

Towards Rigorous Architectures

NOKIA

Formal Methods '08

Industry Day – May 28th 2008

Ari Ahtiainen, Nokia Research Center

Sari Leppänen, Nokia Services & Software

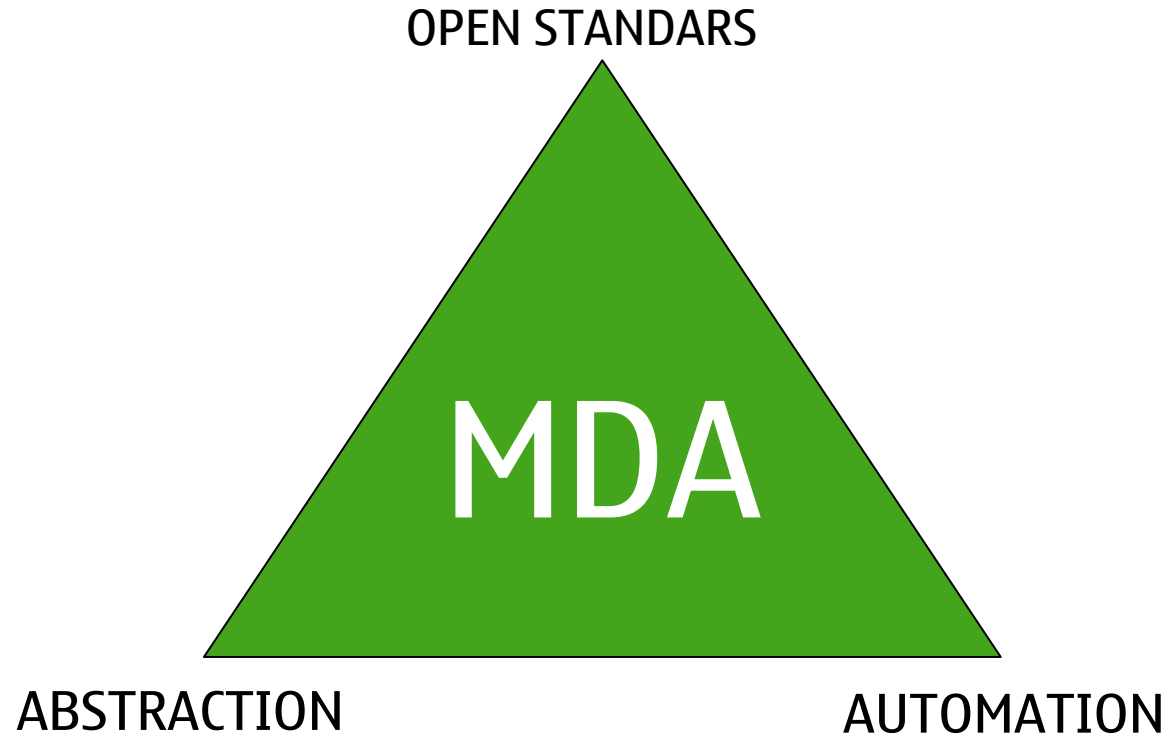
Contents

- Introduction
- Some selected case studies (*)
- University collaboration
- Lessons learnt
- Modeling architectures with Lyra
- Summary

(*) By no means a complete list of Nokia projects where formal methods have been studied

Introduction

OMG's vision on Model-Driven Architecting is widely supported among industry and enterprises



