SHORT TERM SCIENTIFIC MISSION (STSM) – SCIENTIFIC REPORT

The STSM applicant submits this report for approval to the STSM coordinator

Action number: CA15127
STSM title: Assurance of communication resilience under multiple failures implied by technology- and attack-related events
STSM start and end date: 10/07/2018 to 15/07/2018
Grantee name: Jacek Rak

PURPOSE OF THE STSM/

The objective of this STSM was to analyze possible solutions to the problem of assuring communication resilience in the presence of technology-related multiple failures as well as attack-induced multiple failures described by the Members of the Action in their draft versions of chapters (including about 35% of the final content of the chapters) of the final book of the Action. Special focus was on analysis of contributions to chapters addressing the objectives of Working Groups 3 and 4, and on preparation of reports to give advice to authors concerning the further development of chapters.

DESCRIPTION OF WORK CARRIED OUT DURING THE STSMS

(max.500 words)

During this STSM, a joint task of the STSM participant, and STSM host (Action Chair and Action Co-chair, respectively), was to analyze chapter by chapter the contributions of the Action Members to chapters of the Action book addressing the objectives of WG3 and WG4. The work carried out during the STSM was aimed to prepare the evaluation reports that will be next given to the respective authors.

DESCRIPTION OF THE MAIN RESULTS OBTAINED

(max. 500 words)

The main result of this STSM is the report attachment ***CA15127_STSM_41663_report_attachment.doc*** presented below including the evaluation remarks made to the analyzed chapters by STSM Participant and STSM host during this STSM.

FUTURE COLLABORATIONS (if applicable)

(max.500 words)

In the context of the main objective of this STSM, further collaboration (possibly as next STSMs) is planned to evaluate the further contributions of the Action Members related to extensions/updates of the contents of chapters of the final book.

Also future collaboration is planned in the context of involvement of RECODIS in activities of the Resilience Engineering Association.

CA15127_STSM_41663_report_attachment.doc

CA15127_STSM_41663

Remarks on draft versions of chapters (about 35% of the final content) of the final book of CA15127-RECODIS addressing the objectives of Working Groups 3 and 4

July 30, 2018

Chapter 1.5 *Structural measures to evaluate network vulnerability to attacks*

There is a risk that a significant part of this chapter may overlap with the content of Chapter 1.1 (Definition of Metrics of Network Topologies to Measure Resilience of Carrier Networks); we need to review this and take the appropriate action in due course.

Chapter 1.8 *Modelling of SDN software failures*

The list of authors needs to be confirmed. Is the paper based on one already submitted or published?

The paper needs to be reduced, if possible, to 24 pages. It should include some indication of how the modelling work contributes to system resilience.

Chapter 2.8 *Techniques of network design / update of characteristics …*

The content of the chapter presents a limited set of issues (mostly about cloud solutions).
So the title should be adjusted to better match the content.

For instance the title could be *Design of resilient solutions for cloud and datacentre systems*.
The content presented in the chapter - to be relevant - should give advice to data centre and other operators on how to design/update their architectures; this is the general objective of the book.

What is the role of SI in this chapter, concerned with resilience of cloud systems?

Chapter 2.12 *Alert-based network reconfiguration and data evacuation*

It seems presently not clear whether this chapter would fit into Section 2 or 3 of the book. What additional material is planned?

Is the material provided a solution that is agnostic of challenges?

Chapter 3.1 *A Taxonomy of algorithms for resilient routing*

The chapter should perhaps start with presentation of resilient routing schemes for core networks (optical?), then IP, next multilayer (in the context of single failures, multiple failures, region failures).

A decision should be made how to select (shorten) the list of techniques currently declared in the draft to fit within the final chapter size, with a special focus on multiple failure scenarios.

What about schemes used in practice e.g., BGP / OSPF?

What is relation of techniques mentioned here with the ones described in other chapters, e.g. for SDN?

Techniques related to content accessibility should be described elsewhere in the book (and indeed they are already / partially there).

Chapter 3.4 *Detection of attacks and attack-survivable routing in carrier networks*

It is not entirely clear whether this chapterfits into section 3 or 2 of the book (but we need to see more information about the likely content of the chapter).

It seems to be more about technologies tobe used for detection “probes”.

Maybe “Detection of attacks” should be replaced by “Detection of attack-sensitive network elements”.

Chapter 4.2 *Resilient SDN and NFV*

The chapter is currently about SDN and CDN, and alsoon multipath work. Should CDN and security appear in the title? We assume that there will further pages dealing with NFV and resilience. Is this partly based on a paper already submitted or published?

Chapter 4.3 *Resilient cloud networking and fog computing for CPS and IoT*

To be able to judge suitability of the chapter for this part (4) of the book, more content needs to be provided including at least a selection of the references that will be used in the chapter.

A diverse set of applications may be more appropriate than just eHealth.

Notes:

Advanced-> further areas

Operators of a critical infrastructures, cloud providers, data centre providers …