-specified network
- Tight coupling of network functions to NEs, architecture & geography
- Purpose-built hardware running proprietary SW for each network function designed & built in-house
- Circuit-based network where impairment dominated by equipment failures and human errors
- Regulated network with limited competition





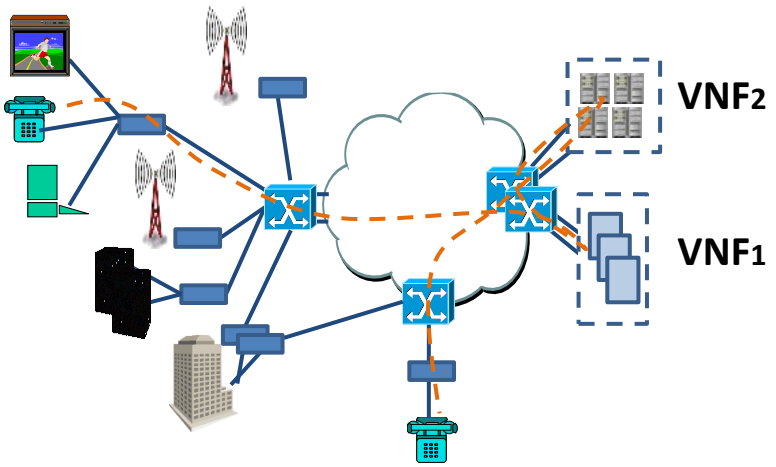
'White box' NE specifications for NEPs enabled Telcos to build PSTN to provide different levels of service R/A within pre-specified PSTN architecture

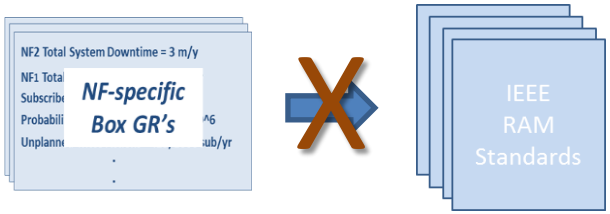
PSTN RAM metrics/targets/criteria derived from and specific to PSTN's service, architecture and technology ("White-box" spec. approach)

KERRNET CONSULTING INC 2014

Emerging Network

- Multi-apps, multi-services over packet network with diverse set of architectural options
- Virtualization de-couples many network functions from HW enabling design and geography flexibility
- Open-source software on standard hardware platforms with proprietary applications are the new NE's
- Connectionless network with virtualized functions with new impairment causes (DoS, congestion, transient HW & SW)
- Security & dynamic traffic management integral to designs
- Increased competition driving new services, TTM & costs

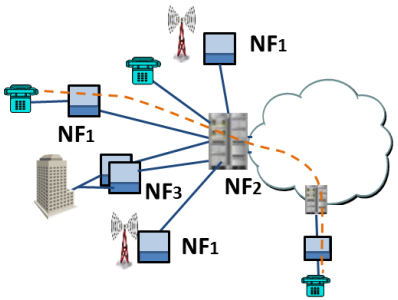


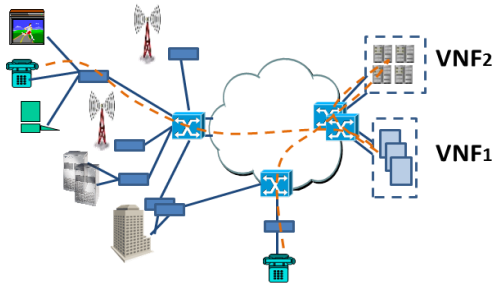


Can no longer transfer NF-specific box metrics to multi-service packet NEs using NFV

Requires over-haul of RAM metrics, targets, criteria, causes and how they are modeled, calculated, measured,… (requires "Black-box" approach