...but transition is gradual

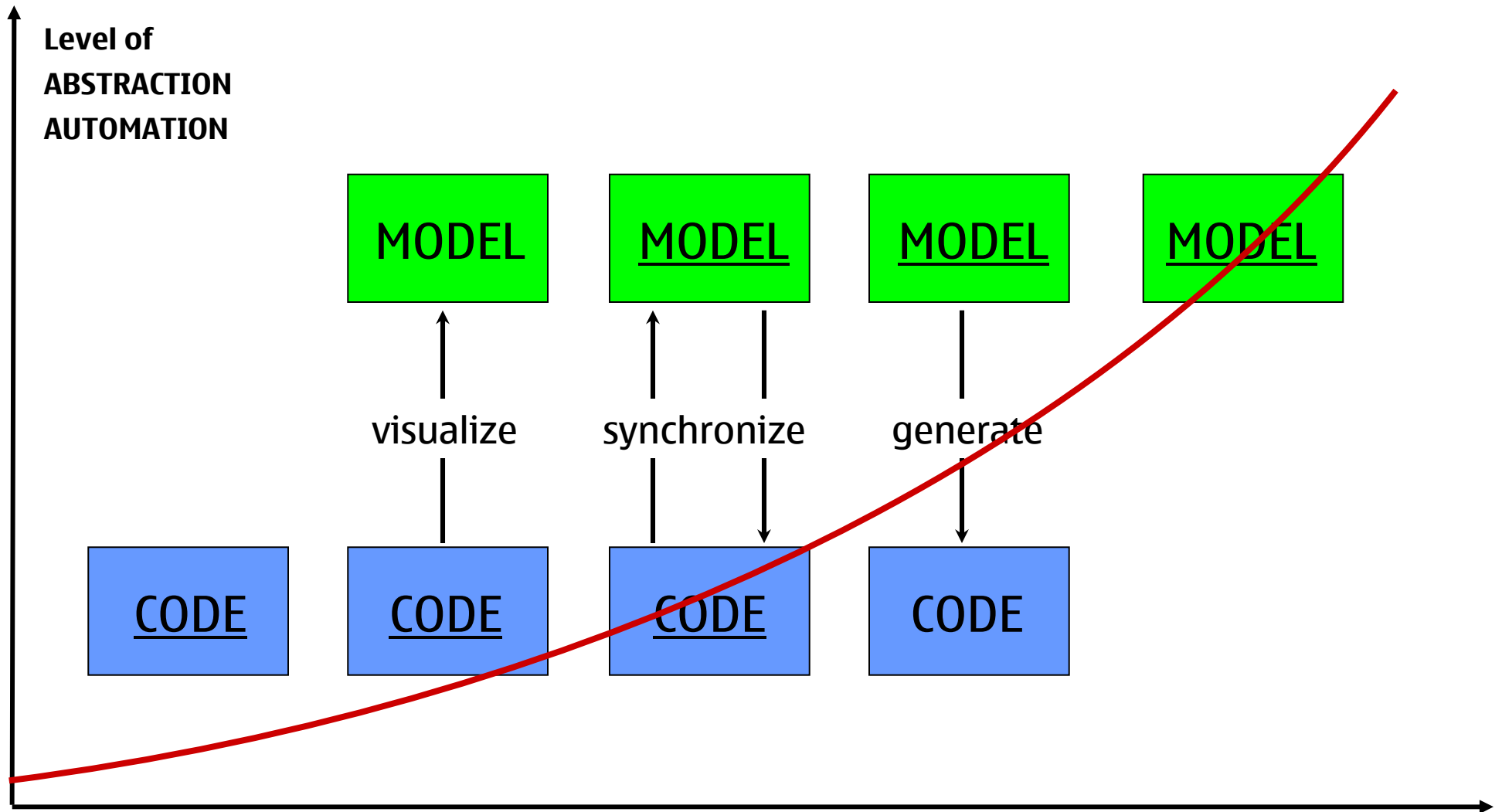


Illustration by Bran Selic, ROC of IBM-Rational

Case Studies at Nokia Research Center 1998-2008

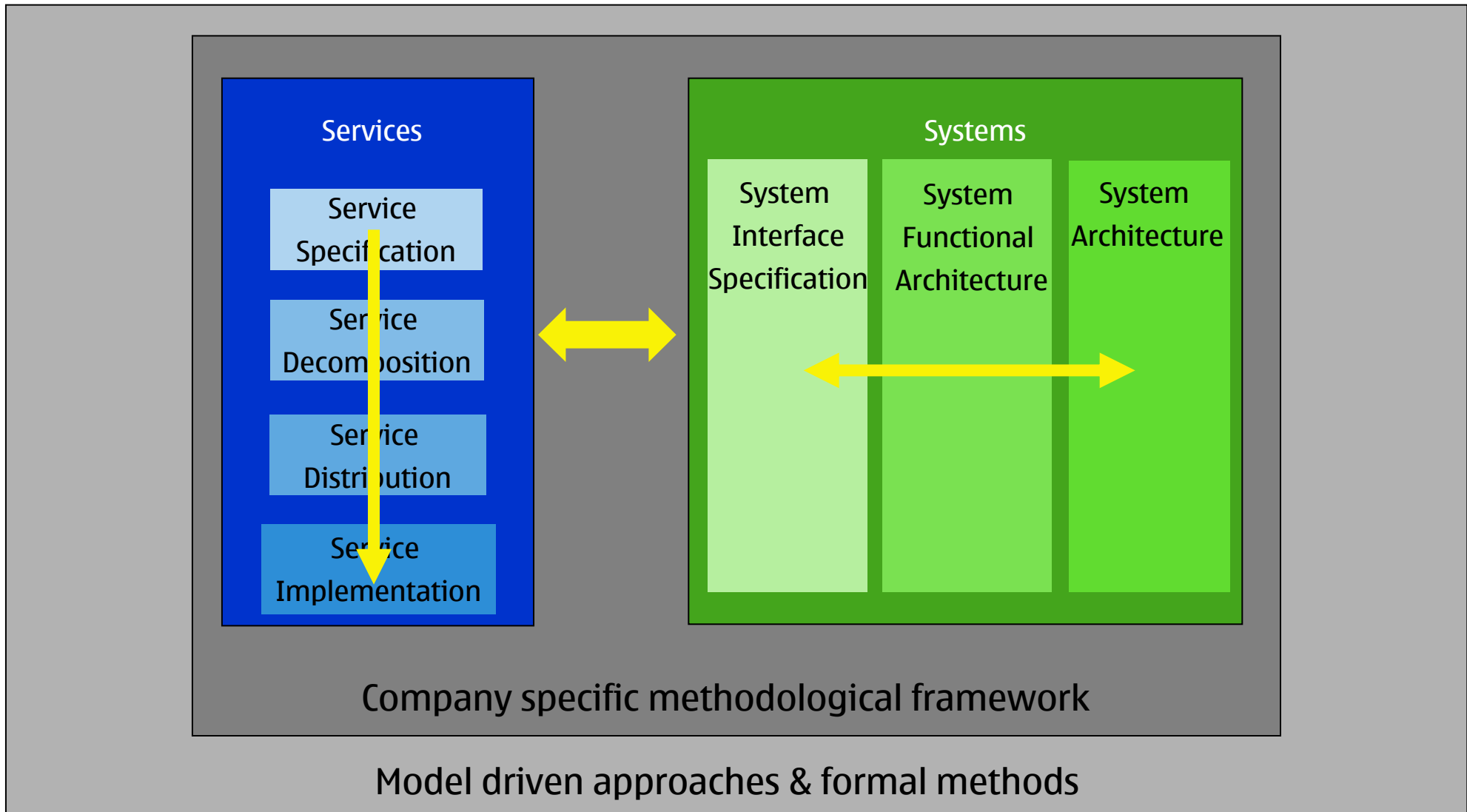
During last 10 years Nokia Research Center has carried out a number of research projects where modeling and formal methods have been trialled in industrial case studies

- 1998 Radio Link Control (RLC) protocol for WCDMA radio
- 2004 Position Calculation Application Part (PCAP) protocol in 3GPP
- 2007 Modeling Camera Functionality in Nokia Series 60 mobile phone
- 2008 Modeling Handovers in WiMAX Network Architecture

