Toward a Tailored Modeling of Non-Functional Requirements for Telecommunication Systems

Mehrdad Saadatmand*, Antonio Cicchetti*, Diarmuid Corcoran† and Mikael Sjödin*
*Mälardalen University, Department of Innovation, Design and Engineering, Västerås, Sweden
{mehrdad.saadatmand, antonio.cicchetti, mikael.sjodin}@mdh.se
†Ericsson Software Research, Stockholm, Sweden
diarmuid.corcoran@ericsson.com

***Abstract*—Addressing non-functional requirements in Real-Time Embedded Systems (RTES) is of critical importance. Proper functionality of the whole system is heavily dependent on satisfying these requirements. In model-based approaches for development of the systems in RTES domain, there are several methods and languages for modeling and analysis of non-functional requirements. However, in this domain there are different types of systems that have different sets of non-functional requirements. The problem is that the general modeling approaches for RTES may not cover all the needs of these subdomains such as telecommunication. In this poster paper, we suggest an approach to complement and apply general RTES modeling languages to better cover different non-functional requirements of telecommunication systems.**

I. Telecommunication Systems

As a type of real-time embedded systems, telecommunication systems have specific characteristics which incur certain requirements and prioritization of some requirements over the others. These systems need to be secure, are highly distributed, have a dynamic nature, require massive processing capacity and high availability (99.999% availability, which is sometimes referred to as *five nines*), and need to be scalable. The distribution in these systems can be regarded in two perspectives: the distribution inside one node (such as using multicore solutions and distribution of software functions among different processing units) and also the geographical distribution of nodes across different regions and the communication among them. A general structure of telecommunication network nodes is shown in Figure 1. As is depicted in this figure, the network consists of many different types of nodes such as Radio Base Stations (RBS), Radio Network Controllers (RNC), Media Gateways (MGW) and others that span across a big georgraphical area and communicate over different kinds of lines.

Regardless of the integration and interconnection of different nodes in the network, design of each node is a big complex challenge in itself. For example, an RNC can easily contain between 500 to 700 CPUs, with software functions spanning across several CPUs. This number, however, is decreasing as new processors with higher capacities are produced. This reduction is important for the total cost, power consumption and heat generation of systems. As for functionality and services, in a typical telecommunication system a big number of connections should be established, routed and managed per second. Besides, cost calculation should also be done on them. Moreover, a typical telecommunication system can have a life span of about 20-30 years. Thus upgrade-ability and maintenance of such systems is also of great importance. The software upgrade should be done in such a way to have the least effect on the availability of the system. That is why features such as hot-swapping and plugging and the ability to perform restarts at different granularity levels (a single board, collection of boards or a complete node) are highly desirable and demanded in this domain.

To cover more aspects regarding modeling and representation of non-functional requirements in the design of such complex systems, we suggest a UML profiling solution consisting of concepts from SysML [1] for traceability, and MARTE [2] for modeling general non-functional properties and their analysis. For security requirements which are inherent in telecommunication domain but are not covered by MARTE we adopt from available UML profiles for security (namely UMLsec [3]). Also since MARTE, SysML and UMLsec are UML profiles, they are faster for developers using UML to catch on and they also serve as a possible unifying factor between development departments.

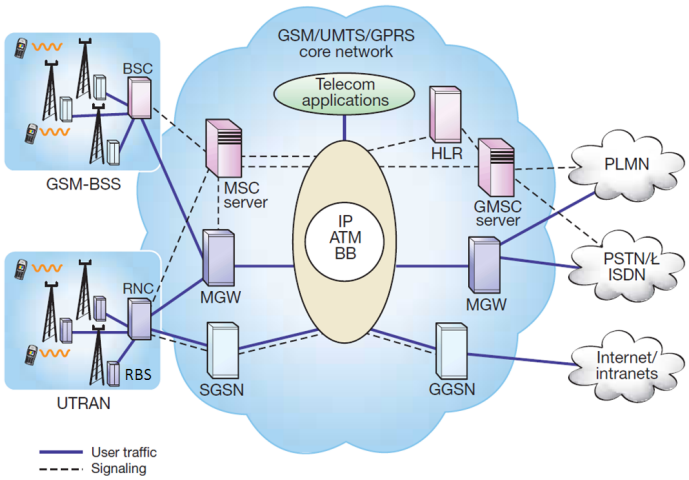

Fig. 1. Telecommunication Network Structure [4]

