Questionnaire on Trust in Autonomics
August 2011

Please kindly provide your answers by September 9th, 2011 at the following address:

Laurent.Ciavaglia@alcatel-lucent.com

1. Autonomous (Self) Features

1.1 In your domain, which functions are automatized or rendered autonomous (i.e. functions where the "human operator" is removed from decision loop, control loop or both)?

Importance: Gaining knowledge from the experiences in other fields, through understanding and identifying what, how and why autonomicity was achieved in other industry domains.

1.2 What were the difficulties and the roadblocks encountered from regulatory, standard, technology, business and market, psychological and societal perspective in deploying autonomous features? What were/are the main enablers and technology leaps introduced to overcome these issues?

Importance: Understanding the general difficulties and the process of achieving solutions in the development of the autonomicity in other industry domains.

1.3 In your domain, does a certification organization, system or process exist? If yes, what have been its initial goal(s) and definition? Which aspects of the system/infrastructure/process/... is the certification organization supposed to guarantee (i.e. the technical objective)? What models or approaches have been selected and developed to implement the certification process (and, if possible to answer, why has this model in particular been selected)?

Importance: Understanding the process (success story?) for the definition and the deployment of the certification process in order to guide our own development and possibly avoid pitfalls and dead-ends.

2. Design and Modelling

2.1 From your perspective, which is the attack model that should be considered in designing an autonomous system containing “trust” functionality?

Importance: "In the history of computing there has often been a 10 or more year gap between the use of technology and the addressing of security issues that arise from it" (Virgil Gligor, University of Maryland, National Security Award 2006, Invited talk at The 3rd Annual VoIP Security Workshop, Berlin, Fraunhofer FOKUS, 01.JUN.2006

2.2 How is trust modelled, designed and which trust mechanisms are applied in your domain – e.g. in aviation for autopilots – which is analogue to the operator control in a telecommunications system?

Importance: Understanding the analogies with other industry domains (as far as trust is concerned) could be the key for convincing telecommunication operators of the reliability of our autonomous solutions.

2.3 Which main functional requirements of the management systems in your domain can be further fulfilled by self-functionalities? For each of them can we set up a methodology in the same way traditional security or safety methodologies do (such as common criteria for example) to attribute them a given level of trust? What would be the changes otherwise?

2.4 How to build "trust and confidence" in autonomics (self) features from the outset e.g. at deployment phase as well as optimization phase? Which process should be embedded within the management architecture from standardization and design principles allowing the operator to keep control if needed?

Importance: Dedicated methodologies exist to measure the assurance that a system satisfies certain objectives when it is question of safety or of information security. We are looking for a method to adapt the assurance mechanisms in order to build a scale of trust for what concerns the objectives specific to our project.

3. Approach in Trust Design - Measurement and Metrics

3.1 From your domain perspective, how is trust modelled and measured currently? What metrics do you consider as most important for the computation and the evaluation/assessment of trust in autonomics?

Importance: Gaining experience from other domains on the design of correct metrics for our trust model. A set of not carefully selected metrics may results on unsuccessful trust computation and consequently to an unstable system.

3.2 If one or multiple autonomic functionality levels are added; how is the trust model and measures going to be affected e.g. how trust is going to be measured between the network providers and the service providers?

Importance: Trust in-between operators or service providers is fundamental for business. The introduction of autonomic functionality may affect it since part of the management functions will be in the network.

3.3 What types of strategies do you envisage for trust in autonomics? How can metrics be exploited or mapped to certain levels of trust? Are different weights considered for various metrics (potentially diverse in various situations)? How can the translation of business goals to network requirements be evaluated in the scope of trust mechanisms?

Importance: For being able to assess the level of "trustworthiness" of an autonomic node/entity it is crucial to have a process of mapping trust metrics to levels/values of trust. Furthermore, depending on the autonomic function/entity addressed certain metrics may be more important than others, thus weighting of metrics/parameters for deriving the level of "trustworthiness" may be required.

3.4 How to ensure global optimum whilst catering for local optimum, as per autonomics (self) feature, each activated through the same optimization parameters in order to ensure stable behaviour of the system? Which coordination process and associated design principles should be provided in order to make the system beneficiary comfortable with optimization phase alongside large scale deployment?

Importance: Current operator networks evolve towards a more “flat” architecture and the introduction of the autonomics paradigm raising at the same time major issues and challenges to be solved. These issues are pertaining to "trust & confidence" of these autonomics or self -features, as well as to the coordination of various autonomics (Self) features running simultaneously from network stability perspective.

4. Trust Mechanisms

4.1 What kind of trust mechanisms are or could be embedded in the autonomic elements in order to secure the cooperation between the different elements of the system?

Importance: A framework for an autonomic network, able to dynamically manage itself without human intervention, needs to address this question to convince the operators it can be safely deployed.

4.2 What kind of trust mechanisms is required during the federation formation of a system and what level of trust are required to support this formation?

Importance: In the current Internet there is a trend for services to be both provided and consumed by loosely coupled networks of consumers, providers and combined consumer/providers, forming federations of networks. Trust mechanisms are valuable during forming, joining and maintaining a federation.

4.3 What kind of trust mechanisms is necessary for building trust between different system providers? Can the same mechanisms as the one for the cooperation between the different elements of the system apply to a multi-system environment?

Importance: Trust should be addressed as a 3-faceted issue: trust between autonomic nodes (since they need to safely cooperate between them), trust of the operator on the autonomic network (can be built by extracting information from the feedback loops to demonstrate the correct functioning of the system), and trust between different networks (that should cooperate for the management of services deployed on networks of different providers).