These case studies have led to the creation of modeling method **Lyra** with

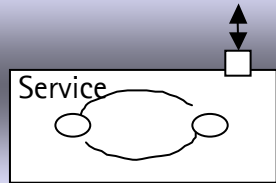
- industrially applicable top-down design flow
- rigorous foundation based on formal methods

Lyra 2.0 – Methodological Framework



Lyra - Service design flow

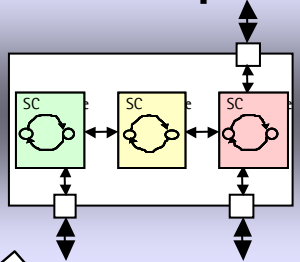
Service Specification



- Specify the externally observable behavior of a system level service

➤ specification of service as CIM/PIM

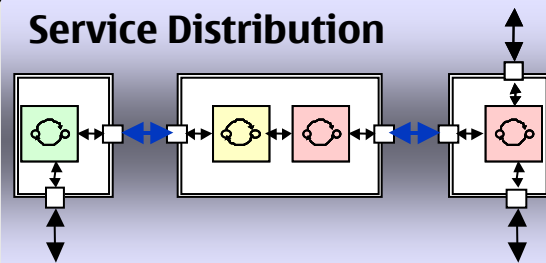
Service Decomposition



- Specify internal architecture and implementation of the service as platform independent behavior