Drivers



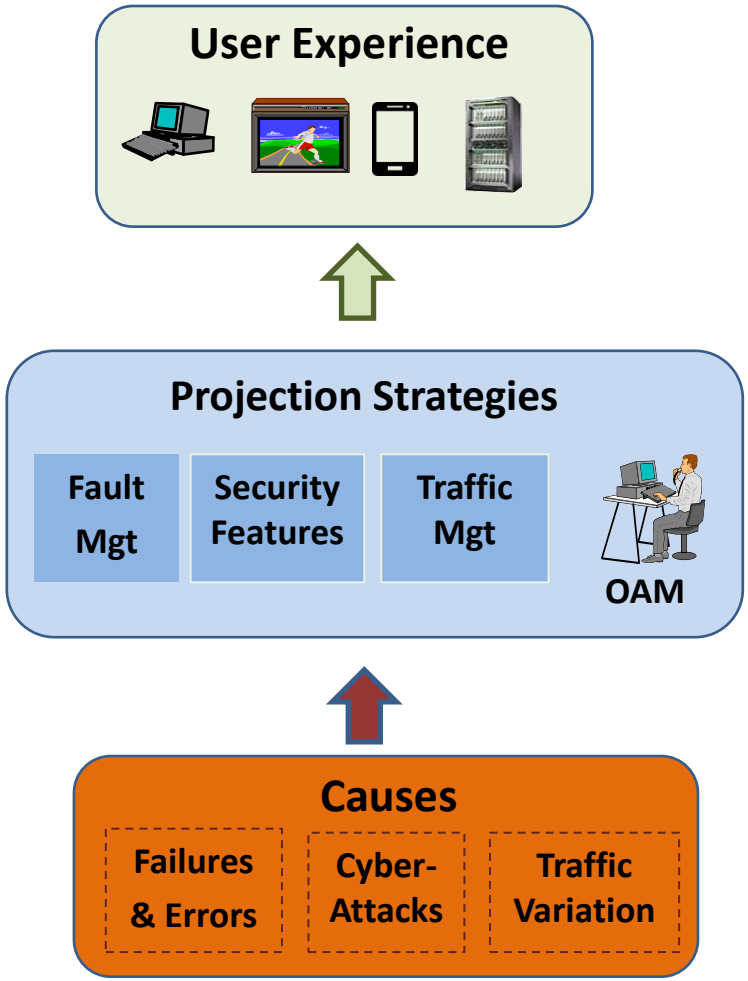


Multiple services over packet network using VNFs	→	User-driven R/A metrics/targets based on service criticality, failure modes, costs
Multi-application services over packet network	→	Performance-based criteria for service failure / outage
De-coupling of NF from hardware with wide NW design flexibility	→	De-couple RAM metrics from equipment to VNF to support design flexibility
Increasing threat to services and network due to new causes	→	Broaden RAM metric causes to include DoS attacks, congestion, ….
Equipment built from ecosystem of ISVs on standard HW platforms	→	Establish metrics hierarchy: service – network – VNF - subsystems

Vestiges of legacy PSTN-derived RAM metrics/targets/criteria still being applied to emerging network in the name of "carrier-grade"

KERRNET CONSULTING INC 2014

RAM - Performance - Security Integration Concept



Service failures, service outages, poor QoE, stolen info, infected user devices, loss of OAM,…

Strategies that prevent or mitigate the threats' impact on both the network and the user experience such as topology, redundancy, provisioning, firewalls, fault, security & traffic mgt protocols and features, and OAM expertise and tools. Goal is to optimize designs to satisfy end-users

Threats to the network and the user experience include failures, errors, attacks, traffic variation that threaten the user experience.

User-driven metrics apply at each level and should not be implemented within the RAM, Security and Performance Silos

Areas for Standardization for Discussion

Overhaul RAM metrics to address multi-service, multi-vendor, packet networking, and virtualization aspects that support not impede benefits of NFV/SDM

RAM Metrics Definitions:

- Re-define RAM metrics based on end-user/end-device perspectives. Requires a service / NF approach based on failure mode impact ("Black-box" or implementation independent)
- Define performance-based criteria for failure & outage for classes of services and OAM
- Update causes to reflect new contributors such as DoS attacks
- Extend current Security metrics from quality-based to RAM-based

RAM Metrics Framework:

- Define metrics hierarchy: network, element, subsystems, and overlay metrics on reference NFV network and VNF architectures for use by CSPs, NEP's, VNF platform vendors, ISVs, …

RAM NFV/SDN Guidelines

- Using the preceding, define a set of guidelines to support the consistent use of standards
  - Deriving RAM targets (largely market-driven)
  - RAM Design Analysis Modeling
  - RAM Field Tracking/Reporting
  - In-service RAM measurement & reporting
  - Setting and measuring RAM SLAs

Need to survey current state to identify gaps, prioritize & schedule

KERRNET CONSULTING INC 2014