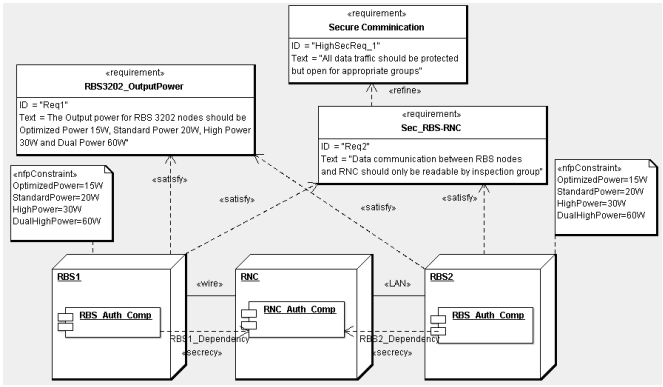

Fig. 2. Security Requirement on RBS Nodes

II. Example of Application

In figure 1, it can be seen how Radio Base Station (RBS), Radio Network Controller (RNC) and Media Gateway (MGW) nodes are connected and communicate. When a Mobile Equipment (ME) wants to join the network, it starts communicating with RBS and authenticating itself to the system. Security operations such as key exchange take place through the communication path from the mobile equipment to the RNC. In our case study, we have two RBS 3202 nodes that communicate with an RNC. The output power requirements for RBS 3202 are as follows:

Req1: Optimized Power 15W, Standard Power 20W, High Power 30W and Dual High Power 60W.

One of the security requirements that exist for the connection between the RBS and RNC is:

Req2: Data communication between RBS nodes and RNC should only be readable by inspection group.

The second requirement incurs that no one from outside and also inside of the network should be able to read the data traffic on the links between RNC and RBS except users in the inspection group. Thus the data should be encrypted using a specific key for this group. We try to violate this in our example model by using unencrypted links and then perform analysis on the model.

As shown in Figure 2, the requirements and the relationships between them and design artifacts are modeled using SysML concepts. MARTE non-functional concepts (i.e. *nfp, nfpconstraint, PowerUnitKind and NFP_Power*) are used for modeling output power requirements of RBS nodes. Security concepts in our model are represented using UMLsec stereotypes. The link between RBS1 and RNC is marked with *wire* stereotype and the one between RBS2 and RNC is marked with *LAN* stereotype.

Doing analysis using UMLsec analysis tool on the model yields the result that is shown in Figure 3. The important part in this analysis output (marked with *) is that *LAN* and *wire* links are not readable by a default (external) attacker thus the model satisfies the secrecy requirement for this attacker type, but an insider attacker on LAN or wire can access the information and therefore the model violates the requirement.

```
::::::::Against Default Attacker
=======Here begins the verification
The name of the dependency is RBS2_Dependency
The stereotype of the communication link of the dependency RBS2_Dependency is LAN
The stereotype of the dependency is: secrecy
* The UML model satisfies the requirement of the stereotype secure links.
...
::::::::Against Insider Attacker
=======Here begins the verification
The name of the dependency is RBS2_Dependency
The stereotype of the communication link of the dependency RBS2_Dependency is LAN
The stereotype of the dependency is: secrecy
* The UML model violates the requirement of the stereotype secure links, but
it has been fixed.
...
```

Fig. 3. Result from UMLsec Analysis Tool

Although UMLsec has a general *encrypted* stereotype to label encrypted communications, it is also possible to define a custom stereotype for example as "*Uniquely encrypted by SIM ID*" and define different threats that different attackers can pose on these links such that only inspection group users can have access. Then we can use this stereotype on the links instead of *LAN* and *wire* that we used earlier, to create a model that satisfies the requirement and verify it with the analysis tool.

III. Conclusion and Future Works

Our suggested approach in this paper was to consider telecommunication systems as a subdomain of RTES and therefore adopt from available modeling solutions for non-functional requirements and their analysis that already exist in RTES domain. A similar approach has been used in automotive domain and in the definition of EAST-ADL [5] which has been adopted successfully and is getting momentum. As a continuation of this work, we plan to apply our approach in the design of a bigger portion of telecommunication systems.

As further studies, modeling and analysis of other non-functional requirements than security in telecommunication systems can be investigated. It is necessary to further augment the suggested approach in this paper, such as introducing it as part of a well-structured methodology similar to the methodology suggested [6]. This work which is more targeted for automotive domain makes use of EAST-ADL and its abstraction levels. Applicability of the same concepts to telecommunication domain could be an interesting topic to investigate especially for adding modeling of *variability*.

References

[1] OMG SysML Specifcation V1.2, June 2010, http://www.sysml.org/specs.htm.

[2] MARTE specification version 1.0 (formal/2009-11-02), http://www.omgmarte.org.

[3] J. Jürjens, "Secure systems development with uml." Springer, 2005.

[4] Kling, Lars-Örjan and Lindholm, Åke and Marklund, Lars and B. Nilsson, Gunnar, "CPP: Cello Packet Platform," http://www.ericsson.com/ericsson/corpinfo/publications/review/2002_02/files/2002023.pdf.

[5] EAST-ADL Specification V2.1 RC3, 2010-06-02, http://www.atesst.org/scripts/home/publigen/content/templates/show.asp?P=125&L=EN&ITEMID=7.

[6] A. Albinet, J.-L. Boulanger, H. Dubois, M.-A. Peraldi-Frati, Y. Sorel, and Q.-D. Van, "Model-based methodology for requirements traceability in embedded systems," in *Proceedings of 3rd European Conference on Model Driven Architecture® Foundations and Applications, ECMDA'07*, Haifa, Israel, Jun. 2007. [Online]. Available: http://www-rocq.inria.fr/syndex/publications/pubs/ecmda07/ecmda07.pdf