➤ implementation of service as PIM

Service Distribution



- Distribute the service to a given platform, (e.g. network topology or protocol stack)

➤ implementation of service as PSM

Service Implementation

RLC Protocol 1997-1998

- RLC protocol controls Layer 2 radio links between 3G mobile and network infra
- study was carried out while 3G standardization was still ongoing
- key parts of the RLC protocol logic were modeled using LOTOS
- verification was done by using ARA toolkit for model minimization and transformation and doing model checking with the Caesar/Aldebaran tool
- counterexamples were generated by using Telelogic SDT Validator tool
- study focused into verification of “SDU Discard” feature of the RLC protocol

Learnings

- model-checking capability was new to standardization and became a valuable tool in validation of various proposals made at the specification team
- need for automatic conversion and MDA approach with model transformations became evident

PCAP Protocol 2003-2004

Case study

- PCAP protocol controls execution of location requests from 3G mobiles between Stand-Alone Mobile Location Center (SMLC) and Radio Network Controller (RNC) in 3GPP network
- protocol was modeled using early UML-2 language and a beta version of Telelogic Tau Developer UML toolkit
- focus was more in code generation than verification

Learnings

- first full-scale study where Lyra design flow with 3-stage service specification was trialled
- newly introduced UML-2 features for Composite Structures and Hierarchical State Charts turned to be productive in modeling of the protocol structure and behaviour

S60 Camera 2005-2006

Case study

- Series 60 is the Nokia software platform for mobile devices running Symbian OS
- functional architecture of S60 Camera SW was analysed by reverse engineering into executable Lyra/UML2 model (Telelogic Tau G2)
- model-based testing tool (beta version) from Conformiq was also trialled
- focus was in analysis of architectural interfaces, e.g. Onboard Camera API

Learnings

- creation of platform-independent functional model from detailed implementation required skilled separation of concerns
- need for automation of model creation became evident and development of Lyra wizards for the Telelogic Tau tool was started
- UML2 language appeared to be too wide and have weak semantics, which led to creation of UML2 Profile for Lyra
- limited access to metadata in Tau tool => exporting a model from Tau to Conformiq tool was difficult
- no verification tool was readily available

Handover in WiMAX 2006-2007

Case study

- WiMAX is a radio protocol suite for mobile broadband system
- Specification of WiMAX handover functionality was created as executable Lyra/UML2 model in close collaboration with the Nokia product specification team
- Newly created Lyra UML2 profile was used successfully
- focus was in model creation, no formal verification was used

Learnings

- Lyra design flow and Tau wizards were enhanced with additional steps to compose system architecture from service components
- Need and possibilities for further automation was identified

University Collaboration

In parallel with NRC case studies Nokia has participated into large number of university projects to promote research on formal methods and modeling and verification technologies

- University of Helsinki: LOTOS and Caesar/Aldebaran tool
- Tampere University of Technology: TVT project⁽¹⁾ and tool creation
- TKK Petri Net research team: PROD⁽¹⁾ and MARIA⁽¹⁾ tools
- Åbo Akademi: EU IST RODIN project and TORES⁽¹⁾ project and CORAL model repository
- TKK/TCS laboratory: SMUML⁽¹⁾ project and tools
- TKK/TCS and Åbo Akademi: LIME⁽¹⁾ project

⁽¹⁾ projects sponsored by Tekes – Finnish Funding Agency for Technology and Innovation

Conclusions

Why formal methods are still under-utilized in industry

- language standardization (UML) has been too weak, especially semantics and model interchange between tools
- commercially supported tools for model verification and testing are scarce

Improvement actions

- Executable UML Foundation @ OMG looks promising
- 3-party collaboration projects with university – tool vendor – industry to speed up commercialization of research results
- industrial-scale tools for verification and model-based testing are badly needed
- more emphasis on parallel programming models in software technology curricula

The Way Forward

Rigorous architecting of large scale software systems

- Lyra method and Executable UML models to be applied in high-level architectural specifications
- verification of architecture models
- model-based testing of implementations for architectural compatibility

One more example on a modeling project at Nokia Research Center

- Functional Architecture for Software Defined Radio

Multiradio is Not a Simple Thing



Interworking problems!
Power consumption!
Size and design!
Ease of use!



