Certification of system architecture dependability

I. Levendel
Director High Availability Technology Program
Motorola
Schaumburg – Illinois
E-mail: i.levendel@motorola.com

Wireless systems are particularly vulnerable to failures and malfunctions for several reasons. First, wireless architectures are naturally distributed over a wide geographic area. Secondly, equipment pricing pressures prohibit massive fault-tolerance similar to that in the slowly deregulating wireline business. Thirdly, the responsibility for insuring dependable functioning of the systems is generally distributed among several independent collaborating entities (wireless equipment owners and leased lines providers). Fourthly, the access medium of wireless (RF) is much more vulnerable than the access medium of wireline (wire to the home).

As a result of this situation, service quality has been much below the standards, which were previously set by the wireline during the decades of regulation and are still in effect in spite of the current deregulation process. Both system availability and call completion are lower than in the wireline by several orders of magnitude. This situation has two down sides. First, it causes significant dissatisfaction for end customers and loss of revenue for service providers. In addition, it limits wireless communication to lower quality voice communication and is a significant barrier for the wireless industry to expand its scope to other lucrative forms of communication. In order for the wireless industry to broaden its span, system dependability is a necessary ingredient that would allow the deployment of extensive high capacity dependable infrastructures and services.

In order to alleviate these problems, it is necessary to introduce in the industry a better discipline for dependable system design in all phases of the design process. The speaker will focus on the introduction of a quantitative approach to the certification of system architecture. The quantitative side of the approach strongly contrasts with the common practice of architecture peer review. Our approach is based on modeling and analysis of the system architecture and includes the following steps:

1) Construct a statistical model for the architecture. The model is driven by outages due to the following components:
a) Hardware
b) Software
c) Geographically distributed links
d) Hardware and software upgrades

2) Evaluate availability, and, if appropriate, its tradeoffs with performance and capacity.
3) Identify potential architectural deficiencies in relation with customer requirements
4) Propose architectural remedies
5) Define the architectural improvement roadmap

This approach can also be applied to legacy systems as well as to new designs and gives a rational character to the architecture certification process.

Our experience has spanned several voice-based systems, and we are engaged in the definition of packet network architecture certification. Examples and templates will be discussed during the talk, and open issues will be brought up. Of course, other phases of the development process deserve the same degree of rationalism.