IEEE Emerging Technology Reliability Roundtable 2019

August 26-27, 2019

Masala (near Helsinki), Finland

http://cqr.committees.comsoc.org/etr-rt-2019/

Participants' Input to the Roundtable Summary of Findings

Introduction

The scope of the Emerging Technologies Reliability Roundtable (ETR-RT) in the past five (5) years was to:

- Discuss and identify the RAS (Reliability, Availability and Serviceability[1]) challenges, requirements and methodologies in the emerging technology areas like the Cloud Computing, Wireless/Mobility (with focus on 5G technologies), NFV (Network Functions Virtualization), SDN (Software Defined Networking), or similar large-scale distributed and virtualization systems.
- Discuss the RAS requirements and technologies for mission-critical industries (e.g., airborne systems, railway communication systems, the banking and financial communication systems, etc.), with the goal to promote the interindustry sharing of related ideas and experiences.
- Identify potential directions for resolving identified issues and propose possible solution.

This year, ***Serviceability*** *and* ***Reliability-impacted Security*** **aspect** were added in the ETR-RT Scope under ***Resilience,*** which is considered as an "umbrella" topic.

Considering the huge impact of virtualization, programmability and automation, the ETR decided to focus its 2019 event to emerging technology areas like, Wireless/Mobility (with focus on 5G technologies), NFV (Network Functions Virtualization), SDN (Software-Defined Networking), blockchain, and similar large-scale distributed and virtualization systems.

This Roundtable was held on August 26-27. 2019 in Masala (near Helsinki), Finland. It was well balanced with speakers from Telecom Service Providers (AT&T, Cosmote, Orange, Swisscom, Telefonica), Telecom Vendors (Ericsson, Huawei, Nokia), IT companies (BaseN), Research Organizations (VTT), and universities (CQUPT).

[1] Serviceability: Focus on the technology, solutions and platforms which can improve Operation and Maintenance (O&M) ability, including Deployment, Monitoring, Upgrade/Patching, Adjustment, Troubleshooting, Fault Recovery, Data Configuration, etc. The target of Serviceability is to make the O&M work more Easily, Remotely, Automatically and Efficiently in order to achieve Low OPEX and High Customer Satisfaction.

The Speakers addressed various issues and challenges of the upcoming 5G deployment, softwarized infrastructures, and 5G combined with blockchain providing further insight and impact on reliability, serviceability, and security. The talks provided some "food for thoughts" in the common discussion held after each presentation and summarized in the closing discussion for highlighting major issues to address. Most of the topics have been considered by several speakers, which showed some common understanding on resilience (reliability, serviceability, security) challenges, among which:

- Intelligence Resilience for a Converged World
- Spime Containers – Internetworked Digital Twins
- NFV Resiliency and 5G Network Slicing
- Achieving High Performance, Reliability, and Security with Zero Touch 5G
- End-to-end Reliability in Industrial 5G Networks
- Impact of Virtualization on Telecom Network Reliability
- Service Provider Thoughts, Use Cases and Requirements for Reliability
- Automation in the Days of the Software Network
- Holistic Safety Security Approach for Complex Systems
- Innovative Application Analysis of Blockchain + 5G.
- Serviceability Considerations for Reliability Engineers
- AIOps Practice in Network Operation and Maintenance
- Establishing Customer Experience: Aspects in Mobile Network Serviceability.

After the Roundtable, participants were offered the opportunity to provide some further analysis, which is reported hereafter. The Roundtable speakers' and participants' inputs and additional comments indeed well reflect the consensus that was discussed during the Roundtable and they provide an interesting "food for thoughts" for future work in ETR-RT. They are listed below and show some similar concerns.

Serviceability Considerations for Reliability Engineers:

1) The proliferation of network services definition and design at customer finger tips enabled by SDN and NFV transformation

2) This leads to service chaining concept that drives simplicity to users while adding complexity to operators of the networks

3) More software, open source SW, adding challenges to integration testing from end-to-end (E2E) point of view, a must to ensure the service quality

4) Industry is moving from network reliability model to E2E service resiliency model

5) This leads to revolutionary changes in BSS/OSS, network control and configuration functions, as well as network and service orchestration flows

6) Enterprise-wide data model and data dictionary are the pillars for successful service chaining and effective service monitoring

7) True E2E Service Quality Management (SQM) requires completely different approach and platform capabilities

8) Application and service transaction-based traceability is also a must to ensure SLA

9) End-user experience quality will be an added metric to drive improvements

10) New operating model with operator, vendor, suppliers requires digital fingerprints shared across multiple companies yet protected

11) Cyber security needs to penetrate along the vertical stack, as well as at service level horizontally

12) Concept of Software Reliability Engineer and future talents/skills to ensure service quality into future.