SFA Overview – SDR Control Framework

SDR functions common to all radios

Configuration Manager (CM)

- install and load radios

Radio Connection Manager (RCM)

- activate/deactivate radios

Flow Controller (FC)

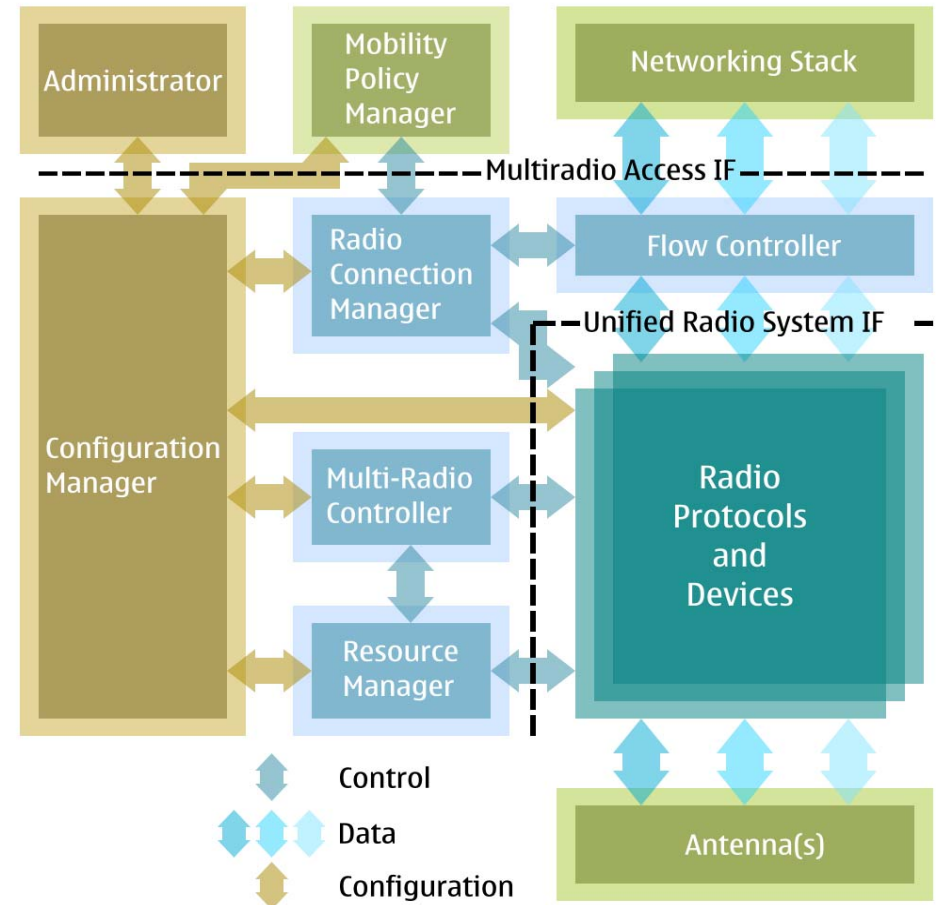
- user data flow control

Multiradio Controller (MRC)

- radio interference control

Resource Manager (RM)

- resource sharing control



References

Lyra Method

- Leppänen, Sari, Rigorous Service-Oriented Development of Communicating Distributed Systems, PhD Thesis, Tampere University of Technology, Publication 718, Tampere, Finland 2008.

Case Studies

- Leppänen, S. and Luukkainen M., Compositional verification of a third generation mobile communication protocol, In: ICDCS/DSVV 2000, Taipei, Taiwan, R.O.C., 2000, IEEE Computer Societe
- Leppänen, S., Turunen, M. and Oliver, I., Application driven methodology for development of communicating systems, In: FDL'04, Lille, France, September 2004.
- Honkola, J., Leppänen, S., Rinne-Rahkola, P., Söderlund, M., Turunen, M. and Varpaanniemi, K., A case study: Applying Lyra in modeling S60 camera functionality, In: ECBS 2007, Tucson, Arizona, USA, March 2007
- M. Turunen, K. Leppänen, S. Leppänen. Workflow automation for system architecting. In Proceedings of the Third International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2008)
- Ahtiainen, A. et al, Architecting Software Radio, in: SDR Forum 2007, Denver, Colorado, USA, November 2007

Thanks!
Questions?

NOKIA