NFV Resiliency and 5G Network Slicing:

1) 5G slicing planned to be based on the NFV framework which constitutes a (completely) new resiliency challenge due to, for example, presence of multi layers and multi vendors, use of COTs

2) How to deal with both resources sharing between slices (e.g., for costs purposes), and isolation requirements (e.g., for failure containment objectives)?

3) Automatic scaling, an attractive feature of virtualization, needs to be managed/controlled, (e.g., against undesirable traffic such as DDoS)

4) Containerization is expected to bring more agility to NFV deployment although some resiliency side effects need to be carefully analyzed (e.g., presence of OS SPoF, absence of software diversity)

5) 5G reliability/availability requirements expressed by some verticals, e.g., "Availability higher than six-nines" → such objectives have never been reached before by communication service providers.

Achieving High Performance, Reliability, and Security with Zero Touch 5G:

1) 5G enables speed, massive scale and ultra-reliable, low-latency services

2) These are offered using a virtualized, highly distributed architecture for both RAN and Core

3) High availability SDN and NFV design principles can be applied to Core components

4) New RAN capabilities include IAB, RIC and MEC further enhance performance, reliability and security.

Impact of Virtualization on Telecom Network Reliability:

1) Both 5G and virtualization are setting some new challenges to reliability engineers working in the telecom industry. Specifically:

   - Mission-critical use cases increase
   - Higher frequencies and higher power levels - Focus from HW to SW
   - From simple reliability block diagrams to deep understanding of functionality
   - OSS and third-party SW

2) Virtualization brings some good news:

   - More controlled use environment
   - Possibility to increase redundancy w/o any significant HW cost
   - IoT creates a huge amount of data that can help in improving reliability
   - Data analytics help to prevent and analyze failures.

Service Provider Thoughts, Use Cases and Requirements for Reliability:

1) Due to high cost for reliability, can we use that for differentiated contracts? How to monetize reliability/availability?

2) Reliability is getting more important for customers. How do we measure/prove that our network is reliable?

3) New technologies like Cloud-native enable different ways of doing reliability. Requires network-wide support for cloud-native for end-to-end reliability.

4) Software and Open Source have an inherent risk of failure due to a single implementation. How can we mitigate that (automated live testing?)

5) Operational people need to trust any reliability mechanisms. How do we create that trust?

Holistic Safety Security Approach for Complex Systems

Here are some points that need further discussion in ETR-RT and other fora:

1) Security and safety are both contributing to the system's resilience
   - Security is more complex and dynamic than safety
   - Can we integrate security and safety assessments?
   - Can we use similar methods and tools?
2) A combined fault and threat detection AI-based overseer system
   - Unsupervised, data driven and able to sense abnormal conditions
   - Supervised, simulation-based, able to predict and detect specific threats, faults, human errors
3) Modelling and monitoring humans of a system
   - Consider cases where an attacker has appropriate access rights
   - Consider privacy/ethics.

AIOps Practice in Network Operation and Maintenance

1) AI can help much in O&M assistant, but not means all in current stage
2) Model, Knowledge/Policy and Algorithm are key factors
3) AIOps need to be scenario oriented, no one way for all

4) AIOps is a long-term work, and need to have different target and emphasis in stages

5) AIOps and Zero-Touch do not mean no Human interfere. It will be a different role for Human.

Establishing Customer Experience: Aspects in Mobile Network Serviceability:

At the Age of Digitalization, the network operators have to harness the power of data by:

1) Establishing a Big-Data infrastructure

2) Bringing in cross-domain data flow

3) Fostering cross-function cooperation

4) Having a clear vision of the expected results:

   - Process speed up (e.g., troubleshooting)
   - Process automation
   - Insights for optimal network development CAPEX
   - CRM insights for improved Customer Operations.